Graphical Languages for Quantum Control and Linear Optics

Alexandre Clément

UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

Langages graphiques pour le contrôle quantique et l'optique linéaire

Graphical Languages for Quantum Control and Linear Optics

THÈSE

présentée et soutenue publiquement le 16 mai 2023

pour l'obtention du

Doctorat de l'Université de Lorraine

(mention informatique)

par

Alexandre Clément

Composition du jury

Président :	Michele Pagani	IRIF, Université Paris Cité
Rapporteurs :	Giulio Chiribella	The University of Hong Kong, University of Oxford
	Chris Heunen	University of Edinburgh
Examinateurs :	Caroline Collange	Inria, IRISA
	Eleni Diamanti	CNRS, LIP6, PCQT
Directeurs :	Emmanuel Jeandel	LORIA, Université de Lorraine
	Simon Perdrix	Inria, LORIA

Laboratoire Lorrain de Recherche en Informatique et ses Applications — UMR 7503

Mis en page avec la classe thesul.

Remerciements

J'aimerais remercier tous ceux sans qui cette thèse n'aurait pas été possible.

D'abord bien sûr mes directeurs. Simon Perdrix, avec qui de fait j'ai essentiellement travaillé, pour les centaines d'heures qu'il m'a accordé, et spécialement pour sa promptitude à répondre au mieux à mes diverses sollicitations. Et Emmanuel Jeandel, pour la même disponibilité et le même engagement à chaque moment clé de ma thèse, ce qui représente également un temps non négligeable.

Merci à Giulio Chiribella et Chris Heunen d'avoir accepté le rôle de rapporteurs. Merci aux autres membres de mon jury : Caroline Collange, Eleni Diamanti et Michele Pagani.

Je remercie Michele Pagani à double titre puisque, avec Benoît Valiron, il a encadré le stage de fin de master où j'ai découvert de l'intérieur l'informatique quantique.

Un grand merci également à Julien Ross et Peter Selinger qui m'ont ensuite chaleureusement accueilli en stage à Halifax. Cela a été une expérience particulièrement enrichissante et constructive. Ce que j'ai appris pendant ce stage s'est de plus révélé étonnamment utile durant cette thèse. Merci aussi à eux pour leurs suggestions de directeurs de thèse potentiels, merci spécialement à Kohei Kishida qui a eu l'idée d'évoquer le nom de Simon Perdrix.

Benoît Valiron, en plus de m'avoir initié à l'informatique quantique et fait prendre contact avec Julien Ross et Peter Selinger, a été un collaborateur durant cette thèse, et a accepté de m'accueillir en postdoctorat à l'issue de celle-ci. Je le remercie à tous ces titres.

Je remercie aussi les autres personnes avec qui j'ai collaboré pendant la thèse : Mehdi Mhalla, Cyril Branciard, Nicolas Heurtel, Shane Mansfield, Noé Delorme et Renaud Vilmart.

Je remercie le même Renaud Vilmart, ainsi que Titouan Carette, pour leur rôle de prédécesseurs en tant que doctorants. Et en particulier pour leurs manuscrits qui m'ont souvent servi de repère pour la rédaction de celui-ci.

Merci aux membres de l'équipe Mocqua — l'équipe a bien grandi au cours de ma thèse, si bien qu'ils sont trop nombreux pour être cités ici — et à tous ceux que j'ai côtoyé ces quatre dernières années, et qui ont contribué à construire un environnement accueillant et amical.

Merci à mes parents, mes grands-parents, mes frères et sœurs, et tous ceux qui m'ont permis de devenir celui que je suis.

Enfin, je ne peux pas terminer ces remerciements sans une mention spéciale pour les personnes que je n'ai pas citées, soit par oubli, soit par choix forcément arbitraire et peut-être trop conventionnel, et qui l'auraient pourtant grandement mérité.

Introduction (fr)

Informatique quantique. Les lois de la physique quantique, qui régissent le comportement des systèmes physiques dont la taille s'approche de celle des atomes, sont sur certains aspects très différentes des lois de la physique classique régissant les systèmes macroscopiques. L'une des principales propriétés non-classiques des systèmes quantiques est la possibilité de superpositions d'états : de manière simplifiée, l'état d'un système quantique (appelé un état quantique) est représenté par une combinaison linéaire à coefficients complexes des états qu'il pourrait prendre en physique classique. D'une certaine manière, le système peut alors être interprété comme étant dans plusieurs états classiques en même temps. Une autre propriété des systèmes quantiques est qu'il est en général impossible de mesurer un système quantique sans affecter son état : la mesure d'un système quantique en superposition de plusieurs états classiques produit pour résultat l'un de ces états, aléatoirement, la probabilité de chaque état étant fonction du coefficient correspondant (appelé amplitude) dans la combinaison linéaire associée ; cela fixe le système dans l'état observé, ainsi d'éventuelles mesures ultérieures donneront le même résultat. Une troisième propriété non-classique est l'intrication (aussi appelée enchevêtrement) : l'état de plusieurs systèmes quantiques considérés ensemble est, en général, une superposition quelconque des diverses combinaisons possibles d'états classiques de ces systèmes, et ne peut pas nécessairement être décrit en considérant chaque système individuellement. En particulier, la mesure de plusieurs systèmes quantiques ne donne pas toujours des résultats indépendants. Un exemple simple est celui de deux systèmes quantiques, tous deux en superposition de deux mêmes états classiques, tels que mesurer l'un des deux systèmes (n'importe lequel) donne l'un des deux états possibles avec probabilité $\frac{1}{2}$ chaque, et que mesurer ensuite l'autre système donne nécessairement le même résultat que la première mesure. Un tel comportement a été observé expérimentalement avec des systèmes éloignés de plusieurs centaines de kilomètres. Comme ce comportement ne dépend pas de la distance qui sépare les deux systèmes, cela peut donner l'impression que ceux-ci communiquent plus vite que la lumière, bien qu'il soit en réalité impossible de transmettre de l'information par ce biais.

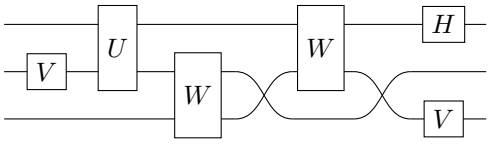
L'informatique quantique est un domaine de l'informatique visant à exploiter de telles propriétés non-classiques afin de réaliser certaines tâches de manière plus performante. Parmi les exemples les plus connus, on peut citer des algorithmes en temps polynomial pour factoriser un nombre entier en produit de facteurs premiers [122] ou pour résoudre des systèmes d'équations linéaires [78], ainsi qu'un algorithme permettant de trouver un élément dans un tableau de taille n en seulement $\mathcal{O}(\sqrt{n})$ opérations [71]. D'autres applications pour lesquelles les lois de la physique quantique peuvent être utilisées de manière avantageuse sont dans les domaines de la communication et de la cryptographie : il existe par exemple des protocoles de communication dans lesquels — en théorie — il est impossible d'intercepter un message sans que cela ne soit repéré par l'expéditeur ou le destinataire [18, 59].

Intuitivement, la différence entre des données quantiques et classiques est la suivante : étant donnée une variable classique, pouvant prendre des valeurs dans un ensemble A, son équivalent quantique prend ses valeurs — ou, pour utiliser la terminologie habituelle, ses *états* — dans $\mathbb{C}^A$. Autrement dit, une variable quantique est dans une superposition de ses valeurs classiques possibles. L'exemple le plus simple de donnée quantique — qui est l'élément de base dans la plupart des modèles d'informatique quantique — est le qubit, l'équivalent quantique du bit. L'état d'un qubit est un vecteur de $\mathbb{C}^2$, généralement écrit sous la forme d'une superposition $\alpha\,|0\rangle + \beta\,|1\rangle$, où $\alpha, \beta \in \mathbb{C}^2$, et $|0\rangle, |1\rangle$ correspondent aux valeurs 0 et 1 d'un bit classique. Un *qudit* est la généralisation d'un qubit en dimension supérieure à 2. Un qudit est décrit par un vecteur soit de $\mathbb{C}^d$ pour un entier d donné, soit de $\mathbb{C}^{\mathbb{N}}$, qui est généralement écrit comme

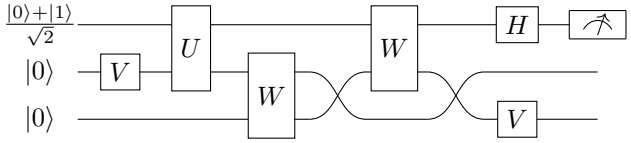
une superposition d'états de base notés $|0\rangle, |1\rangle, |2\rangle, ...$

Un exemple d'état intriqué de deux qubits est $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, qui a précisément le comportement décrit plus haut : mesurer l'un des deux qubits fixe le système soit dans l'état $|00\rangle$, soit dans l'état $|11\rangle$, chacun avec probabilité $\frac{1}{2}$, de sorte que le résultat de la mesure est 0 ou 1 selon le cas, et que mesurer ensuite l'autre qubit donne nécessairement le même résultat.

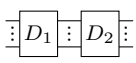
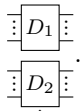
Circuits quantiques. À l'exception des préparations d'états — ou initialisations — et des mesures, les opérations réalisables sur des données quantiques consistent à appliquer (en place) une transformation unitaire à un ou plusieurs états quantiques. Un programme quantique de bas niveau sans intructions de contrôle consiste donc en une suite d'opérations unitaires appliquées chacune à un sous-ensemble des systèmes quantiques disponibles (généralement des qubits), éventuellement précédées par des initialisations et suivies par des mesures. Les circuits quantiques sont une représentation graphique de telles suites d'opérations : chaque opération unitaire est représentée par un élément graphique, appelé une *porte*, avec des fils d'entrée et de sortie, représentés respectivement à gauche et à droite, représentant les systèmes quantiques affectés par l'opération. Un exemple typique de circuit quantique sur 3 qubits est le suivant :



où chaque fil représente un qubit. La notation peut aussi être enrichie pour représenter les initialisations et mesures :



Les circuits quantiques sont omniprésents en informatique quantique. En effet, ils peuvent être vus — approximativement — comme le langage assembleur d'un processeur quantique. En particulier, dans le modèle traditionnel de calcul quantique où un ordinateur classique contrôle un coprocesseur quantique, le rôle de la partie classique consiste essentiellement à construire des circuits quantiques qu'elle envoie au coprocesseur quantique pour exécution, et à traiter ensuite les résultats renvoyés par le coprocesseur.

Langages graphiques. Le formalisme des circuits quantiques appartient à une classe d'outils formels appelés *langages graphiques*. Il est à noter que cette appellation peut désigner divers types de langages dans les divers domaines de l'informatique, leur point commun étant de représenter une certaine information graphiquement, associé généralement au fait que les éléments graphiques peuvent y être combinés pour en former de plus complexes. Les langages graphiques que nous considérons dans cette thèse sont plus précisément des langages de *diagrammes de cordes*, c'est à dire de diagrammes avec des fils d'entrée et de sortie représentés de part et d'autre du diagramme (dans cette thèse nous les représentons respectivement à gauche et à droite), de la même manière que dans les circuits quantiques. Les diagrammes sont en général construits à partir d'un ensemble de diagrammes élémentaires appelés *générateurs*, de manière inductive à l'aide d'un ensemble d'opérations comprenant au moins la composition séquentielle  et la composition parallèle  .

De nombreux types d'objets peuvent être représentés à l'aide de diagrammes de cordes, essentiellement tous ceux qui possèdent une notion d'entrées et de sorties. Dans cette thèse, l'essentiel des objets représentés peuvent être vus soit comme des programmes quantiques, prenant des données quantiques en entrée et renvoyant le résultat en sortie, soit comme des évolutions ou des transformations, dont l'entrée est l'état initial d'un système quantique et la sortie est l'état final du système.

Parmi les langages graphiques utilisés en informatique quantique, en plus des circuits quantiques, on trouve notamment le ZX-calcul [45, 46], qui peut être vu comme une généralisation des circuits

quantiques avec de bonnes propriétés topologiques et de réécriture, ainsi que des langages de structure similaire comme le ZW-calcul [75] et le ZH-calcul [14].

Théories équationnelles. Un langage graphique — comme tout langage ou presque — est généralement équipé d'une sémantique, la plupart du temps donnée sous la forme d'une fonction associant à chaque diagramme une interprétation (aussi appelée la sémantique du diagramme, par un léger abus de langage), qui peut être vue comme une description de ce que le diagramme fait en tant que programme ou processus. Parmi les problèmes habituellement considérés, souvent directement liés applications pratiques des langages, on trouve notamment celui de déterminer si deux diagrammes donnés ont la même interprétation — on dit alors qu'ils sont équivalents — et celui de transformer un diagramme donné en un diagramme équivalent plus adapté à une utilisation particulière.

Par exemple dans l'étude des circuits quantiques, un problème important est celui de l'optimisation des circuits. Les circuits produits au cours de l'exécution d'un programme quantique peuvent en effet facilement devenir de grande taille et coûteux à implémenter physiquement, de sorte qu'en les optimisant en temps réel on peut obtenir un gain significatif en termes de temps de calcul et d'utilisation des ressources. Un autre problème pratique couramment rencontré est celui de la satisfaction des contraintes matérielles des implémentations physiques. En particulier, certaines implémentations de mémoires quantiques ont une topologie particulière qui empêche d'appliquer des portes multi-qubits à certains ensembles de qubits. Pour exécuter un circuit quantique sur une telle implémentation, il est donc nécessaire de le transformer d'abord en un circuit équivalent ne contenant que des portes physiquement réalisables.

Un outil souvent utile pour étudier l'équivalence des diagrammes et pour les transformer est une *théorie équationnelle*. Autrement dit, un ensemble d'égalités entre des diagrammes — dont il est généralement requis qu'elles respectent la sémantique — qui peut être utilisé pour réécrire un diagramme en un autre équivalent en remplaçant des sous-diagrammes l'un après l'autre. Étant donnée une théorie équationnelle, on peut par exemple définir une stratégie de réécriture afin d'optimiser les diagrammes (comme nous le faisons notamment dans le chapitre 4).

Une propriété souvent recherchée chez une théorie équationnelle est qu'elle soit *complète*, c'est à dire telle qu'il soit possible de transformer n'importe quel diagramme en n'importe quel autre diagramme équivalent par réécriture successive de sous-diagrammes. Des théories équationnelles complètes sont connues pour les ZX-, ZW- et ZH-calculs, ainsi que pour de nombreux fragments de ces langages (c'est à dire des sous-langages générés par un sous-ensemble des générateurs). Inversement, bien que le formalisme des circuits quantiques soit largement utilisé depuis près de trois décennies, et que la question ait un réel intérêt pratique, aucune théorie équationnelle complète n'était connue pour les circuits quantiques au moment de débuter cette thèse.

Contrôle quantique. Bien que les circuits quantiques soient un bon outil pour décrire les opérations à effectuer sur des données quantiques, ils ne tiennent pas compte d'un autre aspect de la programmation qu'est le *flux de contrôle*. En effet, dans un circuit quantique, l'ordre des portes est fixé. De nombreux langages de programmation quantiques traitent cet aspect de manière naïve, en adoptant un paradigme habituellement résumé par l'expression "données quantiques, contrôle classique". Autrement dit, l'application d'opérations quantiques sur des données quantiques est contrôlée de manière classique, à l'aide de primitives usuelles comme les instructions conditionnelles if et les boucles for et while. Bien que cela soit suffisant dans beaucoup de cas, cela n'exploite pas l'ensemble des possibilités offertes par les lois de la physique quantique, qui permettent également au flux de contrôle d'être lui-même quantique.

L'ingrédient essentiel pour un flux de contrôle quantique est le *contrôle cohérent*[1], qui est essentiellement la version quantique d'une instruction conditionnelle if. Celui-ci consiste à contrôler le choix d'une opération à appliquer à un système quantique, appelé le *système cible*, à partir de l'état d'un autre système quantique, appelé le *système de contrôle*, qui peut être en superposition : à chacun des états classiques superposés est associée une opération à appliquer au système cible.

[1] À noter que les expressions "contrôle quantique" et "contrôle cohérent" sont également utilisées dans d'autres contextes dans des sens différents, en particulier en physique expérimentale dans des situations où l'on contrôle le comportement d'un système quantique — alors qu'ici on contrôle *à partir* de l'état d'un système quantique.

Un exemple simple de contrôle cohérent est le *quantum switch* [34] : étant donnés un qubit — dont l'état est une combinaison linéaire $\alpha|0\rangle+\beta|1\rangle$ — un second système quantique, et deux opérations U et V agissant sur le second système, le quantum switch de U et V est l'opération sur le système global (composé du qubit, utilisé comme système de contrôle, ainsi que du second système, utilisé comme système cible) définie par linéarité par $|0\rangle \otimes |\varphi\rangle \mapsto |0\rangle \otimes VU|\varphi\rangle$ et $|1\rangle \otimes |\varphi\rangle \mapsto |1\rangle \otimes UV|\varphi\rangle$. Autrement dit, le qubit contrôle l'ordre dans lequel les opérations U et V sont appliquées : s'il est dans l'état $|0\rangle$, l'opération appliquée au système cible est VU, et s'il est dans l'état $|1\rangle$, l'opération appliquée au système cible est UV. Le fait qu'une opération soit appliquée avant l'autre implique que la première peut communiquer de l'information à la seconde, en particulier au moyen de l'état intermédiaire du système cible. C'est pourquoi un tel dispositif est généralement interprété comme opérant un contrôle cohérent de l'*ordre causal* des deux opérations. Lorsque le qubit de contrôle est en superposition, U et V sont appliquées dans un *ordre causal indéfini*.

Avantages pour le calcul et la communication. Le contrôle quantique apporte de nouveaux avantages, pour la réalisation de certaines tâches, par rapport à ce qui est déjà permis par l'informatique quantique avec un contrôle classique. Par exemple, étant donnés deux canaux de communication quantiques qui, pris chacun individuellement, n'ont aucune capacité de transmission d'information (le bruit qu'il contiennent efface complètement le signal donné en entrée), il est néanmoins possible de transmettre de l'information en envoyant un signal dans les deux à la fois en superposition, au moyen du contrôle cohérent [4]. Le contrôle cohérent peut également être utilisé pour améliorer les performances de tâches plus calculatoires. Par exemple, étant données deux opérations quantiques dont on sait qu'elles commutent ou bien anticommutent, l'utilisation du contrôle cohérent permet de déterminer dans lequel de ces deux cas elles se trouvent, en faisant un seul appel à chacune, alors qu'en utilisant un circuit quantique pour répondre à la même question il est en général nécessaire d'effectuer deux appels à l'une des opérations [31]. Guérin *et al.* [72] ont défini une tâche de communication basée sur ce problème et prouvé qu'elle nécessite exponentiellement moins de ressources, en termes de quantité d'information à échanger entre les différents acteurs, lorsqu'il est possible d'effectuer du contrôle cohérent d'ordre causal.

Un autre exemple de tâche où le contrôle quantique apporte un avantage est, étant données n opérations unitaires $U_1, ..., U_n$, d'implémenter une permutation contrôlée (classiquement) de ces opérations — c'est à dire un programme qui étant donnée une permuation σ, applique les opérations dans l'ordre correspondant. Cela peut être fait en utilisant une occurrence de chaque U_i et $\mathcal{O}(n)$ quantum switches, alors que dans le cadre habituel des circuits quantiques, le meilleur algorithme connu nécessite $\Theta(n^2)$ appels aux U_i. Cette dernière complexité a été prouvée optimale sous réserve d'une restriction sur le type de circuit utilisé [50, 60].

Implémentations. Plusieurs implémentations expérimentales de contrôle cohérent ont été réalisées, en particulier de l'ordre causal de deux opérations via le quantum switch, afin de démontrer la réalité physique de certaines de ses conséquences. Dans [112], les auteurs réalisent une implémentation du protocole utilisant le quantum switch pour décider si deux opérations commutent ou anticommutent, et vérifient son fonctionnement sur des exemples. Dans [116, 68, 117], les auteurs démontrent la réalité physique d'un ordre causal indéfini. Dans [67, 73], les auteurs démontrent expérimentalement qu'il est possible de transmettre une quantité significative d'informations à l'aide de deux canaux qui individuellement n'en transmettent aucune, en les mettant l'un à la suite de l'autre dans une superposition des deux ordres causaux possibles. Enfin, [129] montre expérimentalement un gain de performance permis par l'utilisation du quantum switch pour une tâche similaire à celle définie dans [72].

Cadres formels pour le contrôle quantique. L'objectif initial de cette thèse était de développer un cadre formel dans lequel il soit possible de représenter des programmes ou des évolutions impliquant un contrôle quantique, et de raisonner sur ceux-ci.

Cette question a été peu explorée avant le début de cette thèse. En 2008, Chiribella *et al.* [32] ont introduit le concept de *supermap*, pour désigner des opérateurs agissant sur des opérations quantiques. Bien que très utiles par ailleurs, les supermaps ne sont pas adaptées pour l'étude approfondie d'un programme en particulier, puisqu'elles ne prennent en compte que le comportement extensionnel

des opérations. Dans [33], les mêmes auteurs introduisent les *quantum networks*, qui peuvent être vus comme un langage graphique permettant de décrire une classe très générale de programmes quantiques pouvant comporter du contrôle quantique et des transformations d'ordre supérieur (autrement dit des transformations de transformations, et ainsi de suite). Ils traitent cependant ce langage de manière essentiellement sémantique, et à ma connaissance il n'y a pas eu de tentative d'exploiter celui-ci comme un langage permettant de raisonner sur les programmes quantiques qu'il permet de représenter, de la manière dont nous cherchons à le faire dans cette thèse. Dans [50], les auteurs introduisent un langage graphique avec des *connexions programmables* entre les opérations. Le langage utilise le quantum switch comme générateur, et permet de décrire le contrôle cohérent de l'ordre causal de plusieurs canaux quantiques, mais ne permet pas de décrire un contrôle quantique plus général, comme le contrôle cohérent du choix entre plusieurs canaux. Enfin, un cadre formel basé sur ce que les auteurs appellent des *causal boxes* a été introduit dans [111]. Il a cependant l'inconvénient de nécessiter des conditions non-triviales pour garantir la bonne définition des programmes représentés. Pour finir, dans le domaine des langages de programmation à vocation plus appliquée, il faut aussi mentionner plusieurs propositions pour gérer le contrôle quantique [56, 6, 132, 118].

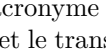
Optique linéaire pour l'informatique quantique. Dans le cadre du développement actuel des technologies quantiques, divers supports physiques permettant de stocker de l'information quantique sont actuellement à l'étude. Parmi ceux-ci on trouve notamment des systèmes matériels comme les circuits supraconducteurs, les atomes froids et les ions piégés, ainsi que des systèmes faits de lumière, où l'information est stockée dans des photons. Parmi les différents supports possibles, les photons ont un rôle privilégié de par le fait qu'ils sont le seul support actuellement envisageable pour transmettre de l'information quantique : afin de faire communiquer des processeurs quantiques entre eux, il est donc nécessaire, quelque soit le support physique utilisé par ceux-ci, de traiter une partie de l'information de manière photonique. Il existe de plus des approches apparemment viables pour une informatique quantique entièrement basée sur les photons, à la fois dans le régime NISQ (pour *noisy intermediate-scale quantum*, c'est à dire pour les systèmes accessibles à court et moyen terme, qui n'ont pas une taille suffisante pour permettre la correction d'erreurs) [94] et dans le régime des systèmes de grande dimension avec correction d'erreurs [17].

L'unité standard d'information quantique est le qubit, et les photons offrent un large choix de manières d'encoder des qubits. Cependant, il est aussi intéressant de noter que d'utiliser directement l'état des photons, sans passer par un encodage, peut parfois être plus avantageux. Un bon exemple pour illustrer cela est le *BosonSampling* [2], une tâche de calcul $\#P$-difficile mais qui peut être réalisée efficacement en faisant intéragir des photons dans un circuit optique linéaire idéal. Avec le *Random Circuit Sampling* [3, 23], c'est l'une des deux principales tâches pour lesquelles des démonstrations expérimentales d'un avantage calculatoire quantique — où un système quantique permet de réaliser une tâche a priori hors de portées des capacités actuelles de calcul classique — ont été proposées [13, 135, 131, 134].

Un autre avantage de l'informatique quantique photonique est de permettre d'implémenter le contrôle cohérent de manière simple. Notamment, toutes les implémentations expérimentales citées plus haut adoptent une approche photonique : celles de [112, 116, 117, 73] utilisent le degré de liberté spatial d'un photon comme qubit de contrôle et sa polarisation comme système cible ; celles de [68, 67] font l'inverse ; enfin, celle de [129] utilise le degré de liberté spatial comme qubit de contrôle et le degré de liberté temporel comme système cible.

Les implémentations optiques du contrôle cohérent utilisent généralement essentiellement l'optique *linéaire*, c'est à dire la partie de l'optique qui n'utilise que des éléments ne modifiant pas la longueur d'onde des photons et obéissant au principe de superposition, comme c'est le cas des éléments les plus courants comme les *beam splitters* — polarisants ou non — les lentilles, les miroirs, les déphaseurs et les lames à retard, auxquels s'ajoutent les sources et détecteurs de photons.

Dans une grande partie de cette cette thèse, nous nous plaçons dans le cadre d'une famille d'implémentations utilisant la polarisation comme qubit de contrôle, comme celles de [68, 67]. Plus précisément, nous considérons un photon, décrit de manière abstraite par sa polarisation, sa position, et un troisième degré de liberté, dont nous ne spécifions pas la nature physique. La polarisation est décrite par un état quantique de dimension 2 engendré par deux polarisations particulières (linéaires), dites respectivement

verticale et horizontale et notées **V** et **H**. Comme nous considérons uniquement des dispositifs où — à un instant donné — le photon peut uniquement être à un nombre fini et borné de positions spécifiques, sa position est décrite par un état quantique de dimension finie n. Concernant le troisième degré de liberté, utilisé intuitivement pour stocker des données sur lesquelles des opérations seront effectuées, nous le prenons également de dimension finie q. Les trois degrés de liberté du photon (position, polarisation et données) se comportent comme des systèmes quantiques distincts, l'état du photon est donc décrit par un élément de l'espace vectoriel $\mathbb{C}^2 \otimes \mathbb{C}^n \otimes \mathbb{C}^q$, généré par des états de base de la forme $|c\rangle \otimes |p\rangle \otimes |x\rangle$ aussi notés $|c, p, x\rangle$ (avec $c \in \{\mathbf{V}, \mathbf{H}\}$, $p \in \{0, ..., n-1\}$ et $x \in \{0, ..., q-1\}$), qui correspondent aux états classiques possibles du photon. On peut alors effectuer du contrôle quantique en utilisant un *beam splitter polarisant* (ou PBS, d'après l'acronyme anglais de *polarising beam splitter*)  , qui réfléchit le photon si sa polarisation est verticale, et le transmet (autrement dit, le laisse passer) si sa polarisation est horizontale. Autrement dit, en considérant que la position du photon a deux états classiques possibles, correspondant aux deux positions verticales possibles (en haut ou en bas), le PBS applique l'opération contrôlée définie par linéarité par $|\mathbf{V}, p, x\rangle \mapsto |\mathbf{V}, p, x\rangle$ et $|\mathbf{H}, p, x\rangle \mapsto |\mathbf{H}\rangle \otimes X|p\rangle \otimes |x\rangle$, où X est définie par $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$. Si la polarisation du photon est en superposition, alors sa position devient superposée également (ce que l'on peut interpréter comme le fait d'être aux deux endroits en même temps), et intriquée avec la polarisation. En plaçant différentes opérations, agissant sur le troisième degré de liberté du photon, sur les différents chemins parcourus en superposition par le photon, on obtient alors un contrôle cohérent de ces opérations par la polarisation.

Contributions de la thèse. L'objectif de départ de cette thèse était de développer un cadre formel dans lequel il soit possible de représenter des dispositifs de contrôle cohérent et de raisonner sur ceux-ci de manière aussi simple et générale que possible. C'est un projet de grande ampleur qui n'en est qu'à son commencement. Notre approche pour ce faire a été d'abstraire et de formaliser une implémentation en optique linéaire du contrôle cohérent, comme esquissé dans le paragraphe précedent. Découlant directement de cette approche, notre première contribution, présentée dans le chapitre 3, est un langage graphique essentiellement inspiré de cette implémentation. Cette approche induit naturellement deux points de vue : le premier, qui sous-tend l'idée initiale, privilégie le contrôle cohérent, et traite l'optique linéaire de manière abstraite et avant tout comme un moyen de représenter des processus impliquant du contrôle cohérent. Le second privilégie l'aspect optique linéaire, et considère les diagrammes comme représentant avant tout des dispositifs optiques physiquement valides : le contrôle cohérent est alors vu comme une conséquence des lois de l'optique quantique. Dans cette thèse nous adoptons tour à tour les deux points de vue.

Dans le chapitre 3, nous introduisons un langage graphique, le PBS-calcul, dont la syntaxe et la sémantique sont directement tirés d'un fragment restreint de l'optique linéaire, et qui permet de représenter le contrôle cohérent d'opérations quantiques. Nous l'équipons d'une axiomatisation complète (c'est à dire une théorie équationnelle complète), qui est de plus minimale (autrement dit, il n'y a aucune redondance entre les axiomes). Le langage a une expressivité relativement limitée, à la fois pour ce qui est des opérations pouvant être contrôlées et de la manière dont elles peuvent être contrôlées. Son but principal est de poser les fondations d'un cadre formel pour l'étude du contrôle quantique et de ses différents aspects. Le reste de cette thèse consiste essentiellement à développer ce cadre formel, en s'appuyant sur le formalisme du PBS-calcul, dans plusieurs directions :

Dans le chapitre 4, nous introduisons un raffinement du PBS-calcul, pour lequel nous donnons également une axiomatisation complète et minimale, et nous examinons le problème de l'optimisation des ressources dans ce cadre. Nous donnons une procédure simple pour le problème naturel de l'optimisation des appels à oracles dans les diagrammes. Nous montrons ensuite qu'un raffinement naturel de ce problème est NP-difficile, malgré les limitations du langage. Enfin nous donnons une heuristique de complexité polynomiale pour ce problème raffiné, et nous montrons qu'elle donne un résultat optimal pour une famille restreinte de diagrammes. Nous n'évaluons cependant pas ses performances dans le cas général.

Les travaux exposés dans le chapitre 5 adoptent le second point de vue évoqué plus haut et se concentrent sur la partie optique linéaire : nous définissons un langage graphique pour les circuits optiques linéaires sans création ni destruction de photons. Ce langage peut être vu comme une extension du PBS-calcul comprenant les principaux éléments optiques linéaires utilisés expérimentalement par les physiciens,

mais sans les boîtes noires qui permettaient de faire intervenir des appel à oracles. Nous donnons une axiomatisation complète de ce langage. La preuve de complétude s'appuie sur une forme normale composée de plusieurs parties dont la principale est un circuit optique appartenant à un fragment du langage, celui des circuits *polarisation-preserving*, définis comme étant ceux composés uniquement d'éléments qui n'agissent pas sur la polarisation. Ce fragment est lui-même équipé d'une théorie équationnelle complète, et le circuit intervenant dans la forme normale pour le langage complet est lui-même une forme normale permettant de démontrer la complétude de l'axiomatisation du fragment. Nous définissons également un système de réécriture fortement normalisant et confluent, permettant de mettre n'importe quel circuit du fragment en forme normale.

Dans le chapitre 6, nous exploitons une correspondance entre les circuits optiques linéaires *polarisation-preserving* et les circuits quantiques avec portes multicontrôlées, pour trouver une théorie équationnelle complète pour les circuits quantiques.

Pour finir, dans le chapitre 7, nous étendons la syntaxe du PBS-calcul (dans sa version du chapitre 3) afin de permettre le contrôle cohérent de canaux de communication quantiques généraux. Comme la description habituelle des canaux quantiques, donnée par un objet mathématique appelé *CPTP map*, est insuffisante dans un contexte de contrôle cohérent, notre principale contribution est de caractériser précisément quelles informations la description d'un canal quantique doit contenir, pour qu'il soit possible de prédire son comportement dans le cadre du contrôle cohérent permis par les diagrammes du PBS-calcul. Nous traitons également cette question en considérant des restrictions naturelles du PBS-calcul.

À quelques ajouts et arrangements près, chaque chapitre correspond à un article publié durant la thèse :

- [39] Alexandre Clément et Simon Perdrix. PBS-calculus: A graphical language for coherent control of quantum computations. In *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, 2020. doi:10.4230/LIPIcs.MFCS.2020.24. **(Chapitre 3)**
- [40] Alexandre Clément et Simon Perdrix. Resource optimisation of coherently controlled quantum computations with the PBS-calculus. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, 2022. doi:10.4230/LIPIcs.MFCS.2022.36. **(Chapitre 4)**
- [38] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix et Benoît Valiron. LO_{v}-calculus: A graphical language for linear optical quantum circuits. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, 2022. doi:10.4230/LIPIcs.MFCS.2022.35. **(Chapitre 5)**
- [37] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix et Benoît Valiron. A complete equational theory for quantum circuits. 2022. arXiv:2206.10577. preprint arXiv, soumis à LICS 2023. **(Chapitre 6)**
- [24] Cyril Branciard, Alexandre Clément, Mehdi Mhalla et Simon Perdrix. Coherent control and distinguishability of quantum channels via PBS-diagrams. In *46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)*, 2021. doi:10.4230/LIPIcs.MFCS.2021.22. **(Chapitre 7)**

L'exposé de ces résultats de recherche est précédée par une introduction rapide des principales notions nécessaires : dans le chapitre 1, nous donnons une définition des structures combinatoires qui sous-tendent les langages graphiques considérés dans cette thèse. Dans le chapitre 2, nous faisons une brève introduction à l'informatique quantique afin en particulier d'introduire les concepts utilisées dans cette thèse.

Contents

Introduction (fr) iii

Introduction xv

Part I Background 1

Chapter 1 Structure of Graphical Languages 3

Chapter 2 Quantum Computing 9

2.1 Key Notions and Concepts . . . 9
2.2 Quantum Circuits . . . 13
2.3 Extended Circuit Notations . . . 14

Part II PBS-Diagrams and Extensions 17

Chapter 3 PBS-Diagrams and the PBS-Calculus 19

3.1 Syntax . . . 20
3.2 Semantics . . . 21
3.2.1 Classical Control – Path Semantics . . . 21
3.2.2 Quantum Control – Denotational Semantics . . . 27
3.3 Equational Theory – PBS-Calculus . . . 30
3.3.1 Axiomatisation . . . 30
3.3.2 Normal Forms . . . 32
3.3.3 Completeness . . . 38
3.3.4 Expressiveness . . . 39
3.4 Minimality of the Set of Axioms . . . 39
3.4.1 Independence of Equations (3.1) to (3.8) and (3.10) . . . 39
3.4.2 Independence of Equation (3.9) . . . 41
3.4.2.1 A Variant of the Traced PROP Structure (PROTWEB) . . . 41
3.4.2.2 Proof of the Independence of Equation (3.9) . . . 43
3.5 Removing the Trace – Loop Unrolling . . . 47
3.6 Final Remark . . . 50

Chapter 4 Coloured PBS-diagrams and Resource Optimisation **51**
4.1 Coloured PBS-Diagrams . . . 52
4.2 Semantics . . . 53
4.2.1 Quantum Semantics . . . 55
4.2.2 Interpretation . . . 55
4.3 Equational Theory . . . 57
4.4 Resource Optimisation . . . 63
4.4.1 Minimising the Number of Oracle Queries . . . 64
4.4.2 Optimising Both Queries and PBS . . . 65
4.4.3 Hardness . . . 73
4.5 Discussions and Future Work . . . 80

Chapter 5 LO_v-Calculus : A Graphical Language for Photon-Preserving Linear Optical Circuits **83**
5.1 Linear Optical Quantum Circuits . . . 84
5.1.1 Syntax . . . 84
5.1.2 Single-Photon Semantics . . . 85
5.2 Equational Theory . . . 89
5.3 Polarisation-Preserving Circuits . . . 92
5.4 Completeness of the LO_v-Calculus . . . 104
5.5 Discussion About the Trace . . . 107
5.5.1 Instant-Travel Model . . . 107
5.5.2 Delayed Trace . . . 110

Chapter 6 A Complete Equational Theory for Quantum Circuits **113**
6.1 Quantum Circuits . . . 114
6.1.1 Quantum Circuits: Syntax and Semantics . . . 114
6.1.2 Structural Equations . . . 115
6.1.3 Controlled Gates . . . 118
6.1.4 Properties of Multi-Controlled Gates . . . 120
6.1.4.1 Inductive Properties for Multi-Controls . . . 121
6.1.4.2 Swapping Controls Together and With Phase Gates . . . 123
6.1.4.3 Monoid Structure . . . 131
6.1.4.4 Complementarity of Control and Anti-Control . . . 136
6.1.4.5 Controlled and Anti-Controlled Gates Commute (Same Target) . . . 137
6.1.4.6 Controlled and Anti-Controlled Gates Commute (Different Targets) 144
6.1.5 Euler Angles and Periodicity . . . 151
6.2 Completeness . . . 158
6.2.1 Forgetting the Monoidal Structure . . . 158
6.2.2 Encoding Quantum Circuits Into Optical Ones . . . 160
6.2.3 Decoding . . . 162
6.2.4 Quantum Circuit Completeness . . . 163

6.2.4.1 $D(E(C))$ is equivalent to C . . . 163
6.2.4.2 Mimicking the Topological Rules . . . 169
6.2.4.3 Mimicking the Rules of QC . . . 174
6.2.4.4 Completeness Proof . . . 184

Chapter 7 Coherent Control and Distinguishability of Quantum Channels via PBS-Diagrams 185
7.1 PBS-Diagrams . . . 185
7.1.1 Bare PBS-Diagrams . . . 186
7.1.1.1 Syntax . . . 186
7.1.1.2 Word Path Semantics . . . 186
7.1.2 Extended PBS-Diagrams . . . 191
7.1.2.1 Purified Channels . . . 191
7.1.2.2 From Bare to Extended PBS-Diagrams . . . 192
7.1.2.3 Quantum Semantics . . . 193
7.2 Observational Equivalence of Purified Channels . . . 194
7.2.1 Contexts . . . 194
7.2.2 Observational Equivalence Using PBS-Free Contexts . . . 195
7.2.3 Observational Equivalence Using Negation-Free Contexts . . . 196
7.2.4 Observational Equivalence Using General Contexts . . . 199
7.3 Observational Equivalence Beyond PBS-Diagrams . . . 206

Conclusion 209

Appendices 211

Appendix A PBS-Diagrams and the PBS-Calculus 211
A.1 Derivations of Ancillary Equations . . . 211
A.1.1 Derivations of the Ancillary Equations of the Proof of Lemma 3.26. . . . 211
A.1.2 Derivations of the Ancillary Equations of the Proof of Lemma 3.28. . . . 219
A.2 Proof of Equivalence Between the Two Diagrams of Figure 3.2 Using the PBS-Calculus 222

Appendix B Coloured PBS-Diagrams and Resource Optimisation 225
B.1 Derivations of Equations (4.21) to (4.27) . . . 225
B.2 Derivations of the Ancillary Equations Used in the PGT procedure . . . 226

Appendix C $\mathbf{LO_v}$-Calculus : A Graphical Language for Photon-Preserving Linear Optical Circuits 231
C.1 Useful Consequences of the Axioms . . . 231
C.2 Derivations of the Ancillary Equations of the Proof of Lemma 5.40 . . . 238
C.3 Equality of Unitary Transformations on a Subspace . . . 240

Appendix D A Complete Equational Theory for Quantum Circuits **241**
D.1 Proofs of Equations (6.8) to (6.19) 241
D.2 End of the Proof of Lemma 6.61: Satisfying the Conditions on the Angles 246

Bibliography **259**

Introduction

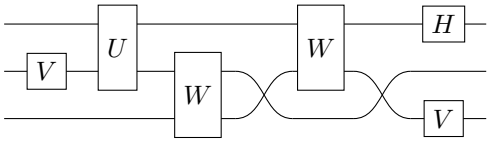
Quantum Computing. The laws of quantum physics, which apply to physical systems when their size comes close to the atomic scale, are in some ways quite different from the laws of classical physics which apply to macroscopic systems. One of the main non-classical properties of quantum systems is the possibility of superposition: roughly speaking, the state of a quantum system, called a quantum state, is represented by a complex linear combination of its possible classical states. This can somehow be interpreted as the system being in several classical states at the same time. Another property of quantum systems is that it is in general impossible to measure a quantum system without affecting it: when measuring a system which is in a superposition of classical states, one gets one of these states, randomly, with the probability of each classical state depending on the coefficients (called *amplitudes*) of the linear combination representing the superposition. This fixes the system in the observed classical state, so that any further measurement gives the same result. A third property is entanglement: the state of several quantum systems is, in general, a superposition of the various combinations of classical states of the systems, which cannot necessarily be described by considering each system separately. This implies that if one measures several quantum systems, the results are not necessarily independent. For instance, there may exist two quantum systems, that are each in a superposition of the same two states, in such a way that measuring any of them gives one of the two states each with probability $\frac{1}{2}$, and then measuring the other system necessarily gives the same result. Such a behaviour has been observed even with systems that are far away from each other, making it look like the two systems communicated faster than light, although actually no information can be transmitted by these means.

Quantum computing is a computational paradigm which consists in exploiting such non-classical properties to improve the performances of some computing tasks. Among the most well-known examples, one can cite polynomial-time algorithms for factoring integers into prime factors [122] or solving linear systems of equations [78], and an algorithm for finding an element in an array of size n with only $\mathcal{O}(\sqrt{n})$ operations [71]. Another application of exploiting the laws of quantum physics in computer science is for communication and cryptography: one can for instance design communication protocols that — in theory — make it impossible to intercept a message unless either the sender or the recipient notices it [18, 59].

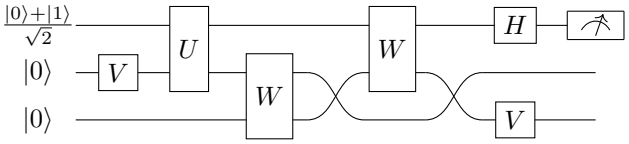
Roughly speaking, the difference between quantum and classical data is the following: given a classical variable, which can take values in a set A, its quantum equivalent takes its values — or more properly speaking, its *states* — in $\mathbb{C}^A$. In other words, a quantum variable is in a superposition of its possible classical states. The simplest example of quantum data — and the basic element in most models of quantum computing — is a qubit, which is the quantum equivalent of a bit. The state of a qubit is a vector of $\mathbb{C}^2$, generally written in the form of a superposition $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$, where $\alpha, \beta \in \mathbb{C}$, and $\left|0\right\rangle, \left|1\right\rangle$ correspond to the values 0 and 1 of a classical bit. A *qudit* is a generalisation of a qubit in dimension greater than two. It is described by a vector in $\mathbb{C}^d$ for some integer d, or in $\mathbb{C}^{\mathbb{N}}$, and generally written as a superposition of basis states that are usually denoted by $\left|0\right\rangle, \left|1\right\rangle, \left|2\right\rangle, ...$

An example of an entangled state of two qubits is $\frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)$, which has exactly the behaviour sketched above: measuring one of the two qubits fixes the global system either in state $\left|00\right\rangle$ or in state $\left|11\right\rangle$, each with probability $\frac{1}{2}$, so that the outcome of the first measurement is either 0 or 1 depending of the case, and a further measurement of the other qubit necessarily gives the same result as the first measurement.

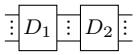
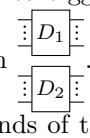
Quantum Circuits. Along with state preparations — i.e. initialisations — and measurements, the main kind of operations that one can perform on quantum data is applying a unitary transformation to one or several quantum states. Therefore, a basic low-level quantum computation is a sequence of unitary transformations each applied to a subset of the available quantum registers — which are often qubits — possibly preceded by some preparations and followed by some measurements. Quantum circuits are a graphical way to represent this: each unitary transformation is represented as a box, called a *gate*, with input and output wires, represented on its left and on its right respectively, which represent the quantum systems that it acts upon. A typical example of a quantum circuit on 3 qubits is the following:



One can also enrich the notation to represent initialisations and measurements:



Quantum circuits are ubiquitous in quantum computing. Indeed, they can — very roughly speaking — be seen as the assembly language of a quantum processor. Hence, in the traditional model of quantum computing, where a classical computer controls a quantum coprocessor, the role of the classical part essentially consists in building quantum circuits to be sent to the quantum coprocessor for execution, and then processing the outputs.

Graphical Languages. The formalism of quantum circuits belongs to a class of formal tools called *graphical languages*. Note that this term can have a variety of meanings in the various sub-fields of computer science, most having in common that they represent some information graphically, and that graphical elements can be combined to build bigger graphical representations. The graphical languages that we consider in this thesis are more precisely languages of *string diagrams*. That is, diagrams with input and output wires, represented by wires on their left and their right respectively, as for quantum circuits. The diagrams are usually generated from a set of small diagrams called *generators*, and built inductively by combining smaller diagrams into bigger ones by several means including sequential composition  and parallel composition  .

String diagrams can represent various kinds of things with inputs and outputs. The diagrams considered in this thesis can mostly be seen as representing either quantum computations, which take some quantum data as input and produce the result of the computation as an output; or quantum evolutions or transformations, whose input is the initial state of a quantum system and whose output is the final state.

Besides quantum circuits, other graphical languages used in the field of quantum computing are the ZX-calculus [45, 46], which can be seen as a generalisation of quantum circuits with good topological and rewriting properties, together with languages with a similar structure such as the ZW-calculus [75], and the ZH-calculus [14].

Equational Theories. A graphical language — as most languages — usually comes with a semantics, generally given as a function associating with every diagram an interpretation,[2] which roughly speaking tells us what the diagram does. Then a natural and practical problem is to be able to know when two diagrams have the same interpretation — one then says that they are equivalent — and to transform a diagram into an equivalent one which is better according to some criterion.

[2]By abuse of language, the interpretation of a diagram is usually called the semantics of the diagram.

For instance, in the study of quantum circuits, an important question is that of circuit optimisation. Indeed, the circuits produced during the execution of a quantum algorithm are often large and costly to implement, so that optimising them can lead to a significant reduction of the execution time and the amount of resources needed. Another application of transforming circuits into equivalent ones is the satisfaction of hardware constraints. Indeed, some physical implementations of quantum memory have a topology that restricts to which sets of qubits one can apply a multi-qubit gate. As a consequence, to execute a quantum circuit on such implementations, one first has to transform it into an equivalent circuit made only of allowed gates.

An often useful tool for the study of equivalence and rewriting of diagrams in a given graphical language is an *equational theory*. That is, a set of equalities between diagrams, which is generally required to be *sound* — that is, in every equality, the two sides have the same semantics — and can be used to rewrite a diagram into an equivalent one, by replacing sub-diagrams one after the other. Given an equational theory, one can then for instance define a rewriting strategy for diagram optimisation (see Chapter 4).

A desirable property of an equational theory is to be *complete*, that is, such that any two equivalent diagrams can be rewritten one into the other by means of the equational theory. The ZX-, ZW- and ZH-calculi are each equipped with a complete equational theory, as well as many of their fragments (that is, sub-languages generated from a subset of the generators). By contrast, although the formalism of quantum circuits have been widely used for more than two decades and the question is of interest, no complete equational theory had been found at the beginning of this PhD.

Quantum Control. While quantum circuits are good at describing the operations that one can perform on quantum data, they do not address another aspect of computing which is the *control flow*. Indeed, in a quantum circuit, the order of the gates is fixed. Many quantum programming languages address this aspect in a naive way by adopting the "quantum data, classical control" paradigm. That is, the application of quantum operations on quantum data is controlled in a classical way, using usual constructs such as if statements, for loops and while loops. However, the laws of quantum physics actually also allow the control flow to be quantum.

The essential ingredient for a quantum control flow is *coherent control*,[3] which is roughly speaking the quantum version of an if statement. It consists in controlling an operation to be performed on a quantum system, called the *target system*, by using the state of another quantum system, called the *control system*, which can be in superposition: each of the classical states in superposition is associated with a particular operation to be applied to the target system. Then the global operation is defined by linearity, and can be interpreted as applying a superposition of the different operations to the target system.

A simple example of coherent control is the quantum switch [34]: given a qubit, whose state is a linear combination $\alpha\,|0\rangle + \beta\,|1\rangle$, another quantum system, and two operations U and V acting on the second system, the quantum switch of U and V is the operation on the global system (of both the qubit, used as a control system, and the other quantum system, used as a target system) defined by linearity by $|0\rangle \otimes |\varphi\rangle \mapsto |0\rangle \otimes VU|\varphi\rangle$ and $|1\rangle \otimes |\varphi\rangle \mapsto |1\rangle \otimes UV|\varphi\rangle$. That is, the qubit controls the order in which U and V are applied: if the control qubit is in state $|0\rangle$ then VU is applied, and if it is in state $|1\rangle$ then UV is applied. The fact that one operation is applied before the other implies that the first one can send information to the second one by means of the intermediate state. For this reason, such a scheme is usually understood as performing coherent control of the *causal order* of the two operations. When the control qubit is in superposition, U and V are applied in an *indefinite causal order*.

Computational and Communication Advantages. Quantum control allows for more than quantum computing with classical control does: for instance, given two quantum communication channels which are so noisy that they do not allow for transmitting any information, by using both in superposition by means of coherent control, it is possible to transmit some information anyway [4]. Moreover, using coherent control can be advantageous for some computing tasks. For instance, given two quantum

[3]Note that the phrases "quantum control" and "coherent control" also appear in the literature with other meanings, in particular in experimental physics to refer to the control of quantum systems, rather than, as here, to a form of control based on the state of a quantum system.

operations U and V with the promise that they either commute or anticommute, deciding whether they commute or not can be done using one call to each of them, whereas in general, a quantum circuit solving this problem needs to call either U or V twice (and the other once) [31]. A communication task based on this problem has been defined and proven to require exponentially less resources, in terms of the amount of quantum information exchanged between the parties, when coherent control (more precisely, of the causal order) is used compared to the same setting with a definite causal order [72].

A related example of advantage is the following: given n unitary operations $U_1, ..., U_n$, we want to implement a classically controlled permutation of them — that is, a program which, given a permutation σ of n elements, performs the U_is in the order specified by σ. This can be done using one occurrence of each U_i and $\mathcal{O}(n)$ quantum switches, whereas in the usual quantum circuits framework, the best known algorithm requires $\Theta(n^2)$ calls to the U_is. It has additionally been proven that the latter is the best possible asymptotic complexity assuming a restriction on the circuits allowed [50, 60].

Implementations. Several experimental implementations of coherent control have been realised, in particular of the causal order of two operations via the quantum switch, to prove the physical reality of some of its consequences, mostly using a photonic approach. Some of them use a path degree of freedom of a photon as a control qubit and its polarisation as a target system [112, 116, 117, 73], or the other way around [68, 67]. Another one uses a path degree of freedom as a control qubit and a time degree of freedom as a target qudit [129].

Specifically, in [112], an implementation of the protocol using the quantum switch for deciding whether two gates commute or anticommute is realised and tested. In [116, 68, 117], the physical reality of the indefiniteness of a causal order is shown. In [67, 73], it is shown that by using two channels in sequence in a superposition of the two possible orders, one can transmit a significant amount of information even though each channel taken individually cannot transmit any information. Finally, [129] gives evidence of an experimental advantage provided by the quantum switch for a task similar to the one defined in [72].

Formal Frameworks for Quantum Control. The first goal of this PhD was to develop a formal framework in which one can represent quantum computations, or evolutions — understood in both cases abstractly, as essentially a process transforming an input into an output — involving quantum control, and reason about them.

Previously to the beginning of this PhD, little work had been done in this direction. In 2008, Chiribella *et al.* [32] introduced the concept of *supermap*. Supermaps are functions mapping quantum operations to quantum operations. Although very useful as a concept, they do not constitute a framework for the study of particular coherently controlled quantum computations, since they only take into account their extensional behaviour. In [33], the same authors have defined *quantum networks*, which can be seen as a graphical language for describing a general class of quantum computations, possibly including quantum control and higher-order transformations (that is, transformations of transformations and so on). It is however treated essentially from a semantic point of view and to my knowledge, it has not been further exploited as a language for representing and reasoning on the quantum computations that it represents, in the way that we aim to do in this thesis. In [50], the authors have introduced a graphical language with *programmable connections*. The language uses the quantum switch as a generator, and makes it possible to describe the coherent control of the causal order of a set of quantum channels, but does not describe more general quantum control, for instance of the choice among different channels. A framework of *causal boxes* has been defined in [111]. It has however the drawback to have non-trivial well-formedness conditions. Finally, note that in the context of programming languages a few proposal have been made for handling quantum control [56, 6, 132, 118].

Linear Optical Quantum Computing. The development of quantum technologies has proceeded at pace over the past number of years, with a variety of different physical supports for quantum information being pursued. These include matter-based systems like superconducting circuits, cold atoms, and trapped ions, as well as light-based systems, in which information is encoded in photons. Among these, photons have a privileged role in the sense that regardless of hardware choice it will eventually

be necessary to network quantum processors, and, as the only sensible support for communicating quantum information, some quantum information will need to be treated photonically. Yet, in their own right, photons also offer viable approaches to quantum computing in the noisy intermediate-scale [94] and large-scale fault-tolerant [17] regimes.

The standard unit of quantum information is the quantum bit or qubit, and photons allow for a rich variety of ways to encode qubits. However it is also interesting to note that treating photons as informational units in their own right can be advantageous. A good example is BosonSampling, originally proposed by Aaronson and Arkhipov [2], a computational task that is $\#P$-hard but which can be efficiently solved by interacting photons in an idealised generic linear optical circuit in which no qubit encoding need be imposed. At present, along with Random Circuit Sampling [3, 23], this provides one of the two main routes to experimental demonstrations of quantum computational advantage [13, 135, 131, 134], in which quantum devices have been claimed to outperform classical capabilities for specific tasks.

As evoked in the "Implementations" section above, coherent control, in particular, can be implemented with optics. More precisely, with *linear* optics, that is, only with optical elements that do not change the wavelength of the photons and obey the superposition principle (like the most commonly used ones such as beam splitters — polarising or not —, lenses, mirrors, phase shifters and wave plates), together with photon sources and detectors. In this thesis, we will especially have in mind a family of implementations that use the polarisation of a photon as a control qubit, as those of [68, 67]. Specifically, we will consider a photon, described in an abstract way by its polarisation, its position, and a third, unspecified, degree of freedom. The polarisation is described by a quantum state of dimension 2 generated by the vertical and horizontal (linear) polarisations, denoted $\mathbf{V}$ and $\mathbf{H}$ respectively; we will only consider settings in which the photon can be at a finite number of specific locations at a given time, so that its position is a quantum system of finite dimension n; finally, the third degree of freedom, thought of as containing some data, is also taken to be of finite dimension q. The three degrees of freedom of the photon behave as distinct quantum systems, thus the state of the photon is described by a vector in $\mathbb{C}^2 \otimes \mathbb{C}^n \otimes \mathbb{C}^q$, generated by basis states of the form $|c\rangle \otimes |p\rangle \otimes |x\rangle$, also written $|c, p, x\rangle$, which correspond to the possible classical states of the photon (with $c \in \{\mathbf{V}, \mathbf{H}\}$, $p \in \{0, ..., n-1\}$ and $x \in \{0, ..., q-1\}$). Then one can perform coherent control by using a *polarising beam splitter (PBS)*  : when the photon encounters it, it is reflected if its polarisation is vertical, or transmitted (that is, it passes through the PBS) if its polarisation is horizontal. That is, considering that the position has two possible classical states, corresponding respectively to the two possible vertical positions (on the top or on the bottom), the PBS performs the controlled operation defined by linearity by $|\mathbf{V}, p, x\rangle \mapsto |\mathbf{V}, p, x\rangle$ and $|\mathbf{H}, p, x\rangle \mapsto |\mathbf{H}\rangle \otimes X|p\rangle \otimes |x\rangle$, where X is defined by $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$. If the polarisation of the photon is in superposition, then its position becomes in superposition too (in other words, the photon is at two places at the same time), and moreover entangled with the polarisation. Then by putting different operations, acting on the third degree of freedom of the photon, on the different paths followed in superposition by the photon, one performs a coherent control of these operations by the polarisation.

Contributions and Plan of the Thesis. The first objective of this PhD was to develop a formal framework in which one could represent coherent control schemes and reason about them in an as general and simple way as possible. This is a wide project which is only at its beginning. Our approach to do so has been by abstracting and formalising a linear optical implementation of coherent control, as described in the preceding paragraph. Following this approach, our first contribution, presented in Chapter 3, is a graphical language essentially inspired by this implementation, with limited features. This approach naturally yields two points of view: the first one, which underlies the initial idea, consists in focusing on coherent control, and considering the linear optical aspect in an abstract way and primarily as a tool to represent coherently controlled processes. The second point of view consists in focusing on the linear optical aspect, and considering our graphical languages primarily as representing physically sound (linear) optical schemes: then coherent control is seen as a consequence of the laws of quantum optics. This thesis touches on both points of view.

In Chapter 3, we introduce a graphical language called the PBS-calculus, whose syntax and semantics directly come from a small fragment of linear optics, for representing the coherent control of quantum evolutions. We equip it with a complete axiomatisation (that is, a complete equational theory), which is

also minimal (that is, there are no redundancies between the axioms). This language has some limitations, both in the quantum evolutions that can be controlled and in the way that they can be controlled. Its main goal is to provide the foundations of a formal framework for studying quantum control and its various aspects. The rest of the thesis essentially consists in developing this framework, by building on the formalism of the PBS-calculus, in several directions:

In Chapter 4, we introduce a refinement of the PBS-calculus, for which we also give a complete and minimal axiomatisation, and explore the question of resource optimisation in this framework. We give a simple procedure for the natural problem of optimising calls to oracles. We find that a natural refinement of this problem is NP-hard, despite the limitations of the language. We also give a heuristic for this refined optimisation problem, that we prove to give the optimal result in a restricted case. However, we do not evaluate its accuracy in the general case.

The work exposed in Chapter 5 focuses on the linear optical part: we define a graphical language for linear optical circuits that are photon-preserving (in the sense that they do not contain elements that can change the number of photons in the circuit), which is an extension of the PBS-calculus but without oracles. Our main result is a complete axiomatisation of this language. The proof relies on a normal form whose main part is a circuit belonging to a fragment of the language, namely of *polarisation-preserving* circuits. This fragment has itself a complete equational theory and a proof of completeness based on a normal form (on which the normal form for the whole language is based), moreover we define a confluent and terminating rewriting system that puts any circuit of this fragment in normal form.

In Chapter 6, we exploit a correspondence between polarisation-preserving linear optical circuits and quantum circuits with multi-controlled gates to find a complete axiomatisation of quantum circuits.

Finally, in Chapter 7, we extend the language of Chapter 3 in order to allow for the coherent control of general quantum channels. Note that the usual description of a quantum channel, namely as a CPTP map, is not sufficient in a coherent control context. Our main contribution is then to precisely characterise what information one needs to provide about a channel, in addition to the usual CPTP map, to be able to predict its behaviour in the coherent control framework allowed by PBS-diagrams, as well as in some of its restrictions.

Up to a few arrangements and additions, each chapter essentially corresponds to an article published during the PhD:

- [39] Alexandre Clément and Simon Perdrix. PBS-calculus: A graphical language for coherent control of quantum computations. In *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, 2020. doi:10.4230/LIPIcs.MFCS.2020.24. **(Chapter 3)**

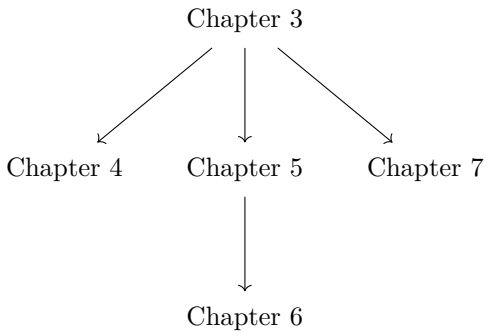
- [40] Alexandre Clément and Simon Perdrix. Resource optimisation of coherently controlled quantum computations with the PBS-calculus. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, 2022. doi:10.4230/LIPIcs.MFCS.2022.36. **(Chapter 4)**

- [38] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. $\mathrm{LO_v}$-calculus: A graphical language for linear optical quantum circuits. In *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, 2022. doi:10.4230/LIPIcs.MFCS.2022.35. **(Chapter 5)**

- [37] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. A complete equational theory for quantum circuits. 2022. arXiv:2206.10577. arXiv preprint, submitted to LICS 2023. **(Chapter 6)**

- [24] Cyril Branciard, Alexandre Clément, Mehdi Mhalla, and Simon Perdrix. Coherent control and distinguishability of quantum channels via PBS-diagrams. In *46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)*, 2021. doi:10.4230/LIPIcs.MFCS.2021.22. **(Chapter 7)**

Although the chapters are written in a way that makes them relatively independent from each other, the logical order between them can be summarised by the following diagram:



The exposition of these research results is preceded by a short introduction of the main necessary notions. In Chapter 1, we define the combinatorial structures that underlie all the graphical languages that we will consider in the thesis. In Chapter 2, we briefly give basic notions of quantum computing and introduce the related concepts being used in this thesis.

Part I

Background

Chapter 1

Structure of Graphical Languages

The graphical languages mentioned in the introduction, namely the ZX-calculus, the ZH-calculus, the ZW-calculus, and quantum circuits, have the following properties in common, together with many other languages of string diagrams:

- The diagrams are defined unambiguously by their graphical representation. This is despite the fact that a given graphical representation can generally be built in several ways: for instance, 

can be build by combining first D_1 and D_2 together, then adding D_3, or by combining first D_2 and D_3 together, then adding D_1.
- Consistently with the fact that the diagrams essentially represent transformations of an input into an output, deforming a diagram into another valid diagram does not change the transformation represented (as long as the input and output wires are not messed up).

These nice properties, almost necessary (in particular the first one) for the languages to be well-defined and practical to use, are provided by the mathematical structures underlying the languages, namely, the so-called structure of PROP and its variants.

The languages that we will define and manipulate in this thesis will also be based on such structures, so as to enjoy the same properties. More precisely, in addition to the structure of PROP itself, we will use the structure of PRO, which is a restriction of it, and the structures of traced PROP and coloured traced PROP, which are extensions of it. The purpose of this chapter is to formally define these structures, and to give the basic notions and some intuition about them.

The usual definitions of these structures (see for instance [98, 133, 74] and nLab) are within the framework of category theory. However, they can be seen as fundamentally combinatorial structures, and there is actually no need to introduce any notion of category theory to define them, or to work with them — at least in the way that we do in this thesis. For this reason, and as introducing the necessary notions of category theory would require much more efforts than needed, we follow here the approach of [27], where the structure of PROP is defined in a combinatorial way. We adapt the definition given in that paper, to the structures that we need:

Definition 1.1. *A* traced PROP $\mathbf{P}$ *is a collection of sets* $\mathbf{P}[n,m]$*, indexed by* $\mathbb{N}^2$*. An element* $f \in \mathbf{P}[n,m]$ *is called a morphism and is written* $f : n \to m$*. These sets are equipped with:*

1. *a* sequential composition $\circ : \mathbf{P}[m,k] \times \mathbf{P}[n,m] \to \mathbf{P}[n,k]$ *satisfying:*
   - associativity: $(h \circ g) \circ f = h \circ (g \circ f)$
2. *a* parallel composition $\oplus : \mathbf{P}[n,m] \times \mathbf{P}[k,\ell] \to \mathbf{P}[n+k, m+\ell]$*, satisfying:*
   - associativity: $(f \oplus g) \oplus h = f \oplus (g \oplus h)$
   - compatibility of the sequential and parallel compositions: $(f_2 \circ f_1) \oplus (g_2 \circ g_1) = (f_2 \oplus g_2) \circ (f_1 \oplus g_1)$
3. *an* empty morphism $\boxed{\ } : 0 \to 0$ *satisfying:*

- neutrality: $\boxed{\ } \oplus f = f \oplus \boxed{\ } = f$ *for all* $f \colon n \to m$

4. an identity morphism $— \colon 1 \to 1$ *satisfying:*

- neutrality: $f \circ —^{\oplus n} = f = —^{\oplus m} \circ f$ *for all* $f \colon n \to m$*, where* $—^{\oplus n}$ *is defined inductively by* $—^{\oplus 0} = \boxed{\ }$ *and* $—^{\oplus n+1} = —^{\oplus n} \oplus —$

5. a swap $\times \colon 2 \to 2$ *satisfying:*

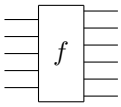
- inverse law: $\times \circ \times = —^{\oplus 2}$
- naturality: $\sigma_m \circ (— \oplus f) = (f \oplus —) \circ \sigma_n$ *for all* $f \colon n \to m$*, where* σ_k *is defined inductively by* $\sigma_0 = —$ *and* $\sigma_{k+1} = (—^{\oplus k} \oplus \times) \circ (\sigma_k \oplus —)$

6. a trace $Tr \colon \mathbf{P}[n+1, m+1] \to \mathbf{P}[n, m]$ *satisfying:*

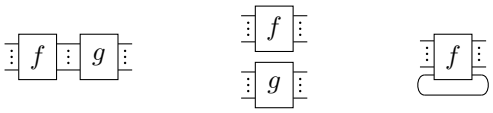
- naturality in the input: $Tr(f \circ (g \oplus —)) = Tr(f) \circ g$ *for all* $f \colon n+1 \to m+1$ *and* $g \colon k \to n$
- naturality in the output: $Tr((g \oplus —) \circ f) = g \circ Tr(f)$ *for all* $f \colon n+1 \to m+1$ *and* $g \colon m \to k$
- dinaturality: $Tr^i((—^{\oplus m} \oplus g) \circ f) = Tr^j(f \circ (—^{\oplus n} \oplus g))$ *for all* $f \colon n+i \to m+j$ *and* $g \colon j \to i$
- superposing: $Tr(g \oplus f) = g \oplus Tr(f)$ *for all* $f \colon n+1 \to m+1$ *and* $g \colon k \to \ell$
- yanking: $Tr(\times) = —$.

Additionally, if we remove Item 6 from the definition then the collection of sets is called a PROP, and if we remove Items 5 and 6 then it is called a PRO. The named equalities above are called axioms.

The concepts of (traced) PRO(P)s are mainly used for graphical languages, as it will be the case in this thesis, therefore the morphisms are generally represented graphically. A morphism $f \colon n \to m$ is represented with n input wires and m output wires. By convention, in this thesis, the diagrams are to be read from left to right. Therefore, the input wires are on the left, and the output wires are on the right. The wires on each side are ordered from top to bottom. For instance, a morphism $f \colon 5 \to 6$ is represented in the following way:



The sequential composition $g \circ f$, the parallel composition $f \oplus g$, and the trace $Tr(f)$ are respectively depicted as follows:

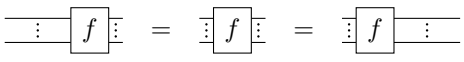


Intuitively, the trace often represents a feedback loop.[4]

The graphical representations of the axioms of traced PROP given in Definition 1.1 are the following:

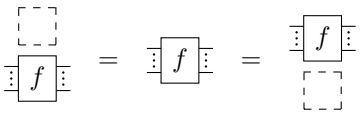
Neutrality of the identity: for any $f \colon n \to m$,

$$f \circ —^{\oplus n} \quad = \quad f \quad = \quad —^{\oplus m} \circ f$$



Neutrality of the empty morphism: for any $f \colon n \to m$,

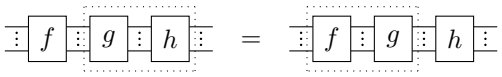
$$\boxed{\ } \oplus f \quad = \quad f \quad = \quad f \oplus \boxed{\ }$$



[4] In this thesis, this will always be the case except for extended quantum circuits (see Section 2.3).

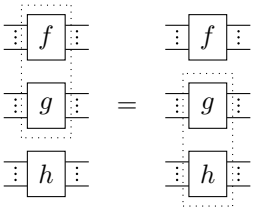
Associativity of the sequential composition: for any $f\colon n \to m$, $g\colon m \to k$, $h\colon k \to \ell$,

$$(h \circ g) \circ f \quad = \quad h \circ (g \circ f)$$



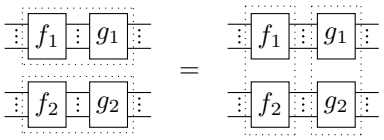
Associativity of the parallel composition: for any $f\colon n_1 \to m_1$, $g\colon n_2 \to m_2$, $h\colon n_3 \to m_3$,

$$(f \oplus g) \oplus h \quad = \quad f \oplus (g \oplus h)$$



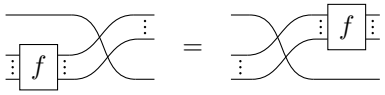
Compatibility of the sequential and parallel compositions: for any $f_1\colon n_1 \to m_1$, $g_1\colon m_1 \to k_1$, $f_2\colon n_2 \to m_2$, $g_2\colon m_2 \to k_2$,

$$(g_1 \circ f_1) \oplus (g_2 \circ f_2) \quad = \quad (g_1 \oplus g_2) \circ (f_1 \oplus f_2)$$



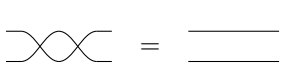
Naturality of the swap: for any $f\colon n \to m$,

$$\sigma_m \circ (- \oplus f) \quad = \quad (f \oplus -) \circ \sigma_n$$



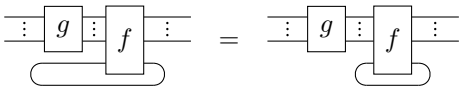
Inverse law:

$$\times \circ \times \quad = \quad -^{\oplus 2}$$



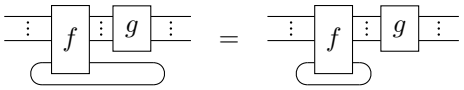
Naturality in the input: for any $f\colon n+1 \to m+1$ and $g\colon k \to n$,

$$Tr(f \circ (g \oplus -)) \quad = \quad Tr(f) \circ g$$



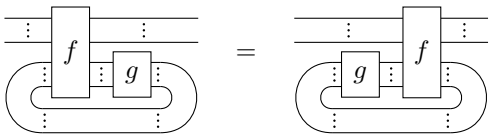
Naturality in the output: for any $f\colon n+1 \to m+1$ and $g\colon m \to k$,

$$Tr((g \oplus -) \circ f) \quad = \quad g \circ Tr(f)$$



Dinaturality: for any $f\colon n + i \to m + j$ and $g\colon j \to i$,

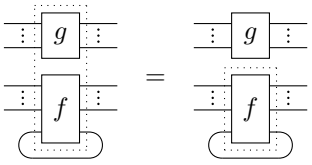
$$Tr^i((-^{\oplus m} \oplus g) \circ f) \quad = \quad Tr^j(f \circ (-^{\oplus n} \oplus g))$$



where Tr^k denotes the k^{th} power of the trace operation.

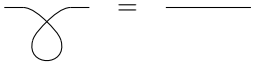
Superposing: for any $f\colon n + 1 \to m + 1$ and $g\colon k \to \ell$,

$$Tr(g \oplus f) \quad = \quad g \oplus Tr(f)$$



Yanking:

$$Tr(\supset\!\subset) \quad = \quad -$$



The axioms of (traced) PRO(P) characterise the fact that, on the one hand, the graphical representation is unambiguous (in particular without needing to add dotted boxes), and on the other hand, that the graphical representations of morphisms, called *diagrams*, can be deformed at will. Indeed, it is considered as established (Theorems 3, 7 and 20 of [120])[5] that two diagrams are equivalent according to the axioms of a (traced) PRO(P) if and only if they are isomorphic in a graph-theoretical sense, that

[5] Theorems 3.1, 3.12 and 5.22 in the arXiv version.

is, if one can be obtained from the other by graphically deforming it in a way that preserves the relative order of the input and output wires. But note, actually, that in [120], the author points out that the result for traced PROPs (Theorem 20) relies on a result by Kelly and Laplaza (Theorem 8.2, [90]) which is only proven in the case where all generators have type $1 \to 1$ — which is not the case for the (traced) PRO(P)s that we will consider in this thesis. Another caveat pointed out in [120] is that the results for PROs and PROPs (Theorems 3 and 7 respectively) rely on results by Joyal and Street (Theorem 1.5 of [87] and Theorem 1.2 of [88] for PROs, and Theorem 2.3 of [88] for PROPs) which assume that during the graphical deformation, all intermediate diagrams have their wires oriented from left to right. In both cases, the general case does not appear in the literature. However, since it is very likely that it is not significantly harder, and no counterexample has been found so far despite the wide use of this kind of graphical languages, we will assume it to be true. Moreover, whenever we use this result in a proof to deform a diagram, we can directly use the axioms instead. If this result were to be false and some proof were to become incomplete because of this, then it would suffice to add the missing axioms to the definition of a (traced) PRO(P) to make the proof complete again.

Remark 1.2. *Note that in the literature, the parallel composition $\oplus$ (also called the monoidal product) is generally written $\otimes$. We prefer to use $\oplus$ here as it is more consistent with the semantics of most of the (traced) PRO(P)s that we will consider in this thesis. The only exception is the PROP of quantum circuits, for which we will revert to the usual $\otimes$ notation.*

Example 1.3. *The collection of sets $\mathcal{M}$, where $\mathcal{M}[n,m] = \mathbb{C}^{2^m \times 2^n}$, is a traced PROP, with* ⬚ $= 1$, — $= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, ⨉ $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, *the sequential composition given by the matrix product, the parallel composition given by the Kronecker product $\otimes$, and the trace given by the partial trace over $\mathbb{C}^2$, where the partial trace is defined as follows: given three Hilbert spaces $\mathcal{A}$, $\mathcal{A}'$ and $\mathcal{B}$, one can identify the space $\mathcal{L}(\mathcal{A} \otimes \mathcal{B}, \mathcal{A}' \otimes \mathcal{B})$ with $\mathcal{L}(\mathcal{A}, \mathcal{A}') \otimes \mathcal{L}(\mathcal{B})$ (where for any vector spaces $\mathcal{V}$ and $\mathcal{V}'$, $\mathcal{L}(\mathcal{V}, \mathcal{V}')$ denotes the space of linear maps from $\mathcal{V}$ to $\mathcal{V}'$, and $\mathcal{L}(\mathcal{V}) \coloneqq \mathcal{L}(\mathcal{V}, \mathcal{V})$); then the partial trace over $\mathcal{B}$ is the linear map $\mathrm{Tr}_{\mathcal{B}} \colon \mathcal{L}(\mathcal{A} \otimes \mathcal{B}, \mathcal{A}' \otimes \mathcal{B}) \to \mathcal{L}(\mathcal{A}, \mathcal{A}')$ defined by $\mathrm{Tr}_{\mathcal{B}}(A \otimes B) = \mathrm{Tr}(B)A$ for any $A \in \mathcal{L}(\mathcal{A}, \mathcal{A}')$ and $B \in \mathcal{L}(\mathcal{B})$.*

Most of the time, we will consider the (traced) PRO(P) generated (more precisely, freely generated) by some particular set of generators. That is, the smallest (traced) PRO(P) containing these generators, the empty diagram and the identity (and the swap if relevant), closed under sequential and parallel composition (and trace if relevant). The definition can be formalised as follows:

Definition 1.4. *Given a set A, together with a type $n_a \to m_a$ for each element $a \in A$, to define the traced PROP (freely) generated by A, we first consider the set of terms inductively defined as follows:*

⬚ $: 0 \to 0$ — $: 1 \to 1$ ⨉ $: 2 \to 2$ $\forall a \in A, \quad a \colon n_a \to m_a$

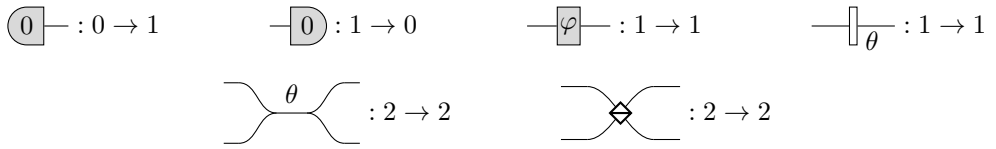
$$\frac{f \colon n \to m \quad g \colon m \to k}{g \circ f \colon n \to k} \qquad \frac{f \colon n \to m \quad g \colon k \to \ell}{f \oplus g \colon n + k \to m + \ell} \qquad \frac{f \colon n + 1 \to m + 1}{Tr(f) \colon n \to m}$$

and then we take its quotient by the axioms of traced PROP.

Note that we use the fraction notation of inference rules, which is widely used in logic-related fields. A fraction such as $\dfrac{f \colon n \to m \quad g \colon k \to \ell}{f \oplus g \colon n + k \to m + \ell}$ means "given any $f \colon n \to m$ and $g \colon k \to \ell$, we build a new term denoted $f \oplus g$, of type $n + k \to m + \ell$". Note that before taking the quotient by the axioms of traced PROP, two syntactically different terms are considered distinct.

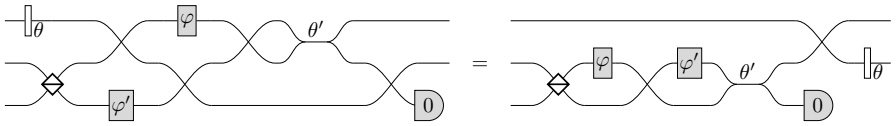
The definition of the PROP (resp. the PRO) generated by a set of generators is the same but without the last rule involving the trace (resp. without the rule involving the trace and without the swap).

Example 1.5. *In Chapter 5, we will consider the PROP* $\mathbf{LO_v}$ *of* $\mathrm{LO_v}$*-circuits*[6] *generated by*

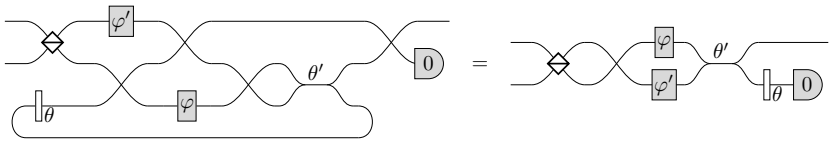


where $\theta, \varphi \in \mathbb{R}$.

A non-trivial example of deformation is the following:



One can also consider the traced PROP generated by the same generators, as we do in the discussion of Section 5.5. An example of deformation involving the trace is the following:



In Chapter 4, we will also use *coloured* traced PROPs. Graphically, this means that each wire has a type taken from a fixed set, and the types of wires are represented using either colours or labels (or both, to avoid loss of information in case of black and white printing or for colour-blind readers). The axioms are the same, and they still characterise the fact that a diagram represents a unique morphism and can be deformed at will (again Theorems 3, 7 and 20 of [120], with the same caveats). The formal definition is analogous to the non-coloured case:

Definition 1.6. *A* coloured traced PROP *(or* traced coloured PROP*)* $\mathbf{P}$ *is a collection of sets* $\mathbf{P}[a, b]$*, indexed by* $(\mathcal{C}^*)^2$*, where* $\mathcal{C}^*$ *is the set of finite words over an alphabet* $\mathcal{C}$*. The elements of* $\mathcal{C}$ *are usually called* colours*, and those of* $\mathcal{C}^*$ *are called* objects*. The empty word of* $\mathcal{C}^*$ *is denoted* ϵ *and the concatenation in* $\mathcal{C}^*$ *is denoted* $\oplus$*. As in the case of (traced) PRO(P)s, an element* $f \in \mathbf{P}[a, b]$ *is called a morphism and is written* $f \colon a \to b$*. These sets are equipped with:*

1. *a* sequential composition $\circ \colon \mathbf{P}[b, c] \times \mathbf{P}[a, b] \to \mathbf{P}[a, c]$ *satisfying:*
   - associativity: $(h \circ g) \circ f = h \circ (g \circ f)$
2. *a* parallel composition $\oplus \colon \mathbf{P}[a, b] \times \mathbf{P}[c, d] \to \mathbf{P}[a \oplus c, b \oplus d]$*, satisfying:*
   - associativity: $(f \oplus g) \oplus h = f \oplus (g \oplus h)$
   - compatibility of the sequential and parallel compositions: $(f_2 \circ f_1) \oplus (g_2 \circ g_1) = (f_2 \oplus g_2) \circ (f_1 \oplus g_1)$
3. *an* empty morphism $\boxed{\ } \colon \epsilon \to \epsilon$ *satisfying:*
   - neutrality: $\boxed{\ } \oplus f = f \oplus \boxed{\ } = f$ *for all* $f \colon a \to b$
4. *an* identity morphism $\overset{a}{\text{—}} \colon a \to a$ *for every* $a \in \mathcal{C}$*, satisfying:*
   - neutrality: $f \circ id_b = f = id_c \circ f$ *for all* $f \colon b \to c$*, where* id_d *is inductively defined by* $id_\epsilon = \boxed{\ }$ *and* $id_{d \oplus a} = id_d \oplus \overset{a}{\text{—}}$ *for any* $d \in \mathcal{C}^*$ *and* $a \in \mathcal{C}$
5. *a* swap $\overset{a}{\underset{b}{\times}} \colon a \oplus b \to b \oplus a$ *for every* $a, b \in \mathcal{C}$*, satisfying:*
   - inverse law: $\overset{b}{\underset{a}{\times}} \circ \overset{a}{\underset{b}{\times}} = \overset{a}{\text{—}} \oplus \overset{b}{\text{—}}$

[6] For **L**inear **O**ptical circuits with **v**acuum state sources and detectors (see Chapter 5 for details).

- naturality: $\sigma_{a,d} \circ (- \oplus f) = (f \oplus -) \circ \sigma_{a,c}$ *for all* $f \colon c \to d$*, where* $\sigma_{a,e}$ *is defined inductively for any* $a \in \mathcal{C}$ *and* $e \in \mathcal{C}^*$ *by* $\sigma_{a,0} =$  *and* $\sigma_{a,e\oplus b} = (id_e \oplus$ $) \circ (\sigma_{a,e} \oplus$ $)$

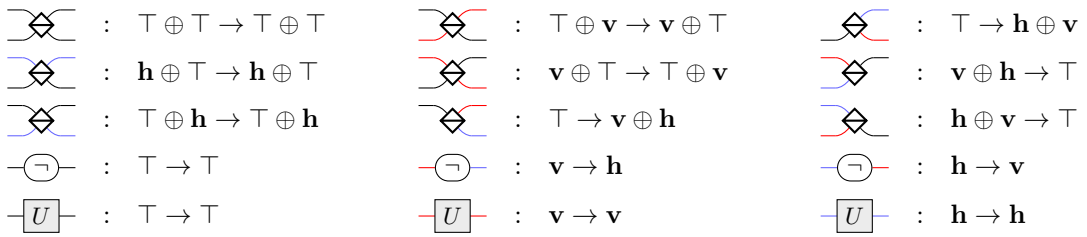
6. *a* trace $Tr_a \colon \mathbf{P}[b \oplus a, c \oplus a] \to \mathbf{P}[b, c]$ *for every* $a \in \mathcal{C}$*, satisfying (where the letters* b, c, d, e, i, j *denote elements of* $\mathcal{C}^*$*):*

   - naturality in the input: $Tr_a(f \circ (g \oplus$ $)) = Tr_a(f) \circ g$ *for all* $f \colon b \oplus a \to c \oplus a$ *and* $g \colon d \to b$
   - naturality in the output: $Tr_a((g \oplus$ $) \circ f) = g \circ Tr_a(f)$ *for all* $f \colon b \oplus a \to c \oplus a$ *and* $g \colon c \to d$
   - dinaturality: $Tr_i((id_d \oplus g) \circ f) = Tr_j(f \circ (id_c \oplus g))$ *for all* $f \colon c \oplus i \to d \oplus j$ *and* $g \colon j \to i$*, where* Tr_e *is inductively defined by* $Tr_\epsilon(f) = f$ *and* $Tr_{a\oplus e}(f) = Tr_a(Tr_e(f))$
   - superposing: $Tr_a(g \oplus f) = g \oplus Tr_a(f)$ *for all* $f \colon b \oplus a \to c \oplus a$ *and* $g \colon d \to e$
   - yanking: $Tr_a($  $) =$.

Additionally, if we remove Item 6 from the definition then the collection of sets is called a coloured PROP, and if we remove Items 5 and 6 then it is called a coloured PRO.

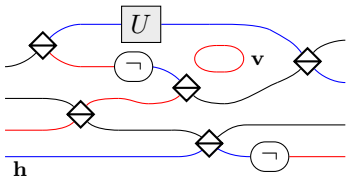
The coloured (traced) PRO(P) generated by a set can be defined in a similar way as Definition 1.4, note that the generators are then given with a coloured type $b_a \to c_a$ with $b_a, c_a \in \mathcal{C}^*$.

Example 1.7. *In Chapter 4, we will consider the coloured traced PROP, with set of colours* $\{\mathbf{v}, \mathbf{h}, \top\}$*, generated by the following generators:*



where U *is an element of some fixed monoid. Note that these are 15 distinct generators.*

Graphically, the wires of type $\mathbf{v}$ *will be represented in red, those of type* $\mathbf{h}$ *in blue, and those of type* $\top$ *in black. An example of diagram is the following:*



Note that we have put some labels to avoid ambiguity in case of black and white printing or for colour-blind readers. However, we have kept their number as small as possible to avoid overloading the diagram. These two labels are sufficient to avoid ambiguity: indeed, for each of the 3-leg generators  *and* *, the type of the three wires is fixed; for the generators of the form* *or* *, the type of one of the two sides uniquely determines the type of the other side; and for the 4-leg generators, knowing that one of the four wires is of type* $\mathbf{h}$ *(resp.* $\mathbf{v}$*) uniquely determines the types of the other three wires. Additionally, in Chapter 4 we will omit the label* $\top$*, so that unless otherwise specified, the wires whose type is ambiguous in a diagram are black by convention.*

Chapter 2

Quantum Computing

2.1 Key Notions and Concepts

Introduction. Quantum computing consists in using intrinsically quantum properties of quantum systems, such as superposition and entanglement, to improve the performances of some computing tasks.

The first task for which the idea of using quantum systems for computing was evoked is the simulation of quantum systems: indeed, these are usually hard to simulate with a classical computer, as one has to handle a vector space whose dimension grows exponentially with the size of the system, and many tasks involving such simulations are known to be NP-hard, like Boson Sampling [2] or Random Circuit Sampling [3, 23]. On the contrary, it is in theory possible to build universal quantum computers able to simulate any kind of quantum system, while keeping the amount of resources needed — in space and time — linear in the size of the system to simulate. This may find applications for instance in chemistry, for designing new molecules while being able to precisely know their properties in advance.

Among the other kinds of tasks in which quantum computers could outperform classical computers, maybe the most widely known example is that of Shor's algorithm [122], which allows one to factor a k-bit composite integer into a non-trivial product of two integers in time $\tilde{\mathcal{O}}(k^2)$, whereas the best known classical algorithm has complexity $2^{\tilde{\Theta}\left(k^{1/3}\right)}$. The existence of this algorithm implies that widely used cryptographic protocols, like RSA, which rely on the hardness of factorisation, would no longer be secure if scalable quantum computers were to be available. A related algorithm, also presented in [122], allows one to find discrete logarithms in polynomial time, which breaks additional cryptographic protocols like EDCSA.

Another example is Grover's algorithm [71], which allows one to search for a particular element in an unstructured n-length array in time $\mathcal{O}(\sqrt{n})$, whereas classically there is no better method than the naive one, which has complexity $\Theta(n)$ on average. Grover's algorithm has a large range of potential applications as it can be adapted to many situations where some kind of search is involved.

Other applications of quantum computing, that are more likely to be reachable in the near future, include optimisation algorithms, like quantum annealing for finding the maximum of a function, or QAOA.

Quantum States and State Spaces. Quantum computing manipulates *quantum states*, that is, states of quantum systems, which are described by a unit vector in some Hilbert space called the *state space* of the system.

The difference between classical and quantum data can be seen as follows. Given a variable a in classical computing, whose possible values are elements of a set $A = \{a_1, a_2, ...\}$, one can consider an orthonormal basis of $\mathbb{C}^A$: $e_{a_1}, e_{a_2}, ...$ Following Dirac's notation,[7] we write the basis vectors as $|e_{a_1}\rangle, |e_{a_2}\rangle, ...$ Then we can simplify the notation and just write $|a_1\rangle, |a_2\rangle, ...$ The quantum equivalent of the variable

[7] In quantum physics, vectors are usually written as $|\varphi\rangle$ (pronounce "ket φ"), and their adjoints (that is, linear forms) are usually written as $\langle\varphi|$ (pronounce "φ bra"), in such a way that given a vector $|\varphi\rangle$, its adjoint (namely, the orthogonal projection onto $|\varphi\rangle$) is written $\langle\varphi|$. Then applying a linear form $\langle\varphi|$ to a vector $|\psi\rangle$ is written $\langle\varphi|\,|\psi\rangle = \langle\varphi|\psi\rangle$ (pronounced "φ bracket ψ", note the pun), which corresponds to the scalar product of $|\varphi\rangle$ and $|\psi\rangle$.

a is a quantum state, that is, a unit vector, of $\mathbb{C}^A$, which can be written as a normalised linear combination $\alpha_1 |a_1\rangle + \alpha_2 |a_2\rangle + ...$, called a *superposition*, of the basis states $|a_i\rangle$, which can be interpreted as a superposition of the possible values of a.

Example 2.1. *For instance, the quantum equivalent of a bit is a qubit, whose state is a unit vector of* $\mathbb{C}^2$*, usually written as* $\alpha |0\rangle + \beta |1\rangle$*, where* $|0\rangle$ *and* $|1\rangle$ *are usually identified with the elements* $\begin{pmatrix}1\\0\end{pmatrix}$ *and* $\begin{pmatrix}0\\1\end{pmatrix}$ *of the canonical basis of* $\mathbb{C}^2$*, and* $|\alpha|^2 + |\beta|^2 = 1$*.*

Combination of Quantum Systems. The state space of two quantum systems put together is the tensor product of their respective state spaces. In other words, the state of two quantum systems is not just the state of each of the two systems separately, but rather a superposition of all possible combinations of basis states. In particular, by putting together a system with state space $\mathbb{C}^A$ and another one with state space $\mathbb{C}^B$, the overall state space is $\mathbb{C}^A \otimes \mathbb{C}^B = \mathbb{C}^{A\times B}$, that is, the state of the joint system is a superposition of all possible pairs (a, b) with $a \in A$ and $b \in B$. In other words, combining the quantum equivalents of two variables gives the quantum equivalent of the pair that we get by puting the two classical variables together.

If one takes a system in state $|\varphi\rangle \in \mathcal{H}$ and another independent system in state $|\varphi'\rangle \in \mathcal{H}'$, the state of the combined system is $|\varphi\rangle \otimes |\varphi'\rangle \in \mathcal{H} \otimes \mathcal{H}'$. Such a state is called a *separable* state. A state that is not separable is said to be *entangled*.

Remark 2.2. *The notation* $|\varphi\rangle \otimes |\varphi'\rangle$ *is often abbreviated into* $|\varphi\rangle |\varphi'\rangle$*. Moreover, following the identification* $\mathbb{C}^A \otimes \mathbb{C}^B = \mathbb{C}^{A\times B}$*, given two basis states* $|a_i\rangle$ *and* $|b_j\rangle$ *with* $a_i \in A$ *and* $b_j \in B$*, the basis state* $|a_i\rangle \otimes |b_j\rangle$ *of* $\mathbb{C}^{A\times B}$ *is often written* $|a_i, b_j\rangle$*, itself sometimes abbreviated into* $|a_i b_j\rangle$*.*

Example 2.3. *The state space of* n *qubits is* $(\mathbb{C}^2)^{\otimes n}$*. The canonical basis of this space is composed of the* 2^n *possible tensor products of* n *basis vectors of* $\{|0\rangle, |1\rangle\}$*, which can be identified with the lists of* n *bits. For instance,* $|0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle$ *is often denoted by* $|01011\rangle$*.*[8] *By means of the binary encoding,*[9] *these lists of bits can also be identifed with the integers* $0, ..., 2^n - 1$*.*

Example 2.4. *The state* $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *of two qubits is entangled.*

Example 2.5. *A quantum system that we will consider in this thesis is a photon, which is a particle with several degrees of freedom:*

- *a polarisation, described as a quantum superposition* $\alpha |\mathbf{V}\rangle + \beta |\mathbf{H}\rangle$ *of two distinguished polarisations that we call vertical (denoted* $\mathbf{V}$*) and horizontal (denoted* $\mathbf{H}$*)*
- *a position, which will be a superposition of a finite number, say* n*, of possible locations*
- *another degree of freedom described by a vector in some Hilbert space* $\mathcal{H}$*.*

The different degrees of freedom behave as distinct quantum systems, thus the overall state of the photon[10] *is described by a vector in* $\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}} \otimes \mathbb{C}^n \otimes \mathcal{H}$*, and is a superposition of basis states of the form* $|c, p, x\rangle$ *with* $c \in \{\mathbf{V}, \mathbf{H}\}$*,* $p \in [n] \coloneqq \{0, ..., n-1\}$*, and* $x \in \mathcal{H}$*.*

Basic Operations. There are essentially three kinds of basic operations that one can do in quantum computing.

- First, preparing a system in a chosen state, whose description is given by non-quantum means (in particular, it cannot depend on the state of another quantum system).

[8] Following Remark 2.2, this state could also be denoted by $|0, 1, 0, 1, 1\rangle$. We will sometimes prefer this notation with a comma, in particular for clarity when referring to an unknown basis state of several qubits, e.g. $|x, y\rangle$.

[9] The binary encoding is the most natural one, and is therefore the one that is almost always used; note however that in Chapter 6, it will be more convenient for us to use a different encoding, called *Gray code* (see Definition 6.40).

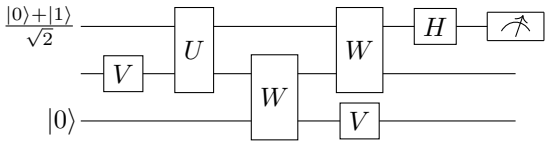
[10] A photon has actually many degrees of freedom, but it is sufficient to consider only those that are relevant in the context of our work.

- Second, applying (in-place) a unitary transformation to one or more quantum systems.
- Third, measuring a quantum system with respect to a given orthonormal basis of its state space. The outcome of such a measurement is probabilistic: given two quantum systems with state spaces $\mathcal{H}$ and $\mathcal{H}'$, and an orthonormal basis $\{|e_1\rangle, |e_2\rangle, ...\}$ of $\mathcal{H}$, so that the composite system is in state $\alpha_1 |e_1\rangle \otimes |\varphi_1\rangle + \alpha_2 |e_2\rangle \otimes |\varphi_2\rangle + ...$, measuring the first system with respect to this basis gives the classical outcome e_i with probability $|\alpha_i|^2$, and leaves the second system in state $|\varphi_i\rangle$. Depending on the nature of the measurement, the first system is either destroyed (destructive measurement), or left in state $|e_i\rangle$ so that the final overall state is the separable state $|e_i\rangle \otimes |\varphi_i\rangle$ (projective measurement).

  Note that the final remaining state φ_i is only defined up to a global phase (that is, up to a multiplicative scalar of the form $e^{i\theta}$). This does not create ambiguity since two quantum states differing only by a global phase are indistinguishable.

No-Cloning. The *no-cloning theorem* states that there is no physically realisable quantum operation which, given a quantum state $|\varphi\rangle$, produces $|\varphi\rangle \otimes |\varphi\rangle$. This is essentially because all physical operations are linear (even the measurement has some kind of linearity, see the CPTP map formalism below, and in particular Example 2.7). For the same reason, the operations must be done in-place, for instance given a transformation of quantum states V, it is in general not possible to build the transformation $|\varphi\rangle \mapsto |\varphi\rangle \otimes V |\varphi\rangle$.

Quantum Circuits. Quantum circuits, originally introduced in [55], are a graphical language for representing low-level quantum computations. They are made of primitives called *gates*, that are unitary operations acting on one or more qubits, possibly together with qubit initialisations and measurements, combined together using parallel and sequential composition. The set of available gates depends on the possibilities offered by the setup that one wants to model. A typical quantum circuit looks like this:



We will talk more in details about quantum circuits in Section 2.2.

Mixed States and Density Matrices. Due to the probabilistic nature of measurement, it is natural to consider probability distributions on quantum states. These distributions are called *mixed states*. One usually represent mixed states using the formalism of *density matrices*. Given a quantum system which is in one of the states $|\varphi_1\rangle, |\varphi_2\rangle, ...$ with probability $p_1, p_2, ...$ respectively, its density matrix is $\sum_i p_i |\varphi_i\rangle\langle\varphi_i|$.[11] A fundamental property of this formalism is that two mixed states are distinguishable by a physical experiment if and only if they have different density matrices ([105], Sections 2.2 and 2.4).

Note that $|\varphi_i\rangle\langle\varphi_i|$ is a matrix of rank 1, and that $\mathrm{Tr}(|\varphi_i\rangle\langle\varphi_i|) = \mathrm{Tr}(\langle\varphi_i| |\varphi_i\rangle) = \langle\varphi_i|\varphi_i\rangle = 1$, since $|\varphi_i\rangle$ is a unit vector. Therefore, the trace of a density matrix is the sum of the probabilities of the different states, which is equal to 1. It is known that density matrices (at least in finite dimension) are exactly the (Hermitian) positive matrices[12] of trace 1.

CPTP Maps. A linear map $f\colon \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}$ is said to be *positive* if for any positive matrix A, $f(A)$ is still positive. It is *completely positive* if for any k, $f \otimes id_{\mathbb{C}^{k\times k}}$ is positive. A completely positive trace-preserving (CPTP) map is a completely positive map f such that for any A, $\mathrm{Tr}(f(A)) = \mathrm{Tr}(A)$. It is

[11] Recall that $\langle\varphi_i| \coloneqq |\varphi_i\rangle^\dagger$, where $A^\dagger$ denotes the adjoint of a matrix — or of a vector seen as a column matrix — which in the context of a Hilbert space is its conjugate transpose.

[12] A matrix $A \in \mathbb{C}^{n\times n}$ is *positive* if for any $v \in \mathbb{C}^n$, one has $v^\dagger A v \geq 0$. In particular, $v^\dagger A v \in \mathbb{R}$, and one can prove that this property implies that A is necessarily Hermitian (that is, $A^\dagger = A$).

known that CPTP maps are exactly the physically realisable functions mapping mixed states (represented by their density matrix) to mixed states ([105], Section 8.2).

Intuitively, positivity, together with trace preservation, means that f maps density matrices to density matrices, and therefore, physical states to physical states. Complete positivity means that it does so even in the presence of a context.

Example 2.6. *Given a unitary operation U acting on quantum states, the corresponding CPTP map acting on density matrices is $\rho \mapsto U\rho U^\dagger$.*

A CPTP map defined in this way is said to be pure.

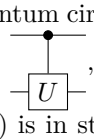
Example 2.7. *Consider a qubit in a pure (that is, not mixed) state $\alpha|0\rangle + \beta|1\rangle$. Its density matrix is $(\alpha|0\rangle+\beta|1\rangle)(\alpha^\dagger\langle 0|+\beta^\dagger\langle 1|) = |\alpha|^2|0\rangle\langle 0|+\alpha\beta^\dagger|0\rangle\langle 1|+\beta\alpha^\dagger|1\rangle\langle 0|+|\beta|^2|1\rangle\langle 1| = \begin{pmatrix}|\alpha|^2 & \alpha\beta^\dagger\\ \beta\alpha^\dagger & |\beta|^2\end{pmatrix}$. Performing a projective measurement of this qubit in the standard basis $\{|0\rangle, |1\rangle\}$ (also called the computational basis) leaves it in state $|0\rangle$ with probability $|\alpha|^2$, and in state $|1\rangle$ with probability $|\beta|^2$, hence its density matrix after the measurement is $|\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| = \begin{pmatrix}|\alpha|^2 & 0\\ 0 & |\beta|^2\end{pmatrix}$.*

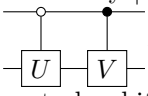
Now, consider a qubit in a mixed state, which is in one of several pure states $\alpha_i|0\rangle + \beta_i|1\rangle$, with respective probabilities p_i. Its density matrix is $\sum_i(\alpha_i|0\rangle+\beta_i|1\rangle)(\alpha_i^\dagger\langle 0|+\beta_i^\dagger\langle 1|) = \begin{pmatrix}\sum_i|\alpha_i|^2 & \sum_i\alpha_i\beta_i^\dagger\\ \sum_i\beta_i\alpha_i^\dagger & \sum_i|\beta_i|^2\end{pmatrix}$. If one performs the same projective measurement on this qubit, the probability that it is left in state $|0\rangle$ is $\sum_i p_i|\alpha_i|^2$, while the probability that it is left in state $|1\rangle$ is $\sum_i p_i|\beta_i|^2$. Hence, its density matrix after the measurement is $\begin{pmatrix}\sum_i|\alpha_i|^2 & 0\\ 0 & \sum_i|\beta_i|^2\end{pmatrix}$.

Thus, the CPTP map corresponding to the projective measurement of a qubit in the standard basis is

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix} \mapsto \begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}.$$

Quantum Channels. A *quantum channel* is something that takes a quantum state as an input, transforms it and outputs the result. It can be described as a CPTP map, which completely characterises its behaviour from an input/output point of view. For this reason, the phrase "quantum channel" is generally understood as a synonym of "CPTP map" in the literature about quantum information theory. However, in particular in Chapter 7, we will see situations where two physical devices described by the same CPTP map can in fact be distinguished: either by using *coherent control* (see below), that is, roughly speaking, by sending a state both in a channel and outside of it, in superposition; or by using the same physical channel twice in a row. This is why we will not abide by this shortcut in this thesis, and will rather see a quantum channel essentially as a physical device, although treated in an abstract way.

Coherent Control. *Coherent control*, also called more simply *quantum control*, consists in controlling the choice of an operation — usually unitary (or pure) — to be applied to a quantum system, by using the state of another quantum system. For instance, it is common in the framework of quantum circuits to introduce *controlled gates*. For instance, the controlled version of a gate  , denoted  , applies U to the second qubit (called the target qubit) if the first one (called the control qubit) is in state $|1\rangle$, and does nothing (or equivalently applies the identity) if it is in state $|0\rangle$. That is, the controlled gate is defined by linearity by $|0\rangle|\varphi\rangle \mapsto |0\rangle|\varphi\rangle$ and $|1\rangle|\varphi\rangle \mapsto |1\rangle \otimes U|\varphi\rangle$. It is also common to consider  ,

defined by $|0\rangle|\varphi\rangle \mapsto |0\rangle \otimes U|\varphi\rangle$ and $|1\rangle|\varphi\rangle \mapsto |1\rangle|\varphi\rangle$. By composing the two kinds of controlled gates 

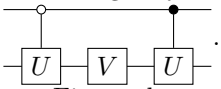
, one applies either U or V — or a "superposition" of both — depending on the state of the control qubit: $|0\rangle|\varphi\rangle \mapsto |0\rangle \otimes U|\varphi\rangle$ and $|1\rangle|\varphi\rangle \mapsto |1\rangle \otimes V|\varphi\rangle$, which is represented by a block-diagonal matrix: $\begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix}$. This is a coherent control of the unitary operations U and V by the control qubit.

Coherent control also works with more general control and target systems: a unitary operation is associated with each element of a particular basis of the state space of the control system, and is applied to the target system if the control system is in the corresponding state. The global operation is still defined by linearity, and can still be represented by a block-diagonal matrix made of all the unitaries.

A commonly considered example of coherent control is the *quantum switch* [34]: given a control qubit and two unitary operations U and V acting on a target system, the quantum switch of U and V is the global operation defined by linearity by $|0\rangle|\varphi\rangle \mapsto |0\rangle \otimes VU|\varphi\rangle$ and $|1\rangle|\varphi\rangle \mapsto |1\rangle \otimes UV|\varphi\rangle$. That is, one performs a coherent control of the order in which U and V are applied.

Note that in quantum circuits, the controlled gate 

has to be introduced as a new generator, one cannot obtain it from the non-controlled gate 

. In fact, it has been proven that there does not exist a quantum circuit in which it would suffice to plug one or more copies of an arbitrary gate to get its controlled version [11, 64]. Moreover, one cannot represent the quantum switch using only one copy of each gate or of its controlled version: one has to represent it for instance as 

.

Coherent control can be extended to control operations that are not unitary. First, what was just explained above works also for non-unitary square matrices (but in this case the resulting global operation is not unitary either). These, strictly speaking, do not represent physical evolutions but can be useful as a mathematical tool. Coherent control can also be extended to quantum channels, but this requires to adopt a more precise description than CPTP maps. We address this question in Chapter 7.

2.2 Quantum Circuits

Definition 2.8. *Given a set $\mathcal{G}$ of unitary matrices whose dimensions are powers of 2, the PROP of quantum circuits with gates in $\mathcal{G}$ is generated by the set of generators composed of, for each $U \in \mathcal{G} \cap \mathbb{C}^{2^n \times 2^n}$, a gate* 

: $n \to n$. That is, the quantum circuits are built from these generators together with the empty circuit 
, the identity — and the swap 
, combined using sequential and parallel compositions, and are considered up to deformation by the axioms given at Items 1 to 5 of Definition 1.1.

The parallel wires in a quantum circuit are meant to represent qubits. A unitary matrix $U \in \mathbb{C}^{2^n \times 2^n}$ therefore yields a gate acting on n qubits. Indeed, with the identification of the integers $0, ..., 2^n - 1$ with lists of bits, U can also be seen as a matrix in $\mathbb{C}^{\{0,1\}^n \times \{0,1\}^n}$. The semantics of a quantum circuit is the overall unitary tranformation that it applies to the state of its input qubits:

Definition 2.9 (Semantics)**.** *For any quantum circuit $C \colon n \to n$, let $[\![C]\!] : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ be the linear map inductively defined as follows:*

$$[\![C_2 \circ C_1]\!] = [\![C_2]\!] \circ [\![C_1]\!], \qquad [\![C_1 \otimes C_3]\!] = [\![C_1]\!] \otimes [\![C_3]\!],$$

and $\forall x, y \in \{0,1\}$,

$$[\![\,]\!] = 1 \mapsto 1, \qquad [\![—]\!] = |x\rangle \mapsto |x\rangle, \qquad [\![\times]\!] = |x, y\rangle \mapsto |y, x\rangle, \qquad \left[\!\!\left[\text{—}\boxed{U}\text{—} \right]\!\!\right] = U.$$

Note that we use here the notation $\otimes$ for the parallel composition, as mentioned in Remark 1.2, since this is more consistent with the semantics.

Note also that according to Definition 2.8, all quantum circuits have the same number of input and output qubits. However, it is common to extend this definition by adding qubit initialisations, represented

as states $|\varphi\rangle \in \mathbb{C}^2$, which can be seen as generators of type $0 \to 1$. It is also common to add a qubit measurement —[↗]—, which can be seen as a generator $1 \to 0$, note however that this requires to extend the formalism in which the semantics is expressed, either by using density matrices and CPTP maps, or more naively by directly considering probability distributions on states.

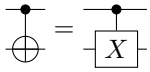
There are other extensions and variants of the formalism of quantum circuits. For instance, one may want to represent the classical outcome of a measurement in the circuit, possibly to reuse it somewhere else in the circuit: this is usually done using double wires —[↗]═. This makes the PROP of quantum circuits into a coloured PROP with two types of wires: simple wires for qubits and double wires for classical bits. Reusing the outcome of a measurement can be done by introducing gates with some double input wires. This means that the unitary map applied to the input qubits depends on some classical bits, thus such a gate with classical inputs can be interpreted as a parametrised gate.

As an example of variant of the formalism, it is sometimes more convenient to consider the swap as a proper gate rather than a structural generator subject to deformation. Then quantum circuits form a PRO instead of a PROP. In this context, the swap gate is usually depicted as  .

Another variant consists in replacing qubits with qutrits, that is, quantum states living in a space of dimension 3 instead of 2, or by more general quantum states, possibly by mixing several types of systems in a circuit.

Finally, another extension consists in considering more general matrices than just unitary ones.

Example 2.10. *A commonly used set of gates, called the* Clifford+T *gate set, is composed of* $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $\mathrm{CNot} = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix}$, $Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$ *and* $T = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix}$.

H is called the Hadamard gate, X is sometimes called the not gate, and CNot *is called the controlled-not gate and is usually depicted as*  . *Note that* CNot *is a controlled version of the not gate X:*  . *Note also that $Z = S^2$ and $S = T^2$.*

2.3 Extended Circuit Notations

We present here two particular extensions of the formalism of quantum circuits, that we will use in particular in Chapter 7.[13] The first one consists in enriching the original PROP of quantum circuits with quantum states and their adjoints, and with a trace (which makes circuits into a traced PROP). The second one consists in adding a discard map to the first extension so that circuits represent operations that are not pure (that is, roughly speaking, that involve measurements) and therefore act on density matrices.

States and Projectors. First, we allow for qubit states $|\varphi\rangle : 0 \to 1$ and their adjoints $\langle\varphi| : 1 \to 0$ as generators, with the obvious semantics. Note that we identify the state $|\varphi\rangle$ with the linear map $\mathbb{C} \to \mathbb{C}^2$ defined as $\lambda \mapsto \lambda|\varphi\rangle$; more generally, in this thesis, we will also do so with states in more general Hilbert spaces $|\varphi\rangle \in \mathcal{H}$, for instance the semantics of a circuit without input qubits will be considered as a state.

Trace. We also add a trace operator to circuits, that is, we consider the traced PROP generated by gates, states and their adjoints. The semantics of the trace is given by $[\![Tr(C)]\!] = \mathrm{Tr}_{\mathbb{C}^2}([\![C]\!])$, where $\mathrm{Tr}_{\mathbb{C}^2}$ is the partial trace over $\mathbb{C}^2$, defined in Example 1.3.

Note that in general, the partial trace does not preserve unitarity.

Remark 2.11. *Note that the matrix of* $[\![$  $]\!]$ *is* $\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$. *Thus, the traced PROP defined in*

[13] In Chapter 7, we will additionally allow for states in arbitrary Hilbert spaces instead of qubits.

Example 1.3 is isomorphic to a variant of the traced PROP of quantum circuits with partial trace, where the gates can be arbitrary matrices.

Discard Map. Following [47, 28], we further extend quantum circuits to represent linear maps $\mathbb{C}^{2^n \times 2^n} \to \mathbb{C}^{2^m \times 2^m}$ (typically, CPTP maps), using a discard map represented by the "ground" symbol $\dashv\!\shortmid$, which represents the fact that the corresponding qubits are traced out.

Tracing out a quantum system means throwing it away, which can be done for instance by measuring it and not looking at the outcome. Actually, it is equivalent from an observational point of view to just just stopping considering this system. In the framework of density matrices, given a quantum system in some mixed state, tracing out a sub-system corresponds to taking the partial trace of the global density matrix over the state space of the sub-system.

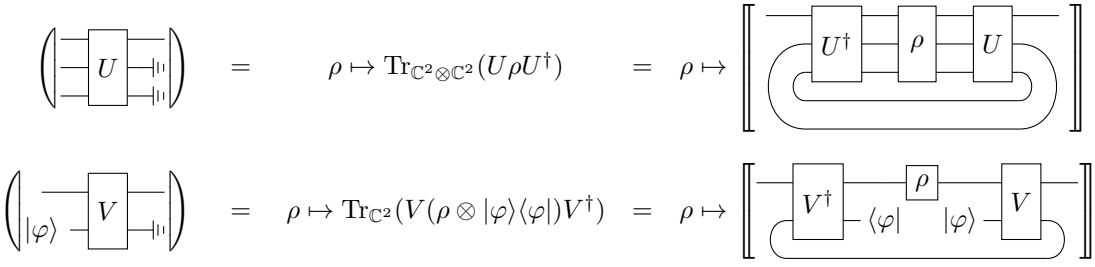
To properly define the semantics of circuits with $\dashv\!\shortmid$ symbols, we need to release the constraint that the partial trace must be taken over the last factor of a tensor product of spaces. For simplicity we do so in the case of density matrices of lists of qubits, but the definition can be extended to tensor products of more general Hilbert space (although this requires to complexify the notation):

Definition 2.12. *Given a list of bits $b_0...b_{n-1} \in \{0,1\}^n$, let $0 \leq i_1 < ... < i_k \leq n$ and $0 \leq \bar{i}_1 < ... < \bar{i}_\ell \leq n$ be the indices of the bits equal to 1 and to 0, respectively. Then the partial trace $\mathrm{Tr}_{b_0...b_{n-1}} : (\mathbb{C}^{2\times 2})^{\otimes n} \to (\mathbb{C}^{2\times 2})^{\otimes \ell}$ is the linear map defined by $\mathrm{Tr}_{b_0...b_{n-1}}\left(\bigotimes_{i=0}^{n-1} A_i\right) = \left(\prod_{j=1}^{k} \mathrm{Tr}(A_{i_j})\right) \bigotimes_{j=1}^{\ell} A_{\bar{i}_j}$.*

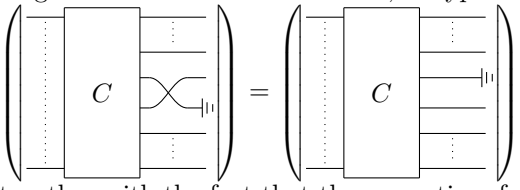
Given a "pure" (i.e. $\dashv\!\shortmid$ -free) circuit, plugging one (or several) $\dashv\!\shortmid$ in its output wire(s) corresponds essentially to tracing out the corresponding qubits — or more precisely, to defining the map that takes a matrix (typically, a density matrix, ρ), applies the pure CPTP map corresponding to the semantics of the circuit (that is, $\rho \mapsto [\![C]\!]\,\rho\,[\![C]\!]^\dagger$, where C is the circuit), and traces out the systems to which the ground symbol is attached. More formally:

Definition 2.13. *Given a "pure" (i.e. $\dashv\!\shortmid$ -free) circuit $C\colon m \to n$, the semantics of the circuit C' obtained by plugging $\dashv\!\shortmid$ in some of its output wires is $(\!|C'|\!) : \rho \mapsto \mathrm{Tr}_{b_0...b_{n-1}}\left([\![C]\!]\,\rho\,[\![C]\!]^\dagger\right)$, where $b_i = 1$ if the ith output wire of C (starting from 0) has a $\dashv\!\shortmid$, and $b_i = 0$ otherwise.*

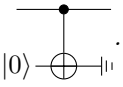
For example:



where the top example defines a map $\mathbb{C}^{8\times 8} \to \mathbb{C}^{2\times 2}$, and the bottom example defines a map $\mathbb{C}^{2\times 2} \to \mathbb{C}^{2\times 2}$. Note the representation of the output of the circuit, for a given input density matrix ρ, in the traced PROP of quantum circuits with partial trace.

Going further, one can consider $\dashv\!\shortmid$ as a generator of the traced PROP, of type $1 \to 0$, and place it anywhere in the circuit. Indeed, one has  for any circuit C (with at least two output qubits), which, together with the fact that the semantics of $\dashv\!\shortmid$ -free circuits is compatible with deformation, ensures that all ways of pulling the $\dashv\!\shortmid$ symbols to the right give the same semantics.[14]

[14] We admit here that given two circuits whose $\dashv\!\shortmid$ symbols are all on the right, deforming one into the other (when possible) can be done just by vertically permuting some $\dashv\!\shortmid$ symbols and output wires, and deforming the rest of the circuit.

Remark 2.14. *Note that projective measurements can be recovered from discard maps, for instance the measurement of a qubit can be implemented as* 

.

Part II

PBS-Diagrams and Extensions

Chapter 3

PBS-Diagrams and the PBS-Calculus

Most models of quantum computation (like quantum circuits) and most quantum programming languages are based on the *quantum data/classical control* paradigm. In other words, based on a set of quantum primitives (e.g. unitary transformations, quantum measurements), the way these primitives are applied on a register of qubits is either fixed or classically controlled.

However, quantum mechanics offers more general control of operations: for instance in quantum optics it is easy to control the trajectory of a system, like a photon, based on its polarisation using a *polarising beam splitter*. One can then position distinct quantum primitives on the distinct trajectories. Since the polarisation of a photon can be in superposition, it achieves some form of quantum control, called coherent control: the quantum primitives are applied in superposition depending on the state of another quantum system. Coherent control is not only a subject of interest for foundations of quantum mechanics [77, 108, 136], it also leads to advantages in solving computational problems [60, 10, 50, 115] and in designing more efficient protocols [61, 31, 4, 58, 72], for instance for deciding whether two unitary transformations are commuting or anti-commuting [31] (see Example 3.17). Several experimental implementations of coherent control, in particular of the quantum switch, have been realised [116, 68, 117], in particular to demonstrate some of its advantages over classical control [112, 67, 73, 129].

Coherent control is loosely represented in the usual formalisms of quantum computing. For instance, in the quantum circuit model, the only available quantum control is the controlled gate mechanism: a gate U is applied or not depending on the state of a control qubit. The quantum switch cannot be implemented with a single copy of U and a single copy of V in the quantum circuit model, and more generally using any language with a fixed or classically controlled order of operations.

Notice that other models of quantum computations (e.g. Quantum Turing Machines) or programming languages (e.g. Lineal [56] or QML [6]), allow for arbitrary coherent control of quantum evolutions, the price to pay is, however, the presence of non-trivial well-formedness conditions to ensure that the represented evolution is valid. Indeed, the superposition (i.e. linear combination) of two unitary evolutions is not necessarily a unitary evolution.

In this chapter, we introduce a graphical language, the PBS-calculus, for representing coherent control of quantum computations, where unitary maps (and more generally arbitrary matrices) can be coherently controlled. Our goal is to provide the foundations of a formal framework which will be further developed to explore the power and limits of the coherent control of quantum evolutions. Contrary to the quantum circuit model, the PBS-calculus allows a representation of the quantum switch with a single copy of each gate to be controlled. Moreover, any PBS-diagram is valid by construction (no side or well-formedness condition). The syntax of PBS-diagrams is inspired by quantum optics and is actually already used in several papers dealing with coherent control of quantum evolutions [4, 10]. Our contribution is to provide formal syntax and semantics (both operational and denotational) for these diagrams, and also to introduce an equational theory which allows one to transform diagrams. Our main technical contribution is the proof that the equational theory is complete (if two diagrams have the same semantics then one

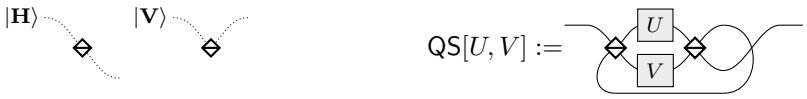


Figure 3.1: (a) Intuitive behaviour of a polarising beam splitter: horizontal polarisation goes through, vertical polarisation is reflected; (b) Quantum switch of two matrices U and V.

can be transformed into the other using the equational theory) and minimal (in the sense that each of the equations is necessary for the completeness of the language).

The syntax of the PBS-calculus is inspired by linear optics, and in particular by the peculiar behaviour of the polarising beam splitter. A polarising beam splitter transforms a superposition of polarisations into a superposition of positions: if the polarisation is horizontal the photon is transmitted whereas it is reflected when the polarisation is vertical (see Figure 3.1.a). As a consequence a photon can be routed in different parts of a scheme, this routing being quantumly controlled by the polarisation of the photon. This is a unique behaviour which has no counterpart in the quantum circuit model for instance. Polarising beam splitters can be used to perform a quantum switch, as depicted as a PBS-diagram in Figure 3.1.b.

Related Works. In the context of categorical quantum mechanics several graphical languages have already been introduced: ZX-calculus [45, 83], ZW-calculus [75], ZH-calculus [14] and their variants. Notice in particular a proposal for representing fermionic (non-polarising) beam splitters in the ZW-calculus [54]. An apparent difference between the PBS-calculus and these languages, is that the category of PBS-diagrams is *traced* but not *compact closed*. This difference is probably not fundamental, as for any traced monoidal category there is a completion of it to a compact closed category [89]. The fundamental difference is the parallel composition: in the PBS-calculus two parallel wires correspond to two possible positions of a single particle (i.e. a direct sum in terms of semantics), whereas, in the other languages it corresponds to two particles (i.e. a tensor product).

The parallel composition makes the PBS-calculus closer to the *graphical linear algebra* approach [22, 21, 20], however the generators and the fundamental structures (e.g. Frobenius algebra, Hopf algebra) are *a priori* unrelated to those of the PBS-calculus.

In the context of quantum programming languages, there are a few proposals for representing quantum control [56, 6, 132, 118]. Colnaghi *et al.* [50] have introduced a graphical language with *programmable connections*. The language uses the quantum switch as a generator, but does not aim to describe schemes with polarising beam splitters. Notice also that the inputs/outputs of the language are quantum channels.

Finally, several formal languages, more specifically designed to represent coherently controlled quantum computations, were introduced short after the PBS-calculus [128, 12, 130, 126, 29].

Structure of the Chapter. In Section 3.1, the syntax of PBS-diagrams is introduced. Thanks to a structure of traced PROP, PBS-diagrams are considered up to a structural congruence which allows one to deform the diagrams at will. Section 3.2 is dedicated to the semantics of the language: two semantics, a path semantics and a denotational semantics, are introduced. The denotational semantics is proved to be adequate with respect to the path semantics. In Section 3.3, the axiomatisation of the PBS-calculus is introduced, and our main result, the soundness and completeness of the language, is proved. In Section 3.4, the axiomatisation is proved to be minimal in the sense that none of the axioms can be derived from the others. Finally, in Section 3.5, we consider the application of the PBS-calculus to the problem of loop unrolling. We show in particular that any PBS-diagram involving unitary matrices can be transformed into a trace-free diagram.

3.1 Syntax

The set of PBS-diagrams is the traced PROP freely generated by the polarising beam splitter  , the polarisation flip (a.k.a. negation)  , and the gates  for all matrices $U \in \mathbb{C}^{q \times q}$, where q is a fixed positive integer. That is, PBS-diagrams are obtained by combining these three generators, together with

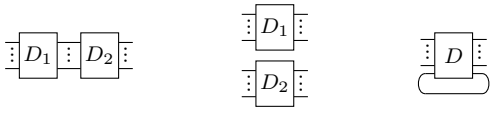
the identity — and the swap $\times$, by means of sequential composition $\circ$, parallel composition $\oplus$, and trace $Tr(\cdot)$, and are considered up to graphical deformation (see Chapter 1 for details). Thus, the syntax of the language is the following:

Definition 3.1. *Given $q \in \mathbb{N} \setminus \{0\}$, a PBS_q-diagram $D : n \to n$ is inductively defined as:*

$: 0 \to 0$ $\quad$ $— : 1 \to 1$ $\quad$ $\neg : 1 \to 1$ $\quad$ $\times : 2 \to 2$ $\quad$ $: 2 \to 2$

$$\frac{U \in \mathbb{C}^{q \times q}}{\boxed{U} : 1 \to 1} \qquad \frac{D_1 : n \to n \quad D_2 : n \to n}{D_2 \circ D_1 : n \to n} \qquad \frac{D_1 : n \to n \quad D_2 : m \to m}{D_1 \oplus D_2 : n+m \to n+m} \qquad \frac{D : n+1 \to n+1}{Tr(D) : n \to n}$$

Recall that the sequential composition $D_2 \circ D_1$, the parallel composition $D_1 \oplus D_2$, and the trace $Tr(D)$ are respectively depicted as follows:



and that the structural congruence given by the axioms of traced PROP guarantees that (i) two terms leading to the same graphical representation are equivalent, and (ii) a diagram can be deformed at will.

In the following, the positive integer q will be omitted when it is useless or clear from the context.

3.2 Semantics

In this section, we introduce the semantics of PBS-diagrams. First, we introduce an operational semantics for PBS-diagrams with a classical control. The operational semantics, called *path semantics* is based on the graphical intuition of a routed particle. Then we introduce a denotational semantics for the general case, with a quantum control. We show the adequacy between the two semantics, providing a graphical way to compute the denotational semantics of a PBS-diagram.

We only consider the case where a *single* particle, say a photon, is present in the diagram. The particle is made of a polarisation and an additional data register. The particle has: an initial polarisation, which is an arbitrary superposition of the vertical ($\mathbf{V}$) and horizontal ($\mathbf{H}$) polarisations (that we call *classical* polarisations in the following); an arbitrary position, which is a superposition of the possible input wires of the diagram; and an input data state, which is a vector $|\varphi\rangle \in \mathbb{C}^q$.

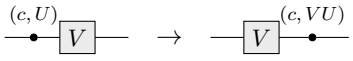
3.2.1 Classical Control – Path Semantics

Classical Control. We first consider input particles with a classical polarisation and a classical position. Roughly speaking, the particle is initially located on one of the input wires with a given polarisation in $\{\mathbf{V}, \mathbf{H}\}$, and moves through the diagram depending on its polarisation. The action of a PBS-diagram can be *informally* described as follows using a token made of the current polarisation c of the particle and a matrix U representing the matrix applied so far to the data register:

- The particle is either reflected or transmitted by a polarising beam splitter, depending on its polarisation:

- The polarisation may vary but remains classical (that is, in $\{\mathbf{V}, \mathbf{H}\}$) as the polarisation flip — the only generator which acts on the polarisation — interchanges horizontal and vertical polarisations:

- $—\boxed{V}—$ acts on the data register, transforming the state $|\varphi\rangle$ into $V|\varphi\rangle$:



- The particle can freely move through wires, e.g.:

Thus the token follows a path from the input to the output and accumulates a matrix along the path. We formalise this intuitive behaviour as a big-step operational semantics that we call *path semantics* in this context. A *configuration* is a triplet (D, c, p), where $D : n \to n$ is a PBS-diagram, $c \in \{\mathbf{V}, \mathbf{H}\}$ is the input polarisation of the particle, and $p \in [n] := \{0, \dots, n-1\}$ is its input position: 0 means that the particle is located on the first upper input wire, 1 on the second one and so on. The result is made of the final polarisation c' and position p', and of the matrix U representing the overall action of D on the data register.

Definition 3.2 (Path semantics)**.** *Given a PBS-diagram $D : n \to n$, a polarisation $c \in \{\mathbf{V}, \mathbf{H}\}$ and a position $p \in [n]$, let $(D, c, p) \overset{U}{\Rightarrow} (c', p')$ (or simply $(D, c, p) \Rightarrow (c', p')$ when U is the identity) be inductively defined as follows:*

$$(—, c, 0) \Rightarrow (c, 0) \qquad (\text{-}\neg\text{-}, \mathbf{H}, 0) \Rightarrow (\mathbf{V}, 0) \qquad (\text{-}\neg\text{-}, \mathbf{V}, 0) \Rightarrow (\mathbf{H}, 0) \qquad (\text{-}\boxed{U}\text{-}, c, 0) \overset{U}{\Rightarrow} (c, 0)$$

$$(\times, c, p) \Rightarrow (c, 1-p) \qquad \frac{(D_1, c, p) \overset{U}{\Rightarrow} (c', p') \qquad (D_2, c', p') \overset{V}{\Rightarrow} (c'', p'')}{(D_2 \circ D_1, c, p) \overset{VU}{\Longrightarrow} (c'', p'')} (\circ)$$

$$(\text{⊗}, \mathbf{V}, p) \Rightarrow (\mathbf{V}, p) \qquad \frac{D_1 : n \to n \qquad p < n \qquad (D_1, c, p) \overset{U}{\Rightarrow} (c', p')}{(D_1 \oplus D_2, c, p) \overset{U}{\Rightarrow} (c', p')} (\oplus 1)$$

$$(\text{⊗}, \mathbf{H}, p) \Rightarrow (\mathbf{H}, 1-p) \qquad \frac{D_1 : n \to n \qquad p \geq n \qquad (D_2, c, p-n) \overset{U}{\Rightarrow} (c', p')}{(D_1 \oplus D_2, c, p) \overset{U}{\Rightarrow} (c', p'+n)} (\oplus 2)$$

$$\frac{D : n+1 \to n+1 \qquad \forall i \in \{0, \dots, k\}, (D, c_i, p_i) \overset{U_i}{\Longrightarrow} (c_{i+1}, p_{i+1})}{(Tr(D), c_0, p_0) \overset{U_k \cdots U_0}{\Longrightarrow} (c_{k+1}, p_{k+1})} (\mathsf{T}_k)$$

with $p_0, p_{k+1} < n$, $\forall i \in \{1, ..., k\}, p_i = n$, and $k \in \{0, 1, 2\}$.

Intuitively, Rule (T_k) means that the photon repeatedly traverses D until it goes out by another wire than the traced wire. Thus its premise is a chain of arrows $(D, c_0, p_0) \overset{U_0}{\Longrightarrow} (c_1, n)$, $(D, c_1, n) \overset{U_1}{\Longrightarrow} (c_2, n), ..., (D, c_k, n) \overset{U_i}{\Longrightarrow} (c_{k+1}, p_{k+1})$ in which all intermediate states have position n.

Remark 3.3. *Here we treat the token only as an informal tool, the formalisation being done via the path semantics. Note however that it can be made more formal, as has been done for instance in the context of ZX-diagrams [30].*

Example 3.4. *As expected, the path semantics of the quantum switch* $\mathsf{QS}[U, V] := Tr\left(\times \circ \text{⊗} \circ (\text{-}\boxed{U}\text{-} \oplus \text{-}\boxed{V}\text{-}) \circ \text{⊗}\right)$ *(see Figure 3.1.b) is* $(\mathsf{QS}[U, V], \mathbf{H}, 0) \overset{UV}{\Longrightarrow} (\mathbf{H}, 0)$ *and* $(\mathsf{QS}[U, V], \mathbf{V}, 0) \overset{VU}{\Longrightarrow} (\mathbf{V}, 0)$.

Example 3.5. *PBS-diagrams implementing a controlled permutation are given in Figures 3.2 and 3.3.*

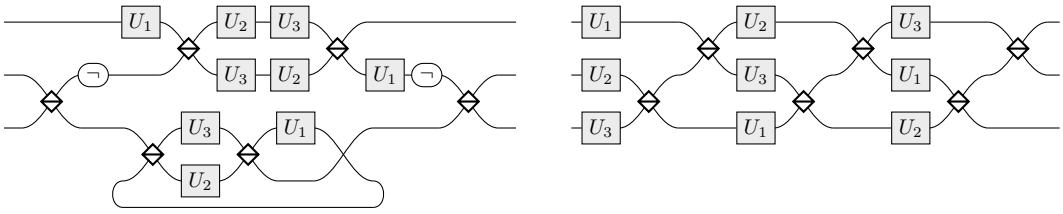


Figure 3.2: Two diagrams having the same semantics, that implement a controlled permutation of 3 unitary maps. Given a permutation (xyz) of (123), we have $(D, c, x) \xRightarrow{U_z U_y U_x} (c, x)$, where D is any of the two diagrams and $c = \mathbf{V}$ if the signature of (xyz) is 1, $c = \mathbf{H}$ otherwise. A generalisation to the controlled permutation of n unitary maps is given in Figure 3.3.

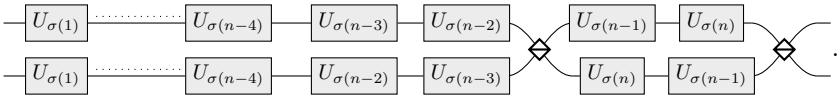


Figure 3.3: Given $n \geq 4$ and n transformations $U_1, ..., U_n \in \mathbb{C}^{q \times q}$, the parallel composition of all diagrams of this form, with σ a permutation such that $\sigma(n-3) < \sigma(n-2)$ and $\sigma(n-1) < \sigma(n)$, is a $\frac{n!}{2} \to \frac{n!}{2}$ diagram, with $\frac{n!}{2}$ occurrences of each gate, that implements a controlled permutation of the U_i.

Note that the path semantics does not need to be defined for the empty diagram $\boxed{\ }$, and more generally for diagrams $D : 0 \to 0$. Indeed, for such diagrams there is no valid configuration (D, c, p) as p should be one of the input wires of D.

The (T_k)-rule is parametrised by an integer k. Intuitively, this parameter is the number of times the photon goes through the corresponding trace. We show in the following that roughly speaking, a particle can never go through a given trace more than twice. In other words, the path semantics, which assumes $k \leq 2$, is well-defined for any valid configuration:

Proposition 3.6. *For any diagram $D : n \to n$ and any $(c, p) \in \{\mathbf{V}, \mathbf{H}\} \times [n]$, there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D, c, p) \overset{U}{\Rightarrow} (c', p')$.*

In the previous proposition, uniqueness means that the path semantics is deterministic: since diagrams are considered modulo structural congruence (i.e. up to deformation), it implies that these deformations preserve the path semantics.

Moreover, all PBS-diagrams are invertible in the following sense:

Proposition 3.7. *For any diagram $D : n \to n$ and any $(c, p) \in \{\mathbf{V}, \mathbf{H}\} \times [n]$, there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D, c', p') \overset{U}{\Rightarrow} (c, p)$.*

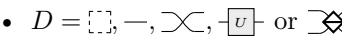
As a consequence, any diagram $D : n \to n$ essentially acts as a permutation on $\{\mathbf{V}, \mathbf{H}\} \times [n]$, if one ignores its action on the data register. We introduce dedicated notations for representing the corresponding permutation, as well as the actions on the data register:

Definition 3.8. *For any diagram $D : n \to n$, we call τ_D the permutation of $\{\mathbf{V}, \mathbf{H}\} \times [n]$, and for any $c, p \in \{\mathbf{V}, \mathbf{H}\} \times [n]$, we call $U^D_{c,p} \in \mathbb{C}^{q \times q}$ the matrix, such that $(D, c, p) \xRightarrow{U^D_{c,p}} \tau_D(c, p)$. We also denote respectively by $c^D_{c,p} \in \{\mathbf{V}, \mathbf{H}\}$ and $p^D_{c,p} \in [n]$ the polarisation and the position such that $\tau_D(c, p) = (c^D_{c,p}, p^D_{c,p})$.*

Proof of Propositions 3.6 and 3.7. The proof consists of two steps: First, we no longer assume the axioms of traced PROP (that is, we no longer consider the diagrams up to deformation), and prove that the two propositions hold in this context, where diagrams are just terms built inductively using the generators and the rules given in Definition 3.1. Then, we prove that any two diagrams equivalent modulo the

axioms of traced PROP have the same path semantics.

Not assuming the axioms of traced PROP implies that for any diagram D, we are in exactly one of the following cases:

- $D =$  or
- there exist unique D_1 and D_2 such that $D = D_2 \circ D_1$
- there exist unique D_1 and D_2 such that $D = D_1 \oplus D_2$
- there exists a unique D' such that $D = Tr(D')$.

We prove both propositions together by structural induction on D.

If $D =$ then $\{\mathbf{V}, \mathbf{H}\} \times [n]$ is empty so both propositions hold.

If D is a generator then we have $n = 1$ if $D =$  or , and $n = 2$ if $D =$ or , and in any case it is easy to see that both propositions hold.

If $D = D_2 \circ D_1$, then for any $(c, p) \in \{\mathbf{V}, \mathbf{H}\} \times [n]$, by induction hypothesis there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D_1, c, p) \overset{U}{\Rightarrow} (c', p')$, and again by induction hypothesis there exist unique $(c'', p'') \in \{\mathbf{V}, \mathbf{H}\} \times [n]$ and $V \in \mathbb{C}^{q \times q}$ such that $(D_2, c', p') \overset{V}{\Rightarrow} (c'', p'')$. Therefore, there is exactly one way of meeting the premises of the only rule that can reduce (D, c, p) and these premises completely determine the conclusion of the rule, so Proposition 3.6 holds for D.

Similarly, for any $(c, p) \in \{\mathbf{V}, \mathbf{H}\} \times [n]$, by induction hypothesis there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D_2, c', p') \overset{U}{\Rightarrow} (c, p)$, and again by induction hypothesis there exist unique $(c'', p'') \in \{\mathbf{V}, \mathbf{H}\} \times [n]$ and $V \in \mathbb{C}^{q \times q}$ such that $(D_1, c'', p'') \overset{V}{\Rightarrow} (c, p)$. Therefore, there is exactly one way to meet the premises of the only rule with which we can reduce D and get a reduction with right-hand side (c, p). These premises completely determine the conclusion of the rule, so Proposition 3.7 holds for D.

If $D = D_1 \oplus D_2$ with $D_1 : n_1 \to n_1$ and $D_2 : n - n_1 \to n - n_1$, let $(c, p) \in \{\mathbf{V}, \mathbf{H}\} \times [n]$.

If $p < n_1$, then by induction hypothesis there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n_1]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D_1, c, p) \overset{U}{\Rightarrow} (c', p')$, so that there is exactly one rule that allows us to reduce (D, c, p) (namely Rule $\oplus 1$), and exactly one way to meet its premises, so Proposition 3.6 holds for D. If $p \geq n_1$, then by induction hypothesis there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n - n_1]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D_2, c, p - n_1) \overset{U}{\Rightarrow} (c', p')$, so that there is exactly one rule that allows us to reduce (D, c, p) (namely Rule $\oplus 2$), and exactly one way to meet its premises, so Proposition 3.6 holds for D.

Similarly, if $p < n_1$, then by induction hypothesis there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n_1]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D_1, c', p') \overset{U}{\Rightarrow} (c, p)$, so that there is exactly one rule that allows us to reduce D and get (c, p) (namely Rule $\oplus 1$), and exactly one way to meet its premises, so Proposition 3.7 holds for D. If $p \geq n_1$, then by induction hypothesis there exist unique $(c', p') \in \{\mathbf{V}, \mathbf{H}\} \times [n - n_1]$ and $U \in \mathbb{C}^{q \times q}$ such that $(D_2, c, p - n_1) \overset{U}{\Rightarrow} (c', p')$, so that there is exactly one rule that allows us to reduce D and get (c, p) (namely Rule $\oplus 2$), and exactly one way to meet its premises, so Proposition 3.7 holds for D.

If $D = Tr(D')$ with $D' : n + 1 \to n + 1$, then for any $(c_0, p_0) \in \{\mathbf{V}, \mathbf{H}\} \times [n]$, by induction hypothesis of Proposition 3.6 there exist unique $(c_1, p_1) \in \{\mathbf{V}, \mathbf{H}\} \times [n + 1]$ and $U_0 \in \mathbb{C}^{q \times q}$ such that $(D', c_0, p_0) \overset{U_0}{\Longrightarrow} (c_1, p_1)$. If $p_1 < n$, then there is exactly one reduction from (D, c_0, p_0) which comes from applying Rule T_0, so Proposition 3.6 holds for D. If $p_1 = n$, then again by induction hypothesis of Proposition 3.6 there exist unique $(c_2, p_2) \in \{\mathbf{V}, \mathbf{H}\} \times [n + 1]$ and $U_1 \in \mathbb{C}^{q \times q}$ such that $(D', c_1, n) \overset{U_1}{\Longrightarrow} (c_2, p_2)$. If $p_2 < n$, then there is exactly one reduction from (D, c_0, p_0), which comes from applying Rule T_1, so Proposition 3.6 holds for D.

By uniqueness in the induction hypothesis of Proposition 3.7, since $(D', c_0, p_0) \overset{U_0}{\Longrightarrow} (c_1, n)$, $(D', c_1, n) \overset{U_1}{\Longrightarrow} (c_2, p_2, U_1)$ and $(c_0, p_0) \neq (c_1, n)$, we have $(c_1, n) \neq (c_2, p_2)$, so that if $p_2 = n$ then $c_2 = \bar{c}_1$. In this case, again by induction hypothesis of Proposition 3.6, there exist unique $(c_3, p_3) \in \{\mathbf{V}, \mathbf{H}\} \times [n+1]$ and $U_2 \in \mathbb{C}^{q \times q}$ such that $(D', \bar{c}_1, n) \overset{U_2}{\Longrightarrow} (c_3, p_3)$. Again by uniqueness in the induction hypothesis of Proposition 3.7, since $(D', c_0, p_0) \overset{U_0}{\Longrightarrow} (c_1, n)$ and $(c_0, p_0) \neq (\bar{c}_1, n)$, we have $(c_3, p_3) \neq (c_1, n)$, and since $(D', c_1, n) \overset{U_1}{\Longrightarrow} (\bar{c}_1, n)$ and $(c_1, n) \neq (\bar{c}_1, n)$, we have $(c_3, p_3) \neq (\bar{c}_1, n)$. Therefore, we cannot have $p_3 = n$, so $p_3 < n$ and there is exactly one reduction from (D, c_0, p_0), which comes from applying Rule T_2. So Proposition 3.6 holds for D.

Similarly, by induction hypothesis of Proposition 3.7 there exist unique $(c_1, p_1) \in \{\mathbf{V}, \mathbf{H}\} \times [n+1]$ and $U_0 \in \mathbb{C}^{q \times q}$ such that $(D', c_1, p_1) \overset{U_0}{\Longrightarrow} (c_0, p_0)$. If $p_1 < n$, then there is exactly one reduction from D with right-hand side (c_0, p_0), which comes from applying Rule T_0. So Proposition 3.7 holds for D. If $p_1 = n$, then again by induction hypothesis of Proposition 3.7 there exist unique $(c_2, p_2) \in \{\mathbf{V}, \mathbf{H}\} \times [n+1]$ and $U_1 \in \mathbb{C}^{q \times q}$ such that $(D', c_2, p_2) \overset{U_1}{\Longrightarrow} (c_1, n)$. If $p_2 < n$, then there is exactly one reduction from D with right-hand side (c_0, p_0), which comes from applying Rule T_1. So Proposition 3.7 holds for D.

By uniqueness in the induction hypothesis of Proposition 3.6, since $(D', c_1, n) \overset{U_0}{\Longrightarrow} (c_0, p_0)$, $(D', c_2, p_2) \overset{U_1}{\Longrightarrow} (c_1, n)$ and $(c_1, n) \neq (c_0, p_0)$, we have $(c_1, n) \neq (c_2, p_2)$, so that if $p_2 = n$ then $c_2 = \bar{c}_1$. In this case, again by induction hypothesis of Proposition 3.7, there exist unique $(c_3, p_3) \in \{\mathbf{V}, \mathbf{H}\} \times [n+1]$ and $U_2 \in \mathbb{C}^{q \times q}$ such that $(D', c_3, p_3) \overset{U_2}{\Longrightarrow} (\bar{c}_1, n)$. Again by uniqueness in the induction hypothesis of Proposition 3.6, since $(D', c_1, n) \overset{U_0}{\Longrightarrow} (c_0, p_0)$ and $(c_0, p_0) \neq (\bar{c}_1, n)$, we have $(c_3, p_3) \neq (c_1, n)$, and since $(D', \bar{c}_1, n) \overset{U_1}{\Longrightarrow} (c_1, n)$ and $(c_1, n) \neq (\bar{c}_1, n)$, we have $(c_3, p_3) \neq (\bar{c}_1, n)$. Therefore, we cannot have $p_3 = n$, so $p_3 < n$ and there is exactly one reduction from D with right-hand side (c_0, p_0), which comes from applying Rule T_2. So Proposition 3.7 holds for D.

To finish proving the result, we have to check that two diagrams equivalent modulo the axioms of traced PROP have the same path semantics. To do this, it suffices to check for each of the axioms given in Definition 1.1 that both sides have the same path semantics (that is, the same permutation τ_D and matrices $U^D_{c,p}$ — which we have just proved to be well-defined for diagrams not considered up to deformation). This is straightforward in each case except for dinaturality. In this case we first prove that Rule (T^m_k) below follows from those of Definition 3.2 (in the sense that it is admissible):

$$\frac{D : n+m \to n+m \qquad \forall i \in \{0, \dots, k\}, (D, c_i, p_i) \overset{U_i}{\Longrightarrow} (c_{i+1}, p_{i+1})}{(Tr^m(D), c_0, p_0) \overset{U_k \cdots U_0}{\Longrightarrow} (c_{k+1}, p_{k+1})} (\mathsf{T}^m_k)$$

for all $k, m \in \mathbb{N}$, with $p_0, p_{k+1} < n$ and $\forall i \in \{1, ..., k\}, p_i \geq n$.

To prove this, we proceed by induction on m. The case $m = 0$ is trivial, and the case $m = 1$ corresponds to Rule (T_k) of Definition 3.2 (the rule is admissible even for $k \geq 3$ since it is then not possible to satisfy its premises).

Now, assume that Rule (T^m_k) follows from those of Definition 3.2. Let $D : n+m+1 \to n+m+1$. Let $c_0 \in \{\mathbf{V}, \mathbf{H}\}$ and $p_0 \in [n]$. Let $(c_1, p_1), \dots, (c_{k+1}, p_{k+1})$ be the (unique) sequence of couples such that $\forall i \in \{0, \dots, k\}, (D, c_i, p_i) \overset{U_i}{\Longrightarrow} (c_{i+1}, p_{i+1})$ with $p_0, p_{k+1} < n$ and $\forall i \in \{1, ..., k\}, p_i \geq n$ (that is, $k+1$ is the first index after 0 such that $p_{k+1} < n$). Let $(c_{i_0}, p_{i_0}), \dots, (c_{i_{k'+1}}, p_{i_{k'+1}})$, with $0 = i_0 < i_1 < \cdots < i_{k'} < i_{k'+1} = k+1$, be the subsequence of $(c_1, p_1), \dots, (c_{k+1}, p_{k+1})$ where all couples with $p_i = n+m$ have been removed. For each $j \in \{0, \dots, k'\}$, by Rule (T_k) one has $(Tr(D), c_{i_j}, p_{i_j}) \overset{U_{i_{j+1}-1} \cdots U_{i_j}}{\Longrightarrow} (c_{i_{j+1}}, p_{i_{j+1}})$. Additionally, one has $Tr(D) : n+m \to n+m$, $p_{i_0}, p_{i_{k+1}} < n$ and $\forall j \in \{1, ..., k'\}, p_{i_j} \geq n$, so that by Rule (T^m_k), one has $(Tr^{m+1}(D), c_0, p_0) \overset{U_k \cdots U_0}{\Longrightarrow} (c_{k+1}, p_{k+1})$, which validates Rule (T^{m+1}_k).

Given Rule (T^m_k) for all k, m, we check the compatibility of the word path semantics with dinaturality

as follows: given any $D_1 : n+m$ and $D_2 : m$ with $n, m \geq 0$, on the one hand one has

$$\begin{cases} ((-^{\oplus n} \oplus D_2) \circ D_1, c, p) \xRightarrow{U_{c,p}^{D_1}} (c_{c,p}^{D_1}, p_{c,p}^{D_1}) & \text{if } p_{c,p}^{D_1} < n \\ ((-^{\oplus n} \oplus D_2) \circ D_1, c, p) \xRightarrow{U_{\left(c_{c,p}^{D_1}\right),\left(p_{c,p}^{D_1}-n\right)}^{D_2} \; U_{c,p}^{D_1}} (c^{D_2}_{\left(c_{c,p}^{D_1}\right),\left(p_{c,p}^{D_1}-n\right)}, p^{D_2}_{\left(c_{c,p}^{D_1}\right),\left(p_{c,p}^{D_1}-n\right)} + n) & \text{if } p_{c,p}^{D_1} \geq n \end{cases}$$

so that given $c_0 \in \{\mathbf{V}, \mathbf{H}\}$ and $p_0 \in [n]$, if one has a sequence $((-^{\oplus n} \oplus D_2) \circ D_1, c_0, p_0) \xRightarrow{U_0} (c_1, p_1), \ldots, ((-^{\oplus n} \oplus D_2) \circ D_1, c_k, p_k) \xRightarrow{U_k} (c_{k+1}, p_{k+1})$ with $p_0, p_{k+1} < n$ and $\forall i \in \{1, ..., k\}, p_i \geq n$, then one has a sequence $(D_1, c_0, p_0) \xRightarrow{U_0'} (c_1', p_1'), (D_2, c_1', p_1' - n) \xRightarrow{U_1''} (c_1, p_1 - n), (D_1, c_1, p_1) \xRightarrow{U_1'} (c_1', p_1'), \ldots, (D_1, c_{k-1}, p_{k-1}) \xRightarrow{U_{k-1}'} (c_k', p_k'), (D_2, c_k', p_k' - n) \xRightarrow{U_k''} (c_k, p_k - n), (D_1, c_k, p_k) \xRightarrow{U_k'} (c_{k+1}, p_{k+1})$ with $\forall i \in \{0, \ldots, k-1\}, U_{i+1}'' U_i' = U_i$, and $U_k' = U_k$, so that $(Tr^m((-^{\oplus n} \oplus D_2) \circ D_1), c_0, p_0) \xRightarrow{U_k' U_k'' U_{k-1}' \cdots U_1'' U_0'} (c_{k+1}, p_{k+1})$.

On the other hand, one has

$$\begin{cases} (D_1 \circ (-^{\oplus n} \oplus D_2), c, p) \xRightarrow{U_{c,p}^{D_1}} (c_{c,p}^{D_1}, p_{c,p}^{D_1}) & \text{if } p < n \\ (D_1 \circ (-^{\oplus n} \oplus D_2), c, p) \xRightarrow{U^{D_1}_{\left(c^{D_2}_{c,p-n}\right),\left(p^{D_2}_{c,p-n}+n\right)} \; U_{c,p-n}^{D_2}} (c^{D_1}_{\left(c^{D_2}_{c,p-n}\right),\left(p^{D_2}_{c,p-n}+n\right)}, p^{D_1}_{\left(c^{D_2}_{c,p-n}\right),\left(p^{D_2}_{c,p-n}+n\right)}) & \text{if } p \geq n \end{cases}$$

so that given $c_0 \in \{\mathbf{V}, \mathbf{H}\}$ and $p_0 \in [n]$, if one has a sequence $(D_1 \circ (-^{\oplus n} \oplus D_2), c_0, p_0) \xRightarrow{\tilde{U}_0} (c_1', p_1'), \ldots, (D_1 \circ (-^{\oplus n} \oplus D_2), c_k', p_k') \xRightarrow{\tilde{U}_k} (c_{k+1}', p_{k+1}')$ with $p_0, p_{k+1}' < n$ and $\forall i \in \{1, ..., k\}, p_i' \geq n$, then one has a sequence $(D_1, c_0, p_0) \xRightarrow{U_0'} (c_1', p_1'), (D_2, c_1', p_1' - n) \xRightarrow{U_1''} (c_1, p_1 - n), (D_1, c_1, p_1) \xRightarrow{U_1'} (c_1', p_1'), \ldots, (D_1, c_{k-1}, p_{k-1}) \xRightarrow{U_{k-1}'} (c_k', p_k'), (D_2, c_k', p_k' - n) \xRightarrow{U_k''} (c_k, p_k - n), (D_1, c_k, p_k) \xRightarrow{U_k'} (c_{k+1}, p_{k+1})$ with $U_0' = \tilde{U}_0$ and $\forall i \in \{0, \ldots, k-1\}, U_i' U_i'' = \tilde{U}_i$, so that one has $(c_{k+1}', p_{k+1}') = (c_{k+1}, p_{k+1})$ and $(Tr^m(D_1 \circ (-^{\oplus n} \oplus D_2)), c_0, p_0) \xRightarrow{U_k' U_k'' U_{k-1}' \cdots U_1'' U_0'} (c_{k+1}, p_{k+1})$. This proves that the two sides of the equality have the same semantics. □

In a PBS-diagram, the particle can go through each wire at most twice. Otherwise, roughly speaking, it would go back to the same position with the same polarisation and thus will come back again and again to this same configuration and thus enter an infinite loop — but by reversibility, this would mean that it had always been in this infinite loop, which contradicts the fact that it comes from an input wire.

Moreover, each wire is traversed at most twice among all possible input states (c, p) of the photon. Indeed, due to reversibility, it is always possible to know from which input state the photon comes from, which implies that there cannot be two input states leading the photon to pass through the same wire with the same polarisation.

In particular, each gate of the diagram is visited at most twice:

Proposition 3.9. *Any gate U of a diagram D contributes to at most two paths U_{c_0,p_0}^D and U_{c_1,p_1}^D, i.e. given D' the diagram D where one occurrence of U has been replaced by an arbitrary matrix V, $\forall (c,p) \notin \{(p_0, c_0), (p_1, c_1)\}$, $U_{c,p}^D = U_{c,p}^{D'}$.*

Proof. The proof is straightforward by induction on D. □

As a consequence the diagrams of Figure 3.2 are optimal in the number of uses of each U_i: since each of the 6 paths must depend on each U_i, at least three copies of each U_i are required in a diagram which solves the permutation problem of 3 unitaries. More generally, for any $n \geq 4$, the diagram of Figure 3.3 is optimal in the number of uses of each U_i for the same reason.

Remark 3.10. *One can see Proposition 3.9 as a formal statement of the fact that every* wire *is traversed at most twice. Indeed, in a given diagram, one can add a gate on any wire and check that it is visited at most twice.*

Additionally, notice that the formalism of bare diagrams *defined in Chapter 7 will allow us to express this property in a somehow more direct way (see Proposition 7.3).*

3.2.2 Quantum Control – Denotational Semantics

A crucial property of PBS-diagrams is to offer the ability to have a quantum control, i.e. a particle whose input state is a superposition of polarisations, positions, or both. To encounter the quantum control, we introduce in this section a denotational semantics which associates with any diagram a map acting on the state space $\mathcal{H}_n := \mathbb{C}^{\{\mathbf{V},\mathbf{H}\}} \otimes \mathbb{C}^n \otimes \mathbb{C}^q$. Using Dirac notations, $\{|\mathbf{V}\rangle, |\mathbf{H}\rangle\}$ (resp. $\{|x\rangle \mid x \in \{0 \dots k-1\}\}$) is an orthonormal basis of $\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}$ (resp. $\mathbb{C}^k$). Thus $\{|c,p,x\rangle \mid c \in \{\mathbf{V},\mathbf{H}\}, p \in [n], x \in [q]\}$ is an orthonormal basis of $\mathcal{H}_n$.

Definition 3.11. *The denotational semantics of a* PBS*-diagram $D : n \to n$ is the linear map $[\![D]\!] : \mathcal{H}_n \to \mathcal{H}_n$ inductively defined as follows:*

$$[\![\text{⊓}]\!] = 0 \qquad [\![—]\!] = |c,0,x\rangle \mapsto |c,0,x\rangle$$

$$[\![\text{⨯}]\!] = |c,p,x\rangle \mapsto |c,1-p,x\rangle \qquad [\![-\boxed{U}-]\!] = |c,0,x\rangle \mapsto |c,0\rangle \otimes U|x\rangle$$

$$[\![\text{⊖}]\!] = \begin{cases} |\mathbf{V},0,x\rangle \mapsto |\mathbf{H},0,x\rangle \\ |\mathbf{H},0,x\rangle \mapsto |\mathbf{V},0,x\rangle \end{cases} \qquad [\![\text{⋈}]\!] = \begin{cases} |\mathbf{V},p,x\rangle \mapsto |\mathbf{V},p,x\rangle \\ |\mathbf{H},p,x\rangle \mapsto |\mathbf{H},1-p,x\rangle \end{cases}$$

$$[\![D_2 \circ D_1]\!] = [\![D_2]\!] \circ [\![D_1]\!] \qquad [\![D_1 \oplus D_2]\!] = [\![D_1]\!] \boxplus [\![D_2]\!] \qquad [\![Tr(D)]\!] = \mathcal{T}([\![D]\!])$$

where:

- $f \boxplus g := \varphi \circ (f \oplus g) \circ \varphi^{-1}$ *with* $\varphi \colon \mathcal{H}_n \oplus \mathcal{H}_m \to \mathcal{H}_{n+m}$ *the isomorphism defined as* $(|c,p,x\rangle, |c',p',x'\rangle) \mapsto |c,p,x\rangle + |c',p'+n,x'\rangle$.
- $\mathcal{T}(f) := \sum_{k\in\mathbb{N}} \pi_1 \circ (f \circ \pi_0)^k \circ f \circ \iota$ *with* $\iota : \mathcal{H}_n \to \mathcal{H}_{n+1} :: |c,x,y\rangle \mapsto |c,x,y\rangle$, $\pi_0 : \mathcal{H}_{n+1} \to \mathcal{H}_{n+1} ::$ $|c,x,y\rangle \mapsto \begin{cases} 0 & \text{if } x < n \\ |c,n,y\rangle & \text{if } x = n \end{cases}$, *and* $\pi_1 : \mathcal{H}_{n+1} \to \mathcal{H}_n :: |c,x,y\rangle \mapsto \begin{cases} |c,x,y\rangle & \text{if } x < n \\ 0 & \text{if } x = n. \end{cases}$.

While the semantics of the trace is defined by means of an infinite sum, this sum is actually made of a finite number of non-zero elements, which guarantees that the denotational semantics is well-defined:

Proposition 3.12. *For any diagram $D : n \to n$, $[\![D]\!]$ is well-defined and $[\![D]\!] \in \mathcal{SLP}_n$, where $\mathcal{SLP}_n$ is the monoid of the linear maps $f \colon \mathcal{H}_n \to \mathcal{H}_n$ such that $f|c,p,x\rangle = |\tau(c,p)\rangle \otimes U_{c,p}|x\rangle$ for some permutation τ on $\{\mathbf{V},\mathbf{H}\} \times [n]$ and matrices $U_{c,p} \in \mathbb{C}^{q\times q}$.*

The denotational semantics is adequate with respect to the path semantics:

Theorem 3.13 (Adequacy)**.** *For any $D : n \to n$, $[\![D]\!] = |c,p,x\rangle \mapsto |\tau_D(c,p)\rangle \otimes U^D_{c,p}|x\rangle$,*
where τ_D and $U^D_{c,p}$ are such that $(D,c,p) \xRightarrow{U^D_{c,p}} \tau_D(c,p)$.

Proof of Proposition 3.12 and Theorem 3.13.

Auxiliary Lemmas. We first prove the following three lemmas:

Lemma 3.14. *Let $n \geq 0$ and $f \in \mathcal{SLP}_{n+1}$, and let τ be the permutation and $U_{c,p}$ the family of matrices, such that $f = |c,p,y\rangle \mapsto |\tau(c,p)\rangle \otimes U_{c,p}|y\rangle$. For any $(c,p,y) \in \{\mathbf{V},\mathbf{H}\} \times [n] \times [q]$, the series $\sum_{k\in\mathbb{N}} \pi_1 \circ (f \circ \pi_0)^k \circ f \circ \iota(|c,p,y\rangle)$ has at most one non-zero term (exactly one if f is injective), of index $k_1 - 1$, where k_1 is the smallest $k \geq 1$ such that $\tau^k(c,p) \in \{\mathbf{V},\mathbf{H}\} \times [n]$, or equivalently, the smallest $k \geq 1$ such that $f^k(|c,p,y\rangle) \in \mathcal{H}_n$. Moreover, we have $k_1 \leq 3$.*

Lemma 3.15. *For any $n \geq 0$ and $f \in \mathcal{SLP}_{n+1}$, $\mathcal{T}(f)$ is well-defined and $\mathcal{T}(f) \in \mathcal{SLP}_n$.*

Lemma 3.16. *Let $n \geq 0$ and $f \in \mathcal{SLP}_{n+1}$. Let τ be the permutation and $U_{c,p}$ the family of matrices, such that $f = |c,p,y\rangle \mapsto |\tau(c,p)\rangle \otimes U_{c,p}|y\rangle$. For any $(c,p,y) \in \{\mathbf{V},\mathbf{H}\} \times [n] \times [q]$, we have $\mathcal{T}(f)(|c,p,y\rangle) = \big|\tau^{k_1}(c,p)\big\rangle \otimes U_{\tau^{k_1-1}(c,p)} \cdots U_{c,p}|y\rangle$, where k_1 is the smallest $k \geq 1$ such that $\tau^k(c,p) \in \{\mathbf{V},\mathbf{H}\} \times [n]$.*

Proof of Lemmas 3.14 and 3.16. Let $(c,p,y) \in \{\mathbf{V},\mathbf{H}\}\times[n]\times[q]$ and let k_1 be the smallest $k \geq 1$ such that $\tau^k(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$. Since the sequence $(\tau^k(c,p))_{k\in\mathbb{N}}$ is periodic and $\tau^0(c,p) = (c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$, k_1 exists. Since τ is injective, if there were $1 \leq k' < k'' \leq k_1$ such that $\tau^{k'}(c,p) = \tau^{k''}(c,p)$, this would mean that $\tau^{k''-k'}(c,p) = (c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$, with $1 \leq k''-k' < k_1$, which contradicts the definition of k_1. Therefore, the couples $\tau(c,p), \tau^2(c,p), ..., \tau^{k_1-1}(c,p)$ are all different. By definition of k_1, these couples are all in the set $\{\mathbf{V},\mathbf{H}\}\times\{n\} = \{(\mathbf{V},n),(\mathbf{H},n)\}$, which has only two elements, so that $k_1 \leq 3$.

Let us prove by finite induction that for every $k \in \{0,...,k_1-1\}$, we have $(f\circ\pi_0)^k \circ f\circ\iota(|c,p,y\rangle) = f^{k+1}(|c,p,y\rangle)$. This is obviously true for $k=0$, and assuming that this is true for some $0 \leq k < k_1-1$, we have $(f\circ\pi_0)^{k+1}\circ f\circ\iota(|c,p,y\rangle) = f(\pi_0((f\circ\pi_0)^k\circ f\circ\iota(|c,p,y\rangle))) = f(\pi_0(f^{k+1}(|c,p,y\rangle)))$, and by definition of k_1, we have $f^{k+1}(|c,p,y\rangle) \in \{\mathbf{V},\mathbf{H}\}\times\{n\}$ so that $\pi_0(f^{k+1}(|c,p,y\rangle)) = f^{k+1}(|c,p,y\rangle)$, and consequently $(f\circ\pi_0)^{k+1}\circ f\circ\iota_j(|c,p,y\rangle) = f^{k+2}(|c,p,y\rangle)$. This finishes the induction.

Additionally, for any $k \in \mathbb{N}$, we have $f^k(|c,p,y\rangle) = \left|\tau^k(c,p)\right\rangle \otimes U_{\tau^{k-1}(c,p)}\cdots U_{c,p}\,|y\rangle$.

For any $k < k_1-1$, by definition of k_1, we have $\tau^{k+1}(c,p) \in \{\mathbf{V},\mathbf{H}\}\times\{n\}$ so that $\pi_1(f^{k+1}(|c,p,y\rangle)) = 0$, that is, the term of index k of the series is zero.

We have $\tau^{k_1}(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$, so that the term of index k_1-1 of the series is not zero unless $U_{\tau^{k_1-1}(c,p)}\cdots U_{c,p}\,|y\rangle = 0$, and this term is equal to $\pi_1(f^{k_1}(|c,p,y\rangle)) = \left|\tau^{k_1}(c,p)\right\rangle \otimes U_{\tau^{k_1-1}(c,p)}\cdots U_{c,p}\,|y\rangle$.

For any $k \geq k_1$, we have $(f\circ\pi_0)^k\circ f\circ\iota(|c,p,y\rangle) = (f\circ\pi_0)^{k-k_1}\circ f(\pi_0(f^{k_1}(|c,p,y\rangle)))$, and since $\tau^{k_1}(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$, we have $\pi_0(f^{k_1}(|c,p,y\rangle)) = 0$, so that the term of index k of the series is zero. □

Proof of Lemma 3.15. The well-definedness is a direct consequence of Lemma 3.16. Given $f \in \mathcal{SLP}_{n+1}$, by Lemma 3.16 there exist a family of matrices $V_{c,p}$ such that $\mathcal{T}(f) = |c,p,y\rangle \mapsto |\tau^*(c,p)\rangle \otimes V_{c,p}\,|y\rangle$, where $\tau^* : \{\mathbf{V},\mathbf{H}\}\times[n] \to \{\mathbf{V},\mathbf{H}\}\times[n] :: (c,p) \mapsto \tau^{k_1}(c,p)$ with k_1 the smallest $k \geq 1$ such that $\tau^k(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$. What we have to prove is that τ^* is a permutation, that is, that it is a bijection.

We claim that this is the case and that its inverse is $(\tau^{-1})^* : \{\mathbf{V},\mathbf{H}\}\times[n] \to \{\mathbf{V},\mathbf{H}\}\times[n] :: (c,p) \mapsto (\tau^{-1})^{k_2}(c,p)$ with k_2 the smallest $k \geq 1$ such that $(\tau^{-1})^k(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$.

Indeed, let $(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$ and k_1 be the smallest $k \geq 1$ such that $\tau^k(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$. Then for any $k \in \{1,...,k_1-1\}$, we have $(\tau^{-1})^k(\tau^*(c,p)) = (\tau^{-1})^k(\tau^{k_1}(c,p)) = \tau^{k_1-k}(c,p)$, which, by definition of k_1, is not in $\{\mathbf{V},\mathbf{H}\}\times[n]$ because $1 \leq k_1-k < k_1$. We also have $(\tau^{-1})^{k_1}(\tau^*(c,p)) = (\tau^{-1})^{k_1}(\tau^{k_1}(c,p)) = (c,p)$, which is in $\{\mathbf{V},\mathbf{H}\}\times[n]$. Therefore, the smallest $k \geq 1$ such that $(\tau^{-1})^k(\tau^*(c,p)) \in \{\mathbf{V},\mathbf{H}\}\times[n]$ is k_1, so that $(\tau^{-1})^*(\tau^*(c,p)) = (\tau^{-1})^{k_1}(\tau^{k_1}(c,p)) = (c,p)$. This proves that $(\tau^{-1})^*\circ\tau^* = id$. We can prove in the same way that $\tau^*\circ(\tau^{-1})^* = id$, which proves our claim. □

Proof of Theorem 3.13. We proceed by structural induction on D.

- If $D = $ —, then we have $\tau_D = id$, $U^D_{c,p} = I_q$ for every c,p, and $[\![D]\!] = |c,0,x\rangle \mapsto |c,0,x\rangle$, so the result holds.
- If $D = $  , then we have $\tau_D = \begin{array}{l}(\mathbf{V},p)\mapsto(\mathbf{H},p)\\(\mathbf{H},p)\mapsto(\mathbf{V},p)\end{array}$, $U^D_{c,p} = I_q$ for every c,p, and $[\![D]\!] = \begin{array}{l}|\mathbf{V},p,y\rangle\mapsto|\mathbf{H},p,y\rangle\\|\mathbf{H},p,y\rangle\mapsto|\mathbf{V},p,y\rangle\end{array}$, so the result holds.
- If $D = $  , then we have $\tau_D = (c,p)\mapsto(c,1-p)$, $U^D_{c,p} = I_q$ for every c,p, and $[\![D]\!] = |c,p,y\rangle \mapsto |c,1-p,y\rangle$, so the result holds.
- If $D = $  , then we have $\tau_D = \begin{array}{l}(\mathbf{V},p)\mapsto(\mathbf{V},p)\\(\mathbf{H},p)\mapsto(\mathbf{H},1-p)\end{array}$, $U^D_{c,p} = I_q$ for every c,p, and $[\![D]\!] = \begin{array}{l}|\mathbf{V},p,y\rangle\mapsto|\mathbf{V},p,y\rangle\\|\mathbf{H},p,y\rangle\mapsto|\mathbf{H},1-p,y\rangle\end{array}$, so the result holds.
- If $D = $  , then we have $\tau_D = id$, $U^D_{c,p} = U$ for every c,p, and $[\![D]\!] = |c,p,y\rangle \mapsto |c,p\rangle \otimes U\,|y\rangle$, so the result holds.
- If $D = D_2 \circ D_1$, then on the one hand, for any $(c,p) \in \{\mathbf{V},\mathbf{H}\}\times[n]$, we have $(D_1,c,p) \xrightarrow{U^{D_1}_{c,p}} \tau_{D_1}(c,p)$ and $(D_2,\tau_{D_1}(c,p)) \xrightarrow{U^{D_2}_{\tau_{D_1}(c,p)}} \tau_{D_2}(\tau_{D_1}(c,p))$, so by Rule $(\circ)$ we have

$(D,c,p) \xRightarrow{U^{D_2}_{\tau_{D_1}(c,p)}U^{D_1}_{c,p}} \tau_{D_2}(\tau_{D_1}(c,p))$, so that $\tau_D = \tau_{D_2} \circ \tau_{D_1}$ and $U^D_{c,p} = U^{D_2}_{\tau_{D_1}(c,p)}U^{D_1}_{c,p}$. On the other hand, by induction hypothesis, we have $[\![D_1]\!] = |c,p,y\rangle \mapsto |\tau_{D_1}(c,p)\rangle \otimes U^{D_1}_{c,p}|y\rangle$ and $[\![D_2]\!] = |c,p,y\rangle \mapsto |\tau_{D_2}(c,p)\rangle \otimes U^{D_2}_{c,p}|y\rangle$. Therefore, for any $(c,p,y) \in \{\mathbf{V},\mathbf{H}\} \times [n] \times [q]$ we have $[\![D]\!](|c,p,y\rangle) = [\![D_2]\!]([\![D_1]\!](|c,p,y\rangle)) = [\![D_2]\!](|\tau_{D_1}(c,p)\rangle \otimes U^{D_1}_{c,p}|y\rangle = |\tau_{D_2}(\tau_{D_1}(c,p))\rangle \otimes U^{D_2}_{\tau_{D_1}(c,p)}U^{D_1}_{c,p}|y\rangle$. So the result holds for D.

- If $D = D_1 \oplus D_2$ with $D_1 : n_1 \to n_1$, then on the one hand, we have $\tau_D = (c,p) \mapsto \begin{cases} \tau_{D_1}(c,p) & \text{if } p < n_1 \\ (c', p' + n_1) & \text{if } p \geq n_1, \text{ where } (c',p') = \tau_{D_2}(c, p-n_1) \end{cases}$ and for any $(c,p) \in \{\mathbf{V},\mathbf{H}\} \times [n]$ we have $U^D_{c,p} = \begin{cases} U^{D_1}_{c,p} & \text{if } p < n_1 \\ U^{D_2}_{c,p-n_1} & \text{if } p \geq n_1 \end{cases}$. On the other hand, by induction hypothesis, we have $[\![D_1]\!] = |c,p,y\rangle \mapsto |\tau_{D_1}(c,p)\rangle \otimes U_{c,p}|y\rangle$ and $[\![D_2]\!] = |c,p,y\rangle \mapsto |\tau_{D_2}(c,p)\rangle \otimes U^{D_2}_{c,p}|y\rangle$, so that $[\![D]\!] = [\![D_1]\!] \boxplus [\![D_2]\!] = |c,p,y\rangle \mapsto \begin{cases} |\tau_{D_1}(c,p)\rangle \otimes U^{D_1}_{c,p}|y\rangle & \text{if } p < n_1 \\ |c', p' + n_1\rangle \otimes U^{D_2}_{c,p-n_1}|y\rangle & \text{if } p \geq n_1 \end{cases}$ where $(c',p') = \tau_{D_2}(c, p-n_1)$. So the result holds for D.

- If $D = Tr(D')$, let $(c,p,y) \in \{\mathbf{V},\mathbf{H}\} \times [n] \times [q]$, and let k_1 be the smallest $k \geq 1$ such that $\tau^k_{D'}(c,p) \in \{\mathbf{V},\mathbf{H}\} \times [n]$. On the one hand, if we write $\tau^k_{D'}(c,p)$ as (c_k,p_k), then for all $i \in \{0,...,k_1-1\}$ we have $(D',c_i,p_i) \xRightarrow{U^{D'}_{c_i,p_i}} (c_{i+1},p_{i+1})$, and by definition of k_1, we have $\tau^{i+1}_{D'}(c,p) \notin \{\mathbf{V},\mathbf{H}\} \times [n]$, that is, $p_{i+1} = n$, if and only if $i < k_1$. Therefore, by Rule (T_{k_1}), we have $(Tr(D'),c,p) \xRightarrow{U^{D'}_{\tau^{k_1-1}_{D'}(c,p)} \cdots U^{D'}_{c,p}} (\tau_{D'}(c,p))$. On the other hand, by induction hypothesis we have $[\![D]\!]' = |c,p,y\rangle \mapsto |\tau_{D'}(c,p)\rangle \otimes U^{D'}_{c,p}|y\rangle$. By Lemma 3.16, this implies that $[\![D]\!](|c,p,y\rangle) = \mathcal{T}([\![D']\!])(|c,p,y\rangle) = \left|\tau^{k_1}_{D'}(c,p)\right\rangle \otimes U^{D'}_{\tau^{k_1-1}_{D'}(c,p)} \cdots U^{D'}_{c,p}|y\rangle$. So the result holds for D. □

Proof of Proposition 3.12. First, we do not assume the axioms of traced PROP and we prove by structural induction that for any diagram $D : n \to n$, $[\![D]\!]$ is well-defined and in $\mathcal{SLP}_n$.

If $D =$  , then this is a direct consequence of the definition of $[\![.]\!]$.

If $D = D_2 \circ D_1$, then by induction hypothesis, $[\![D_1]\!]$ and $[\![D_2]\!]$ are well-defined and in $\mathcal{SLP}_n$. By definition we have $[\![D]\!] = [\![D_2]\!] \circ [\![D_1]\!]$, and it is easy to see that $\mathcal{SLP}_n$ is closed under composition.

If $D = D_1 \oplus D_2$, with $D_1 : n_1 \to n_1$, then $D_2 : n - n_1 \to n - n_1$ and by induction hypothesis, $[\![D_1]\!]$ and $[\![D_2]\!]$ are well-defined and we have $[\![D_1]\!] \in \mathcal{SLP}_{n_1}$ and $[\![D_2]\!] \in \mathcal{SLP}_{n-n_1}$. It is easy to see that for any $f \in \mathcal{SLP}_m$ and $g \in \mathcal{SLP}_k$ we have $f \boxplus g \in \mathcal{SLP}_{m+k}$, so that $[\![D]\!] := [\![D_1]\!] \boxplus [\![D_2]\!] \in \mathcal{SLP}_n$.

If $D = Tr(D')$, then by induction hypothesis, $[\![D']\!]$ is well-defined and in $\mathcal{SLP}_{n+1}$. By Lemma 3.15 this implies that $[\![D]\!] := \mathcal{T}([\![D']\!])$ is well-defined and in $\mathcal{SLP}_n$.

The last thing to prove is (still not assuming the axioms of traced PROP) that two diagrams that are equivalent modulo the axioms of traced PROP have the same denotational semantics. For this it suffices to remark that the proof of Theorem 3.13 does not need to assume the axioms of traced PROP, so Theorem 3.13 still holds if we do not assume them. Then, since, as a consequence of Proposition 3.6, two diagrams equivalent modulo these axioms have the same path semantics, by Theorem 3.13 they have the same denotational semantics. □

The adequacy theorem implies that two diagrams have the same denotational semantics if and only if they have the same path semantics. As a consequence, it provides a graphical characterisation of the denotational semantics. Indeed, for any diagram $D : n \to n$, $[\![D]\!]$ is, by linearity, entirely defined by τ_D and $\{U^D_{c,p}\}_{c \in \{\mathbf{V},\mathbf{H}\}, p \in [n]}$. Since τ_D and $U^D_{c,p}$ have a nice graphical interpretation as paths from the inputs to the outputs, the adequacy theorem provides a graphical way to compute the denotational semantics of any PBS-diagram.

Example 3.17. *The quantum switch (Figure 3.1.b and Example 3.4) can be used to decide whether U and V are commuting or anti-commuting [31]. The semantics of the quantum switch is* $[\![\mathsf{QS}[U,V]]\!] = \begin{cases} |\mathbf{V},0,x\rangle \mapsto |\mathbf{V},0\rangle \otimes VU\,|x\rangle \\ |\mathbf{H},0,x\rangle \mapsto |\mathbf{H},0\rangle \otimes UV\,|x\rangle \end{cases}$. *We assume that $UV = (-1)^k VU$ and call the quantum switch with a control qubit in a uniform superposition:* $[\![\mathsf{QS}[U,V]]\!]\,\frac{|\mathbf{V}\rangle+|\mathbf{H}\rangle}{\sqrt{2}} \otimes |0,x\rangle = \frac{|\mathbf{V},0\rangle\otimes VU|x\rangle+|\mathbf{H},0\rangle\otimes UV|x\rangle}{\sqrt{2}} = \frac{|\mathbf{V},0\rangle\otimes VU|x\rangle+(-1)^k|\mathbf{H},0\rangle\otimes VU|x\rangle}{\sqrt{2}} = \frac{|\mathbf{V}\rangle+(-1)^k|\mathbf{H}\rangle}{\sqrt{2}} \otimes VU\,|0,x\rangle$. *Thus, by measuring the control qubit in the* $\{\frac{|\mathbf{V}\rangle+|\mathbf{H}\rangle}{\sqrt{2}}, \frac{|\mathbf{V}\rangle-|\mathbf{H}\rangle}{\sqrt{2}}\}$*-basis, one can decide whether U and V are commuting or anti-commuting.*

3.3 Equational Theory – PBS-Calculus

The representation of a quantum computation using PBS-diagrams is not unique, in the sense that two distinct PBS-diagrams may have the same semantics (e.g. the diagrams of Figure 3.2). In this section, we introduce 10 equations on PBS-diagrams (see Figure 3.4) as the axioms of a language that we call the PBS-calculus. We prove that the PBS-calculus is sound (that is, consistent with the semantics), complete (that is, it captures entirely the semantic equivalence) and minimal (that is, all axioms are necessary to have completeness). Completeness is proved by means of a normal form.

3.3.1 Axiomatisation

Definition 3.18. *A* congruence *is an equivalence relation $\mathcal{R}$ on the set of diagrams such that if $D_1\ \mathcal{R}\ D_1'$ and $D_2\ \mathcal{R}\ D_2'$ then $(D_2 \circ D_1)\ \mathcal{R}\ (D_2' \circ D_1')$ and $(D_1 \oplus D_2)\ \mathcal{R}\ (D_1' \oplus D_2')$, and if $D\ \mathcal{R}\ D'$ then $Tr(D)\ \mathcal{R}\ Tr(D')$.*

Definition 3.19 (PBS-calculus)**.** *Two* PBS*-diagrams D_1, D_2 are equivalent according to the rules of the* PBS*-calculus, denoted* $\text{PBS} \vdash D_1 = D_2$*, if one can transform D_1 into D_2 using the equations given in Figure 3.4. More precisely,* $\text{PBS} \vdash \cdot = \cdot$ *is defined as the smallest congruence which satisfies the equations of Figure 3.4 together with the axioms of Definition 1.1.*

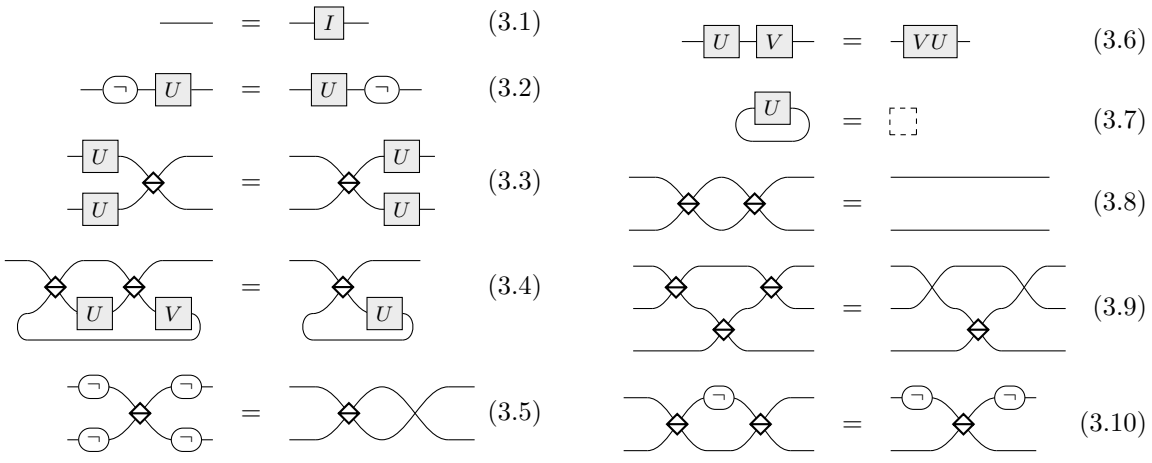


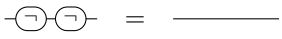
Figure 3.4: Axioms of the PBS-calculus. Given q a positive integer, $U, V \in \mathbb{C}^{q\times q}$ are arbitrary matrices, $I \in \mathbb{C}^{q\times q}$ is the identity.

Equations (3.1) and (3.6) in Figure 3.4 reflect the monoidal structure of the matrices, with the identity element (Equation (3.1)) and the associative binary operation (Equation (3.6)). Equations (3.2) and (3.3) mean that both the polarising beam splitter and the polarisation flip commute with a gate. Equation (3.8) tells us that the polarising beam splitter is self-inverse (note that the negation is also self-inverse

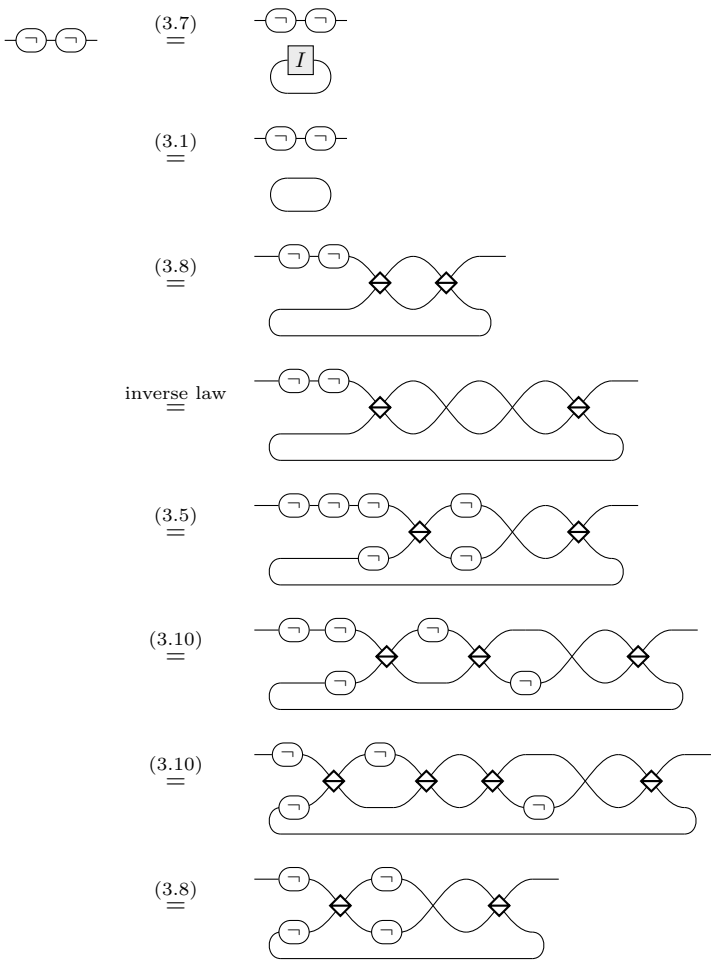
and that this is a consequence of the axioms, see Example 3.20). Equation (3.5) translates the fact that flipping the control state before and after performing a control of the position results in flipping the final position. To give a meaning to Equation (3.10), it is useful to flip it upside down, and to remark that in a two-wire diagram, polarising beam splitters and negations on the bottom wire each perform a CNot on the qubits representing the polarisation and the position, in opposite ways, so that each side of the equation combines 3 CNots and thus performs a swap between these two qubits. In Equation (3.4), there are essentially two steps: first, the wire with the gate V is a dead code, as no photon can go to the wire, so it can be discarded; the second step consists in merging the two polarising beam splitters. Equation (3.9) is the only equation acting on three wires: if the polarisation is vertical then the polarising beam splitters behave as identities, so the swaps on the right-hand side cancel out and the two sides are equivalent, and if the polarisation is vertical then the polarising beam splitters behave as swaps, so the two sides are equivalent too. Equation (3.7) reflects the fact that isolated parts of a diagram have no effect on the rest.

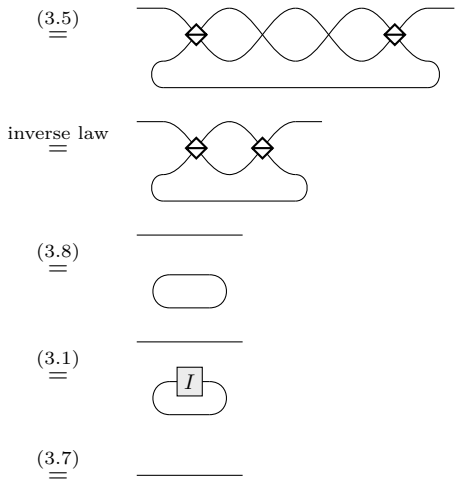
Example 3.20. *The fact that the negation is self-inverse can be derived in the PBS-calculus:* PBS $\vdash$  $=$  *(see Proposition 3.21 below). A more sophisticated example is the proof that the two diagrams of Figure 3.2 are equivalent, given in Appendix A.2.*

Proposition 3.21. *The following equation is a consequence of the axioms of the* PBS*-calculus:*

 (3.11)

Proof. To prove this equation, we have:





□

All these equations preserve the semantics of the PBS-diagrams:

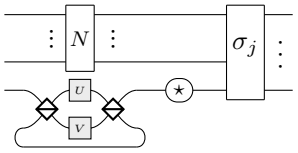
Proposition 3.22 (Soundness)**.** *For any two diagrams D_1 and D_2, if* PBS $\vdash D_1 = D_2$ *then* $[\![D_1]\!] = [\![D_2]\!]$.

Proof. Let $\sim$ be the relation such that $D_1 \sim D_2$ if and only if $[\![D_1]\!] = [\![D_2]\!]$, and $\approx$ be the relation such that $D_1 \approx D_2$ if and only if PBS $\vdash D_1 = D_2$. By definition, $\approx$ is the smallest congruence preserving Equations (3.1) to (3.10). It is clear that $\sim$ is a congruence, so it suffices to prove that it preserves Equations (3.1) to (3.10) too. This can be done easily by using the graphical way to compute the denotational semantics provided by Theorem 3.13. □

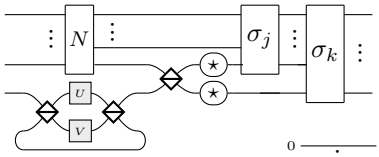
3.3.2 Normal Forms

In this section, we introduce a notion of diagrams in normal form which is used in the next sections both to characterise the expressiveness and to prove the completeness of the PBS-calculus. They are made of two parts: the first one corresponds to a superposition of linear maps, and the second one corresponds to a permutation of the polarisations and positions, written in a way that is convenient here.

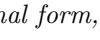
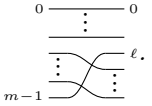
Definition 3.23 (Normal form)**.** *Diagrams in normal form are inductively defined as:* *is in normal form, and for any $N : n \to n$ in normal form,*



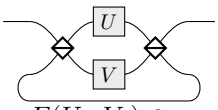
, and, if $n > 0$,

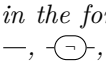


,

are in normal form, where  *denotes either* — *or* *, and* $\sigma_\ell : m \to m =$ 

.

Remark 3.24. *For any $U, V \in \mathbb{C}^{q \times q}$ let* $\mathrm{E}(U,V) :=$ 

. A diagram in normal form can be written in the form $P \circ E$, where E is of the form $E(U_0, V_0) \oplus \cdots \oplus E(U_{n-1}, V_{n-1})$, and P is built using only —,  , ,  , $\circ$ *and* $\oplus$.

In the following we show that any diagram is equivalent to a diagram in normal form.

Lemma 3.25. *If N_1 and N_2 are in normal form then $N_1 \oplus N_2$ is in normal form.*

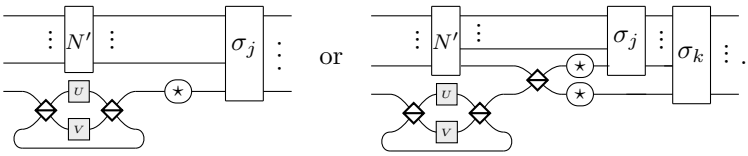
Proof. By definition of the normal forms. □

Lemma 3.26. *For any diagram $N : n \to n$ in normal form and any diagram g of the form $(—^{\oplus i}) \oplus h \oplus (—^{\oplus n-i-1})$ with $h =$ —, ⊸¬⊸ or $E(U,V)$, or $(—^{\oplus i}) \oplus h \oplus (—^{\oplus n-i-2})$ with $h =$ ⤫ or ⋈, there exists N' in normal form such that* $\mathrm{PBS} \vdash g \circ N = N'$.

Proof. We proceed by induction on n.

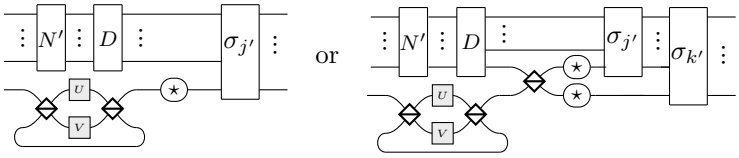
If $n = 0$, then there is no such g so the result trivially holds.

If $n \geq 1$, we write N in the form



We call these two forms type A and B respectively.

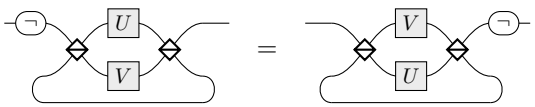
By induction hypothesis we only have to prove that $g \circ N$ can be put in the form



for some diagram $D : n-1 \to n-1$ built using ⬚, —, ⊸¬⊸, ⤫, ⋈, $E(U',V')$, $\circ$ and $\oplus$.

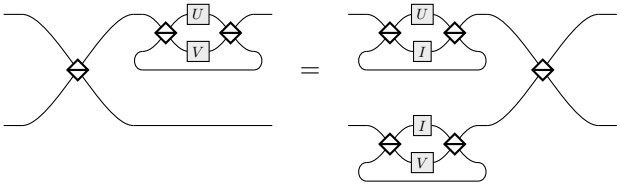
To prove this, we proceed by case distinction:

- If $h =$ —, then $g \circ N = N$, so there is nothing to do.
- If $h =$ ⊸¬⊸, then we slide it through σ_j (σ_k and σ_j if N is of type B),
  - if it does not arrive on the last wire if N is of type A, or one of the last two wires if N is of type B, then we get the desired form with $D = (—^{\oplus i'}) \oplus$ ⊸¬⊸ $\oplus (—^{\oplus n-i'-2})$
  - if it arrives on the last wire (resp. on one of the last two wires), then it merges with the ⊸⋆⊸ on its wire and changes its value: if ⊸⋆⊸ is — then h simply takes its place, and if ⊸⋆⊸ is ⊸¬⊸ then the two negations cancel out by Equation (3.11).
- If $h = E(U',V')$, then we slide it through σ_j (σ_k and σ_j if N is of type B),
  - if it does not arrive on the last wire if N is of type A, or one of the last two wires if N is of type B, then we get the desired form with $D = (—^{\oplus i'}) \oplus h \oplus (—^{\oplus n-i'-2})$
  - if it arrives on the last wire (resp. on one of the last two wires), then it commutes with the ⊸⋆⊸ on its wire, trivially if ⊸⋆⊸ is — , and by the following equation (that we will prove to be a consequence of the axioms of the PBS-calculus) if ⊸⋆⊸ is ⊸¬⊸ :[15]



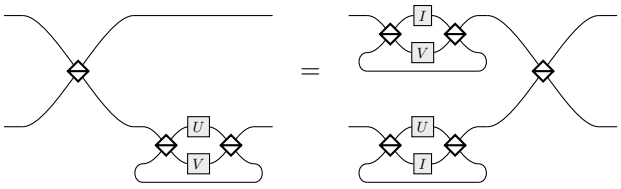
(3.12)

then, if N is of type B, it passes through the beam splitter by one of the following two equations:



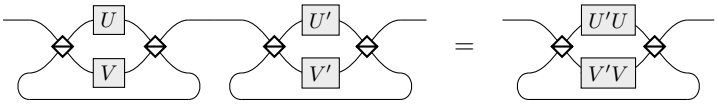
(3.13)

[15] In the equations, U, V, U' and V' stand for generic matrices, not necessarily related to the context.



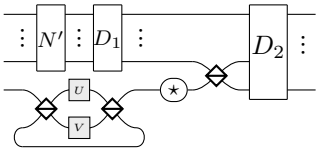
(3.14)

finally, the top part becomes part of D, and the bottom part merges with the $E(U,V)$ from N by the following equation:

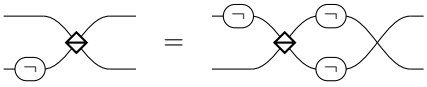


(3.15)

- If $h =$  , then by manipulating the wires according to the axioms of traced PROP, we can write $g \circ N$ in one of the desired forms, with D being a permutation of the wires (that is, a sequential composition of parallel compositions of and —).
- If $h =$ then we look at the indices i_1 and i_2 of the wires to which h is connected on the other side of σ_j (on the other side of $\sigma_k \circ (\sigma_j \oplus —)$ if N is of type B). The wire i_1 is connected to the top wire of h and the wire i_2 to the bottom wire of h.
  - If $i_1, i_2 < n-1$ in the case of type A ($i_1, i_2 < n-2$ in the case of type B), then $i_2 = i_1 + 1$ and we can slide the beam splitter across σ_j (σ_k and σ_j in the case of type B) to put N in the desired form with $D = (—^{\oplus i'}) \oplus h \oplus (—^{\oplus n-i'-3})$.
  - If N is of type A and $i_2 = n-1$, then by manipulating the wires we can write $g \circ N$ in the form



where D_1 and D_2 are permutations of the wires. Then, if is , we apply the following equation:



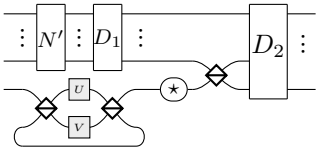
(3.16)

and the on the left is composed with D_1 to give us D. Finally, we get the desired form by manipulation of the wires.

  - If N is of type A and $i_1 = n-1$, then by manipulating the wires, and applying once the following equation :

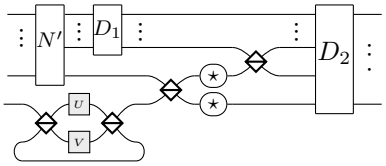
(3.17)

we can write $g \circ N$ in the form

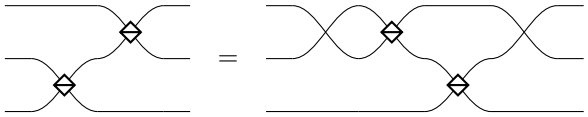


where D_1 and D_2 are permutations of the wires. Then we proceed as in the previous case.

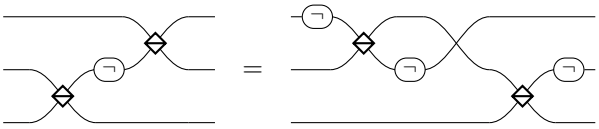
  - If N is of type B, $i_1 < n-2$ and $i_2 = n-2$, then by manipulating the wires we can write $g \circ N$ in the form



where D_1 and D_2 are permutations of the wires. Then, depending on the –⊛– between the two beam splitters, we use one of the following two equations:



(3.18)

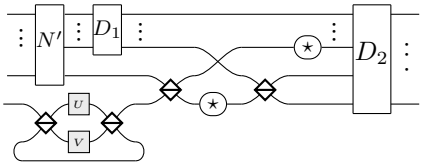


(3.19)

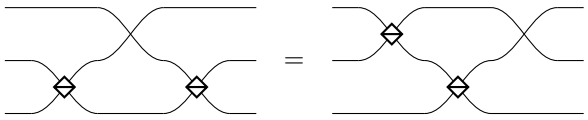
Immediately in the second case, or after a few manipulation of wires in the first case, we get the desired form.

– If N is of type B, $i_2 < n-2$ and $i_1 = n-2$, then by manipulating the wires and using once Equation (3.17), we can write $g \circ N$ in the same form as in the previous case. Then we proceed in the same way.

– If N is of type B, $i_1 < n-2$ and $i_2 = n-1$, then by manipulating the wires we can write $g \circ N$ in the form

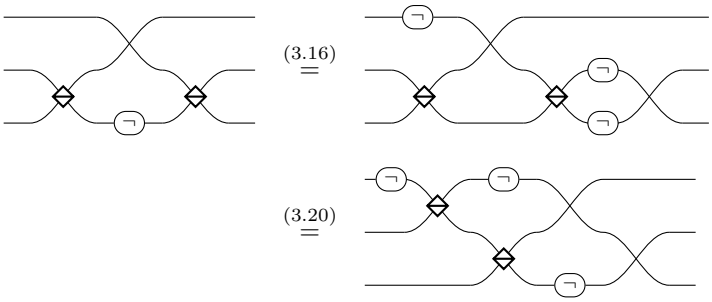


where D_1 and D_2 are permutations of the wires. Then if the –⊛– between the two beam splitters is — , then we apply the following equation:



(3.20)

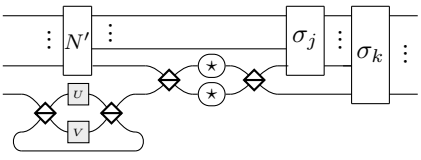
if the –⊛– between the two beam splitters is –¬– , then we proceed as follows:



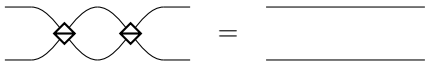
which gives us the desired form after some manipulation of wires.

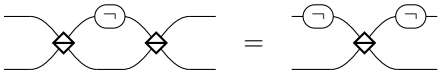
– If N is of type B, $i_2 < n-2$ and $i_1 = n-1$, then by manipulating the wires and applying Equation (3.17) we write $g \circ N$ in the same form as in the previous case, and we proceed in the same way.

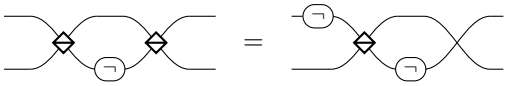
– If N is of type B, $i_1 = n-2$ and $i_2 = n-1$, then by manipulating the wires, we can write $g \circ N$ in the following form:

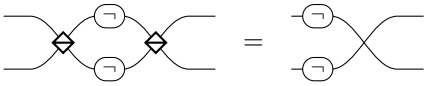


then we apply one of the following equations:


(3.8)


(3.10)


(3.21)


(3.22)

In the four cases, this gives us the desired form, after a few manipulation of wires if necessary.

– If N is of type B, $i_1 = n-1$ and $i_2 = n-2$, then by manipulating the wires and applying Equation (3.17) once, we can write $g \circ N$ in the same form as in the previous case and proceed in the same way. This finishes the case distinction.

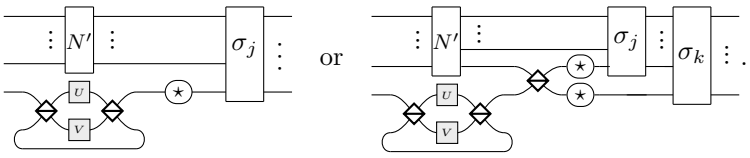
It remains to prove Equations (3.12) to (3.22). We give the derivations in Appendix A.1.1. □

Lemma 3.27. *If $N_1 : n \to n$ and $N_2 : n \to n$ are in normal form then there exists $N' : n \to n$ in normal form such that* PBS $\vdash N_2 \circ N_1 = N'$.

Proof. Notice that up to using the axioms of PROP, $N_2 = g_\ell \circ \ldots \circ g_0$ where each g_k consists of either $E(U,V)$, —,  ,  or  acting on any one or two consecutive positions, in parallel with the identity on the other positions. By Lemma 3.26, each g_k can be successively integrated to the normal form. □

Lemma 3.28. *If $N : n+1 \to n+1$ is in normal form then there exists $N' : n \to n$ in normal form such that* PBS $\vdash Tr(N) = N'$.

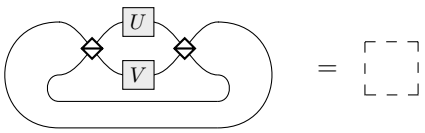
Proof. We write N in the form



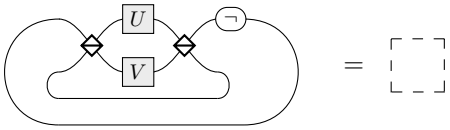
As in the proof of Lemma 3.26, we call these two forms type A and B respectively.

We proceed by case distinction:

- If N is of type A and $j = n-1$, then we apply one of the following two equations, that we will prove to be consequences of the axioms of the PBS-calculus:



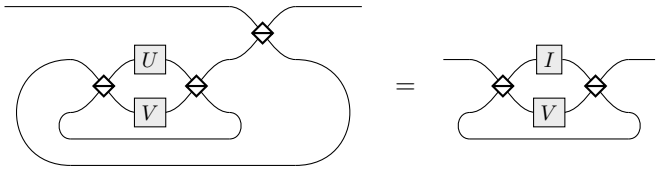
(3.23)



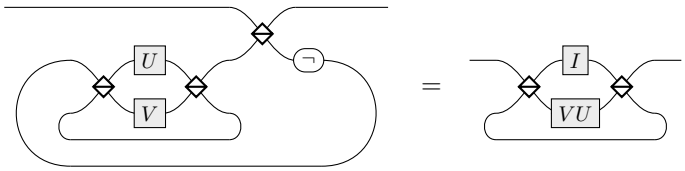
(3.24)

- If N is of type A and $j \neq n-1$, then we slide the $E(U,V)$ and the through the trace and σ_j, then integrate them to N' by Lemma 3.26. Finally, we remove the trace by yanking (see Chapter 1), which gives us a normal form after a few additional manipulation of wires.

- If N is of type B and $k = n - 1$, then we apply one of the following two equations:



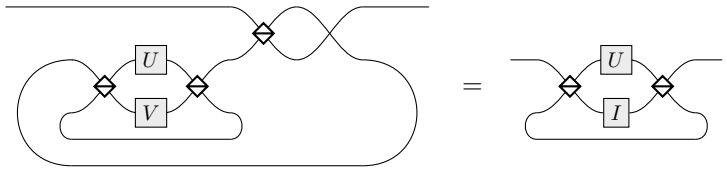
(3.25)



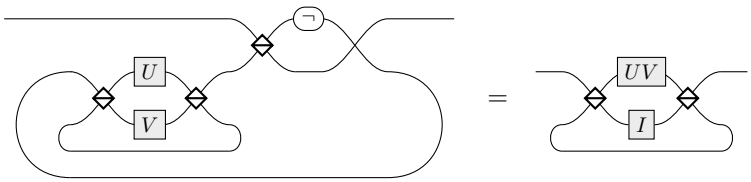
(3.26)

  then we conclude by Lemma 3.26 and manipulation of wires.

- If N is of type B, $k < n - 1$ and $j = n - 2$, then we apply one of the following two equations:



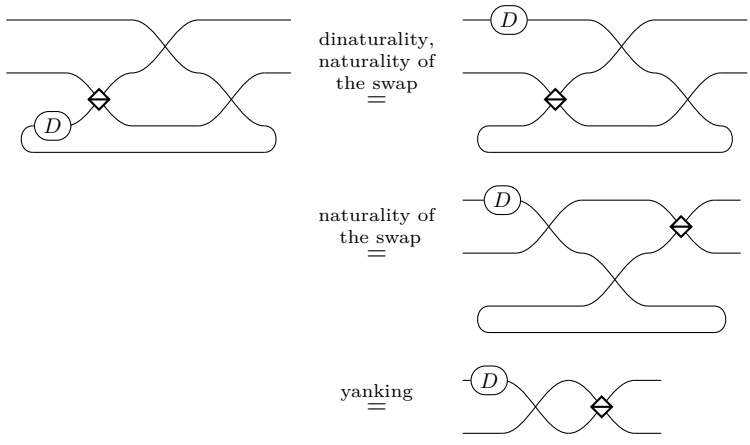
(3.27)



(3.28)

  then we conclude by Lemma 3.26 and manipulation of wires.

- If N is of type B, $k < n - 1$ and $j < n - 2$, let —(D)— represent $E(U, V)$. We proceed as follows:



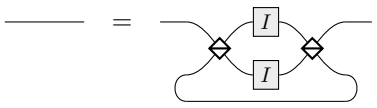
  then we conclude by applying Lemma 3.26 three times and manipulating the wires.

It remains to prove Equations (3.23) to (3.28). This is done in appendix, Section A.1.2. □

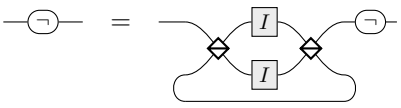
We are now ready to prove that any PBS-diagram can be put in normal form:

Proposition 3.29. *For any $D : n \to n$, there exists a* PBS*-diagram $N : n \to n$ in normal form such that* $\mathrm{PBS} \vdash D = N$.

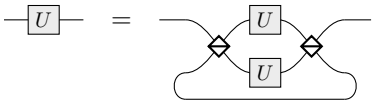
Proof. Combining Lemmas 3.25, 3.27 and 3.28, it remains to prove that any generator of the language can be put in normal form:



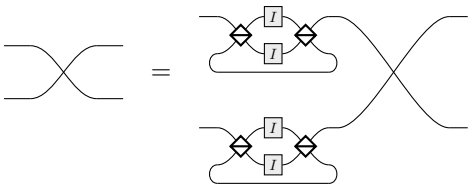
(3.29)



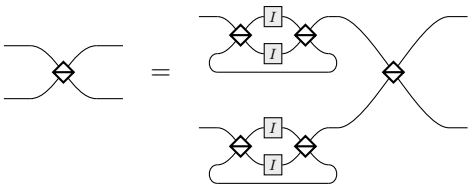
(3.30)



(3.31)

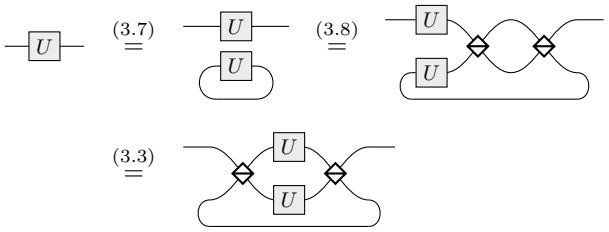


(3.32)

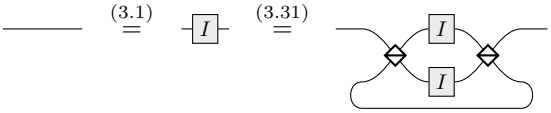


(3.33)

To prove Equation (3.31), we have:



To prove Equation (3.29), we have:



Equations (3.30), (3.32) and (3.33) are direct consequences of Equation (3.29). □

Remark 3.30. *By unfolding the proof of Proposition 3.29, one can obtain a deterministic procedure to transform any diagram into its normal form. Its complexity, defined as the number of transformations by one of Equations* (3.1) *to* (3.10)*, is* $\mathcal{O}(tm^2)$*, where* m *is the number of generators (**,* *, and* *), and* t *the number of traces in the diagram. Note that this procedure has probably not the best possible complexity.*

3.3.3 Completeness

The main application of the normal forms is the proof of completeness:

Theorem 3.31 (Completeness)**.** *For any* $D, D' : n \to n$*, if* $[\![D]\!] = [\![D']\!]$ *then* $\mathrm{PBS} \vdash D = D'$*.*

Proof. By Proposition 3.29, there exist N, N' in normal form such that $\mathrm{PBS} \vdash D = N$ and $\mathrm{PBS} \vdash D' = N'$. Moreover, by soundness (Proposition 3.22), $[\![N]\!] = [\![D]\!] = [\![D']\!] = [\![N']\!]$. Finally, one can show that $[\![N]\!] = [\![N']\!]$ implies that $N = N'$. Specifically, one can show inductively that the normal form is entirely determined by its semantics by considering the path semantics for a particle located on the last input wire. □

3.3.4 Expressiveness

A PBS-diagram represents a superposition of linear maps together with a permutation of polarisations and positions. Indeed, Proposition 3.12 shows that for any diagram $D : n \to n$, $[\![D]\!] \in \mathcal{SLP}_n$, where $\mathcal{SLP}_n$ is the monoid of the linear maps $f \colon \mathcal{H}_n \to \mathcal{H}_n$ such that $f\,|c,p,x\rangle = |\tau(c,p)\rangle \otimes U_{c,p}\,|x\rangle$ for some permutation τ on $\{\mathbf{V},\mathbf{H}\} \times [n]$ and matrices $U_{c,p} \in \mathbb{C}^{q\times q}$. We show in the following that conversely, any linear map in $\mathcal{SLP}_n$ can be represented by a PBS-diagram:

Theorem 3.32. *For any $f \in \mathcal{SLP}_n$, $\exists D : n \to n$, $[\![D]\!] = f$.*

Proof. The proof relies on the normal forms: given a linear map $f \in \mathcal{SLP}_n$ one can inductively construct a diagram in normal form, by considering the image of f when the particle is located on the last position ($p = n-1$). □

Note that $\mathcal{SLP}_n$ is strictly included in the set of linear maps from $\mathcal{H}_n$ to $\mathcal{H}_n$. As a consequence, while being universal for $\mathcal{SLP}_n$, PBS-diagrams are not expressive enough to represent a (non-polarising) beam splitter for instance.

3.4 Minimality of the Set of Axioms

In the following we show that each of the ten equations of Figure 3.4 is necessary for the completeness of the PBS-calculus:

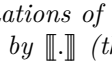
Theorem 3.33 (Minimality)**.** *None of Equations* (3.1) *to* (3.10) *is a consequence of the others.*

Note that all equations involving matrices, except Equation (3.1), are schemes of equations i.e. one equation for each possible matrix (or matrices). In Theorem 3.33, we show that each of the ten axioms, for most of the matrices, cannot be derived from the nine others. More precisely, Equation (3.4) (resp. (3.7)) is not a consequence of the nine others for any U (resp. any U, V); Equation (3.2) (resp. (3.6)) is not a consequence of the others for any $U \neq I$ (resp. any $U, V \neq I$). Finally, if $\det(U) \notin \{0,1\}$, then Equation (3.3) is not a consequence of the others. We conjecture that the condition $\det(U) \notin \{0,1\}$ can be relaxed to $U \neq I$.

We prove this result by examining each equation and proving that it is not a consequence of the others. Equations (3.1) to (3.8) and (3.10) are treated in Section 3.4.1. Equation (3.9) is treated in Section 3.4.2.

3.4.1 Independence of Equations (3.1) to (3.8) and (3.10)

We prove for each equation that it is not a consequence of the others in a dedicated lemma. For Equations (3.1), (3.2), (3.5) and (3.6), the proof follows a common pattern: we introduce an alternative denotational semantics $[\![.]\!]$, whose definition follows that of $[\![.]\!]$ but differs for some of the generators. Then we check that it preserves every equation except the one that we want to prove to be independent from the others. In each case, Lemma 3.34 below gives us that the consequences of the preserved equations are preserved too, which implies that the unpreserved equation is not a consequence of the others.

Lemma 3.34. *Let $[\![.]\!]$ be a function mapping any diagram $D : n \to n$ to a linear map $[\![D]\!] \in \mathcal{SLP}_n$, defined inductively in the same way as $[\![.]\!]$ except maybe in the case of*  *,*  *and* *. Let A be a set of equations of the form $D_1 = D_2$ where D_1, D_2 are* PBS*-diagrams, such that every equation of A is preserved by $[\![.]\!]$ (that is, for every equation $D_1 = D_2$ in A we have $[\![D_1]\!] = [\![D_2]\!]$). Then A is sound with respect to $[\![.]\!]$, that is, for any two diagrams $D_1, D_2 : n \to n$, if $A \vdash D_1 = D_2$ then $[\![D_1]\!] = [\![D_2]\!]$.*

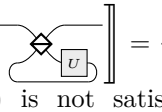
Proof. The same proof as for $[\![.]\!]$ shows that $[\![.]\!]$ is well-defined.

By definition, $A \vdash . = .$ is the smallest congruence satisfying the equations of A. Since $[\![D_2 \circ D_1]\!]$ and $[\![D_1 \oplus D_2]\!]$ only depend on $[\![D_1]\!]$ and $[\![D_2]\!]$, and $[\![Tr(D)]\!]$ only depends on $[\![D]\!]$, the relation $\sim$, defined as $D_1 \sim D_2$ if and only if $[\![D_1]\!] = [\![D_2]\!]$, is a congruence. Therefore, it contains $A \vdash . = .$, which is what we wanted to prove. □

Lemma 3.35. *Equation* (3.1) *is not a consequence of Equations* (3.2) *to* (3.10)*.*

Proof. Let $[\![.]\!]$ be defined inductively in the same way as $[\![.]\!]$, except in the case of  , for which we define $[\![$  $]\!] : \mathcal{H}_1 \to \mathcal{H}_1 :: |c, 0, y\rangle \mapsto 0$.
Equations (3.2), (3.3) and (3.6) are preserved by $[\![.]\!]$ because both sides are interpreted as the zero map. Equation (3.7) is preserved because both side are interpreted as the unique map $\mathcal{H}_0 \to \mathcal{H}_0$. Equation (3.4) is preserved because both sides are interpreted as $\begin{cases} |\mathbf{V}, 0, y\rangle \mapsto |\mathbf{V}, 0, y\rangle \\ |\mathbf{H}, 0, y\rangle \mapsto 0 \end{cases}$. Finally, Equations (3.5) and (3.8) to (3.10) are preserved because both sides are interpreted in the same way as by $[\![.]\!]$. As a consequence, by Lemma 3.34, all consequences of equations (3.2) to (3.10) are preserved by $[\![.]\!]$. By contrast, Equation (3.1) is not preserved by $[\![.]\!]$ because one side is interpreted as the identity whereas the other side is interpreted as the zero map. Hence, Equation (3.1) is not a consequence of Equations (3.2) to (3.10). □

Lemma 3.36. *If $U \neq I$, then Equation* (3.2) *is not a consequence of Equations* (3.1) *and* (3.3) *to* (3.10).

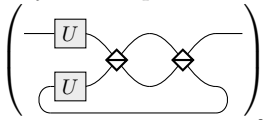
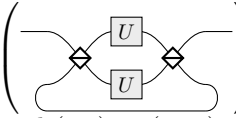
Proof. Let $[\![.]\!]$ be defined inductively in the same way as $[\![.]\!]$, except in the case of , for which we define $[\![$$]\!] :=$  $= \begin{cases} |\mathbf{V}, 0, y\rangle \mapsto |\mathbf{V}, 0, y\rangle \\ |\mathbf{H}, 0, y\rangle \mapsto |\mathbf{H}, 0\rangle \otimes U\,|y\rangle \end{cases}$.

Equation (3.2) is not satisfied unless $U = I$, because the left-hand side is interpreted as $\begin{cases} |\mathbf{V}, 0, y\rangle \mapsto |\mathbf{H}, 0\rangle \otimes U\,|y\rangle \\ |\mathbf{H}, 0, y\rangle \mapsto |\mathbf{V}, 0, y\rangle \end{cases}$ whereas the right-hand side is interpreted as $\begin{cases} |\mathbf{V}, 0, y\rangle \mapsto |\mathbf{H}, 0, y\rangle \\ |\mathbf{H}, 0, y\rangle \mapsto |\mathbf{V}, 0\rangle \otimes U\,|y\rangle \end{cases}$.
By using the graphical characterisation of the denotational semantics, adapted to $[\![.]\!]$, it is easy to check that Equations (3.1) and (3.3) to (3.10) are preserved by $[\![.]\!]$. By Lemma 3.34, this implies that all consequences of these equations are preserved by $[\![.]\!]$, so that Equation (3.2) is not a consequence of them. □

Lemma 3.37. *If* $\det(U) \notin \{0, 1\}$*, then Equation* (3.3) *is not a consequence of Equations* (3.1)*,* (3.2) *and* (3.4) *to* (3.10).

Proof. Given a diagram $D : n \to n$, let us say that a wire in D is *used* if there exists $c \in \{\mathbf{V}, \mathbf{H}\}$ and $p \in [n]$ such that an input photon with classical polarisation c and position p passes through this wire. Let us define $d(D)$ as the product of all determinants of the matrices labelling the gates that are on used wires of D.

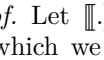
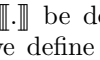
Let us fix a diagram D and consider the effect of applying the axioms inside it. It is easy to check that all axioms of traced PROP, as well as Equations (3.1), (3.2), (3.5) and (3.8) to (3.10) preserve the gates of D and the fact that their wire is used or not. Equation (3.7) can only add or remove gates on unused wires. Equation (3.4) adds or removes on an unused wire and does change the fact that the wire of is used or not, indeed, in the patterns on both sides of the equation, the wire of is used if and only if it is possible to have a photon with polarisation $\mathbf{H}$ arrive at the input of the pattern. Applying Equation (3.6) replaces and by (or by and) on a given wire, which does not change $d(D)$. Thus, applying Equations (3.1), (3.2) and (3.4) to (3.10) does not change $d(D)$.

By contrast, although the two sides of Equation (3.3) have the same d-quantity, whenever $\det(U) \notin \{0, 1\}$ this property is not preserved when one transforms an arbitrary diagram using this equation. For instance, $d\left(\right.$  $\left.\right) = \det(U)$ whereas $d\left(\right.$  $\left.\right) = \det(U)^2$. Hence, Equation (3.3) is not a consequence of Equations (3.1), (3.2) and (3.4) to (3.10). □

Lemma 3.38. *For any U, V, Equation* (3.4) *is not a consequence of Equations* (3.1) *to* (3.3) *and* (3.5) *to* (3.10).

Proof. This is clear, because Equations (3.1) to (3.3) and (3.5) to (3.10), as well as the axioms of traced PROP, preserve the parity of the total number of and in a given diagram, whereas Equation (3.4) changes this parity. □

Lemma 3.39. *Equation* (3.5) *is not a consequence of Equations* (3.1) *to* (3.4) *and* (3.6) *to* (3.10).

Proof. Let $[\![.]\!]$ be defined inductively in the same way as $[\![.]\!]$, except in the cases of  and  , for which we define $[\![$  $]\!]$ and $[\![$  $]\!]$ as being the identity (notice that the proof also works if we additionally define $[\![$  $]\!]$ as the identity). Then it is clear that Equations (3.1) to (3.4) and (3.6) to (3.10) are preserved, and Equation (3.5) is not preserved because its left-hand side is interpreted as the identity whereas its right-hand side is interpreted as $[\![$  $]\!]$. By Lemma 3.34, this implies that Equation (3.5) is not a consequence of Equations (3.1) to (3.4) and (3.6) to (3.10). □

Lemma 3.40. *If $U, V \neq I$, then Equation* (3.6) *is not a consequence of Equations* (3.1) *to* (3.5) *and* (3.7) *to* (3.10).

Proof. Let $[\![.]\!]$ be defined inductively in the same way as $[\![.]\!]$, except in the case of  , for which we define $[\![$$]\!] := \begin{cases} |c,p,x\rangle \mapsto |c,p,x\rangle & \text{if } U = I \\ |c,p,x\rangle \mapsto |c,p\rangle \otimes M\,|x\rangle & \text{if } U \neq I \end{cases}$ where M is a fixed arbitrary matrix such that $M^2 \neq M$. Then it is easy to check that Equations (3.1) to (3.5) and (3.7) to (3.10) are preserved by $[\![.]\!]$. But Equation (3.6) is not preserved if $U, V \neq I$, because then the left-hand side is interpreted as $|c,p,x\rangle \mapsto |c,p\rangle \otimes M^2\,|x\rangle$ whereas the right-hand side is interpreted as $|c,p,x\rangle \mapsto |c,p\rangle \otimes M\,|x\rangle$, and $M^2 \neq M$. By Lemma 3.34, this implies that Equation (3.6) is not a consequence of Equations (3.1) to (3.5) and (3.7) to (3.10). □

Lemma 3.41. *For any U, Equation* (3.7) *is not a consequence of Equations* (3.1) *to* (3.6) *and* (3.8) *to* (3.10).

Proof. This is clear, because Equation (3.7) is the only one that allows us to make a non-empty diagram equivalent to the empty diagram. □

Lemma 3.42. *Equation* (3.8) *is not a consequence of Equations* (3.1) *to* (3.7), (3.9) *and* (3.10).

Proof. This is clear, because Equation (3.8) is the only one that allows us to make a diagram without beam splitters equivalent to a diagram containing beam splitters. □

Lemma 3.43. *Equation* (3.10) *is not a consequence of Equations* (3.1) *to* (3.9).

Proof. It suffices to remark that Equation (3.10) is the only one that allows us to change the parity of the number of in a diagram. □

3.4.2 Independence of Equation (3.9)

3.4.2.1 A Variant of the Traced PROP Structure (PROTWEB)

To prove that Equation (3.9) is not a consequence of Equations (3.1) to (3.8) and (3.10), we need to introduce a variant of the structure of traced PROP with fewer congruence axioms, more precisely without those that allow us to create or remove swaps.

Definition 3.44. *A* PROTWEB $\mathbf{P}$ *is a collection of sets $\mathbf{P}[n,m]$, indexed by $\mathbb{N}^2$. An element $f \in \mathbf{P}[n,m]$ is called a morphism and is written $f\colon n \to m$. These sets are equipped with:*

1. *a* sequential composition $\circ\colon \mathbf{P}[m,k] \times \mathbf{P}[n,m] \to \mathbf{P}[n,k]$ *satisfying:*
   - associativity: $(h \circ g) \circ f = h \circ (g \circ f)$
2. *a* parallel composition $\oplus\colon \mathbf{P}[n,m] \times \mathbf{P}[k,\ell] \to \mathbf{P}[n+k, m+\ell]$, *satisfying:*
   - associativity: $(f \oplus g) \oplus h = f \oplus (g \oplus h)$
   - compatibility of the sequential and parallel compositions: $(f_2 \circ f_1) \oplus (g_2 \circ g_1) = (f_2 \oplus g_2) \circ (f_1 \oplus g_1)$
3. *an* empty morphism $\boxdot\colon 0 \to 0$ *satisfying:*
   - neutrality: $\boxdot \oplus f = f \oplus \boxdot = f$ *for all* $f\colon n \to m$
4. *an* identity morphism $—\colon 1 \to 1$ *satisfying:*
   - neutrality: $f \circ —^{\oplus n} = f = —^{\oplus m} \circ f$ *for all* $f\colon n \to m$, *with the convention* $—^{\oplus 0} = \boxdot$

5. *a* swap $\times : 2 \to 2$ *satisfying:*
   - naturality: $\sigma_m \circ (- \oplus f) = (f \oplus -) \circ \sigma_n$ *for all* $f : n \to m$*, where* σ_k *is defined inductively by* $\sigma_0 = -$ *and* $\sigma_{k+1} = (-^{\oplus k} \oplus \times) \circ (\sigma_k \oplus -)$
6. *a* trace $Tr : \mathbf{P}[n+1, m+1] \to \mathbf{P}[n, m]$ *satisfying:*
   - naturality in the input: $Tr(f \circ (g \oplus -)) = Tr(f) \circ g$ *for all* $f : n+1 \to m+1$ *and* $g : k \to n$
   - naturality in the output: $Tr((g \oplus -) \circ f) = g \circ Tr(f)$ *for all* $f : n+1 \to m+1$ *and* $g : m \to k$
   - dinaturality: $Tr^i((-^{\oplus m} \oplus g) \circ f) = Tr^j(f \circ (-^{\oplus n} \oplus g))$ *for all* $f : n+i \to m+j$ *and* $g : j \to i$
   - superposing: $Tr(g \oplus f) = g \oplus Tr(f)$ *for all* $f : n+1 \to m+1$ *and* $g : k \to \ell$.

By comparing Definition 3.44 with Definition 1.1, one can see that we have just removed two axioms, namely inverse law and yanking:

Lemma 3.45. *A collection of sets is a traced PROP if and only if it is a PROTWEB and satisfies inverse law and yanking:*

Remark 3.46. *To give a definition of the structure of PROTWEB in the language of category theory, one can first define a* traced weak braided category *as a strict monoidal category that is additionally a weak braided monoidal category in the sense of [62] or [123] and a right traced category in the sense of [120]. Then a* PROTWEB *is a traced weak braided category whose objects are freely generated from the monoidal unit and a single object by monoidal product, and identified with the natural integers.*

The two axioms that we have removed are the only ones that allow for creating or removing swaps. The main reason why we will use a PROTWEB instead of a PROP in the proof of independence of Equation (3.9) is to be able to count the number of swaps in a diagram. Intuitively, in a PROTWEB, the diagrams can still be deformed at will, as long as one does not create or remove intersections between wires.

To prove that Equation (3.9) is not a consequence of the others, we will need to talk about sub-diagrams in a context where the diagrams are defined up to the axioms of PROTWEB instead of those of traced PROP. Although the notion of sub-diagram is clear in a traced PROP, it may be less obvious in a PROTWEB, where swaps cannot be freely created or removed. This is why we give a formal inductive definition of it:

Definition 3.47. *We define the notion of sub-diagram inductively as follows. Given two diagrams* d *and* D*, we say that* d *is a sub-diagram of* D *if at least one of the following properties is satisfied (up to the relevant structural congruence axioms, which are the axioms of a traced PROP in all of this chapter except in the proof of Lemma 3.48 (after the two preliminary remarks), where they will be the axioms of a PROTWEB):*

- $d = D$
- *there exists two non-identity*[16] *diagrams* D_1 *and* D_2 *such that* $D = D_2 \circ D_1$ *and* d *is a sub-diagram of* D_1 *or a sub-diagram of* D_2
- *there exists two non-empty diagrams* D_1 *and* D_2 *such that* $D = D_1 \oplus D_2$ *and* d *is a sub-diagram of* D_1 *or a sub-diagram of* D_2
- *there exists a diagram* D' *such that* $D = Tr(D')$ *and* d *is a sub-diagram of* D'.

[16] That is, not of the form $-^{\oplus n}$.

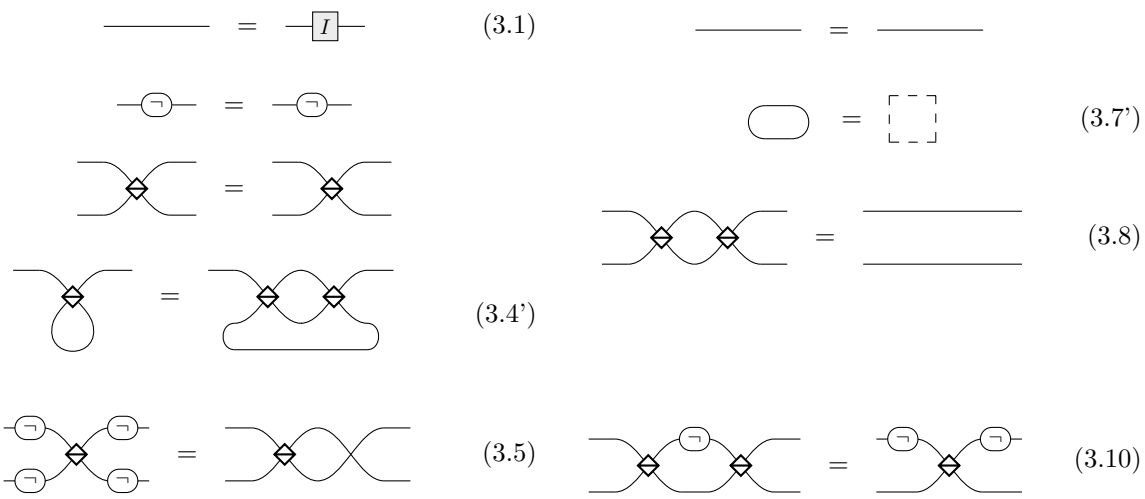
3.4.2.2 Proof of the Independence of Equation (3.9)

Lemma 3.48. *Equation* (3.9) *is not a consequence of equations* (3.1) *to* (3.8) *and* (3.10).

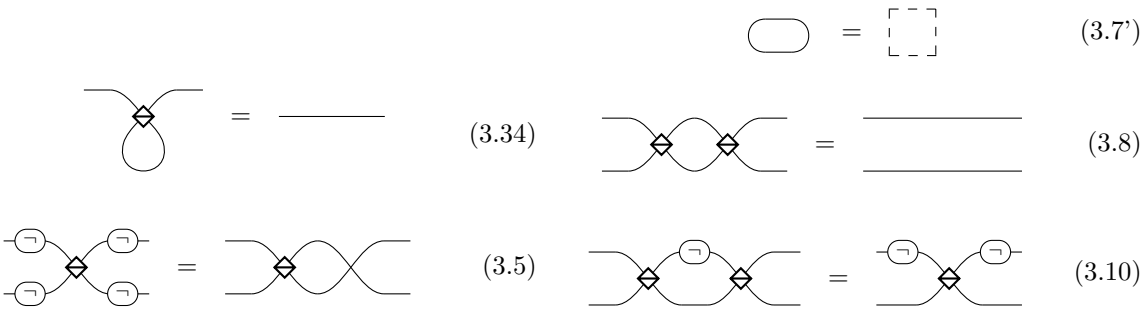
Proof. Let us first make two remarks.

First, since Equation (3.9) does not contain gates, if it is a consequence of the other equations, then it is a consequence of these equations where all U and V are instantiated by I. Indeed, all of these equations that contain gates are still true when all U and V are instantiated by I. Hence, given a valid derivation of Equation (3.9) from the others, by replacing every unitary matrix by I in this derivation, we get a valid derivation of Equation (3.9).

Second, by Equation (3.1), being a consequence of Equations (3.1) to (3.8) and (3.10) where all U and V are instantiated by I is equivalent to being a consequence of these equations where the gates have been removed (except in Equation (3.1)). That is, being a consequence of the following equations:



Equation (3.1) is now useless since it only allows us to create and remove I gates without changing anything else, and neither the other equations nor Equation (3.9) contain gates. Equations that have become an instance of reflexivity are now useless too. Finally, Equation (3.4') can be simplified through Equations (3.8) and (3.7') into Equation (3.34) below. Thus, what we have to prove is that Equation (3.9) is not a consequence of the following equations:



In the rest of the proof, we no longer assume the yanking and inverse law axioms, but we consider the corresponding equations instead:

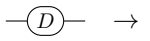
We have to prove that Equation (3.9) is not a consequence of Equations (3.34), (3.5), (3.7'), (3.8), (3.10), (y) and $(\sigma\sigma)$, still assuming the other axioms of the traced PROP, which by definition are the axioms of a PROTWEB.

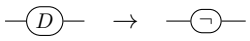
Note that we also consider the notion of sub-diagram with respect to the axioms of a PROTWEB, that is, in Definition 3.47, the conditions are considered up to these axioms. Intuitively, a sub-diagram in this sense is a part of a diagram that can be separated from the rest of the diagram by drawing a box around it.

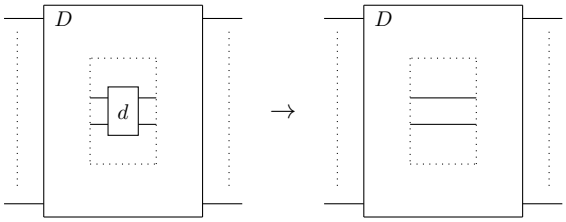
We will say that a diagram is *circle-free* if it does not have non-empty $0 \to 0$ sub-diagrams. Intuitively, a $0 \to 0$ sub-diagram in the context of a PROTWEB is graphically represented as a union of connected components, which cannot be reached by a photon and do not affect the semantics of the diagram.

We consider the following set of rewriting rules on the set of gate-free diagrams:

$D \quad \to$  for every non-empty diagram $D : 0 \to 0$ (3.35)

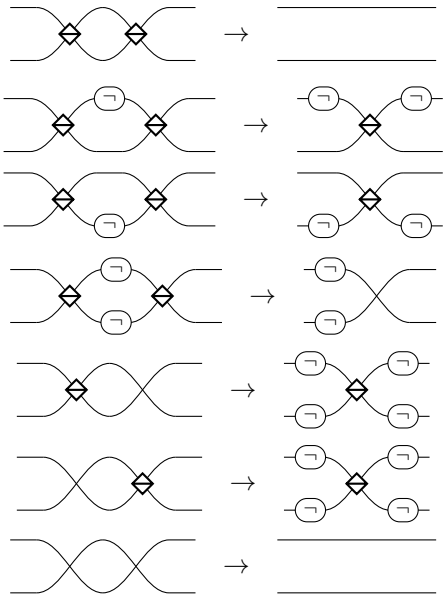
 for every circle-free $D : 1 \to 1$ such that $D \neq -$ and $[\![D]\!] = Id$ (3.36)

 for every circle-free $D : 1 \to 1$ such that $D \neq \neg$ and $[\![D]\!] = [\![\neg]\!]$ (3.37)



(3.38)

for every diagram D with a circle-free, non-identity sub-diagram $d : 2 \to 2$ that we can slide along its two wires inside D, by using the axioms of the PROTWEB, in a constant direction and make it come back to the initial point, without having to use dinaturality to slide anything else than d while doing so (in other words, roughly speaking, d can do a round trip in D without encountering any obstacle that would have to be pushed in front of it while it moves)


(3.39)

(3.40)

(3.41)

(3.42)

(3.43)

(3.44)

(3.45)

It is easy to see that these rules preserve the semantics.

Remark 3.49. *Any gate-free* $1 \to 1$ *diagram is interpreted as Id or* $[\![\ominus]\!]$*, and can therefore be reduced to either* $-$ *or* $\ominus$*, by first applying Rule* (3.35) *repeatedly to remove all its* $0 \to 0$ *sub-diagrams, and then applying Rule* (3.36) *or* (3.37)*.*

The axioms of PROTWEB do not change the number of $\diamondsuit$, $\times$, $\ominus$, or of trace wires, in a diagram (even naturality of the swap and dinaturality, due to the fact that all diagrams have number of input wires equal to their number output wires), so these numbers are well-defined for a given diagram. This allows us to define the *level* of a diagram as a tuple (b, x, n, t), where:

- b is the number of $\diamondsuit$
- x is the number of $\times$
- n is the number of $\ominus$
- t is the number of trace wires.

It is easy to check that each of the rewriting rules strictly decreases the level, according to the lexicographic order. Since the lexicographic order on $\mathbb{N}^4$ is well-founded, this implies that the rewriting system is strongly normalising.

Let us prove that the rewriting system is confluent. Because of strong normalisation, it suffices to prove that it is locally confluent. Let $\to^*$ be the reflexive transitive closure of $\to$. Let D be a diagram and let $D \overset{(a)}{\to} D_1$ and $D \overset{(b)}{\to} D_2$ be two reduction steps, where (a) and (b) are the respective rules applied. We have to prove that there exists a diagram D' such that $D_1 \to^* D'$ and $D_2 \to^* D'$. We proceed by case distinction.

If the two patterns in D that are transformed by (a) and (b) do not overlap, then after applying (a) to the first pattern or (b) to the second one, we can still apply the other rule to the other pattern and the final result does not depend on the order in which (a) and (b) are applied. That is, there exists D' such that $D_1 \overset{(b)}{\to} D'$ and $D_2 \overset{(a)}{\to} D'$.

In the rest of the case distinction, we assume that the patterns concerned by (a) and (b) overlap.

It is easy to see that if (a) is Rule (3.35), (3.36) or (3.37) and (b) is among Rules (3.39) to (3.45), then the only way the concerned patterns in D can overlap is if the pattern concerned by (b) is included in that concerned by (a). In this case, on the one hand, (a) transforms its pattern into $\lceil\_\rceil$, $-$ or $\ominus$, and on the other hand, the effect of applying (b) is to transform the pattern of (a) into a semantically equivalent diagram (which is not $\lceil\_\rceil$, $-$ or $\ominus$ because it contains at least a trace), which can then be transformed into $\lceil\_\rceil$, $-$ or $\ominus$ by applying (a). Since the rules preserve the semantics, the final sub-diagrams obtained in each case are the same. Therefore, $D_2 \overset{(a)}{\to} D_1$. Of course, the same argument applies with (a) and (b) exchanged.

If (a) is Rule (3.35) and (b) is Rule (3.36) or (3.37), then since the pattern concerned by (b) does not contain any $0 \to 0$ sub-diagram, it is necessarily included in the pattern concerned by (a), which, after applying (b), can still be transformed into the empty diagram by applying (3.35). Therefore, $D_2 \overset{(3.35)}{\to} D_1$. The same argument applies with (a) and (b) exchanged.

If both (a) and (b) are Rule (3.35), then the union of the two patterns concerned by (a) and (b) is a $0 \to 0$ sub-diagram of D. Applying (a) or (b) does not change the fact that it is of type $0 \to 0$, so that right after we can transform it into the empty diagram by applying Rule (3.35) (unless it has already become empty in which case there is nothing more to do). This gives us the desired diagram D'

If both (a) and (b) are among the two rules (3.36) and (3.37), then the union of the two concerned patterns can be written in the form $d_2 \circ d \circ d_1$ in such a way that, up to exchanging the roles of (a) and

(b), the pattern concerned by (a) is $d \circ d_1$ and the pattern concerned by (b) is $d_2 \circ d$. Then, after applying (a) or (b), we can apply Rule (3.36) or (3.37) to transform the resulting whole sub-diagram into $-$ or $\ominus$, and since the rules preserve the semantics, the result is the same regardless of whether (a) or (b) was first applied. This gives us the desired diagram D'.

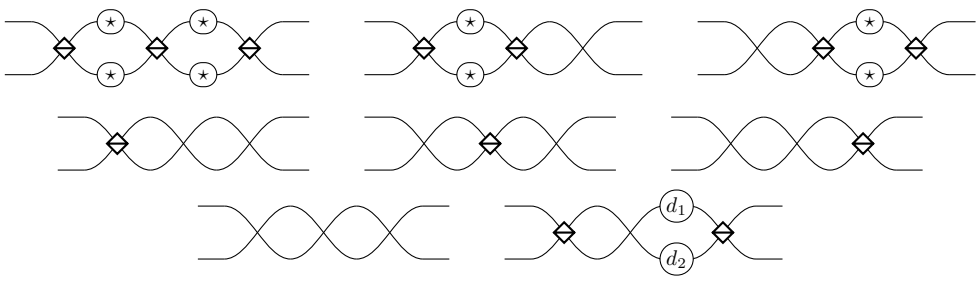
If (a) is Rule (3.38), then:

- if (b) is Rule (3.35), then since d is circle-free, it does not intersect the pattern concerned by (b). Therefore, the situation is the same as when the two patterns do not overlap and there exists D' such that $D_1 \overset{(b)}{\to} D'$ and $D_2 \overset{(a)}{\to} D'$.
- if (b) is Rule (3.36) or (3.37), then the condition of Rule (3.38) implies that the pattern concerned by (b) either is included in d, in which case we have $D_2 \overset{(3.38)}{\to} D_1$, or contains d as a sub-diagram, in which case we have $D_1 \overset{(b)}{\to} D_2$, or is disjoint from it, in which case we are in the same situation as when the two patterns do not overlap and there exists D' such that $D_1 \overset{(b)}{\to} D'$ and $D_2 \overset{(a)}{\to} D'$.
- if (b) is Rule (3.38) too, then (a) and (b) each transform an instance of d into the identity. After this, the other instance of d can be transformed into the identity by applying Rule (3.38) again (unless it has already become equal to the identity), and the result is the same regardless of whether (a) or (b) was first applied. This gives us the desired diagram D'.
- if (b) is among Rules (3.39) to (3.45), then the condition of Rule (3.38) implies that the pattern concerned by (b) is either included in d, in which case we have $D_2 \overset{(3.38)}{\to} D_1$, or disjoint from it, in which case we are in the same situation as when the two patterns do not overlap and there exists D' such that $D_1 \overset{(b)}{\to} D'$ and $D_2 \overset{(a)}{\to} D'$.

If both (a) and (b) are among Rules (3.39) to (3.45), then by looking at the possible left-hand sides of these rules, we can see that unless they are the same and $D_1 = D_2$, the two patterns cannot have a $\neg$ in common, and any generator in common cannot be the leftmost one of both patterns, neither can it be the rightmost one of both patterns. So the cases to consider are:

- those in which the two patterns have one generator in common, which is on the right of one pattern and on the left of the other
- those in which the two patterns have two generators in common, the leftmost generator of each pattern being the rightmost one of the other pattern.

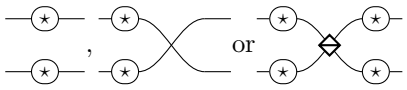
The first possibility means that the two patterns in D are in a sub-diagram of one of the following forms:



where $-\!\!\star\!\!-$ denotes either — or $\ominus$, and $d_1, d_2 : 1 \to 1$ are arbitrary diagrams.

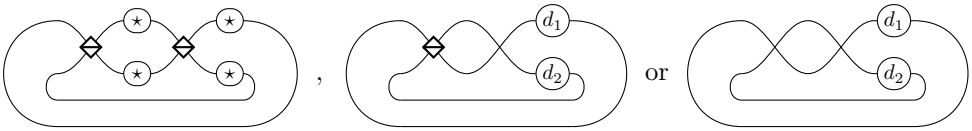
D_1 and D_2 are obtained from D by applying one of the rules (3.39) to (3.45), to the left part of the sub-diagram for one of the two, and to the right part of the sub-diagram for the other (possibly after sliding d_1 and d_2 through the swap by naturality of it — note that d_1 and d_2 appear in only one case, as in the other cases it is possible to slide them out of the considered sub-diagram). To reduce them to a common diagram, we still focus on the same sub-diagram. If relevant, we reduce d_1 and d_2 to $-$ or $\ominus$

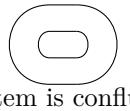
as described in Remark 3.49. Then we apply Rule (3.36) to all double negations to remove them. Then, if there are still two generators of type or , we apply the appropriate rule among (3.39) to (3.45). Finally, we apply Rule (3.36) repeatedly to all resulting double negations in order to remove them. After that, the sub-diagram is of the form

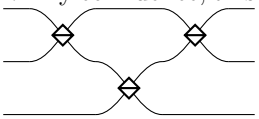
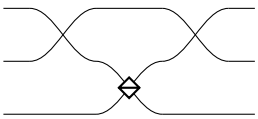


where –⊛– still denotes either — or –¬–. It is easy to see that two diagrams of these forms have the same semantics only if they are equal. And since the reduction rules preserve the semantics, the two final sub-diagrams must have the same semantics, hence they are equal.

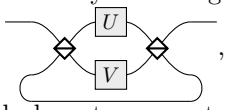
The second possibility means that the union of the two patterns is of the form



where $d_1, d_2 : 1 \to 1$ are arbitrary diagrams. This union is not necessarily a sub-diagram of D. Indeed, on the one hand, there can be some $0 \to 0$ diagrams inside the loop, and on the other hand we may have to use the naturality of the swap to transform each of the two patterns into the other, which means that there are external wires that intersect the union. However, in any case, after applying (a) or (b), we can apply Rule (3.38) to transform it into  . This reduces D_1 and D_2 to a common diagram, and finishes proving that the rewriting system is confluent.

Transforming a diagram by applying Equation (3.34), (3.5), (3.7'), (3.8), (3.10), (y) or $(\sigma\sigma)$ amounts to applying, or to applying the opposite of, Rule (3.36), (3.43), (3.35), (3.39), (3.40), (3.36) or (3.45) respectively. Therefore, if two diagrams D_1 and D_2 are equivalent according to these equations, they are equivalent according to the equivalence relation generated by the reduction relation $\to$. By confluence, this implies that there exists a diagram D' such that $D_1 \to^* D'$ and $D_2 \to^* D'$. Since  and  are normal forms for the rewriting system, this proves that they are not equivalent according to Equations (3.34), (3.5), (3.7'), (3.8), (3.10), (y) and $(\sigma\sigma)$, and therefore that Equation (3.9) is not a consequence of these equations, which is what we wanted to prove. □

3.5 Removing the Trace – Loop Unrolling

We consider in this section an application of the PBS-calculus. The semantics of the language points out that each trace, or feedback loop, is used at most twice. As a consequence, a natural question is to decide whether all loops can be unrolled, in order to transform any PBS-diagram into a trace-free PBS-diagram. Note first that in many cases, like in $E(U, V) =$ 

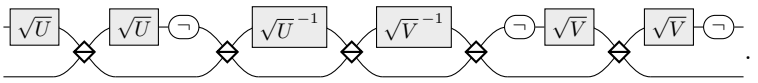
, the trace wires are useless in the sense that no particle can reach them, and are only here to guarantee that the diagram is well-formed. In particular, this is the case of all trace wires in diagrams in normal form, since these trace wires are part of diagrams of the form $E(U, V)$. This implies that any diagram can be transformed into a diagram without any "useful" trace wire. By slightly changing the formalism, for instance like in Chapter 4, one can avoid writing useless trace wires, and in this sense a diagram in which all trace wires are useless

can be considered trace-free. Nonetheless, we examine here the question of writing a diagram trace-free within the current formalism of PBS-diagrams. Such a transformation is possible when all matrices are invertible:

Proposition 3.50. *Let $D : n \to n$ with $n \geq 2$ be a* PBS*-diagram such that all matrices appearing in the gates of D are invertible. Then there exists a trace-free* PBS*-diagram D' such that* $\mathrm{PBS} \vdash D = D'$.

Proof. By Proposition 3.29, there exists a diagram N in normal form such that $\mathrm{PBS} \vdash D = N$. What we have to prove is that N is equivalent through the axioms of the PBS-calculus to a trace-free diagram. By Remark 3.24, let us decompose N into $P \circ E$, where E is of the form $E(U_0, V_0) \oplus \cdots \oplus E(U_{n-1}, V_{n-1})$, and P is trace-free and gate-free. We just have to prove that E is equivalent to a trace-free diagram. By the axioms of PROP, we can write E in the form $E = \prod_{p=0}^{n-1} (-^{\oplus p} \oplus E(U_{\mathbf{V},p}, U_{\mathbf{H},p}) \oplus -^{\oplus n-1-p})$, so it is sufficient to prove that every factor $-^{\oplus p} \oplus E(U_{\mathbf{V},p}, U_{\mathbf{H},p}) \oplus -^{\oplus n-1-p}$ is equivalent to a trace-free diagram. To do so, it is enough to prove that any diagram of the form $E(U,V) \oplus -$ or $- \oplus E(U,V)$ is equivalent to a trace-free diagram. And since $- \oplus E(U,V) = \times \circ (E(U,V) \oplus -) \circ \times$, it suffices to prove that $E(U,V) \oplus -$ is equivalent to a trace-free diagram.

First, assume that U and V have a square root. Then $E(U,V) \oplus -$ is equivalent to



If U or V does not have a square root, let us consider their polar decompositions $U = QS$ and $V = Q'S'$ with Q, Q' unitary and S, S' positive-definite Hermitian. Then by Equation (3.15), $PBS \vdash E(U,V) \oplus - = (E(Q,Q') \oplus -) \circ (E(S,S') \oplus -)$, and since each of Q, S, Q' and S' have a square root, $E(Q,Q') \oplus -$ and $E(S,S') \oplus -$ are equivalent to trace-free diagrams of the form above, so that by composition, $E(U,V) \oplus -$ is equivalent to a trace-free diagram too. □

Notice that Proposition 3.50 is not true for PBS-diagrams with a single input/output. Indeed a trace-free diagram of type $1 \to 1$ is made of generators acting on 1 wire only, so in particular it has no polarising beam splitter and as a consequence cannot have a behaviour which depends on the polarisation. For instance, the diagram $E(U,V)$ used in the normal forms (see Remark 3.24) cannot be transformed into a trace-free diagram unless $U = V$.

On the other hand, PBS-diagrams involving at least one non-invertible matrix are not necessarily equivalent to a trace-free one. Indeed, we have the following property:

Lemma 3.51. *For any trace-free PBS-diagram D, either all $U^D_{c,p}$ are invertible or at least two of them are not.*

Proof. We prove the result by structural induction on D.

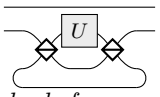
If $D = \boxed{\ }, -, \neg, \times$ or $\times\!\!\times$ then for every (c,p) we have $U^D_{c,p} = I_q$, which is invertible, so the result holds.

If $D = \boxed{U}$ then for every $c \in \{\mathbf{V}, \mathbf{H}\}$ we have $U^D_{c,0} = U$. If U is invertible, then the result holds, and if U is not invertible, then the result holds too.

If $D = D_2 \circ D_1$, then for any (c,p) we have $U^D_{c,p} = U^{D_2}_{\tau_{D_1}(c,p)} U^{D_1}_{c,p}$. The product $U^{D_2}_{\tau_{D_1}(c,p)} U^{D_1}_{c,p}$ is invertible if and only if both $U^{D_2}_{\tau_{D_1}(c,p)}$ and $U^{D_1}_{c,p}$ are. Therefore, if all $U^{D_1}_{c,p}$ and all $U^{D_2}_{c,p}$ are invertible then all $U^D_{c,p}$ are invertible. If not all $U^{D_1}_{c,p}$ are invertible, then by induction hypothesis at least two of them are not, and consequently at least two $U^D_{c,p}$ are not invertible. If not all $U^{D_2}_{c,p}$ are invertible, then by induction hypothesis at least two of them are not; since τ_{D_1} is surjective, this implies that at least two $U^{D_2}_{\tau_{D_1}(c,p)}$ are not invertible and consequently that at least two $U^D_{c,p}$ are not invertible. In all three cases, the result holds.

If $D = D_1 \oplus D_2$, then the set of all $U^D_{c,p}$ is the union of the set of all $U^{D_1}_{c,p}$ and the set of all $U^{D_2}_{c,p}$. Therefore, if all $U^{D_1}_{c,p}$ and $U^{D_2}_{c,p}$ are invertible then all $U^D_{c,p}$ are, and if not all are invertible, then by induction hypothesis at least two $U^{D_1}_{c,p}$ or two $U^{D_2}_{c,p}$ are not invertible, so that at least two $U^D_{c,p}$ are not invertible. In both cases the result holds. □

This prevents the following diagram from being equivalent to a trace-free one:

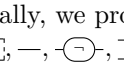
Example 3.52. *If U is not invertible, then the diagram $D_U : 2 \to 2 =$*  *is not equivalent, according to the rules of the PBS-calculus, to any trace-free diagram. Indeed, for any $(c,p) \neq (\mathbf{V},1)$ we have $U^{D_U}_{c,p} = I_q$, which is invertible, whereas $U^{D_U}_{\mathbf{V},1} = U$.*

Another interesting property is that loop unrolling, when it is possible, requires the use of matrices that were not present in the original diagram. This is a consequence of the following lemma:

Lemma 3.53. *Given any diagram $D : n \to n$, let us define $|D| := \prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^D_{c,p}\right)$. Then for any trace-free diagram D, we have $|D| = \prod_{G \text{ gate in } D} \det\left(U(G)\right)^2$ where $U(G)$ denotes the matrix with which G is labelled.*

Proof. Intuitively, due to the invertibility of the PBS-diagrams (Proposition 3.7), for each wire of a trace-free diagram D, there are exactly two initial configurations which go through this particular wire. As a consequence each gate of D contributes twice to $|D|$.

More formally, we proceed by structural induction on D.

If $D =$  then D does not contain any gate, and for any (c,p) we have $\det(U^D_{c,p}) = 1$. So with the usual convention that the empty product is equal to 1, the result holds.

If $D =$  , then we have $|D| = \prod_{c\in\{\mathbf{V},\mathbf{H}\}} \det(U) = \det(U)^2$, and is the only gate in D, so the result holds.

If $D = D_2 \circ D_1$, then on the one hand, the set of gates of D is the disjoint union of the respective sets of gates of D_1 and D_2, so that

$$\prod_{G \text{ gate in } D} \det\left(U(G)\right)^2 = \left(\prod_{G \text{ gate in } D_1} \det\left(U(G)\right)^2\right)\left(\prod_{G \text{ gate in } D_2} \det\left(U(G)\right)^2\right),$$

which by induction hypothesis is equal to $|D_1||D_2|$. On the other hand, we have

$$\begin{aligned}
|D| &= \prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^D_{c,p}\right) \\
&= \prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^{D_2}_{\tau_{D_1}(c,p)} U^{D_1}_{c,p}\right) \\
&= \prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^{D_2}_{\tau_{D_1}(c,p)}\right) \det\left(U^{D_1}_{c,p}\right) \\
&= \left(\prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^{D_2}_{\tau_{D_1}(c,p)}\right)\right)\left(\prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^{D_1}_{c,p}\right)\right) \\
&= \left(\prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^{D_2}_{c,p}\right)\right)\left(\prod_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \det\left(U^{D_1}_{c,p}\right)\right) \\
&= |D_1||D_2|
\end{aligned}$$

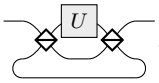
which proves the result for D.

If $D = D_1 \oplus D_2$, then on the one hand, the set of gates of D is the disjoint union of the respective sets of gates of D_1 and D_2, so that

$$\prod_{G \text{ gate in } D} \det\left(U(G)\right)^2 = \left(\prod_{G \text{ gate in } D_1} \det\left(U(G)\right)^2\right)\left(\prod_{G \text{ gate in } D_2} \det\left(U(G)\right)^2\right),$$

which by induction hypothesis is equal to $|D_1||D_2|$. On the other hand, the set of the $U_{c,p}^D$ is the disjoint union of the set of the $U_{c,p}^{D_1}$ and the set of the $U_{c,p}^{D_2}$, so that $|D| = |D_1||D_2|$. This proves the result for D. □

Example 3.54. *Unless* $\det(U)$ *is a* k*th root of unity for some odd integer* k*, the following diagram* D_U *does not have the same semantics as any trace-free diagram in which all gates are labelled by* U*:*



. Indeed, we have $|D_U| = \det(U)$*, and by Lemma 3.53, if* D_U *is equivalent modulo the axioms of the* PBS*-calculus to a trace-free diagram* D'_U *in which all gates are labelled by* U*, then we have* $|D_U| = \det(U) = \det(U)^{2N}$*, where* N *is the number of gates in* D'_U*. By Lemma 3.51, we have* $\det(U) \neq 0$*, so that* $\det(U)^{2N-1} = 1$*, that is,* $\det(U)$ *is a* k*th root of unity with* $k = 2N - 1$ *odd (if* $N = 0$ *then* $\det(U) = 1$ *so the result is still true).*

3.6 Final Remark

In the definition of the PBS-calculus, we have restricted the gates to being indexed by square matrices of finite dimension. However, note that one can extend the PBS-calculus by allowing the gates to be indexed by the elements of an arbitrary monoid, while preserving most of the results exposed in this chapter:

On the one hand, it is then not possible anymore to define the denotational semantics, except in the cases of some particular monoids, which makes Proposition 3.12 and Theorems 3.13 and 3.32 pointless, and may alter the results and the proofs of Section 3.5.

On the other hand, it is possible to define $[\![D]\!]$ for instance as the function $(c, p) \mapsto (c_{c,p}^D, p_{c,p}^D, U_{c,p}^D)$. Then the equational theory is still sound and complete, and the proofs are the same. The proofs that the equations are not consequences of each other are the same, except for Equations (3.1), (3.3) and (3.6). Note that for Equations (3.1) and (3.6), the independence can still be proven using the arguments given for Equations (4.1) and (4.2) respectively in the proof of Theorem 4.19. The question of proving the independence of Equation (3.3) in the case of an arbitrary monoid has not been investigated.

In Chapter 4, we will introduce such an extension and allow an arbitrary monoid to index the gates, in addition to allowing for removing the useless trace wires. The case of a free monoid (that is, a monoid of words) will be of particular interest in the context of this chapter where we will be interested in resource optimisation, as then the letters can be interpreted as independent queries to oracles.

Chapter 4

Coloured PBS-diagrams and Resource Optimisation

As pointed out before, some problems can be solved more efficiently by using coherent control rather than the usual quantum circuits. This separation has been proved in a multi-oracle model where the measure of complexity is the number of queries to (a single or several distinct) oracles, which are generally unitary maps. The simplest example is the following problem [31]: given two oracles U and V with the promise that they are either commuting or anti-commuting, decide whether U and V are commuting or not. This problem can be solved using the quantum switch, which can be implemented using only two queries by means of coherent control, whereas solving this problem requires at least 3 queries (e.g. two queries to U and one query to V) in the quantum circuit model (see Figure 4.1).

In this chapter, we address the problem of optimising the resources of coherently controlled quantum computations represented as PBS-diagrams. To do so, we first refine the framework of the PBS-calculus to make it more resource-sensitive. Then, we consider the problem of optimising the number of queries, and also the number of polarising beam splitters, of a given coherently controlled quantum computation, described as a PBS-diagram.

Note that a PBS-diagram may have some useless wires, like in the example of the "half quantum switch", see Figure 4.2 (left). We refine the PBS-calculus in order to allow one to remove these useless wires, leading to unsaturated PBS (or 3-leg PBS) like  or  . To avoid ill-formed diagrams like  , a typing discipline is necessary. To this end, we use the framework of coloured PROPs: each wire has 3 possible colours: black, red and blue which can be interpreted as follows: a photon going through a blue (resp. red) wire must have a horizontal (resp. vertical) polarisation.

The introduction of unsaturated polarising beam splitters requires to revisit the equational theory of the PBS-calculus. The heart of the refined equational theory is the axiomatisation of the 3-leg polarising beam splitters, together with some additional equations which govern how 4-leg polarising beam splitters can be decomposed into 3-leg ones. To show the completeness of the refined equational theory, we introduce normal forms and show that any diagram can be put in normal form. Finally, we also show the minimality of the equational theory by proving that none of the equations can be derived from the

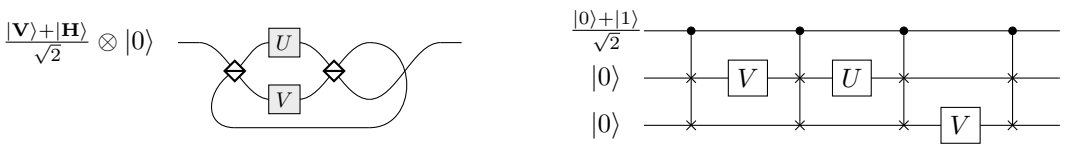


Figure 4.1: [*Left*] Coherently controlled quantum computation for solving the commuting problem. Only two queries are used: one query to U and one query to V. [*Right*] Optimal circuit for solving the commuting problem, where the 3-qubit gate is a control-swap. Note that three queries are necessary in the quantum circuit model.

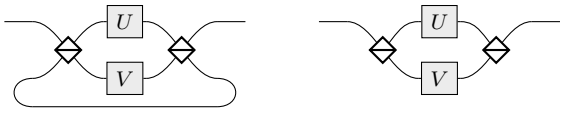


Figure 4.2: A coherent control of U and V, also called a half quantum switch: when the initial polarisation is vertical ($\mathbf{V}$), U is applied on the data register, when the polarisation is horizontal ($\mathbf{H}$), V is applied. Whatever the polarisation is, the particle always goes out of the top port of the second beam splitter. On the right-hand side the diagram is made of beam splitters with a missing leg, whereas on the left-hand side standard beam splitters are used, and a useless trace is added.

other ones.

Note also that as opposite to Chapter 3 where we have restricted the gates to be indexed by square matrices of finite size, here we allow the gates to be indexed by the elements of an arbitrary monoid. The case that we will consider for resource optimisation is that of a free monoid, that is, the monoid of words over some alphabet. Then each letter can be interpreted as an oracle, or as an external resource, which is called each time it appears in a gate.

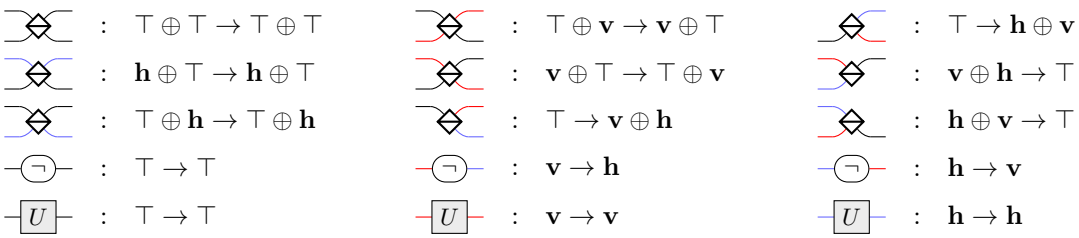
Resource Optimisation. The coloured PBS-calculus, thanks to its refined equational theory, provides a way to detect and remove dead code in a diagram. We exploit this property to address the question of resource optimisation. We introduce a specific form of diagrams that minimises the number of gates, more precisely the number of queries to oracles, with an appropriate modelisation of oracles. We provide an efficient procedure to transform any diagram into this specific form. We then focus on the problem of optimising both the number of queries and the number of polarising beam splitters. We refine the previous procedure, leading to an efficient heuristic. We show that the produced diagrams are optimal when every oracle is queried at most once, but might not be optimal in general. We actually show that the general optimisation problem is NP-hard using a reduction from the *maximum Eulerian cycle decomposition problem* [25].

Related Works. While there are numerous works on resource-optimisation of quantum computations, in particular for quantum circuits [93, 9, 103], there was, up to our knowledge, no procedure for resource optimisation of coherently controlled quantum computation.

4.1 Coloured PBS-Diagrams

We represent the refined language of PBS-diagrams as a coloured traced PROP (see Definition 1.6 in Chapter 1). We are going to use the "colours" $\mathbf{v}$, $\mathbf{h}$, $\top$, to denote respectively vertical, horizontal or possibly both polarisations.

Definition 4.1. *Given a monoid* M*, let* $\mathbf{Diag}^{\mathsf{M}}$ *be the traced coloured PROP with colours* $\{\mathbf{v}, \mathbf{h}, \top\}$ *freely generated by the following generators, for any* $U \in \mathsf{M}$*:*



The morphisms of $\mathbf{Diag}^{\mathsf{M}}$ are called M-diagrams or simply diagrams when M is irrelevant or clear from the context.

Regarding notations, we use actual colours for wires: blue for $\mathbf{h}$-wires, red for $\mathbf{v}$-wires, and black for $\top$-wires. We also add labels on the wires, so that there is no loss of information in the case of a colour-blind reader or black and white printing. To avoid overloading the diagrams, we omit the types that are clear from the context (see Example 1.7 for additional explanations about infering them), and

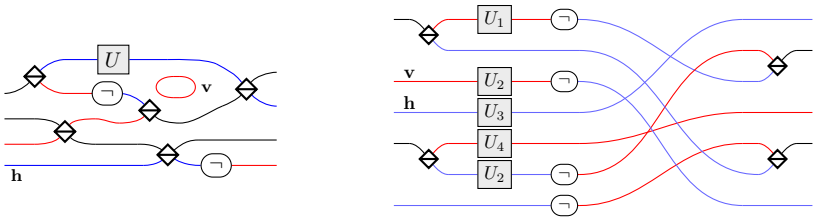


Figure 4.3: (*Left*) An example of diagram of type $\top \oplus \top \oplus \mathbf{v} \oplus \mathbf{h} \to \top \oplus \mathbf{h} \oplus \top \oplus \mathbf{v}$. (*Right*) An example of a diagram of type $\top \oplus \mathbf{v} \oplus \mathbf{h} \oplus \top \oplus \mathbf{h} \to \mathbf{h} \oplus \top \oplus \mathbf{v} \oplus \top \oplus \mathbf{h}$, in a particular form that we will call *normal form* (see Definition 4.15).

we take the convention that the type $\top$ is always omitted (in other words, a wire of ambiguous type is black by convention). Two examples of diagrams are given in Figure 4.3.

Unless specified, the unit of M is denoted I and its composition is $\cdot$ which will be generally omitted (VU rather than $V \cdot U$). The main two examples of monoids we consider in the rest of this chapter are:

- The monoid $\mathcal{U}(\mathcal{H})$ of isometries of a Hilbert space $\mathcal{H}$ with the usual composition. When $\mathcal{H}$ is of finite dimension, the elements of $\mathcal{U}(\mathcal{H})$ are unitary maps. With a slight abuse of notations, the corresponding traced coloured PROP of diagrams is denoted $\mathbf{Diag}^{\mathcal{H}}$.
- The free monoid $\mathcal{G}^*$ on some set $\mathcal{G}$. The gates, when the monoid is freely generated, can be interpreted as queries to oracles (each element of $\mathcal{G}$ corresponds to an oracle): the gates implement *a priori* arbitrary operations with no particular structures. We use the term *abstract diagram* when the underlying monoid is freely generated, and we refer to the elements of $\mathcal{G}$ as *names*. Notice that the free monoid case can also be seen as an extension of the *bare diagrams* defined in Section 7.1.1 in Chapter 7.

There are other examples of interests: One can consider for instance a monoid of commuting or anticommuting gates, that can be used to model the problem studied in [31]. Another example is the monoid of n-qubit quantum circuits whose generators are layers of gates acting on n qubits (e.g. $H \otimes \mathrm{CNot} \otimes I \otimes H$ when $n = 5$ where H is the 1-qubit Hadamard gate, CNot the 2-qubit controlled-not gate, and I the 1-qubit identity) and whose composition is the sequential composition of circuits. The monoid can be quotiented by equations like $(H \otimes I) \cdot (I \otimes H) = H \otimes H$ and $(H \otimes I) \cdot (H \otimes I) = I \otimes I$. Finally, one can consider the monoid of unitary purifications[17] used to describe coherent control of quantum channels in Chapter 7 (see Section 7.1.2).

The PBS-diagrams of Chapter 3 correspond to the special case where the monoid M is $\mathbb{C}^{q \times q}$ for some $q \geq 1$ and no coloured wires are used, namely the diagrams are restricted to those generated from  ,  ,  , — and  , using $\circ$, $\oplus$ and $Tr_{\top}$.

4.2 Semantics

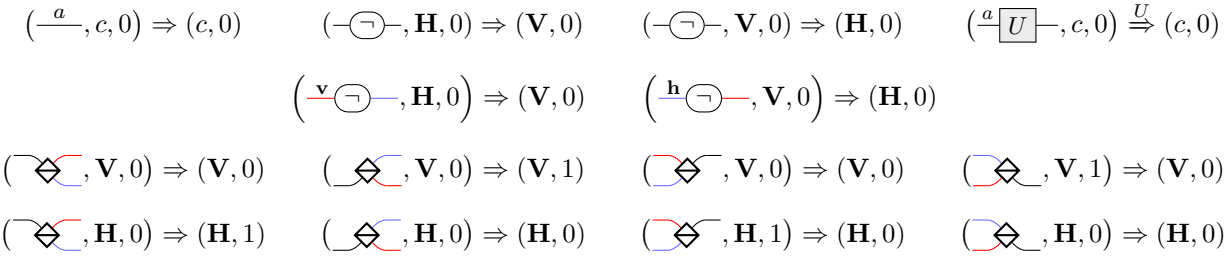
As for vanilla PBS-diagrams (that is, those of Chapter 3), the input of a diagram is a single particle, which has a polarisation, a position and a data register. A basis state for the polarisation is either vertical or horizontal, and a basis state for the position is an integer which corresponds to the wire on which the particle is located. The type of a diagram restricts the possible input/output configurations: if $D : \mathbf{v} \oplus \top \to \mathbf{h} \oplus \mathbf{h} \oplus \mathbf{v}$ then the possible input (resp. output) configurations are the following polarisation-position pairs: $\{(\mathbf{V}, 0), (\mathbf{V}, 1), (\mathbf{H}, 1)\}$ (resp. $\{(\mathbf{H}, 0), (\mathbf{H}, 1), (\mathbf{V}, 2)\}$). More generally for any object[18] a, let $[a]$ be the set of possible configurations, and $|a|$ be its size, inductively defined as follows: $|\epsilon| = 0$, $|a \oplus \top| = |a \oplus \mathbf{v}| = |a \oplus \mathbf{h}| = |a| + 1$, and $[\epsilon] = \emptyset$, $[a \oplus \mathbf{v}] = [a] \cup \{(\mathbf{V}, |a|)\}$, $[a \oplus \mathbf{h}] = [a] \cup \{(\mathbf{H}, |a|)\}$ and $[a \oplus \top] = [a] \cup \{(\mathbf{V}, |a|), (\mathbf{H}, |a|)\}$.

[17] Given a Hilbert space $\mathcal{H}$, the elements of the monoid are triplets $[U, |\varepsilon\rangle, \mathcal{E}]$ where $\mathcal{E}$ is a Hilbert space, $U : \mathcal{H} \otimes \mathcal{E} \to \mathcal{H} \otimes \mathcal{E}$ is a unitary transformation, and $|\varepsilon\rangle \in \mathcal{E}$. The composition is defined as $[U_2, |\varepsilon_2\rangle, \mathcal{E}_2] \cdot [U_1, |\varepsilon_1\rangle, \mathcal{E}_2] = [(\sigma_{\mathcal{E}_1, \mathcal{H}} \otimes I)(I \otimes U_2)(\sigma_{\mathcal{H}, \mathcal{E}_1} \otimes I)(U_1 \otimes I), |\varepsilon_1\rangle \otimes |\varepsilon_2\rangle, \mathcal{E}_1 \otimes \mathcal{E}_2]$ where $\sigma_{\mathcal{K}, \mathcal{K}'}$ is the swap between the two Hilbert spaces $\mathcal{K}$, $\mathcal{K}'$.

[18] As of Definition 1.6.

Coloured diagrams have a path semantics similar to that defined in Section 3.2 in Chapter 3. However, since the monoid M is not in general a monoid of linear maps, the definition of a denotational semantics is less straightforward. We make the path semantics into a denotational one by defining the semantics $[\![D]\!]_{\text{path}}$ of an M-diagram $D : a \to b$ as a map $[a] \to [b] \times \mathsf{M}$ which associates with an input configuration (c, p), an output configuration (c', p') and a side effect $U_k \dots U_1 \in \mathsf{M}$ which represents the action performed on a data register of the particle. Thus the semantics of a diagram can be formulated as follows:

Definition 4.2 (Path semantics)**.** *Given an M-diagram $D : a \to b$, a polarisation $c \in \{\mathbf{V}, \mathbf{H}\}$ and a position $p \in [a]$, let $(D, c, p) \overset{U}{\Rightarrow} (c', p')$ (or simply $(D, c, p) \Rightarrow (c', p')$ when U is the identity) be inductively defined as follows:*



$$\frac{(D_1, c, p) \overset{U}{\Rightarrow} (c', p') \qquad (D_2, c', p') \overset{V}{\Rightarrow} (c'', p'')}{(D_2 \circ D_1, c, p) \overset{VU}{\Longrightarrow} (c'', p'')}(\circ)$$

$$\frac{D_1 : a \to b \qquad p < |a| \qquad (D_1, c, p) \overset{U}{\Rightarrow} (c', p')}{(D_1 \oplus D_2, c, p) \overset{U}{\Rightarrow} (c', p')}(\oplus 1)$$

$$\frac{D_1 : a \to b \qquad p \geq |a| \qquad (D_2, c, p - |a|) \overset{U}{\Rightarrow} (c', p')}{(D_1 \oplus D_2, c, p) \overset{U}{\Rightarrow} (c', p' + |a|)}(\oplus 2)$$

$$\frac{D : a \oplus d \to b \oplus d \qquad (D, c_0, p_0) \overset{U_0}{\Longrightarrow} (c_1, p_1) \qquad \forall i \in \{1, \dots, k\}, (D, c_i, |a|) \overset{U_i}{\Longrightarrow} (c_{i+1}, p_{i+1})}{(Tr_d(D), c_0, p_0) \overset{U_k \cdots U_0}{\Longrightarrow} (c_{k+1}, p_{k+1})}(\mathsf{T}_k)$$

with $p_0 < |a|$, $p_{k+1} < |b|$, $\forall i \in \{1, ..., k\}, p_i = |b|$, and $k \in \{0, 1, 2\}$.

Given $D : a \to b$ and $(c, p) \in [a]$, we denote respectively by $c^D_{c,p}$, $p^D_{c,p}$ and $U^D_{c,p}$ the polarisation, the position and the element of M, such that $(D, c, p) \overset{U^D_{c,p}}{\Longrightarrow} (c^D_{c,p}, p^D_{c,p})$. In the case where M is the free monoid $\mathcal{G}^*$, its elements can be seen as words, so we will use the notation $w^D_{c,p}$ instead of $U^D_{c,p}$.

Finally, let $[\![D]\!]_{\text{path}} : [a] \to [b] \times \mathsf{M}$ be defined as $[\![D]\!]_{\text{path}}(c, p) = ((c^D_{c,p}, p^D_{c,p}), U^D_{c,p})$.

The intuition behind Rule (T_k) is the same as in Chapter 3. Here, due to the fact that a diagram can have different numbers of input and output wires, we have to change the position p_i from $|b|$ to $|a|$ at each step, so that it matches the position of the traced wire on the input side.

Note that like for vanilla PBS-diagrams, the semantics of the trace requires only a finite number of unfoldings, namely 2. Indeed, like for PBS-diagrams, one can show that any wire of a diagram is used at most twice, each time with a distinct polarisation (cf. Propositions 7.3 and 3.9).

Proposition 4.3. *$[\![.]\!]_{\text{path}}$ is well-defined, i.e. the axioms of the traced coloured PROP are sound and the semantics of the trace is well-defined.*

Proof. This can be proved in a similar way as Proposition 3.6 of Chapter 3. □

4.2.1 Quantum Semantics

Any diagram whose underlying monoid consists of linear maps admits a *quantum semantics*, which corresponds to the denotational semantics of vanilla PBS-diagrams, defined as follows:

Definition 4.4 (Quantum semantics)**.** *Given a monoid* M *of linear maps (with the standard composition) on a complex vector space* $\mathcal{V}$*, for any* M*-diagram* $D : a \to b$ *the quantum semantics of* D *is the linear map* $V_D : \mathbb{C}^{[a]} \otimes \mathcal{V} \to \mathbb{C}^{[b]} \otimes \mathcal{V} :: |c,p\rangle \otimes |\varphi\rangle \mapsto \left|c^D_{c,p}, p^D_{c,p}\right\rangle \otimes U^D_{c,p} |\varphi\rangle$

The diagrams in $\mathbf{Diag}^{\mathcal{H}}$ are valid by construction, in the sense that their semantics are valid quantum evolutions:

Proposition 4.5. *For any* $D \in \mathbf{Diag}^{\mathcal{H}}$*,* $V_D : \mathbb{C}^{[a]} \otimes \mathcal{H} \to \mathbb{C}^{[b]} \otimes \mathcal{H}$ *is an isometry.*

Proof. Since there exists an orthonormal basis of $\mathbb{C}^{[a]} \otimes \mathcal{V}$ composed of vectors of the form $|c,p\rangle \otimes |\varphi\rangle$, it suffices to check that V_D preserves all scalar products of vectors of this form. For any c, p, c', p', $|\varphi\rangle$ and $|\varphi'\rangle$, one has $(\langle c,p| \otimes \langle\varphi|)V_D^\dagger V_D(|c',p'\rangle \otimes |\varphi'\rangle) = \left\langle c^D_{c,p}, p^D_{c,p} \middle| c^D_{c',p'}, p^D_{c',p'} \right\rangle \otimes \langle\varphi| {U^D_{c,p}}^\dagger U^D_{c',p'} |\varphi'\rangle$. On the one hand, it can be proved in the same way as in Chapter 3 that the function $(c,p) \mapsto (c^D_{c,p}, p^D_{c,p})$ is a bijection (see Propositions 3.6 and 3.7), so that $(c^D_{c,p}, p^D_{c,p}) = (c^D_{c',p'}, p^D_{c',p'})$ if and only if $(c,p) = (c',p')$. That is, $\left\langle c^D_{c,p}, p^D_{c,p} \middle| c^D_{c',p'}, p^D_{c',p'} \right\rangle = \langle c,p|c',p'\rangle = \begin{cases} 1 & \text{if } (c,p) = (c',p') \\ 0 & \text{if } (c,p) \neq (c',p') \end{cases}$. On the other hand, since $U^D_{c,p}$ is an isometry, if $(c,p) = (c',p')$ then $\langle\varphi| {U^D_{c,p}}^\dagger U^D_{c,p} |\varphi'\rangle = \langle\varphi|\varphi'\rangle$. Thus,

$$(\langle c,p| \otimes \langle\varphi|)V_D^\dagger V_D(|c',p'\rangle \otimes |\varphi'\rangle) = \begin{cases} \langle\varphi|\varphi'\rangle & \text{if } (c,p) = (c',p') \\ 0 & \text{if } (c,p) \neq (c',p') \end{cases} = (\langle c,p| \otimes \langle\varphi|)(|c',p'\rangle \otimes |\varphi'\rangle). \qquad \square$$

Note that $[\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}}$ implies $V_D = V_{D'}$; the converse is true if and only if $0 \notin \mathsf{M}$:

Proposition 4.6. *Given a monoid* M *of complex linear maps, we have* $\forall D, D', [\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}} \Leftrightarrow V_D = V_{D'}$*, if and only if* $0 \notin \mathsf{M}$*.*

Proof. Let us assume that M is a monoid of linear maps on a complex vector space $\mathcal{V}$.

Since the quantum semantics is defined from the path semantics, it is clear that $\forall D, D', [\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}} \Rightarrow V_D = V_{D'}$.

Given an M-diagram D, if $0 \notin \mathsf{M}$, then for all c, p, $U^D_{c,p} \neq 0$, so that there exists $|\varphi\rangle \in \mathcal{V}$ such that $U^D_{c,p} |\varphi\rangle \neq 0$. Then $\left|c^D_{c,p}, p^D_{c,p}\right\rangle \otimes U^D_{c,p} |\varphi\rangle \neq 0$, which implies that $c^D_{c,p}$ and $p^D_{c,p}$ are uniquely determined from the data of c, p and V_D. Since in any case, $U^D_{c,p}$ is uniquely determined from the data of c, p and V_D, this implies that if $0 \notin \mathsf{M}$ then $[\![D]\!]_{\text{path}}$ is uniquely determined from V_D. Hence if $0 \notin \mathsf{M}$ then for any two M-diagrams D and D', $V_D = V_{D'} \Rightarrow [\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}}$.

Conversely, if $0 \in \mathsf{M}$, then for example, with $D = \boxed{0}$ and $D' = \boxed{0}\!\!-\!\!\bigcirc$, both of type $\top \to \top$, one has $V_D = V'_D = 0$ but $[\![D]\!]_{\text{path}}(\mathbf{V}, 0) = ((\mathbf{V}, 0), 0) \neq [\![D']\!]_{\text{path}}(\mathbf{V}, 0) = ((\mathbf{H}, 0), 0)$. $\square$

In particular, two diagrams in $\mathbf{Diag}^{\mathcal{H}}$ have the same path semantics if and only if they have the same quantum semantics.

4.2.2 Interpretation

Given a monoid homomorphism $\gamma : \mathsf{M} \to \mathsf{M}'$, one can transform any M-diagram into a M'-diagram straightforwardly, by applying γ on each gate of the diagram:

Definition 4.7. *Given an* M*-diagram* $D : a \to b$ *and a monoid homomorphism* $\gamma\colon \mathsf{M} \to \mathsf{M}'$*, we define its* γ*-interpretation* $\gamma(D) : a \to b$ *as the* M'*-diagram obtained by applying* γ *to each gate of* D*. It is defined inductively as:* $\gamma(\overset{a}{\boxed{U}} : a \to a) = \overset{a}{\boxed{\gamma(U)}} : a \to a$*, for any other generator* g*,* $\gamma(g) = g$*,* $\gamma(D_2 \circ D_1) = \gamma(D_2) \circ \gamma(D_1)$*,* $\gamma(D_1 \oplus D_2) = \gamma(D_1) \oplus \gamma(D_2)$*, and* $\gamma(Tr_e(D)) = Tr_e(\gamma(D))$*.*

Proposition 4.8. *Any* M*-diagram is the interpretation of an abstract diagram.*

Proof. Given an M-diagram D, let $\mathcal{G}$ be the underlying set of M and $\gamma : \mathcal{G} \to \mathsf{M}$ s.t. $\forall U \in \mathcal{G}$, $\gamma(U) = U$. The function γ can be extended trivially into a homomorphism $\gamma\colon \mathcal{G}^* \to \mathsf{M}$. Notice that D can be seen as a (abstract) diagram of $\mathbf{Diag}^{\mathcal{G}^*}$ and $\gamma(D) = D$. □

It is easy to see that the action of monoid homomorphisms on diagrams is well-behaved with respect to the semantics:

Proposition 4.9. *Given any* M*-diagram* $D : a \to b$ *and any monoid homomorphism* $\gamma\colon \mathsf{M} \to \mathsf{M}'$*, for any configuration* $(c, p) \in [a]$*, if* $[\![D]\!]_{\text{path}}(c, p) = ((c', p'), U)$ *then* $[\![\gamma(D)]\!]_{\text{path}}(c, p) = ((c', p'), \gamma(U))$.

Proof. Straightforward by induction. □

As a consequence, given two abstract diagrams $D_1, D_2 \in \mathbf{Diag}^{\mathcal{G}^*}$, if $[\![D_1]\!]_{\text{path}} = [\![D_2]\!]_{\text{path}}$ then for any homomorphism $\gamma : \mathcal{G}^* \to \mathsf{M}$, $[\![\gamma(D_1)]\!]_{\text{path}} = [\![\gamma(D_2)]\!]_{\text{path}}$. The converse is not true in general. Nonetheless, interpreting abstract diagrams using 2-dimensional Hilbert spaces is enough to completely characterise their semantics:

Proposition 4.10. *Given a Hilbert space* $\mathcal{H}$ *of dimension at least* 2 *and a set* $\mathcal{G}$*,* $\forall D_1, D_2 \in \mathbf{Diag}^{\mathcal{G}^*}$*, there exists a monoid homomorphism* $\gamma\colon \mathcal{G}^* \to \mathcal{U}(\mathcal{H})$ *s.t.* $[\![D_1]\!]_{\text{path}} = [\![D_2]\!]_{\text{path}} \Leftrightarrow [\![\gamma(D_1)]\!]_{\text{path}} = [\![\gamma(D_2)]\!]_{\text{path}}$.

Note that a similar result has been proved in the more general[19] framework of graphical languages. Namely, it has been proved [79, 121] that an equation is a consequence of the axioms of a traced symmetric (resp. dagger compact closed) monoidal category — a structure very similar to a traced PROP (resp. a slight generalisation of this structure) — if and only if it is preserved by any interpretation of the diagrams in finite-dimensional vector (resp. Hilbert) spaces.

A stronger version of Proposition 4.10, where the homomorphism γ is independent of the diagrams, is also true, assuming the axiom of choice:

Proposition 4.11. *Given a Hilbert space* $\mathcal{H}$ *of dimension at least* 2*, and a set* $\mathcal{G}$ *of cardinality at most the cardinality of* $\mathcal{U}(\mathcal{H})$*, there exists a monoid homomorphism* $\gamma\colon \mathcal{G}^* \to \mathcal{U}(\mathcal{H})$ *s.t.* $\forall D_1, D_2 \in \mathbf{Diag}^{\mathcal{G}^*}$*,* $[\![D_1]\!]_{\text{path}} = [\![D_2]\!]_{\text{path}} \Leftrightarrow [\![\gamma(D_1)]\!]_{\text{path}} = [\![\gamma(D_2)]\!]_{\text{path}}$.

Remark 4.12. *Notice that the cardinality of* $\mathcal{U}(\mathcal{H})$ *is* $\max(2^{\aleph_0}, 2^{\dim(\mathcal{H})})$ *(where* $2^{\aleph_0}$ *is the cardinality of* $\mathbb{R}$ *and* $\dim(\mathcal{H})$ *is the Hilbert dimension of* $\mathcal{H}$*).*[20]

Proof of Propositions 4.11 and 4.10. Given a monoid homomorphism $\gamma\colon \mathcal{G}^* \to \mathcal{U}(\mathcal{H})$, a $\mathcal{G}^*$-diagram D and any c, p, one has $[\![\gamma(D)]\!]_{\text{path}}(c, p) = ((c^D_{c,p}, p^D_{c,p}), \gamma(w^D_{c,p}))$. Therefore, to prove that $\forall D_1, D_2, [\![\gamma(D_1)]\!]_{\text{path}} = [\![\gamma(D_2)]\!]_{\text{path}} \Rightarrow [\![D_1]\!]_{\text{path}} = [\![D_2]\!]_{\text{path}}$, it suffices to prove that for any two words $w_1, w_2 \in \mathcal{G}^*$, if $\gamma(w_1) = \gamma(w_2)$ then $w_1 = w_2$.

We first prove Proposition 4.11.

By Zorn's lemma, there exists a maximal family $(\alpha_i)_{i\in I}$ of $\mathbb{Q}$-algebraically independent complex numbers of absolute value 1. Such a family must have the cardinality of $\mathbb{C}$ (that is, $2^{\aleph_0}$). Indeed, the cardinality of the set of polynomials in one variable with coefficients in the field extension of $\mathbb{Q}$ generated by the α_i, is $\max(\aleph_0, \text{card}(I))$, and since each of these polynomials has finitely many roots, the set of their roots has cardinality at most $\max(\aleph_0, \text{card}(I))$. If $\text{card}(I)$ is strictly less than $2^{\aleph_0}$, then so is

[19] In the sense that proving Proposition 4.10 reduces to proving that for any two words w_1, w_2 there exists $\gamma\colon \mathcal{G}^* \to \mathcal{U}(\mathcal{H})$ s.t. $w_1 = w_2 \Leftrightarrow \gamma(w_1) = \gamma(w_2)$, and that a word can be seen as a very simple diagram consisting of just a sequence of generators. The reason why these results (in particular that of [121]) do not directly imply Proposition 4.10 is because they allow the space to depend on the diagrams given, and to be of arbitrary (finite) dimension.

[20] Indeed, an element of $\mathcal{U}(\mathcal{H})$ can be described as a matrix with rows and columns indexed by the elements of a given Hilbert basis of $\mathcal{H}$, in which the columns (and the rows) are normalised and pairwise orthogonal. Conversely, every such matrix describes a unique element of $\mathcal{U}(\mathcal{H})$. To bound the cardinality of $\mathcal{U}(\mathcal{H})$ from below, note that the possible first columns of such matrices are exactly the normalised sequences of complex numbers indexed by the chosen Hilbert basis of $\mathcal{H}$, and that the set of those sequences has cardinality $\left(2^{\aleph_0}\right)^{\dim(\mathcal{H})} = 2^{\aleph_0 \times \dim(\mathcal{H})} = \max(2^{\aleph_0}, 2^{\dim(\mathcal{H})})$. To bound it from above, note that the set of all matrices with rows and columns indexed by the chosen Hilbert basis of $\mathcal{H}$ has cardinality $\left(2^{\aleph_0}\right)^{\dim(\mathcal{H})\times\dim(\mathcal{H})} = 2^{\aleph_0 \times \dim(\mathcal{H}) \times \dim(\mathcal{H})} = \max(2^{\aleph_0}, 2^{\dim(\mathcal{H})})$.

$\max(\aleph_0, \mathrm{card}(I))$; therefore, since the set $\left\{\alpha \in \mathbb{C} \;\middle|\; |\alpha| = 1\right\}$ has cardinality $2^{\aleph_0}$, it contains an element $\alpha_\perp$ which is not a root of any of these polynomials, so that by adding $\alpha_\perp$ to the family $(\alpha_i)_{i\in I}$, we still have a family of $\mathbb{Q}$-algebraically independent complex numbers of absolute value 1, which contradicts the maximality of $(\alpha_i)_{i\in I}$.

If the cardinality of $\mathcal{G}$ is no greater than $2^{\aleph_0}$, then without loss of generality, we can assume that $\mathcal{G} \subseteq I$. We start with the case where $\mathcal{H} = \mathbb{C}^2$. We consider the function $\gamma\colon U \in \mathcal{G} \mapsto H \begin{pmatrix} 1 & 0 \\ 0 & \alpha_U \end{pmatrix}$, extended into a monoid homomorphism $\gamma\colon \mathcal{G}^* \to \mathcal{U}(\mathbb{C}^2)$ (where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$). Given two words $w_1, w_2 \in \mathcal{G}^*$ such that $w_1 \neq w_2$, the entries of $\gamma(w_1)$ and $\gamma(w_2)$ are polynomials in the α_U with coefficients in $\mathbb{Q}$. The two matrices of polynomials obtained by replacing each α_U by a variable X_U in $\gamma(w_1)$ and $\gamma(w_2)$ differ by at least one entry: indeed, by instantiating each variable X_U by either $e^{\mathrm{i}\pi/4}$ or $e^{3\mathrm{i}\pi/4}$ in such a way that the sequence of angles induced by w_1 and w_2 are different, we get two different sequences of the patterns HT and HTS with $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\mathrm{i}\pi/4} \end{pmatrix}$ and $S = T^2$, and it follows from Theorem 4.1 of [66] (which is Theorem 1(II) of [102]) that these two products of matrices have distinct values.[21] Since the α_U are algebraically independent, this implies that $\gamma(w_1) \neq \gamma(w_2)$.

Still in the case where the cardinality of $\mathcal{G}$ is no greater than $2^{\aleph_0}$, if $\mathcal{H} \neq \mathbb{C}^2$, then it suffices to consider a subspace of $\mathcal{H}$ of dimension 2, and to define for any $U \in \mathcal{G}$, $\gamma(U)$ as having matrix $H \begin{pmatrix} 1 & 0 \\ 0 & \alpha_U \end{pmatrix}$ on this subspace (in an arbitrary, fixed, othonormal basis) and as being the identity on the orthogonal complement.

If the (Hilbert) dimension of $\mathcal{H}$ is strictly greater than $\aleph_0$, then Zorn's lemma implies that $\mathcal{H}$ can be decomposed into a direct sum of $\dim(\mathcal{H})$ orthogonal subspaces of dimension 2: $\mathcal{H} = \bigoplus_{j\in J} \mathcal{H}_j$ with $\mathrm{card}(J) = \dim(\mathcal{H})$ and $\forall j, \dim(\mathcal{H}_j) = 2$. For each of the $(2^{\aleph_0})^{\dim(\mathcal{H})} = 2^{\dim(\mathcal{H})}$ possible families $(i_j)_{j\in J}$ of elements of I indexed by J, one can define a linear map $\delta((i_j)_{j\in J}) \in \mathcal{U}(\mathcal{H})$ as having matrix $H \begin{pmatrix} 1 & 0 \\ 0 & \alpha_i \end{pmatrix}$ in an arbitrary orthonormal basis of $\mathcal{H}_j$ (chosen with the help of the axiom of choice) for every j. If the cardinality of $\mathcal{G}$ is no greater than $2^{\dim(\mathcal{H})}$, then without loss of generality, we can assume that $\mathcal{G} \subseteq I^J$. We define the function $\gamma\colon \mathcal{G} \to \mathcal{U}(\mathcal{H})$ by $\forall U, \gamma(U) = \delta(U)$, and extend it into a monoid homomorphism $\gamma\colon \mathcal{G}^* \to \mathcal{U}(\mathbb{C}^2)$. Given two words $w_1, w_2 \in \mathcal{G}^*$ such that $w_1 \neq w_2$, there exists an index $j \in J$ such that the two sequence of elements of i induced by w_1 and w_2 at index j are distinct, which, by the argument given above, implies that the unitary maps on $\mathcal{H}_j$ induced respectively by $\gamma(w_1)$ and $\gamma(w_2)$ are distinct. Hence, $\gamma(w_1) \neq \gamma(w_2)$.

Finally, to prove Proposition 4.10 without using the axiom of choice, it suffices to exhibit an infinite family of $\mathbb{Q}$-algebraically independent complex numbers of absolute value 1. One can consider for example the $e^{\mathrm{i}\pi^k}$, for $k \geq 2$, whose algebraic independence follows from the Lindemann-Weierstrass theorem and the fact that π is transcendental. Given such a family, one can use a similar argument as above to prove a weaker version of Proposition 4.11 in which the cardinality of $\mathcal{G}$ is required to be at most $\aleph_0$, which immediately implies Proposition 4.10. □

4.3 Equational Theory

In this section, we introduce an equational theory which allows one to transform any M-diagram into an equivalent one. As for the PBS-calculus, we prove that it is sound, complete and minimal. The axioms are given in Figure 4.4. We call the corresponding language the CPBS-calculus (for "Coloured PBS-calculus"):

[21] Indeed, the regular expression $(HT|HTS)^*$ describes the same set of words as $\epsilon|(HT(HT|SHT)^*(\epsilon|S))$, which, since both the identity operator and S belong to the Clifford group, clearly describes a subset of the Matsumoto-Amano normal forms defined in [66] (Equation (2)).

Definition 4.13 (CPBS-calculus)**.** *Two* M*-diagrams* D_1, D_2 *are equivalent according to the rules of the* CPBS*-calculus, denoted* $\mathrm{CPBS} \vdash D_1 = D_2$*, if one can transform* D_1 *into* D_2 *using the equations given in Figure 4.4. More precisely,* $\mathrm{CPBS} \vdash \cdot = \cdot$ *is defined as the smallest congruence which satisfies equations of Figure 4.4 in addition to the axioms of coloured traced PROP.*

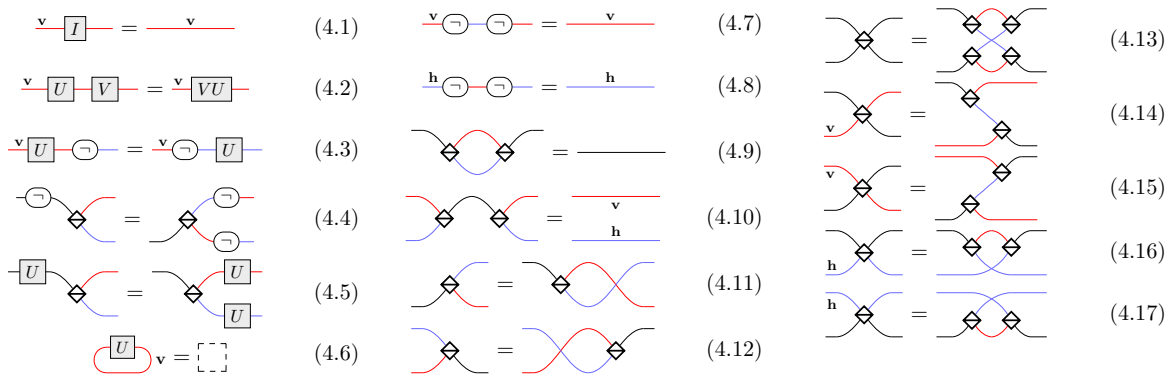


Figure 4.4: Axioms of the CPBS-calculus. $U, V \in \mathsf{M}$. Equations (4.1) and (4.2) reflect the monoid structure of M; Equations (4.3) to (4.5) show how the three generators commute; Equation (4.6) means that a disconnected diagram (with no inputs/outputs) can be removed; Equations (4.7) to (4.10) witness the fact that the negation and the 3-leg PBS are invertible; Equations (4.11) and (4.12) are essentially topological rules; Equations (4.13) to (4.17) show how 4-leg PBS can be decomposed into 3-leg PBS. Notice in particular that the other rules do not use 4-leg PBS, as a consequence one could define the language using 3-leg PBS only and see the 4-leg PBS as syntactic sugar.

Notice that the CPBS-calculus subsumes the PBS-calculus: the fragment of monochromatic (black) $\mathbb{C}^{q\times q}$-diagrams of the CPBS-calculus coincides with the set of PBS-diagrams, moreover, the completeness of both languages (see Theorem 4.18 below and Theorem 3.31) implies that for any two PBS-diagrams D_1 and D_2, $\mathrm{PBS} \vdash D_1 = D_2$ if and only if $\mathrm{CPBS} \vdash D_1 = D_2$.

Proposition 4.14 (Soundness)**.** *For any two* M*-diagrams* D_1 *and* D_2*, if* $\mathrm{CPBS} \vdash D_1 = D_2$ *then* $[\![D_1]\!]_{\mathrm{path}} = [\![D_2]\!]_{\mathrm{path}}$.

Proof. Since the semantic equality is a congruence, it suffices to check that for every equation of Figure 4.4, both sides have the same semantics, which is easy to do. □

We introduce normal forms, which will be useful to prove that the equational theory is complete, and will also play a role in optimising the number of gates in a diagram in Section 4.4.

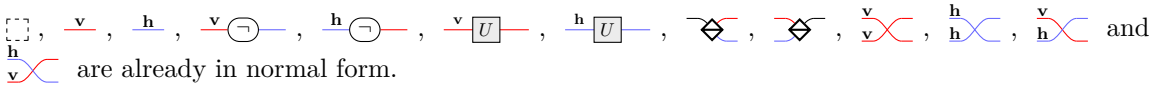
Definition 4.15. *A diagram is said to be in* normal form *if it is of the form* $M \circ P \circ F \circ G \circ S$*, where:*

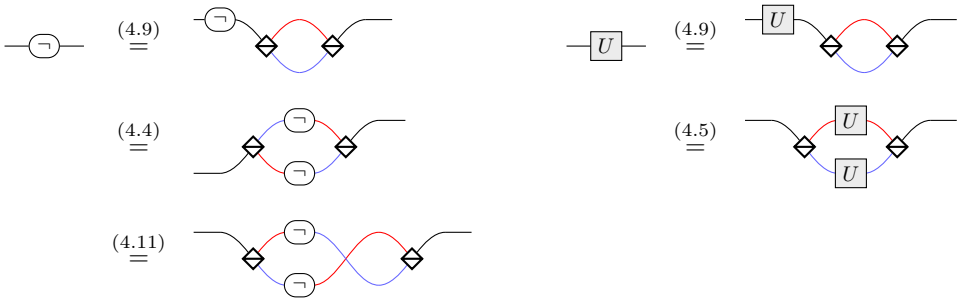
- S *is of the form* $b_1 \oplus \cdots \oplus b_n$*, where each* b_i *is either*  *or* 
- G *is of the form* $g_1 \oplus \cdots \oplus g_k$*, where each* g_i *is either*  , , *or* *, with* $U_i \neq I$
- F *is of the form* $n_1 \oplus \cdots \oplus n_k$*, where each* n_i *is either*  ,  , *or*
- P *is a permutation of the wires, that is, a trace-free diagram in which all generators are identity wires or swaps*
- M *is of the form* $w_1 \oplus \cdots \oplus w_m$*, where each* w_i *is either*  ,  *or*  .

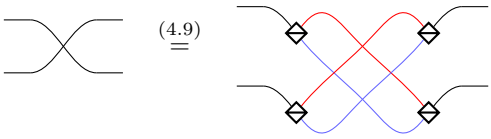
For example, the diagram shown in Figure 4.3 (right) is in normal form.

Theorem 4.16. *For any* M*-diagram* D*, there exists an* M*-diagram in normal form* N *such that* $\mathrm{CPBS} \vdash D = N$.

Proof. The proof is by structural induction on D.

- 
  and are already in normal form.
- The normal forms of  ,  ,  ,  ,  , ,  and are given by Equation (4.9), (4.11), (4.12), (4.13), (4.14), (4.15), (4.16) and (4.17) respectively.
- The normal forms of  ,  ,  ,  ,  ,  and  are obtained as follows:



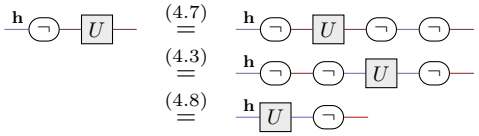


- If $D = D_1 \oplus D_2$, then by induction hypothesis there exist two diagrams in normal form N_1 and N_2 such that CPBS $\vdash D_1 = N_1$ and CPBS $\vdash D_2 = N_2$. Then CPBS $\vdash D = N_1 \oplus N_2$ and it is easy to see that $N_1 \oplus N_2$ is in normal form.
- If $D = D_2 \circ D_1$, then by induction hypothesis, let N_1 and N_2 be two diagrams in normal form such that CPBS $\vdash D_1 = N_1$ and CPBS $\vdash D_2 = N_2$. Let us decompose them as $N_1 = M_1 \circ P_1 \circ F_1 \circ G_1 \circ S_1$ and $N_2 = M_2 \circ P_2 \circ F_2 \circ G_2 \circ S_2$, following Definition 4.15. One has CPBS $\vdash D = N_2 \circ N_1 = M_2 \circ P_2 \circ F_2 \circ G_2 \circ S_2 \circ M_1 \circ P_1 \circ F_1 \circ G_1 \circ S_1$. Equation (4.10) makes $S_2 \circ M_1$ equal to a parallel composition of red and blue identity wires, so that CPBS $\vdash D = M_2 \circ P_2 \circ F_2 \circ G_2 \circ P_1 \circ F_1 \circ G_1 \circ S_1$. By naturality of the swap, one has $G_2 \circ P_1 = P_1 \circ G_2'$, where G_2' is a parallel composition of

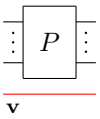
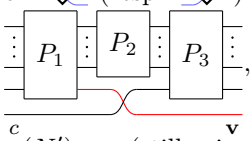
coloured non-identity gates and identity wires, obtained by permuting the "rows" of G_2. One has $(4.3), (4.18) \vdash G_2' \circ F_1 = F_1 \circ G_2''$, where G_2'' is obtained by changing some colours in G_2', and Equation (4.18) is the following variant of Equation (4.3):

(4.18)

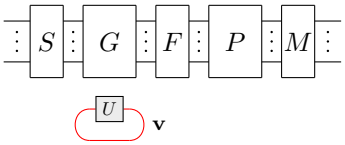
which is derived from the equations of Figure 4.4 as follows:

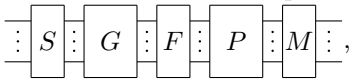


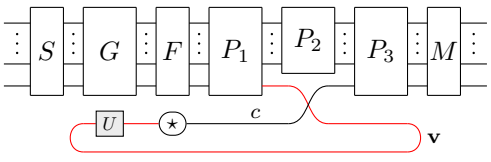
Thus, CPBS $\vdash D = M_2 \circ P_2 \circ F_2 \circ P_1 \circ F_1 \circ G_2'' \circ G_1 \circ S_1$. By naturality of the swap, one has $F_2 \circ P_1 = P_1 \circ F_2'$, where F_2' is a parallel composition of coloured identities and negations (obtained by permuting F_2). One has $(4.7), (4.8) \vdash F_2' \circ F_1 = F''$, where F'' is obtained by removing all double negations in $F_2' \circ F_1$. Finally, $(4.2), (4.1) \vdash G_2'' \circ G_1 = G'''$, where G''' is still a parallel composition of coloured non-identity gates and identity wires. Thus, CPBS $\vdash D = M_2 \circ (P_2 \circ P_1) \circ F'' \circ G''' \circ S_1$, with S_1, G''', F'', $(P_2 \circ P_1)$ and M_2 respectively of the forms described in Definition 4.15, so that their composition is in normal form. This gives us the result.

- If $D = Tr_{\mathbf{v}}(D') : a \to b$, then by induction hypothesis, let N' be a diagram in normal form such that CPBS $\vdash D' = N'$. Let us decompose it as $N' = M' \circ P' \circ F' \circ G' \circ S'$, following Definition 4.15. Since N' is of type $a \oplus \mathbf{v} \to b \oplus \mathbf{v}$, S' (resp. M') is of the form $S \oplus$  (resp. $M \oplus$) where S (resp. M) is a parallel composition of coloured identity wires and copies of  (resp.). Using the structural congruence, one can write P' in the form  or  ,

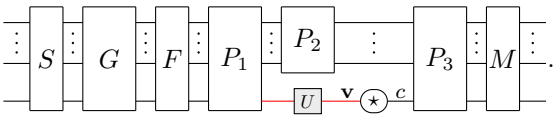
where P, or P_1, P_2 and P_3, are permutations of the wires. In the first case, $Tr_{\mathbf{v}}(N')$ can (still using the structural congruence) be written in the form



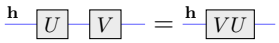
with S, G, F, P and M of the forms demanded by Definition 4.15 (in particular, F' cannot have a negation on its bottom wire since this would prevent N' from being of type $a \oplus \mathbf{v} \to b \oplus \mathbf{v}$), so that $(4.6) \vdash Tr_{\mathbf{v}}(N') =$  , which is in normal form. In the second case, $Tr_{\mathbf{v}}(N')$ can be written in the form



where  is either or . Then using the structural congruence (in particular the yanking axiom), one can write it in the form



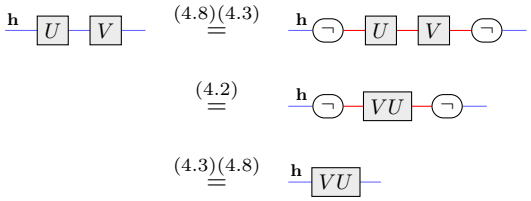
By naturality of the swap, one can slide the gate U and the possible negation through P_1. Then, possibly using Equation (4.18), one can move the gate U to the other side of F. Finally, it may remain to merge U with a gate of G using Equation (4.2) or its following variant:



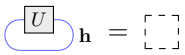
(4.19)

and/or to remove a double negation using Equation (4.8). Then one gets a diagram in normal form.

Equation (4.19) is derived from the equations of Figure 4.4 as follows:

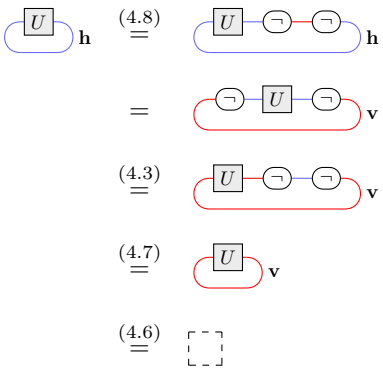


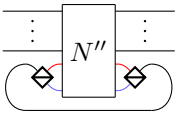
- The case $D = Tr_{\mathbf{h}}(D') : a \to b$ is analogous to the previous case. Instead of using Equations (4.3) and (4.6)one uses respectively Equation (4.18) and the following variant of Equation (4.6):

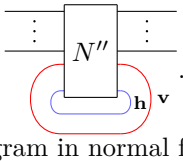


(4.20)

which is derived from the equations of Figure 4.4 as follows:



- If $D = Tr_{\top}(D') : a \to b$, then by induction hypothesis, let N' be a diagram in normal form such that CPBS $\vdash D' = N'$. $Tr_{\top}(N')$ can be written in the form 

, which by dinaturality and Equation (4.10), can be transformed into 

. It suffices then to proceed successively as in the two preceding cases to get a diagram in normal form. □

Note that the structure of the normal form as well as the proof of Theorem 4.16 use in an essential way the removal of useless wires made possible by the use of colours, and in particular Equation (4.10), which has no equivalent in the monochromatic PBS-calculus of Chapter 3. An example of a diagram and its normal form are given in Figure 4.5.

Now we use the normal form to prove the completeness of the CPBS-calculus:

Figure 4.5: An example of a diagram (*left*) and its equivalent diagram in normal form (*right*).

Lemma 4.17 (Uniqueness of the normal form)**.** *For any two diagrams in normal form N and N', if $[\![N]\!]_{\text{path}} = [\![N']\!]_{\text{path}}$ then $N = N'$.*

Proof. If $[\![N]\!]_{\text{path}} = [\![N']\!]_{\text{path}}$, then in particular N and N' have same type: $N, N' : a \to b$ for some a, b.

Let us decompose N and N' into $N = M \circ P \circ F \circ G \circ S$ and $N' = M' \circ P' \circ F' \circ G' \circ S'$.

It follows directly from the definition that S and S' are uniquely determined by their input type, so that since they both have input type a, $S = S'$. Similarly, M and M' are uniquely determined by their output type, so that since they both have output type b, $M = M'$.

Let S^{-1} and M^{-1} be the horizontal reflections of respectively S and M, that is, the diagrams obtained by replacing  by in S and by in M. One has (4.10) $\vdash M^{-1} \circ N \circ S^{-1} = P \circ F \circ G$ and (4.10) $\vdash M^{-1} \circ N' \circ S^{-1} = P' \circ F' \circ G'$, so that by Proposition 4.14, $[\![M^{-1} \circ N \circ S^{-1}]\!]_{\text{path}} = [\![P \circ F \circ G]\!]_{\text{path}} = [\![M^{-1} \circ N' \circ S^{-1}]\!]_{\text{path}} = [\![P' \circ F' \circ G']\!]_{\text{path}}$. For any c, p, one has $[\![P \circ F \circ G]\!]_{\text{path}}(c,p) = ((c^F_{c,p}, p^P_{c,p}), U^G_{c,p})$ and $[\![P' \circ F' \circ G']\!]_{\text{path}}(c,p) = ((c^{F'}_{c,p}, p^{P'}_{c,p}), U^{G'}_{c,p})$, so that $U^G_{c,p} = U^{G'}_{c,p}$, $c^F_{c,p} = c^{F'}_{c,p}$ and $p^P_{c,p} = p^{P'}_{c,p}$. Because of their respective forms required by Definition 4.15, G, G', F, F', P and P' are uniquely determined by the family of, respectively, the $U^G_{c,p}$, the $U^{G'}_{c,p}$, the $c^F_{c,p}$, the $c^{F'}_{c,p}$, the $p^P_{c,p}$, and the $p^{P'}_{c,p}$. Hence, $G = G'$, $F = F'$ and $P = P'$. □

Theorem 4.18 (Completeness)**.** *Given any two* M*-diagrams D_1 and D_2, if $[\![D_1]\!]_{\text{path}} = [\![D_2]\!]_{\text{path}}$ then* CPBS $\vdash D_1 = D_2$.

Proof. By Theorem 4.16, there exist N_1, N_2 in normal form such that CPBS $\vdash D_1 = N_1$ and CPBS $\vdash D_2 = N_2$. By Proposition 4.14, $[\![N_1]\!]_{\text{path}} = [\![D_1]\!]_{\text{path}} = [\![D_2]\!]_{\text{path}} = [\![N_2]\!]_{\text{path}}$. Therefore, by Lemma 4.17, $N_1 = N_2$. By transitivity, this proves that CPBS $\vdash D_1 = D_2$. □

Finally, each equation of Figure 4.4 is necessary for the completeness:

Theorem 4.19 (Minimality)**.** *None of the equations of Figure 4.4 is a consequence of the others.*

Proof. For

- each of Equations (4.1), (4.4) and (4.7) to (4.17)
- each instance of Equations (4.3) and (4.5)
- the class of all instances of Equation (4.2) without I gates in the left-hand side
- each class of instances of Equation (4.6) given by an equivalence class of elements of M for the equivalence relation $\sim^*_{\text{conj}}$, defined as the transitive closure of $\sim_{\text{conj}}$, itself defined by $U \sim_{\text{conj}} V$ if there exist $W, T \in \mathsf{M}$ such that $U = WT$ and $V = TW$

we give an invariant that is satisfied by exactly one side of the considered equation (or of each element of the considered class of instances of Equation (4.2) or (4.6)), and such that for any diagram D, applying any other equation or instance inside D (that is, replacing a sub-diagram of D that matches one side of the equation by the other side) preserves the fact that D satisfies the invariant or not. In each case, this proves that the equations that break the invariant are not consequences of those that preserve it in any diagram.

Note that the instances of Equation (4.2) with an I gate in the left-hand side are consequences of Equation (4.1), and that the elements of a class of instances of Equation (4.6) are consequences of any particular instance of Equation (4.6) of the same class together with Equation (4.2).

- For Equation (4.1), the invariant is that at least one gate can be reached by a particle from an input wire.
- For the class of all instances of Equation (4.2) without I gates in the left-hand side, the invariant is the maximum number of non-I gates that a particle coming from an input wire can traverse along its path in the diagram.
- For each instance of Equation (4.3) given by a particular U, the invariant is that all gates labelled with U are red.
- For Equation (4.4), the invariant is that the diagram contains a (black)  .
- For each instance of Equation (4.5) given by a particular U, the invariant is that the diagram contains a (black)  .
- For each class of instances of Equation (4.6), the invariant is that there exists a wire in the diagram and a polarisation **V** or **H** such that the path of a particle starting from this wire with this polarisation is a closed loop, and that the product of the labels of the gates traversed by the particle before getting back to its starting point with its initial polarisation for the first time, is an element of the equivalence class (note that this does not depend on the choice of the starting point).
- For Equation (4.7), the invariant is that all wires are red.
- For Equation (4.8), the invariant is that no particle entering the diagram by a blue input wire can reach the output without passing through a negation at some point in the diagram. Note that Equation (4.7) cannot change this invariant because in order to reach a red wire, the particle coming from a blue wire has to get its polarisation changed, and therefore to pass through a negation.
- For Equation (4.9), the invariant is that all wires are black and the diagram is non-empty and does not contain any  .
- For Equation (4.10), the invariant is that the diagram contains at least one black wire.
- For Equation (4.11), the invariant is that the diagram contains at least one generator among  ,  ,  , and .
- For Equation (4.12), the invariant is that the diagram contains at least one generator among , , and .
- For Equation (4.13), the invariant is that the diagram contains a .
- For Equation (4.14), the invariant is that the diagram contains a  .
- For Equation (4.15), the invariant is that the diagram contains a  .
- For Equation (4.16), the invariant is that the diagram contains a .
- For Equation (4.17), the invariant is that the diagram contains a  . □

4.4 Resource Optimisation

We show in this section that the equational theory of the CPBS-calculus can be used for resource optimisation.

4.4.1 Minimising the Number of Oracle Queries

We consider the problem of minimising the number of oracle queries: given a set $\mathcal{G}$ of (distinct) oracles and a $\mathcal{G}^*$-diagram D, the objective is to find a diagram D' equivalent to D (i.e. $[\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}}$) such that D' uses a minimal number of queries to each oracle. Since there are several oracles, the definition of the optimal diagrams should be made precise.

First, we define the number of queries to a given oracle:

Definition 4.20. *Given a $\mathcal{G}^*$-diagram D, for any $U \in \mathcal{G}$, let $\#_U(D)$ be the number of queries to U in D, inductively defined as follows: $\#_U(\overset{a}{\boxed{w}}) = |w|_U$, $\#_U(g) = 0$ for all the other generators, $\#_U(D_1 \oplus D_2) = \#_U(D_2 \circ D_1) = \#_U(D_1) + \#_U(D_2)$, and $\#_U(Tr_a(D)) = \#_U(D)$, where $|w|_U$ is the number of occurrences of U in the word $w \in \mathcal{G}^*$.*

We can now define a query-optimal diagram as follows:

Definition 4.21. *A $\mathcal{G}^*$-diagram D is query-optimal if $\forall D' \in \mathbf{Diag}^{\mathcal{G}^*}$, $\forall U \in \mathcal{G}$, $[\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}}$ implies $\#_U(D) \leq \#_U(D')$.*

Note that given a diagram, it is not *a priori* guaranteed that there exists an equivalent diagram which is query-optimal: for instance, it might be that all the diagrams which minimise the number of queries to some oracle U do not minimise the number of queries to another oracle V. However, we actually show (Proposition 4.23) that any diagram can be turned into a query-optimal one. To this end, we first need a lower bound on the number of queries to a given oracle:

Proposition 4.22 (Lower bound)**.** *For any $\mathcal{G}^*$-diagram $D : a \to b$ and any $U \in \mathcal{G}$, $\#_U(D) \geq \left\lceil \sum_{(c,p)\in[a]} \frac{|w^D_{c,p}|_U}{2} \right\rceil$ where $w^D_{c,p} \in \mathcal{G}^*$ is such that $[\![D]\!]_{\text{path}}(c,p) = ((c',p'), w^D_{c,p})$.*

Proof. Note that each gate $\overset{a}{\boxed{w}}$ of the diagram D is used at most twice according to the semantics,[22] in other words, there are either at most two pairs (c,p), (c',p') such that w contributes once to $w^D_{c,p}$ and once to $w^D_{c',p'}$; or at most a single pair (c,p) such that w contributes twice to $w^D_{c,p}$. As a consequence, $\sum_{(c,p)\in[a]} |w^D_{c,p}|_U \leq 2\#_U(D)$, which leads to the lower bound. □

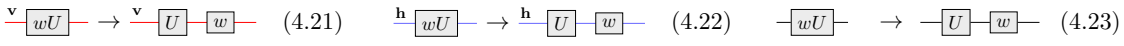
Note that Proposition 4.22 provides a lower bound on the minimal number of queries to U one can reach in optimising a diagram since the right-hand side of the inequality only depends on the semantics of the diagram.

We are now ready to introduce an optimisation procedure that transforms any diagram into an equivalent query-optimal one:

Query optimisation procedure of a $\mathcal{G}^*$-diagram D:

1. Transform D into its normal form D_{NF}. A recursive procedure for doing this can easily be deduced from the proof of Theorem 4.16.

2. Split all gates into elementary gates (that is, gates whose label is a single letter), using the following variants of Equation (4.2), which are consequences of the equations of Figure 4.4 (see Appendix B.1): $\forall U \in \mathcal{G}$, $\forall w \in \mathcal{G}^*$, $w \neq I$:



3. As long as the diagram contains two non-black gates with the same label, merge them. To do so, deform the diagram to put one over the other, and apply one of the following equations, which are also consequences of the equations of Figure 4.4:

[22] This can be stated more formally by replacing the contents of the gates by distinct names in order to get a (coloured) bare diagram (see Section 7.1.1), and then proved in a similar way as Proposition 7.3.

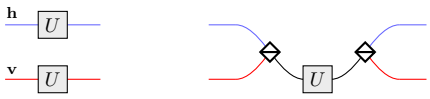
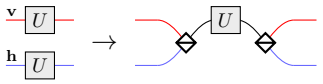
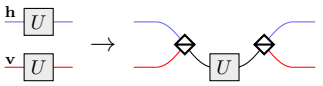


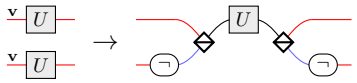
Figure 4.6: Two equivalent diagrams: the diagram on the left is optimal in terms of number of polarising beam splitters, the diagram on the right is optimal in terms of queries. Note that there is no equivalent diagram with no polarising beam splitter and at most a single query.



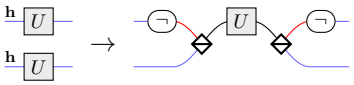
(4.24)



(4.25)



(4.26)



(4.27)

An example of query-optimised diagram is given in Figure 4.9. The query-optimisation procedure transforms any diagram into an equivalent query-optimal one:

Proposition 4.23. *The diagram D_0 output by the query optimisation procedure is query-optimal: for any U and any D' s.t. $[\![D']\!]_{\text{path}} = [\![D_0]\!]_{\text{path}}$, one has $\#_U(D_0) \leq \#_U(D')$.*

Proof. Note that in D_{NF}, for each gate there is one and only one input state (c, p) which goes to this gate. As a consequence $\forall U, \#_U(D_{NF}) = \sum_{(c,p)\in[a]} |w^D_{c,p}|_U$ (where $D_{NF} : a \to b$). Moreover $\forall U, \#_U(D_0) = \left\lceil \frac{\#_U(D_{NF})}{2} \right\rceil$, thus D_0 meets the lower bound of Proposition 4.22 and hence is query-optimal. □

Note that the query-optimisation procedure is efficient: one can naturally define the size $|D|$ of a diagram $D \in \mathbf{Diag}^{\mathcal{G}^*}$ as follows: $|\overset{a}{\boxed{w}}| = |w|$, $|g| = 1$ for all the other generators, $|D_1 \oplus D_2| = |D_2 \circ D_1| = |D_1| + |D_2|$, and $|Tr_a(D)| = |D| + 1$. Step 1 of the procedure, which consists in putting the diagram in normal form, can be done using a number of elementary equations of Figure 4.4 which is quadratic in the size of the diagram, the other two steps being linear. Notice that here we only count the number of basic equations. The procedure also requires some diagrammatic transformations (that is, deformations), which can be handled efficiently (more precisely, at most in quadratic time) using appropriate data structures.

4.4.2 Optimising Both Queries and PBS

We refine the resource optimisation of a diagram by considering not only the number of queries but also the number of instructions, and in particular the number of polarising beam splitters. Note that the number of beam splitters and the number of queries cannot be minimised independently, in the sense that there might not exist a diagram that is both query-optimal and PBS-optimal (see such an example in Figure 4.6). As the implementation of an oracle is *a priori* more expensive than the implementation of a single PBS, we optimise the number of queries and then the number of PBS in this order, i.e. the measure of complexity is the lexicographic order number of queries, number of polarising beam splitters.

Definition 4.24. *A diagram D is query-PBS-optimal if D is query-optimal and for any query-optimal diagram D' equivalent to D (i.e. $[\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}}$), $\#_{\text{PBS}}(D) \leq \#_{\text{PBS}}(D')$, where $\#_{\text{PBS}}(D)$ be the number of PBS of D.*

We introduce an efficient heuristic, called *PGT procedure* that, when applied on a query-optimal diagram D_0, preserves the number of queries. The produced diagram, called in PGT form (see Figure 4.7), contains at most as many PBS as the original diagram, and moreover is query-PBS-optimal when there is at most one query to each oracle (see Proposition 4.30 and Theorem 4.31).[23]

[23] At least if the gates used only once are represented as coloured gates, which is the case in the diagrams output by the query optimisation procedure, see Remark 4.32.

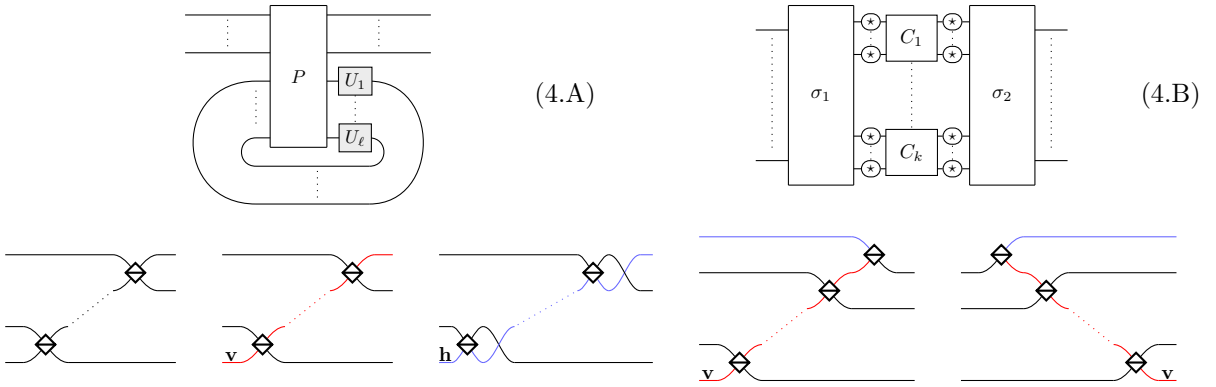
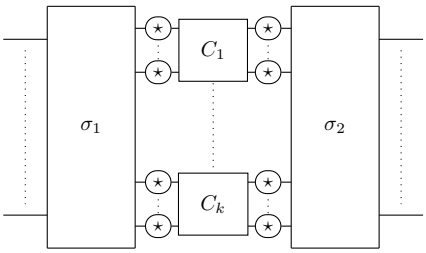


Figure 4.7: Schematic description of a diagram in PGT form (for Permutation, Gates and Traces). A diagram is in PGT form if it is of the form (4.A), with P of the form (4.B), and the C_i of the forms depicted on the second line. -⟨⋆⟩- denotes either —^{a}— or —^{a}⟨¬⟩— with $a \in \{\mathbf{v}, \mathbf{h}\}$, and σ_1, σ_2 are permutations of the wires.

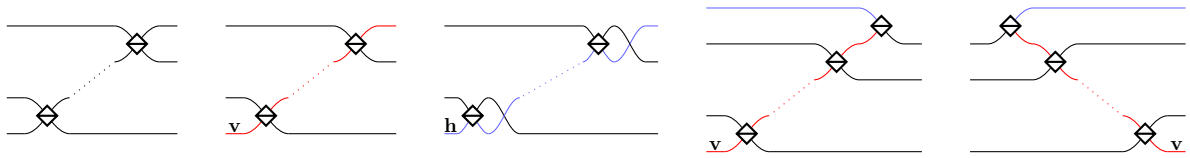
More precisely, the PGT procedure consists in putting D_0 in the so-called PGT form, which we prove to contain few PBS. First, we consider query-free diagrams:

Definition 4.25. *A diagram D is in* stair form *if it is of the form*



(4.B)

where σ_1 and σ_2 are permutations of the wires, -⟨⋆⟩- denotes either —^{a}— or —^{a}⟨¬⟩— with $a \in \{\mathbf{v}, \mathbf{h}\}$, and $C_1, ..., C_k$ are each of one of the following forms:



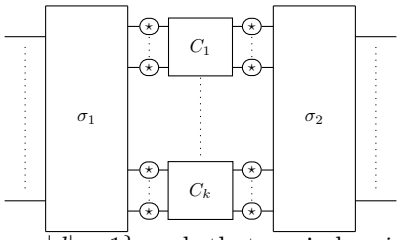
The diagrams of these forms will be called staircases. *The C_i will be called the staircases of D.*

Remark 4.26. *Note that in the diagram* (4.B)*, all wires can be of arbitrary colours. We did not represent the labels in order to not overload the figures.*

Diagrams in stair form are optimal in terms of number of polarising beam splitters:

Theorem 4.27. *Any diagram $D : a \to b$ in stair form is PBS-optimal (that is, for any diagram $D' : a \to b$, $[\![D]\!]_{\text{path}} = [\![D']\!]_{\text{path}} \Rightarrow \#_{\text{PBS}}(D) \leq \#_{\text{PBS}}(D')$).*

Proof. Given any gate-free diagram $Q : d \to e$, we denote by $\{d_i^Q\}_{i=1,...,k_Q}$ the finest partition of $\{0, ..., |d| - 1\}$ such that there exists a partition $\{e_i^Q\}_{i=1,...,k_Q}$ of $\{0, ..., |e| - 1\}$ satisfying $\forall i, \forall c, p, (p \in d_i^Q \Leftrightarrow p_{c,p}^P \in e_i^Q)$. It is easy to see that the partition $\{e_i^Q\}_{i=1,...,k_Q}$ is unique and that symmetrically, it is the finest partition of $\{0, ..., |e| - 1\}$ such that there exists a partition $\{f_i^Q\}_{i=1,...,k_Q}$ of $\{0, ..., |d| - 1\}$ satisfying $\forall i, \forall c, p, (p \in f_i^Q \Leftrightarrow p_{c,p}^P \in e_i^Q)$ (which of course implies that $\forall i, f_i^Q = d_i^Q$).

Given $P =$ 

$: d \to e$ a diagram in stair form, let $\{d_i\}_{i=1,...,k}$ be the partition of $\{0, ..., |d| - 1\}$ such that an index j is in d_i if the input wire of P of index j is connected to C_i. Similarly, let $\{e_i\}_{i=1,...,k}$ be the partition of $\{0, ..., |e| - 1\}$ such that an index j is in e_i if the output wire of P of index j is connected to C_i. One has $\forall i, \forall c, p, (p \in d_i \Leftrightarrow p^P_{c,p} \in e_i)$. It is easy to see that $\{d_i\}_{i=1,...,k}$ is the finest partition of $\{0, ..., |d| - 1\}$ such that there exists $\{e_i\}_{i=1,...,k}$ satisfying this property, that is, up to reordering the partitions, one has $k = k_P$ and $\forall i, d_i = d^P_i$ and $e_i = e^P_i$.

Again given an arbitrary gate-free diagram $Q : d \to e$, let us decompose $d = x_1 \oplus \cdots \oplus x_n$ and $e = y_1 \oplus \cdots \oplus y_m$, with $\forall j, x_j, y_j \in \{\mathbf{v}, \mathbf{h}, \top\}$. Since any gate-free diagram is equivalent to a diagram in stair form (indeed, by applying Steps 2 to 7 of the PGT procedure described below — which does not rely on Theorem 4.27 — one can put any gate-free diagram in stair form), the preceding paragraph, because of the input/output types of the five kinds of staircases, implies that for every i there are four cases:

1. $\left|d^Q_i\right| = \left|e^Q_i\right|, \quad \forall j \in d^Q_i, x_j = \top \quad \text{and} \quad \forall j \in e^Q_i, y_j = \top$
2. $\left|d^Q_i\right| = \left|e^Q_i\right|$ and exactly one element of d^Q_i and one element of e^Q_i are not equal to $\top$
3. $\left|d^Q_i\right| = \left|e^Q_i\right| + 1, \quad \forall j \in e^Q_i, y_j = \top$ and exactly two elements of d^Q_i are not equal to $\top$
4. $\left|e^Q_i\right| = \left|d^Q_i\right| + 1, \quad \forall j \in d^Q_i, x_j = \top$ and exactly two elements of e^Q_i are not equal to $\top$

We denote by $s_L(Q)$ the number of indices i for which we are in Case 3.

Moreover, by examining more in details the semantics of the five kinds of staircases, one can show that for every index $i \in \{1, ..., k_Q\}$, there exists two bijections $\rho_i \colon \mathbb{Z}/\left(\left|d^Q_i\right|\mathbb{Z}\right) \to d^Q_i$ and $\tau_i \colon \mathbb{Z}/\left(\left|e^Q_i\right|\mathbb{Z}\right) \to e^Q_i$ such that for any $p \in \{1, ..., |d^Q_i|\}$, if $(\mathbf{V}, \rho_i(\pi(p))) \in [d]$ then $(Q, \mathbf{V}, \rho_i(\pi(p))) \Rightarrow \left(c^Q_{\mathbf{V},\rho_i(\pi(p))}, \tau_i(\pi(p))\right)$, and if $(\mathbf{H}, \rho_i(\pi(p))) \in [d]$ then $(Q, \mathbf{H}, \rho_i(\pi(p))) \Rightarrow \left(c^Q_{\mathbf{H},\rho_i(\pi(p))}, \tau_i(\pi(p+1))\right)$, where $\pi \colon \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ denotes the canonical projection.

Concrete instances of the bijections ρ_i and τ_i can be built by starting from any element $j \in d^Q_i$ and defining $\rho_i(1) = x$. Then, the properties of ρ_i and τ_i imply that knowing the path semantics of Q, for any $p \in \mathbb{Z}/\left(\left|d^Q_i\right|\mathbb{Z}\right)$, the data of $\rho_i(p)$ uniquely determines $\tau_i(p)$ and $\tau_i(p+1)$, and the data of $\tau_i(p)$ uniquely determines $\rho_i(p)$ and $\rho_i(p-1)$, so that ρ_i and τ_i can be built incrementally.

It is easy to see that given a diagram in stair form $P : d \to e$, one has $\#_{\mathrm{PBS}}(P) = |e| - k_P + s_L(P)$. In the rest of this proof, our goal is to prove that for any gate-free diagram $Q : d \to e$, one has $\#_{\mathrm{PBS}}(Q) \geq |e| - k_Q + s_L(Q)$. Then, since $|e| - k_Q + s_L(Q)$ only depends on the semantics of Q, and diagrams in stair form reach this lower bound, this will imply that they are PBS-optimal.

Since any gate-free diagram $Q : d \to e$ can be deformed into a diagram of the form (4.A) with P trace-free, it suffices to prove, on the one hand, that the inequality holds for trace-free diagrams, and on the other hand, that it is preserved by the trace operation.

To prove that the trace preserves the inequality, given a gate-free diagram $Q : d \oplus a \to e \oplus a$ with $a \in \{\mathbf{v}, \mathbf{h}, \top\}$, it suffices to consider the sets d^Q_i and e^Q_j that contain the index of the bottom input (resp. output) wire, and to examine the possible cases (essentially, whether $i = j$, to which of the four cases described above the pairs (d^Q_i, e^Q_i) and (d^Q_j, e^Q_j) correspond, and whether the traced wire has type $\top$ or

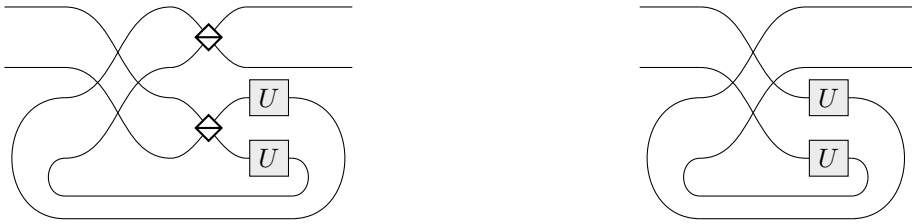
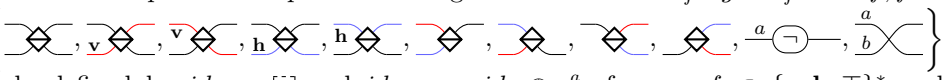


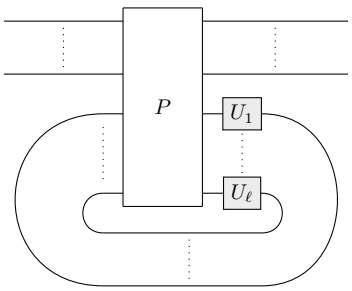
Figure 4.8: [*Left*] An example of diagram in PGT form which is optimal in the number of queries but not in the number of polarising beam splitters. Indeed it is equivalent to the diagram on the right which is query-optimal and PBS-free.

not). In each case, it suffices to build the bijections ρ_i and τ_i and to look at the effect of applying the trace.

To prove that it holds for trace-free diagrams, we remark that up to deformation, a trace-free (gate-free) diagram can be written as a sequential composition of diagrams of the form $id_f \oplus g \oplus id_{f'}$ with $f, f' \in \{\mathbf{v}, \mathbf{h}, \top\}^*$ and $g \in$  (where id_f is inductively defined by $id_\epsilon = \boxed{\ }$ and $id_{f\oplus a} = id_f \oplus \overset{a}{—}$ for any $f \in \{\mathbf{v}, \mathbf{h}, \top\}^*$ and $a \in \{\mathbf{v}, \mathbf{h}, \top\}$). We call such diagrams *layers*. Then we proceed by induction on the number of layers. The base case is that of an identity diagram $id_d : d \to d$, for which $k_{id_d} = |d|$ and $S_L(id_d) = 0$, so that the inequality holds. It remains to prove that given any trace-free diagram $Q : d \to e$ satisfying the inequality, and any layer $id_f \oplus g \oplus id_{f'}$ of input type e, the composition $(id_f \oplus g \oplus id_{f'}) \circ Q$ still satisfies the inequality. This can be done by considering the set(s) e_i^Q and e_j^Q that contain the indice(s) of the wire(s) of Q where g is plugged (together with the corresponding d_i^Q and d_j^Q), and examining the possible cases. In each case, it suffices to build the bijections ρ_i and τ_i and to look at the effect of appending the layer $(id_f \oplus g \oplus id_{f'})$. □

We extend the stair form to diagrams with queries as follows, leading to the PGT form (for Permutation/Gates/Traces):

Definition 4.28. *A $\mathcal{G}^*$-diagram is in* PGT form *(for Permutation, Gates and Traces) if it is of the form*



(4.A)

where P is in stair form and $U_1, ..., U_\ell \in \mathcal{G}$.

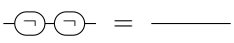
Remark 4.29. *Like in the diagram* (4.B)*, all wires of* (4.A) *can be of arbitrary colours.*

Contrary to the stair form, the PGT form is not optimal (see as an example Figure 4.8). Intuitively, if there are several queries to an oracle U, then decomposing the corresponding gates into blue and red gates and then recomposing them in a different way may lead to a diagram with a smaller number of PBS. However, we will prove that applying the PGT procedure after the query optimisation procedure gives us a query-PBS-optimal diagram when there is at most one query to each oracle (see Theorem 4.31).

The procedure relies on equations of Figure 4.4, together with easy to derive variants of these equations. The derivations of the additional equations are given in Appendix B.2.

PGT procedure: Given a query-optimal diagram D_0:

0. During the whole procedure, every time there are two consecutive negations, we remove them using Equation (4.7), (4.8) or their all-black version:

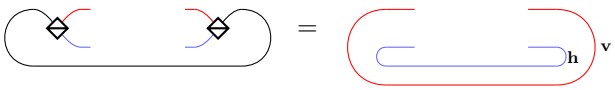


(4.28)

1. Deform D_0 to put it in the form (4.A) with P gate-free. The goal of the following steps is to put P in stair form.

2. Split all PBS of the form  into combinations of  ,  ,  and  , using Equations (4.13) to (4.17).

3. As long as there are two PBS connected by a black wire, with possibly a black negation on this wire, push this negation out (if present) using Equation (4.4), and cancel the PBS together using Equation (4.10). It may be necessary to flip the PBS upside down using Equation (4.11) and/or (4.12) in order to be able to apply Equations (4.4) and (4.10). Note also that to cancel the two PBS together one may have to use dinaturality:



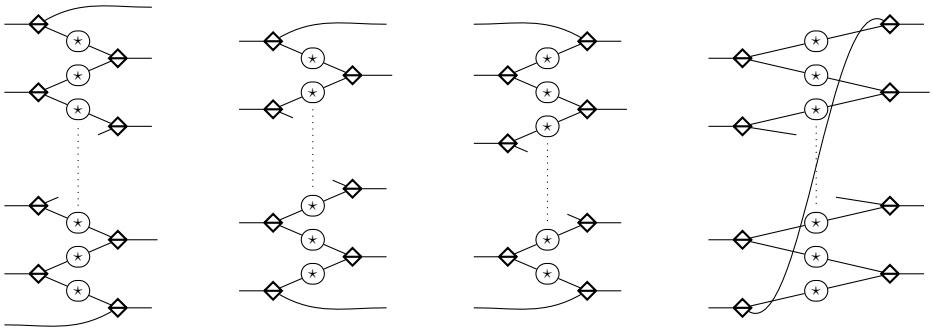
When there are not two such PBS anymore, all black wires are connected to at least one side of P (possibly through negations), and the PBS are connected together with red and blue wires with possibly negations on them.

4. Remove all loops using the following equations:

(4.29) (4.30) (4.31) (4.32)

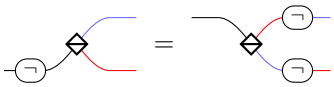
Note that since D_0 is query-optimal, there cannot be loops containing gates at this point.

5. Deform P to put it in the form (4.B) with σ_1 and σ_2 being wire permutations and the C_i being trace-free and connected. It remains to transform the C_i into staircases. Up to additional deformation of P in order to reorder the input and output wires of the C_i, and to using Equations (4.11) and (4.12), every C_i is of one of the following forms:

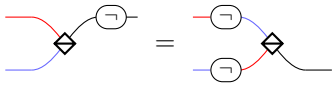


where  is either  or  with $a \in \{\mathbf{v}, \mathbf{h}\}$,  is either  or  and  is either  or  .

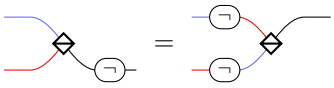
6. Remove the negations in the middle of the C_i by pushing them to the bottom by means of Equation (4.4) and its following variants (all of the form "a three-wire PBS with a negation on one of the three wires is equal to this PBS reflected vertically with negations on the other two wires"; note that Equations (4.4), (4.33), (4.34) and (4.35) have to be applied from right to left, while Equations (4.36), (4.37), (4.38) and (4.39) have to be applied from left to right):



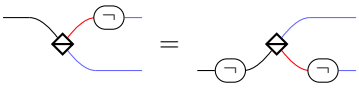
(4.33)



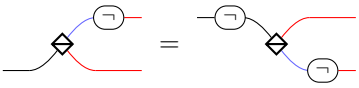
(4.34)



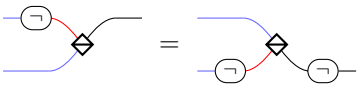
(4.35)



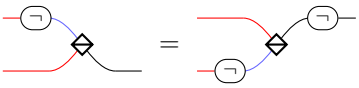
(4.36)



(4.37)

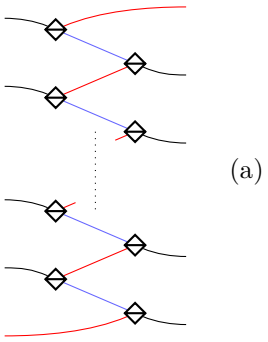


(4.38)

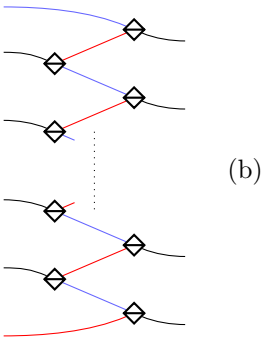


(4.39)

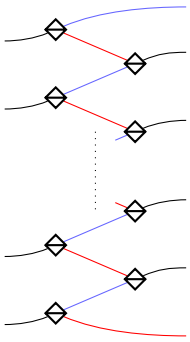
7. Up to deforming P in order to flip the C_i upside down, and to using Equations (4.11) and (4.12) wherever necessary, every C_i is now of one of the following forms (note that it is easy to know of which form each C_i should be, before deforming it, by looking at its input/output type):



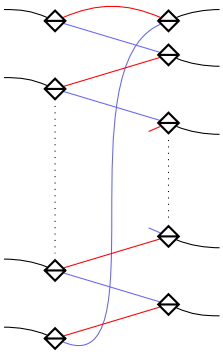
(a)



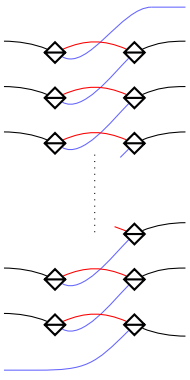
(b)



(c)



(d)



(e)

Transform each of them into one of the five kind of staircases depicted in Definition 4.25, depending

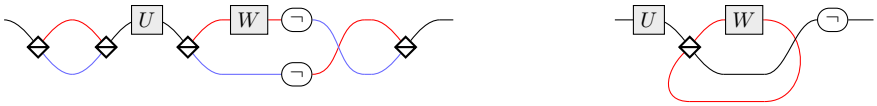
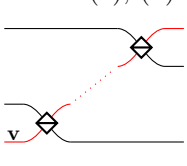
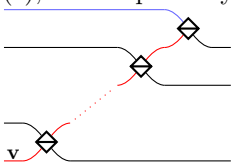
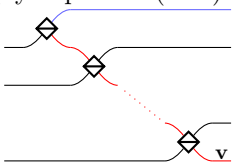
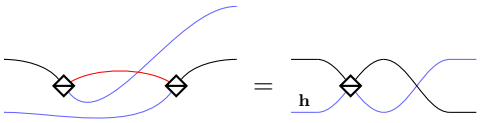


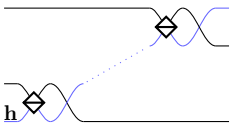
Figure 4.9: The diagram on the left is the obtained by applying the query-optimisation procedure on the example of Figure 4.5. The diagram on the right is (up to deformation) obtained by applying the PGT procedure to the diagram on the left. Note that this diagram is both query- and PBS-optimal.

on its type:

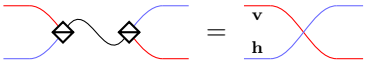
- If C_i is of the form (a), (b) or (c), then repeatedly apply Equation (4.14) or (4.15) to put it in the form  ,  or  respectively.
- If C_i is of the form (e), then repeatedly apply the following equation:



(4.40)

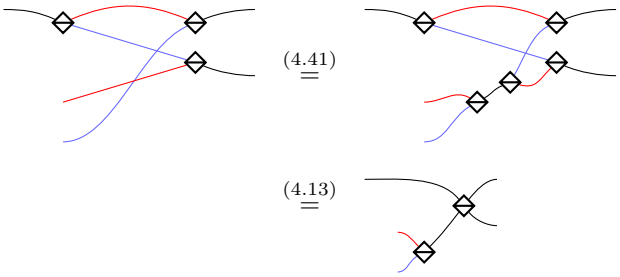
to put it in the form  .

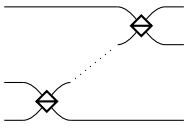
- If C_i is of the form (d), then repeatedly apply the following variant of Equation (4.10):



(4.41)

and Equation (4.13), as follows:



and finally apply Equation (4.9) once, in order to put it in the form  .

This gives us the desired diagram D_1 and finishes the procedure.

An example of diagram produced by the PGT procedure is given in Figure 4.9.

Since the PGT procedure consists in putting a subdiagram of D_0 in stair form (except Step 1 which is just deformation and does not change the number of PBS), Theorem 4.27 implies in particular that this procedure does not increase the number of PBS in D_0:

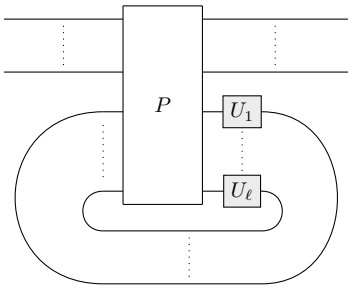
Proposition 4.30. *The diagram D_1 output by the PGT procedure contains at most as many PBS as the initial diagram D_0.*

This also implies that given any diagram D, there exists an equivalent query-PBS-optimal diagram in PGT form. Indeed, by Proposition 4.23, there exist query-optimal diagrams equivalent to D, and among these diagrams, some of them have minimal number of PBS and are therefore query-PBS-optimal. Finally, applying the PGT procedure to one of these diagrams gives us an equivalent diagram in PGT form, which, since the PGT procedure does not change the gates or increase the number of PBS, is still query-PBS-optimal.

Applying the PGT procedure after the query optimisation procedure produces an interesting heuristic: the output diagram is necessarily query-optimal and, although it is not necessarily query-PBS-optimal in general, it is whenever it does not contain two queries to the same oracle:

Theorem 4.31. *Given a diagram D_1 obtained by applying first the query optimisation procedure then the PGT procedure to a diagram D, if D_1 does not contain two queries to the same oracle (i.e. $\forall U \in \mathcal{G}, \#_U(D_1) \leq 1$), then it is query-PBS-optimal.*

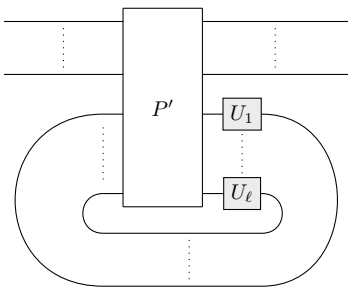
Proof. Let $D_1 : a \to b$ be an abstract diagram obtained from applying the query optimisation procedure followed by the PGT procedure, in which all gates bear different labels. We write it in the form



with P in stair form and $U_1, ..., U_\ell \in \mathcal{G}$ (where all wires and gates can be of arbitrary colours).

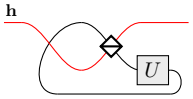
For each $(c,p) \in [a]$, let $p_{c,p}^{(1)}, ..., p_{c,p}^{(\ell_{c,p})}$ be the sequence of positions such that $w_{c,p}^{D_1} = U_{p_{c,p}^{(1)}} ... U_{p_{c,p}^{(\ell_{c,p})}}$ (with $\ell_{c,p} = |w_{c,p}^{D_1}|$). This sequence is determined without ambiguity since the names U_i are pairwise distinct. There exists a sequence of polarisations $c_{c,p}^{(1)}, ..., c_{c,p}^{(\ell_{c,p})}$ such that $[\![P]\!]_{\text{path}}(c,p) = ((c_{c,p}^{(1)}, |b| + p_{c,p}^{(1)}), \epsilon)$, $\forall i \in \{1, ..., \ell_{c,p} - 1\}, [\![P]\!]_{\text{path}}(c_{c,p}^{(i)}, |a| + p_{c,p}^{(i)}) = ((c_{c,p}^{(i+1)}, |b| + p_{c,p}^{(i+1)}), \epsilon)$, and $[\![P]\!]_{\text{path}}(c_{c,p}^{(\ell_{c,p})}, |a| + p_{c,p}^{(\ell_{c,p})}) = ((c_{c,p}^{D_1}, p_{c,p}^{D_1}), \epsilon)$ (where ϵ denotes the empty word).

Given a query-PBS-optimal diagram D_1' equivalent to D_1, up to applying the query optimisation procedure and the PGT procedure, we can assume that D_1' is in PGT form. Note that any diagram E obtained from applying the query optimisation procedure necessarily satisfies that, for every $U \in \mathcal{G}$, it contains exactly $\left\lfloor \sum_{(c,p)\in[a]} \frac{|w_{c,p}^E|_U}{2} \right\rfloor$ black gates labelled with U, and one red or blue gate labelled with U if and only if $\sum_{(c,p)\in[a]} |w_{c,p}^E|_U$ is odd. Since the PGT procedure does not change the gates, it preserves this property. Therefore, D_1 and D_1' both satisfy this property, and since they have the same semantics, this implies that they have the same gates up to turning some red gates into blue gates and vice-versa. That is, up to slightly deforming it in order to permute the gates, we can put D_1' in the form



with P' in stair form. For each $(c,p) \in [a]$, there also exists a sequence of polarisations $c'^{(1)}_{c,p}, ..., c'^{(\ell_{c,p})}_{c,p}$ such that $[\![P']\!]_{\text{path}}(c,p) = ((c'^{(1)}_{c,p}, |b| + p^{(1)}_{c,p}), \epsilon)$, $\forall i \in \{1, ..., \ell_{c,p} - 1\}, [\![P']\!]_{\text{path}}(c'^{(i)}_{c,p}, |a| + p^{(i)}_{c,p}) = ((c'^{(i+1)}_{c,p}, |b| + p^{(i+1)}_{c,p}), \epsilon)$, and $[\![P']\!]_{\text{path}}(c'^{(\ell_{c,p})}_{c,p}, |a| + p^{(\ell_{c,p})}_{c,p}) = ((c^{D_1}_{c,p}, p^{D_1}_{c,p}), \epsilon)$.

Let P'' be the diagram obtained from P' by adding, for every position q such that there exist c, p and $i \in \{1, ..., \ell_{c,p}\}$ satisfying $q = p^{(i)}_{c,p}$ and $c^{(i)}_{c,p} \neq c'^{(i)}_{c,p}$, a negation on input wire $|a| + q$ and on output wire $|b| + q$. Let d be such that $P : a \oplus d \to b \oplus d$. It is easy to see that for every $(c,p) \in [a]$, and for every couple $(c,p) \in [a \oplus d]$ with $p \geq |a|$ that can be written as $(c'^{(i)}_{c',p'}, |a| + p^{(i)}_{c',p'})$ for some $c', p' \in [a]$ and $i \in \{1, ..., \ell_{c',p'}\}$, one has $[\![P'']\!]_{\text{path}}(c,p) = [\![P]\!]_{\text{path}}(c,p)$. Since D_1 is query-optimal, every black gate can be reached from two basis states $(c,p) \in [a]$ and every non-black gate can be reached from one basis state, which implies that every couple $(c,p) \in [b \oplus d]$ with $p \geq |b|$ can be written as $(c'^{(i)}_{c',p'}, |b| + p^{(i)}_{c',p'})$, and therefore, every couple $(c,p) \in [a \oplus d]$ with $p \geq |a|$ can be written as $(c'^{(i)}_{c',p'}, |a| + p^{(i)}_{c',p'})$. Hence, P'' has the same semantics as P. Since by construction, P'' contains the same number of PBS as P', and by Theorem 4.27, P is PBS-optimal, this implies that P contains at most as many PBS as P', that is, D_1 contains at most as many PBS as D'_1. Hence, D_1 is query-PBS-optimal. □

Remark 4.32. *The proof of Theorem 4.31 uses the fact that the diagrams output by the query optimisation procedure, in addition of being query-optimal, have the property that if a gate is used only once (that is, if it is accessible from only one input state (c,p), and a particle with this input state traverses only once the gate), then it is represented as red or blue. Note that a diagram in PGT form with only one query to each oracle may not be query-PBS-optimal if it contains a black gate used only once. For instance,* 

is in PGT form but not query-PBS-optimal as it is equivalent to 

.

Finally, note that, like the query optimisation procedure, the PGT procedure is efficient: it can be done using a number of elementary graphical transformations (those of Figure 4.4) which is linear in the size of the diagram. It also requires some diagrammatic transformations, which can be handled using appropriate data structures, leading to a quadratic algorithm.

4.4.3 Hardness

We show in this section that the query-PBS optimisation problem is actually NP-hard.

Theorem 4.33. *The problem of, given an abstract diagram, finding an equivalent query-PBS-optimal diagram, is NP-hard.*

Proof. Let $\mathcal{G}$ be a set of names. We will prove that the problem is already NP-hard when we restrict the input diagram to the family $\mathcal{P}$ defined as follows:

Definition 4.34. *Given a word $w = w_0...w_{n-1}$ with $w_0, ..., w_{n-1} \in \mathcal{G}$ and a permutation σ of $[n]$, we define $\sigma(w)$ as the rearranged word $w_{\sigma(0)}...w_{\sigma(n-1)}$.*

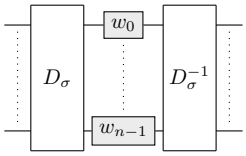
Definition 4.35. *We denote by $\mathcal{P}$ the set of $\mathcal{G}^*$-diagrams $D : \top^{\oplus n} \to \top^{\oplus n}$ such that there exists a word $w = w_0...w_{n-1} \in \mathcal{G}^n$ and a permutation σ of $[n]$ such that for every $p \in [n]$, $[\![D]\!]_{\text{path}}(\mathbf{V}, p) = ((\mathbf{V}, p), w_p)$ and $[\![D]\!]_{\text{path}}(\mathbf{H}, p) = ((\mathbf{H}, p), w_{\sigma(p)})$.*

We polynomially reduce this restricted problem from the *maximum Eulerian cycle decomposition problem*, also called MAX-ECD [25], which consists in, given an Eulerian undirected graph G, finding a maximum-cardinality edge-partition of G into cycles (that is, partitioning the set of edges of G into the maximum number of cycles). Note that the NP-hardness of MAX-ECD follows directly from the NP-completeness of the problem of deciding whether G can be edge-partitioned into triangles, which is proved in [81] (it corresponds to the case of the edge-partition into copies of the complete graph K_3).

The MAX-ECD problem is equivalent to the problem of, given an Eulerian graph G, finding a suitable orientation of its edges together with an edge-partition of the resulting directed graph into directed cycles, so that the number of cycles is maximal among all possible choices of orientation and partition. Indeed,

given these, it suffices to erase the directions of the edges to get an undirected edge-partition into cycles, and given such a partition, it suffices to choose, for each cycle, one of the two possible ways of orienting it.

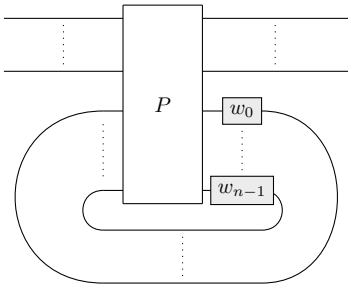
Given an Eulerian graph G, we construct a diagram of $\mathcal{P}$ as follows: first, we choose an arbitrary orientation of the edges of G so as to get an Eulerian directed graph $\vec{G}$ (which can be done by following an Eulerian circuit of G, which itself can be found in polynomial time [63]) and we associate a label, more precisely an element of $\mathcal{G}$, with each vertex of G, in such a way that any two distinct vertices bear distinct labels. Without loss of generality, we can assume that the vertices of G are elements of $\mathcal{G}$ and thereby identify them with their labels. We enumerate the edges of $\vec{G}$ as $e_0, ..., e_{n-1}$. In $\vec{G}$ — since it is Eulerian — each vertex has in- and out-degree equal, that is, each vertex appears as many times as the head of an arrow as as the tail of an arrow, hence there exists a permutation σ of $[n]$ and a word $w = w_0...w_{n-1} \in \mathcal{G}^n$ such that for any $p \in [n]$, e_p is of the form $(w_p, w_{\sigma(p)})$. We consider the following diagram:

$C_{w,\sigma} :=$ 

where $D_\sigma : \top^{\oplus n} \to \top^{\oplus n}$ is a $-\!\!\ulcorner\!\urcorner\!\!-$-free diagram in stair form[24] such that for any $p \in [n]$, $[\![D_\sigma]\!]_{\text{path}}(\mathbf{V}, p) = ((\mathbf{V}, p), \epsilon)$ and $[\![D_\sigma]\!]_{\text{path}}(\mathbf{H}, p) = ((\mathbf{H}, \sigma(p)), \epsilon)$, and D_σ^{-1} is the horizontal reflection of D_σ, which therefore satisfies that for any $p \in [n]$, $[\![D_\sigma^{-1}]\!]_{\text{path}}(\mathbf{V}, p) = ((\mathbf{V}, p), \epsilon)$ and $[\![D_\sigma^{-1}]\!]_{\text{path}}(\mathbf{H}, p) = ((\mathbf{H}, \sigma^{-1}(p)), \epsilon)$.

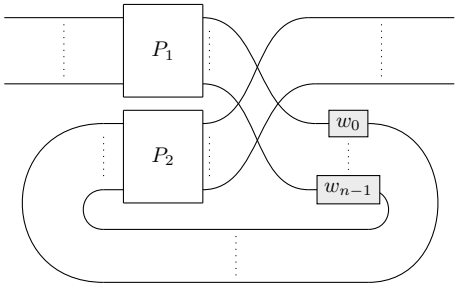
For any $p \in [n]$, one has $[\![C_{w,\sigma}]\!]_{\text{path}}(\mathbf{V}, p) = ((\mathbf{V}, p), w_p)$ and $[\![C_{w,\sigma}]\!]_{\text{path}}(\mathbf{H}, p) = ((\mathbf{H}, p), w_{\sigma(p)})$. In particular, $C_{w,\sigma}$ is in $\mathcal{P}$, and for any $p \in [n]$, $w_{\mathbf{V},p}^{C_{w,\sigma}}$ is the tail of e_p and $w_{\mathbf{H},p}^{C_{w,\sigma}}$ is the head of e_p.[25]

Let $C_{w,\sigma}^{\text{opt}}$ be a query-PBS-optimal diagram equivalent to $C_{w,\sigma}$. Up to applying the PGT procedure, which can be done in polynomial time and neither changes the gates nor increases the number of PBS, we can assume that $C_{w,\sigma}^{\text{opt}}$ is in PGT form. That is, up to reordering some wires, it is of the form



with P in stair form. Since for every c, p, the word $w_{c,p}^{C_{w,\sigma}^{\text{opt}}}$ has length 1, P is such that for any $c \in \{\mathbf{V}, \mathbf{H}\}$ and $p \in [n]$, one has $p_{c,p}^P \in \{n, ..., 2n-1\}$ and $p_{c,p+n}^P \in [n]$.

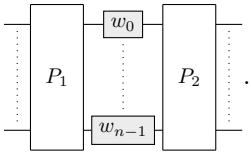
By looking at the semantics of a generic diagram in stair form (in particular by considering the functions ρ_i and τ_i defined in the proof of Theorem 4.27), it is easy to see that this implies that up to reordering the wires on the sides of P, we can write $C_{w,\sigma}^{\text{opt}}$ in the form



[24]Note that the type of D_σ forces all of its staircases to be made only of all-black PBS.

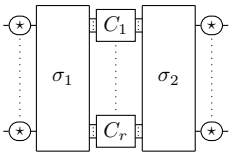
[25]See the end of Definition 4.2 for the definition of $w_{c,p}^{C_{w,\sigma}}$. Note that we identify words of length 1 with their single letter.

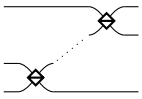
where P_1 and P_2 are two diagrams in stair form. Up to a few more deformations, $C^{\mathrm{opt}}_{w,\sigma}$ is of the form

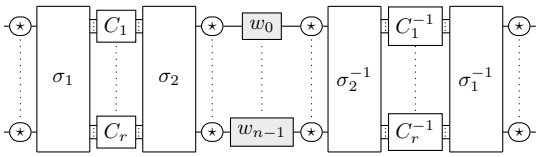


Due to the semantics of $C^{\mathrm{opt}}_{w,\sigma}$, for any $c, c' \in \{\mathbf{V}, \mathbf{H}\}$ and $p, p' \in [n]$, if $[\![P_1]\!]_{\mathrm{path}}(c,p) = ((c',p'),\epsilon)$ then $[\![P_2]\!]_{\mathrm{path}}(c',p') = ((c,p),\epsilon)$. Hence, one can replace P_1 or P_2 by the horizontal reflection of the other without changing the semantics. This implies that P_1 and P_2 contain the same number of PBS (otherwise, by replacing the one with more PBS by the horizontal reflection of the other, one would obtain a diagram equivalent to $C^{\mathrm{opt}}_{w,\sigma}$ with strictly fewer PBS, which would contradict its query-PBS-optimality), and subsequently, that the diagram $C^{\mathrm{opt}\prime}_{w,\sigma}$ obtained by replacing P_2 by the horizontal reflection P_1^{-1} of P_1 is still query-PBS-optimal.

Up to slightly deforming P_1, we can write it in the form

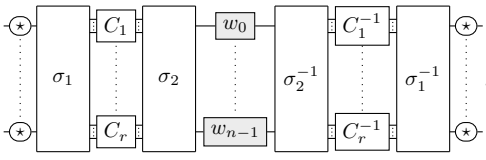


where σ_1 and σ_2 are permutations of the wires, the C_k are of the form  , and denotes either  or . Using this, we can write $C^{\mathrm{opt}\prime}_{w,\sigma}$ in the form

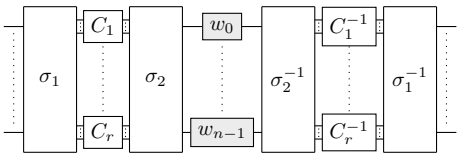


where given any gate-free diagram D, D^{-1} denotes its horizontal reflection.

Since the diagram is symmetric, we can remove the negations in the middle without changing the semantics of the diagram or its query-PBS-optimality. This gives us

$C^{\mathrm{opt}\prime\prime}_{w,\sigma} :=$ 

Let us consider the diagram

$C^{\mathrm{opt},\not\sim}_{w,\sigma} :=$ 

obtained by removing all negations on the sides of $C^{\mathrm{opt}\prime\prime}_{w,\sigma}$. For each $p \in [n]$ such that there was a negation on the pth input and output wire, one now has $[\![C^{\mathrm{opt},\not\sim}_{w,\sigma}]\!]_{\mathrm{path}}(\mathbf{V},p) = ((\mathbf{V},p), w_{\sigma(p)})$ and $[\![C^{\mathrm{opt},\not\sim}_{w,\sigma}]\!]_{\mathrm{path}}(\mathbf{H},p) = ((\mathbf{H},p), w_p)$. Let us consider the directed graph $\tilde{G}$ obtained by reversing the edge e_p in $\vec{G}$ for every such p. For every $p \in [n]$, we denote by $\tilde{e}_p$ the pth edge of $\tilde{G}$, which is either e_p or its reverse $(w_{\sigma(p)}, w_p)$. Then for every $p \in [n]$, $w^{C^{\mathrm{opt},\not\sim}_{w,\sigma}}_{\mathbf{V},p}$ is the tail of $\tilde{e}_p$ and $w^{C^{\mathrm{opt},\not\sim}_{w,\sigma}}_{\mathbf{H},p}$ is the head of $\tilde{e}_p$.

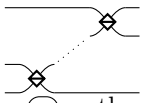
$\tilde{G}$ can be edge-partitioned into r cycles as follows: For each $k \in \{1, ..., r\}$, let n_k be such that $C_k : \top^{\oplus n_k} \to \top^{\oplus n_k}$. Let also $N_k \coloneqq \sum_{j=1}^{k-1} n_k$. By abuse of notation, we denote by σ_1 and σ_2 the permutations of $[n]$ respectively associated with the diagrams σ_1 and σ_2, so that $\forall c, p, [\![\sigma_1]\!]_{\text{path}}(c, p) = ((c, \sigma_1(p)), \epsilon)$ and $[\![\sigma_2]\!]_{\text{path}}(c, p) = ((c, \sigma_2(p)), \epsilon)$. Note that for any $k \in \{1, ..., r\}$ and any $p \in [n_k]$, one has

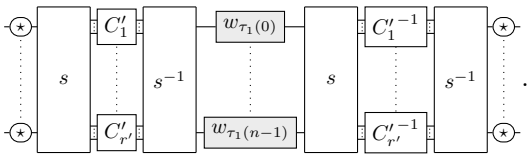
- $\forall i \in [n_k], [\![C^{\text{opt},\not\prec}_{w,\sigma}]\!]_{\text{path}}(\mathbf{V}, \sigma_1^{-1}(N_k + i)) = ((\mathbf{V}, \sigma_1^{-1}(N_k + i)), w_{\sigma_2(N_k+i)})$
- $\forall i \in [n_k - 1], [\![C^{\text{opt},\not\prec}_{w,\sigma}]\!]_{\text{path}}(\mathbf{H}, \sigma_1^{-1}(N_k + i)) = ((\mathbf{H}, \sigma_1^{-1}(N_k + i)), w_{\sigma_2(N_k+i+1)})$
- $[\![C^{\text{opt},\not\prec}_{w,\sigma}]\!]_{\text{path}}(\mathbf{H}, \sigma_1^{-1}(N_k + n_k - 1)) = ((\mathbf{H}, \sigma_1^{-1}(N_k + n_k - 1)), w_{\sigma_2(N_k)})$.

Hence, there is a cycle $w_{\sigma_2(N_k)} \to w_{\sigma_2(N_k+1)} \to \cdots \to w_{\sigma_2(N_k+n_k-1)} \to w_{\sigma_2(N_k)}$ in $\tilde{G}$, associated with C_k. Considering the cycle associated with each C_k gives us an edge-partition of $\tilde{G}$ into r cycles, since these cycles are edge-disjoint and cover all edges of $\tilde{G}$.

It remains to prove that there is no orientation of the edges of G such that the resulting directed graph can be edge-partitioned into more than r cycles. Reasoning by contradiction, assume that there exists such an orientation yielding an Eulerian directed graph $\tilde{\vec{G}}$ with an edge-partition into r' cycles with $r' > r$. We enumerate these cycles in an arbitrary order, and denote by m_k the length of the kth cycle, for $k \in \{1, ..., r'\}$. We denote by $\tilde{\tilde{e}}_p$ the pth edge of $\tilde{\vec{G}}$, which is either $\tilde{e}_p$ or its reverse. Note that the in- and out-degree of each vertex are the same in $\tilde{\vec{G}}$ as in $\vec{G}$ and $\tilde{G}$, so that there exist two permutations τ_1 and τ_2 of $[n]$ such that $\forall p \in [n], \tilde{\tilde{e}}_p = (w_{\tau_1(p)}, w_{\tau_2(p)})$. Therefore, there exists an enumeration of $[n]$ as $(i^k_\ell)_{k\in\{1,...,r'\},\ell\in[m_k]}$, such that the kth cycle can be written

$$w_{\tau_1(i^k_0)} \xrightarrow{\tilde{\tilde{e}}_{i^k_0}} w_{\tau_1(i^k_1)} \xrightarrow{\tilde{\tilde{e}}_{i^k_1}} \cdots \xrightarrow{\tilde{\tilde{e}}_{i^k_{m_k-2}}} w_{\tau_1(i^k_{m_k-1})} \xrightarrow{\tilde{\tilde{e}}_{i^k_{m_k-1}}} w_{\tau_1(i^k_0)}.$$

Let s be the permutation of $[n]$ such that $\forall k, \ell, s(i^k_\ell) = M_k + \ell$, where $M_k \coloneqq \sum_{j=1}^{k-1} m_k$. We make the same abuse of notation as for σ_1 and σ_2 by also denoting by s the diagram that is a permutation of the wires according to s. We consider the following diagram, where for each $k \in \{1, ..., r'\}$, $C'_k : \top^{\oplus m_k} \to \top^{\oplus m_k}$ is of the form  , and for each $p \in [n]$, the on wire p is —— if $\tilde{\tilde{e}}_p$ and $\tilde{e}_p$ have the same direction, or otherwise:

$C_{w,\tau} \coloneqq$ 

For any $k \in \{1, ..., r'\}$ and $\ell \in [m_k]$, if $\tilde{\tilde{e}}_p$ and $\tilde{e}_p$ have the same direction then one has $[\![C_{w,\tau}]\!]_{\text{path}}(\mathbf{V}, i^k_\ell) = ((\mathbf{V}, i^k_\ell), w_{\tau_1(i^k_\ell)})$ and $[\![C_{w,\tau}]\!]_{\text{path}}(\mathbf{H}, i^k_\ell) = ((\mathbf{H}, i^k_\ell), w_{\tau_1(i^k_{\ell+1 \bmod m_k})})$, and if they have opposite directions then one has $[\![C_{w,\tau}]\!]_{\text{path}}(\mathbf{V}, i^k_\ell) = ((\mathbf{V}, i^k_\ell), w_{\tau_1(i^k_{\ell+1 \bmod m_k})})$ and $[\![C_{w,\tau}]\!]_{\text{path}}(\mathbf{H}, i^k_\ell) = ((\mathbf{H}, i^k_\ell), w_{\tau_1(i^k_\ell)})$. That is, in any case, $w^{C_{w,\tau}}_{\mathbf{V},i^k_\ell}$ is the tail of $\tilde{e}_{i^k_\ell}$ and $w^{C_{w,\tau}}_{\mathbf{H},i^k_\ell}$ is its head. Since the indices i^k_ℓ span $[n]$ entirely, this implies that $C_{w,\tau}$ has the same semantics as $C^{\text{opt},\not\prec}_{w,\sigma}$. But $C_{w,\tau}$ contains $n - r'$ PBS whereas $C^{\text{opt},\not\prec}_{w,\sigma}$ contains $n - r$ PBS, so that $C_{w,\tau}$ contains strictly fewer PBS than $C^{\text{opt},\not\prec}_{w,\sigma}$, which contradicts the query-PBS-optimality of $C^{\text{opt},\not\prec}_{w,\sigma}$.

This proves that the edge-partition of $\tilde{G}$ into cycles obtained from $C^{\text{opt},\not\prec}_{w,\sigma}$ has maximum number of cycles among all possible choices of orientation and partition. In other words, the undirected edge-partition of G obtained by erasing the directions of the edges in this edge-partition of $\tilde{G}$ has maximum number of cycles. This finishes the reduction. □

In the following, we explore a few variants of the problem, which remain NP-hard.

First, query-PBS optimisation is still hard when restricted to negation-free diagrams:

Corollary 4.36. *The problem of, given a negation-free abstract diagram, finding an equivalent diagram which is query-PBS-optimal among negation-free diagrams, is NP-hard.*

Proof. We reduce this problem from the problem maxDCD of, given an Eulerian directed graph $\vec{G}$, finding a maximum-cardinality edge-partition of $\vec{G}$ into directed cycles. This problem is defined and proved to be NP-hard in [7].

The proof has the same structure as the proof of Theorem 4.33 : we define $C_{w,\sigma}$ in the same way, and we consider an equivalent diagram $C^{\mathrm{opt}}_{w,\sigma}$ which is now query-PBS-optimal only among negation-free diagrams. Since the PGT procedure preserves the property of being negation-free, we can still assume that it is in PGT form. With the same arguments as in the proof of Theorem 4.33, we can do the same deformations and define $C^{\mathrm{opt}\prime}_{w,\sigma}$ in the same way. This time, $C^{\mathrm{opt}\prime}_{w,\sigma}$ is negation-free, so that $C^{\mathrm{opt},\not\sim}_{w,\sigma} = C^{\mathrm{opt}\prime}_{w,\sigma}$ and $\tilde{G} = \vec{G}$, so the construction of the proof of Theorem 4.33 gives us an edge-partition of $\vec{G}$. To prove that this edge-partition has maximum cardinality, we only have to prove that there is no edge-partition of $\vec{G}$ into strictly more cycles, and the proof of this is the same as for Theorem 4.33 (with the difference that we necessarily have $\tilde{\vec{G}} = \vec{G}$, which allows for many simplifications). □

Additionally, it is also hard, in a query-optimal diagram, to optimise the PBS and the negations together, respectively: with respect to a cost function (at least in the case where the cost of a negation is not less than the cost of a PBS); with the negations prioritised over the PBS; and with the PBS prioritised over the negations. Note that the NP-hardness is clear in the third case since the considered problem is a refinement of the query-PBS-optimisation problem addressed in Theorem 4.33.

Corollary 4.37. *For any $\alpha \geq 1$, the problem of, given an abstract diagram D, finding an equivalent query-optimal diagram D' such that $\#_{\mathrm{PBS}}(D') + \alpha\#_{\neg}(D')$ is minimal, is NP-hard, where $\#_{\neg}(D)$ is the number of negations in D.*

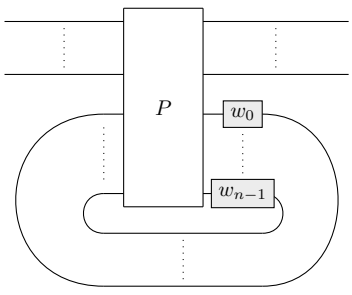
The proof relies on the following lemma:

Lemma 4.38. *Given any diagram D of $\mathcal{P}$ which is query-optimal and contains at least one negation, there exists an equivalent negation-free diagram with the same gates containing at most $\#_{\mathrm{PBS}}(D) + \#_{\neg}(D) - 1$ PBS.*

Proof of Corollary 4.37. Note that the proofs of Theorem 4.33 and Corollary 4.36 actually give us slightly stronger results than the exact statements of Theorem 4.33 and Corollary 4.36, since they in fact consider the restricted versions of their respective problems in which the input diagram is required to be in $\mathcal{P}$.

Given Lemma 4.38, Corollary 4.37 follows from this stronger version of Corollary 4.36. Indeed, it suffices to prove that the problem of optimising $\#_{\mathrm{PBS}}(D) + \alpha\#_{\neg}(D)$ together with the queries is already NP-hard when restricted to the case where the input diagram D is negation-free and in $\mathcal{P}$. Given such a diagram D, any query-optimal diagram D' equivalent to D such that $\#_{\mathrm{PBS}}(D') + \alpha\#_{\neg}(D')$ is minimal, is negation-free. Indeed, if it was not, then, since it is in $\mathcal{P}$, by Lemma 4.38 there would exist an equivalent query-optimal, negation-free diagram D'' that would satisfy $\#_{\mathrm{PBS}}(D'') + \alpha\#_{\neg}(D'') = \#_{\mathrm{PBS}}(D'') \leq \#_{\mathrm{PBS}}(D') + \#_{\neg}(D') - 1 < \#_{\mathrm{PBS}}(D') + \alpha\#_{\neg}(D')$, which would contradict the fact that $\#_{\mathrm{PBS}}(D') + \alpha\#_{\neg}(D')$ is minimal. Thus, finding a query-optimal diagram D' equivalent to D such that $\#_{\mathrm{PBS}}(D') + \alpha\#_{\neg}(D')$ is minimal, amounts to finding a diagram equivalent to D and query-PBS-optimal among negation free diagrams. □

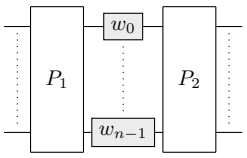
Proof of Lemma 4.38. Let $D : \top^{\oplus n} \to \top^{\oplus n}$ be a query-optimal diagram of $\mathcal{P}$ containing at least one negation. Let us first apply Step 1 of the PGT procedure, that is, by mere deformation, we put D in the form



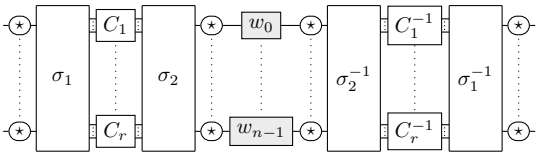
with P gate-free. Let $f(P)$ be the number of positions p such that $c^P_{\mathbf{V},p} = \mathbf{H}$ (note that this number does not depend on the way of deforming D). Since the semantics of P applies a permutation to the couples (c,p), there are the same number of positions p such that $c^P_{\mathbf{H},p} = \mathbf{V}$, so that there are $2f(P)$ couples (c,p) such that $c^D_{c,p} \neq c$. Each photon that enters P with a basis state corresponding to one of these couples gets its polarisation changed while traversing P, which means that it traverses at least one negation. Since each negation can be reached from at most two basis states, this implies that $f(P) \leq \#_\neg(D)$.

Note that additionally, due to the semantics of D (since it is in $\mathcal{P}$), for any $c, c' \in \{\mathbf{V}, \mathbf{H}\}$ and $p, p' \in [2n]$ such that $[\![P]\!]_{\text{path}}(c,p) = (c',p')$, one has $p \in [n]$ if and only if $p' \in \{n, ..., 2n-1\}$ and vice-versa, and $[\![P]\!]_{\text{path}}(c',p') = (c,p)$. Combined with the fact that $[\![P]\!]_{\text{path}}$ applies a permutation to the couples (c,p), this implies that there are the same number of positions p such that respectively: $p \in [n]$ and $c^P_{\mathbf{V},p} = \mathbf{H}$; $p \in [n]$ and $c^P_{\mathbf{H},p} = \mathbf{V}$; $p \in \{n, ..., 2n-1\}$ and $c^P_{\mathbf{V},p} = \mathbf{H}$; $p \in \{n, ..., 2n-1\}$ and $c^P_{\mathbf{H},p} = \mathbf{V}$. Since the sum of these four numbers of positions is equal to $2f(P)$, this implies that $f(P)$ is even and that the number of positions p is equal to $\dfrac{f(P)}{2}$ in each case.

By applying the rest of the PGT procedure, we put P in stair form and thereby transform D into a diagram D' in PGT form. With a similar argument as in the proof of Theorem 4.33, we can put D' in the form

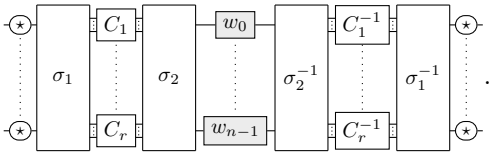


where P_1 and P_2 are in stair form. Since $D \in \mathcal{P}$, for any $c, c' \in \{\mathbf{V}, \mathbf{H}\}$ and $p, p' \in [n]$, if $[\![P_1]\!]_{\text{path}}(c,p) = ((c',p'),\epsilon)$ then $[\![P_2]\!]_{\text{path}}(c',p') = ((c,p),\epsilon)$. Hence, P_1 has the same semantics as the horizontal reflection of P_2 and vice-versa. By Theorem 4.27, this implies that P_1 and P_2 contain the same number of PBS. Therefore, by replacing P_2 by the horizontal reflection of P_1, we get a diagram D'' which is still equivalent to D and still has at most as many PBS as D. As in the proof of Theorem 4.33, we can write D'' in the form



where σ_1 and σ_2 are permutation of the wires, the C_k are staircases (see Definition 4.25), and given any gate-free diagram E, E^{-1} denotes its horizontal reflection. Since D'' is symmetric, we can remove the negations in the middle without changing its semantics, which gives us

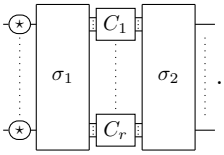
$D''' :=$



.

Let

$L :=$



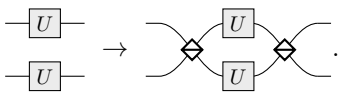
.

For every letter $U \in \{w_0, ..., w_{n-1}\}$, let $d_U(D)$ be the number of positions p such that for some p_1, p_2, one has $p^L_{\mathbf{V},p_1} = p^L_{\mathbf{V},p_2} = p$ and $w_p = U$. Since $D \in \mathcal{P}$, U appears as many times among the $w^D_{\mathbf{V},p}$ as among the $w^D_{\mathbf{H},p}$. Since $\forall c, p, w^D_{c,p} = w_{p^L_{c,p}}$, this implies that the number of positions p' such that for some p'_1, p'_2 one has $p^L_{\mathbf{H},p'_1} = p^L_{\mathbf{H},p'_2} = p'$ and $w_{p'} = U$ is also $d_U(D)$. We arbitrarily associate a position p' of the second kind with each position p of the first kind, so as to distribute these $2d_U(D)$ positions into $d_U(D)$ couples (p,p'). By doing so for every $U \in \{w_0, ..., w_{n-1}\}$, we obtain $d(D)$ couples,

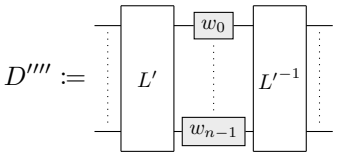
where $d(D) \coloneqq \sum_{U \in \{w_0,\dots,w_{n-1}\}} d_U(D)$, with the property that every position q satisfying for some p_1, p_2, c, $p^L_{c,p_1} = p^L_{c,p_2} = q$, appears exactly once among these couples (as a left element if $c = \mathbf{V}$, and as a right element if $c = \mathbf{H}$).

For each position q among these $2d(D)$ positions, there is exactly one polarisation c such that $c^L_{c,p} \neq c$. This property is not affected by appending negations at the right of L, so that there is also exactly one polarisation c (for each q) such that $c^{P_1}_{c,q} \neq c$. By definition of P_1, there is also exactly one polarisation c such that $c^P_{c,q} \neq c$. Since all of these $2d(D)$ positions q are in $[n]$, this implies that $2\,\frac{f(P)}{2} \geq 2d(D)$. Since $f(P) \leq \#_\neg(D)$, this inequality implies that $2d(D) \leq \#_\neg(D)$.

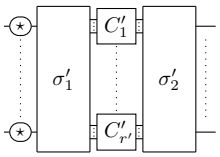
For each of the $d(D)$ couples (p, p'), we do the following transformation in D''' (up to deformation):



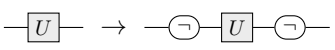
Each time, we put L in stair form again, we transform L^{-1} symmetrically so that it remains the horizontal reflection of L, and we remove any negations at the right of L and at the left of L^{-1}, which is possible because D''' remains symmetric. One can check that if the PBS appended to L is connected to two different C_is, then this results in merging them together, so that the number of PBS stays the same (after adding the additional PBS), and if it is connected to a single C_i then this results in splitting it into two staircases, so that the number of PBS in L decreases by 2. The behaviour of L^{-1} is symmetric. At the end, the total number of PBS is at most $\#_{\mathrm{PBS}}(D) + 2d(D)$, and the equality can be reached only if at every step two C_is have been merged. This gives us a diagram



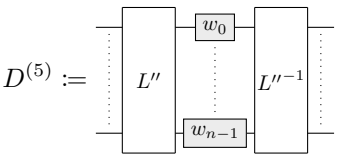
with L' of the form



in which there are no couples of positions p_1, p_2 such that $p^L_{\mathbf{V},p_1} = p^L_{\mathbf{V},p_2}$ anymore. In particular, for each position p such that for some p_1, $[\![L']\!]_{\mathrm{path}}(\mathbf{V}, p_1) = ((\mathbf{H}, p), \epsilon)$, there exists p_2 such that $[\![L']\!]_{\mathrm{path}}(\mathbf{H}, p_2) = ((\mathbf{V}, p), \epsilon)$. For each of these positions, we apply the following transformation:

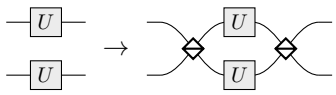


This gives us a diagram



with L'' such that for all c, p, $c^{L''}_{c,p} = c$. By putting L'' in normal form, then in stair form again, we get a diagram L''' without negations and with at most as many PBS as L''. In particular, the resulting diagram $D^{(6)}$ (after proceeding symmetrically in L''^{-1}) contains at most $\#_{\mathrm{PBS}}(D) + 2d(D)$ PBS. If it has strictly fewer PBS, or if $2d(D) < \#_\neg(D)$, then we have the desired result. If it has exactly $\#_{\mathrm{PBS}}(D) + 2d(D)$ PBS and $2d(D) = \#_\neg(D)$, then this means in particular that at each of the steps of the transformation of D''' into D'''', two C_is have been merged. By hypothesis, $\#_\neg(D) \geq 1$, so the fact that $2d(D) = \#_\neg(D)$ implies that $d(D) > 0$. This implies that there has been at least one step in the transformation of D'''

into D'''', in which two staircases connected to two gates with the same label have been merged. Since these staircases have not been split, there is at least one couple of gates in $D^{(5)}$ that have the same label and are connected to the same staircase. Then by applying to them the same transformation as before:



and putting L''' (and L'''^{-1}) in stair form again, we get a diagram with $\#_{\mathrm{PBS}}(D) + \#_{\neg}(D) - 2$ PBS and no negations, which is equivalent to D. □

Although we were only able to prove Corollary 4.37 for $\alpha \geq 1$, we conjecture that the optimisation is actually NP-hard even if the negations cost less than the PBS:

Conjecture 4.39. *For any $\alpha \geq 0$, the problem of, given an abstract diagram D, finding an equivalent query-optimal diagram D' such that $\#_{\mathrm{PBS}}(D') + \alpha\#_{\neg}(D')$ is minimal, is NP-hard, where $\#_{\neg}(D)$ is the number of negations in D.*

Corollary 4.40. *The problem of, given an abstract diagram D, finding an equivalent query-¬-PBS-optimal*[26] *diagram is NP-hard.*

Proof. The NP-hardness of this problem directly follows from Corollary 4.36. Indeed, given a negation-free diagram D, the query optimisation procedure gives us a negation-free query-optimal diagram D' equivalent to D. Any query-¬-PBS-optimal diagram equivalent to D has to contain at most as many negations as D', namely 0, that is, be negation-free. Thus, finding a query-¬-PBS-optimal equivalent to D amounts to finding a negation-free query-PBS-optimal diagram equivalent to D. □

Finally, as noted above, the NP-hardness when the PBS are prioritised over the negations is a direct consequence of Theorem 4.33:

Remark 4.41. *The problem of, given an abstract diagram D, finding an equivalent query-PBS-¬-optimal diagram is NP-hard.*

4.5 Discussions and Future Work

The power and limits of quantum coherent control is an intriguing question. Maybe surprisingly,[27] we have proved that coherently controlled quantum computations, when expressed in the PBS-calculus, can be efficiently optimised: any PBS-diagram can be transformed in polynomial time into a diagram that is optimal in terms of oracle queries. We have refined the procedure to also decrease the number of polarising beam splitters. It leads to an optimal diagram when each oracle is queried only once, but the corresponding optimisation problem is NP-hard in general. We leave to future work an experimental evaluation of the PGT procedure when each oracle is not necessarily queried only once.

It might be that the NP-hardness result is even more significant than the optimisation heuristic, as the hardness might scale up as the language is further developed. There is however no certainty that things will necessarily happen as badly, and it might be a perspective for further developments of this language to find extensions of it in which such optimisation problems are easy to solve.

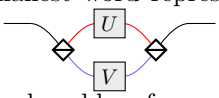
To perform the resource optimisation, we have introduced a few add-ons to the framework of the PBS-calculus. First, we have refined the syntax in order to allow the representation of unsaturated (or 3-leg) polarising beam splitters. They are essential ingredients for resource optimisation, as they provide a way to decompose a diagram into elementary components and then remove the useless ones. However, note that one can perform resource optimisation of vanilla PBS-diagrams, using the refined one only as

[26] A diagram is query-¬-PBS-optimal if it is optimal according to the lexicographic order: the number of queries then the number of negations and finally the number of polarising beam splitters. The definition of a query-PBS-¬-optimal diagram is analogous.

[27] One may argue that this could be due to the simplicity of the language. It belongs to future work to know whether things would be as simple if the language were to be extended to allow for a more general quantum control.

an intermediate language. Indeed, given a vanilla PBS-diagram (where all wires are black), one can apply the optimisation procedures described in this chapter. The resulting optimised PBS-diagram may contain some unsaturated PBS, but all these 3-leg PBS can be saturated by adding useless traces and then one can make the diagram monochromatic. The resulting vanilla PBS-diagram keeps the same number of queries and PBS.

We have also generalised the gates of the diagrams, by considering arbitrary monoids. This is a natural abstraction that allows one to consider various examples and in particular the one of the free monoid which is appropriate to model the oracle queries. The query complexity is a convenient model to prove lower bounds, but note that the optimisation procedures described in this chapter can be applied with any arbitrary monoid (for instance using Proposition 4.8). However, there is no guarantee of minimality with an arbitrary monoid.

A natural question would then be to consider the problem of resource optimisation in the case of an arbitrary monoid. This requires to introduce a complexity measure, the most natural way to do so would probably be to define a cost function on the elements of the monoid, that is, a function $c\colon \mathsf{M} \to \mathbb{R}_{\geq 0}$ (M being the monoid), satisfying $c(I) = 0$ and $c(UV) \leq c(U) + c(V)$. Note however that this problem is hard in general, and sometimes even not solvable. This may be the case, for instance, if M is a free monoid quotiented by a list of equalities between words which in particular make it into a group, and the cost function associates with each element of M the length of the smallest word representing this element. Indeed, optimising the resources of a simple diagram of the form 

requires in general to decide whether U and V are equal. This is an instance of the word problem for groups, which is known to have undecidable instances, even with a finite alphabet and a finite list of equalities defining M [106, 49].

Chapter 5

$\mathrm{LO_v}$-Calculus : A Graphical Language for Photon-Preserving Linear Optical Circuits

In Chapters 3 and 4, we have developed a language — the PBS-calculus — and a variant of it, which are inspired by linear optics but are essentially considered as an abstract tool for describing coherently controlled quantum processes. In this chapter, we take the opposite point of view and focus on the linear optical aspect: we develop a language dedicated to linear optical quantum computing (LOQC), with a similar structure as the PBS-calculus, which formalises the kinds of diagrammatics that are currently in use in the physics community.

Compared to the PBS-calculus, this language, called the $\mathrm{LO_v}$-calculus, does not have gates as generators, but instead has the main physical apparatuses used in the physics literature about linear optics, the polarising beam splitter (PBS) being one of them. The language comes equipped with an equational theory that is sound and complete with respect to the standard semantics of LOQC. Our other main contribution is a strongly normalising and globally confluent rewriting system for the polarisation-preserving fragment, for which the normal form is a refinement of the Reck *et al.* [114] decomposition, with natural conditions imposed on the parameters which we prove to make it unique.

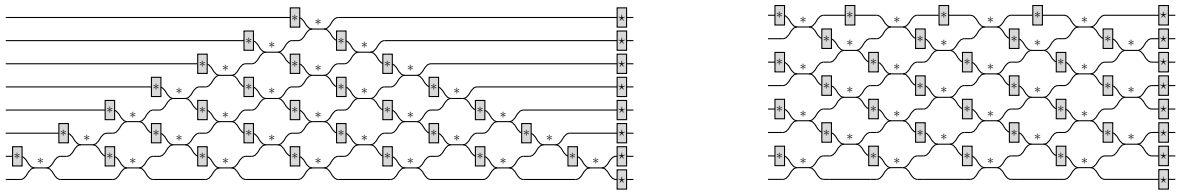
In practice such a language can find many uses including for the design, optimisation, verification, error-correction, and systematic study of linear optical quantum circuits for quantum information. Additionally, and maybe more importantly, our language makes it possible to formalise and reason within a common framework on various presentations of LOQC stemming from parallel research paths. Our semantics not only allows us to recover, extend and improve on some key results in LOQC such as the universal decompositions of Reck *et al.* [114] and Clements *et al.* [41], but it also gives a unifying language for the different formalisms from the literature.

Note that the rewriting system for the polarisation-preserving fragment has been implemented in the Perceval software [80].[28]

Finally, it turns out that finding complete equational theories for linear optical circuits paves the way towards the design of complete equational theories for quantum circuits (see Chapter 6).

Plan of the chapter. The chapter is structured as follows. In Section 5.1, we present the syntax and the semantics of the $\mathrm{LO_v}$-calculus. The equational theory and its soundness are given in Section 5.2. In Section 5.3 we present the strongly normalising and globally confluent rewriting system. This allows us to prove the completeness of the $\mathrm{LO_v}$-calculus in Section 5.4. Finally, in Section 5.5, we discuss a perspective consisting in adding a trace construction, similar to the trace of the PBS-calculus, to the $\mathrm{LO_v}$-calculus.

[28] See `https://perceval.quandela.net/docs/notebooks/Rewriting rules in Perceval.html`.



(a) Triangular form [114]. (b) Rectangular form [41].

Figure 5.1: Triangular and rectangular universal forms for polarisation-preserving circuits.

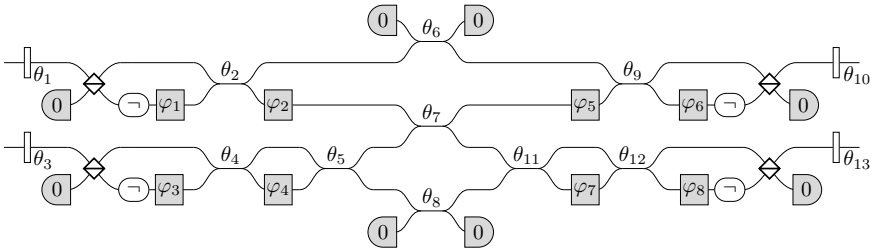


Figure 5.2: $\mathrm{LO_v}$-circuit implementing a variational quantum eigensolver [110], an algorithm with applications including calculation of ground-state energies in quantum chemistry.

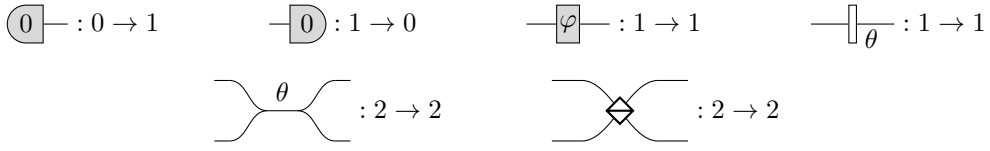
5.1 Linear Optical Quantum Circuits

A linear optical quantum computation [96, 95] (LOQC) consists of spatial modes through which photons pass — which may be physically instantiated by optical fibers, waveguides in integrated circuits, or simply by paths in free space (bulk optics) — and operations that act on the spatial and polarisation degrees of freedom of the photons, including in particular *beam splitters* (θ), *polarising beam splitters* (PBS), *phase shifters* (φ), *wave plates* (θ), *pola-negations* (¬) and finally the *vacuum state sources* and *detectors* (0 and 0). Their action and the semantics are described in Section 5.1.2.

5.1.1 Syntax

We formalise linear optical quantum circuits as a PROP (not traced, that is without the trace operator, see the bottom of Definition 1.1 in Chapter 1 for a formal definition. The main reasons for this choice are that feedback loops are not needed to represent the linear optical schemes used in practice, and that there is not a clear, unique way to give them a physical meaning. See Section 5.5 for discussions about how to give a semantics to linear optical circuits with trace):

Definition 5.1. $\mathbf{LO_v}$ *is the PROP of* $\mathrm{LO_v}$*-circuits generated by*



where $\theta, \varphi \in \mathbb{R}$*. We write* ¬ *as a shortcut notation for* $-\frac{\pi}{2}$.

Example 5.2. *An example of a linear optical quantum circuit using all of the connectives presented in Definition 5.1 is shown in Figure 5.2.*

Remark 5.3. *Similarly as in the preceding chapters, the axioms of PROP guarantee that linear optical quantum circuits are defined up to deformations: Figure 5.3 shows two equivalent circuits under the axioms of PROP.*

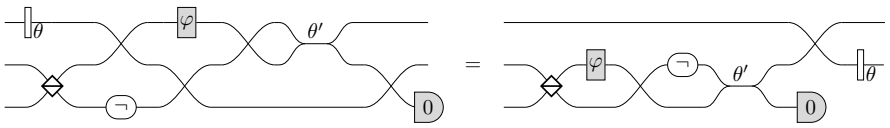


Figure 5.3: Two equivalent representations of the same $\mathrm{LO_v}$-circuit.

$$\left[\!\left[\boxed{0}\!- \right]\!\right] = 0 \qquad \left[\!\left[-\boxed{0} \right]\!\right] = 0 \qquad [\![\boxed{}]\!] = 0$$

$$\left[\!\left[\overset{\theta}{\times} \right]\!\right] = |c,p\rangle \mapsto \cos(\theta)\,|c,p\rangle + i\sin(\theta)\,|c,1-p\rangle$$

$$\left[\!\left[-\boxed{\theta}- \right]\!\right] = \begin{cases} |\mathbf{V},0\rangle \mapsto \cos(\theta)\,|\mathbf{V},0\rangle + i\sin(\theta)\,|\mathbf{H},0\rangle \\ |\mathbf{H},0\rangle \mapsto \cos(\theta)\,|\mathbf{H},0\rangle + i\sin(\theta)\,|\mathbf{V},0\rangle \end{cases}$$

$$\left[\!\left[-\boxed{\varphi}- \right]\!\right] = |c,0\rangle \mapsto e^{i\varphi}\,|c,0\rangle$$

$$[\![\diamond]\!] = \begin{cases} |\mathbf{V},p\rangle \mapsto |\mathbf{V},p\rangle \\ |\mathbf{H},p\rangle \mapsto |\mathbf{H},1-p\rangle \end{cases}$$

$$[\![\times]\!] = |c,p\rangle \mapsto |c,1-p\rangle$$

$$[\![-]\!] = |c,0\rangle \mapsto |c,0\rangle$$

Table 5.1: Semantics of $\mathrm{LO_v}$-circuits.

Among the generators, the beam splitters and phase shifters are known to preserve the polarisation of the photons. As a consequence, we define a *polarisation-preserving* sub-PROP of $\mathbf{LO_v}$ as follows.

Definition 5.4. $\mathbf{LO_{PP}}$ *is the PROP of* polarisation-preserving circuits *generated by beam splitters* $\overset{\theta}{\times}$ *and phase shifters* $-\boxed{\varphi}-$.

In the following, it will also be useful to work in the PRO of polarisation-preserving circuits (see the bottom of Definition 1.1), in which swaps are not allowed.

Definition 5.5. $\mathbf{LO_{PP}^{PRO}}$ *is the PRO generated by beam splitters* $\overset{\theta}{\times}$ *and phase shifters* $-\boxed{\varphi}-$.

5.1.2 Single-Photon Semantics

We will characterise photons by their spatial and polarisation modes. Spatial modes refer to position, and polarisation can be horizontal ($\mathbf{H}$) or vertical ($\mathbf{V}$). Unlike in the previous chapters, we do not consider an additional degree of freedom. For any $n \in \mathbb{N}$, let $M_n = \{\mathbf{V},\mathbf{H}\} \times [n]$, where $[n] = \{0,\dots n-1\}$, be the set of basis states (spatial and polarisation modes). The state space of a single photon is $\mathbb{C}^{M_n} = span(|\mathbf{V},p\rangle, |\mathbf{H},p\rangle \mid p \in [n])$. Notice that $\mathbb{C}^{M_0} = \mathbb{C}^{\emptyset} = \{0\}$ is the Hilbert space of dimension 0. The semantics of a $\mathrm{LO_v}$-circuit is defined as follows.

Definition 5.6. *For any* $\mathrm{LO_v}$*-circuit* $D : n \to m$*, let* $[\![D]\!] : \mathbb{C}^{M_n} \to \mathbb{C}^{M_m}$ *be the linear map inductively defined by Table 5.1*[29]*, and by* $[\![D_2 \circ D_1]\!] = [\![D_2]\!] \circ [\![D_1]\!]$*,* $[\![D_1 \oplus D_2]\!] = [\![D_1]\!] \oplus [\![D_2]\!]$*, where for all* $f \in \mathbb{C}^{M_n} \to \mathbb{C}^{M_m}$ *and* $g \in \mathbb{C}^{M_{n'}} \to \mathbb{C}^{M_{m'}}$*,* $(f \oplus g)(|c,k\rangle) = f(|c,k\rangle)$ *if* $k < n$ *and* $S_{m,m'}(g(|c,k-n\rangle))$ *if* $k \geq n$*, with* $S_{m,m'} : \mathbb{C}^{M_{m'}} \to \mathbb{C}^{M_{m+m'}} = |c,k\rangle \mapsto |c,k+m\rangle$ *a shift of the positions by* m*.*

Example 5.7. *The negation inverts polarisation:* $[\![-\neg-]\!] : |\mathbf{V},0\rangle \mapsto |\mathbf{H},0\rangle$ *and* $|\mathbf{H},0\rangle \mapsto |\mathbf{V},0\rangle$*.*

Remark 5.8. *The semantics of the circuits is sound with respect to the axioms of PROP. In other words two circuits that are equal up to deformation have the same semantics.*

Remark 5.9. *All the generators of* $\mathrm{LO_v}$*-circuits are photon-preserving, even the vacuum state sources (*$\boxed{0}-$*) and detectors (*$-\boxed{0}$*). Indeed the vacuum state source produces no photons, whereas the semantics of the detector corresponds to a postselection on the case where no photons are detected.*

[29] There are many possible conventions for beam splitters. We have chosen this one as it is a symmetric operation with good composition properties (see Figure 5.5). The convention for the wave plate has been chosen for similar reasons (see for instance Equations (5.17), (5.34) and (5.37)).

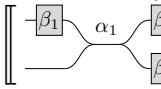
Remark 5.10. *Note that a multi-photon semantics can be defined from the single-photon semantics using the Fock space formalism in a similar way as in Section 3 of [53]. However, since we only study photon-preserving linear optical circuits, and only consider circuits in themselves (that is, not in the context of a particular experiment), it is sufficient here to work only with the single-photon semantics. Since the multi-photon semantics is uniquely determined by the single-photon semantics, our results that use the single-photon semantics can be straightforwardly reformulated in terms of the multi-photon semantics.*

Note that $\mathbb{C}^{M_n}$ is isomorphic to $\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}} \otimes \mathbb{C}^n$, and that up to identifying these two spaces, the semantics of a $\mathrm{LO_{PP}}$-circuit, and more generally of any $\mathrm{LO_v}$-circuit which does not contain  or  , is of the form $I_{\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}} \otimes f$ for some $f\colon \mathbb{C}^n \to \mathbb{C}^m$. This is why we also define a polarisation-preserving semantics which is sometimes more appropriate for those circuits:

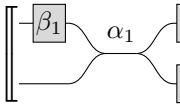
Definition 5.11. *For any* $\mathrm{LO_v}$*-circuit* $D\colon n \to m$ *such that* $[\![D]\!] = I_{\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}} \otimes f$ *for some* $f\colon \mathbb{C}^n \to \mathbb{C}^m$*, we define* $[\![D]\!]_{\mathrm{pp}} \coloneqq f$*. In other words,* $[\![D]\!]_{\mathrm{pp}} : \mathbb{C}^n \to \mathbb{C}^m$ *is the unique linear map such that* $[\![D]\!] \circ \iota = \iota \circ [\![D]\!]_{\mathrm{pp}}$ *where* $\iota : \mathbb{C}^n \to \mathbb{C}^{M_n} :: |k\rangle \mapsto |\mathbf{H}, k\rangle$*.*

For instance $\left[\!\!\left[\right.\right.$  $\left.\right]\!\!\right]_{\mathrm{pp}} = \begin{pmatrix} \cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & \cos(\theta) \end{pmatrix}$.

Polarisation-preserving circuits are universal for unitary transformations, this is a direct consequence of the result of Reck *et al.* [114]. One can actually make the representation of each unitary unique in a natural way, as illustrated by the following two cases on 2 and 3 modes, the general case being proved in Section 5.3 (see Proposition 5.37).

Lemma 5.12. *For any unitary* 2×2 *matrix* U*, there exist unique* $\beta_1, \alpha_1 \in [0, \pi)$ *and* $\beta_2, \beta_3 \in [0, 2\pi)$ *such that* $\left[\!\!\left[\right.\right.$  $\left.\right]\!\!\right]_{\mathrm{pp}} = U$*, and* $\alpha_1 \in \{0, \frac{\pi}{2}\} \Rightarrow \beta_1 = 0$*.*

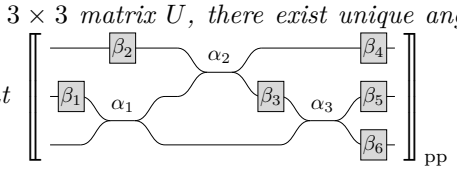
Proof. Let us consider such $\beta_1, \alpha_1 \in [0, \pi)$ and $\beta_2, \beta_3 \in [0, 2\pi)$. We first prove that, assuming that they exist, their values are uniquely determined by U. We have:

$$U = \left[\!\!\left[\right.\right. \text{  } \left.\right]\!\!\right]_{\mathrm{pp}} = \begin{pmatrix} e^{i(\beta_1+\beta_2)}\cos(\alpha_1) & ie^{i\beta_2}\sin(\alpha_1) \\ ie^{i(\beta_1+\beta_3)}\sin(\alpha_1) & e^{i\beta_3}\cos(\alpha_1) \end{pmatrix}$$

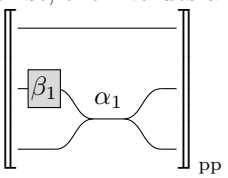
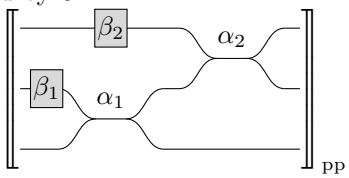
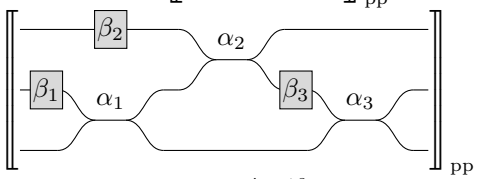
If U has a null entry, then since it is unitary, it is either diagonal or anti-diagonal. If it is diagonal, then $\sin(\alpha_1) = 0$, which, since $\alpha_1 \in [0, \pi)$, implies that $\alpha_1 = 0$, which by the constraint on β_1 and α_1, implies that $\beta_1 = 0$. Consequently, $\beta_2 = \arg(U_{0,0})$ and $\beta_3 = \arg(U_{1,1})$. If U is anti-diagonal, then $\cos(\alpha_1) = 0$, which, since $\alpha_1 \in [0, \pi)$, implies that $\alpha_1 = \frac{\pi}{2}$, which by the constraint on β_1 and α_1, implies that $\beta_1 = 0$. Consequently, $\beta_2 = \arg(\frac{U_{0,1}}{i})$ and $\beta_3 = \arg(\frac{U_{1,0}}{i})$.

If U has no null entry, since $UU^\dagger = I$, we have $e^{i(\beta_1+\beta_2)}\cos(\alpha_1)U^\dagger_{1,0} + ie^{i\beta_2}\sin(\alpha_1)U^\dagger_{1,1} = 0$. Hence, β_1 is the unique angle in $[0, \pi)$ such that $\frac{e^{i\beta_1}U^\dagger_{1,0}}{iU^\dagger_{1,1}} \in \mathbb{R}$, namely $\arg(U_{1,0}) - \arg(U_{1,1}) + \frac{\pi}{2} \bmod \pi$. Then α_1 is the unique angle in $[0, \pi)$ such that $\tan(\alpha_1) = -\frac{e^{i\beta_1}U^\dagger_{1,0}}{iU^\dagger_{1,1}}$, and since $\alpha_1 \in (0, \pi)$, we have $\sin(\alpha_1) > 0$, so that $\beta_2 = \arg\frac{U_{0,1}}{i}$ and $\beta_3 = \arg(\frac{U_{1,0}}{ie^{i\beta_1}})$. This finishes proving the uniqueness.

Conversely, it is easy to see that given any unitary U, the unique possible values given above for β_1, α_1, β_2 and β_3 are well-defined and satisfy the desired properties (note that the existence also follows from the result of [114]). □

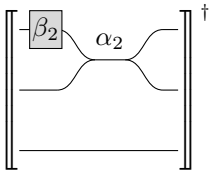
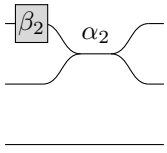
Lemma 5.13. *For any unitary* 3×3 *matrix* U*, there exist unique angles* $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in [0, \pi)$ *and* $\beta_4, \beta_5, \beta_6 \in [0, 2\pi)$ *such that* $\left[\!\!\left[\right.\right.$  $\left.\right]\!\!\right]_{\mathrm{pp}} = U$*, where* $\forall i \in \{1, 2, 3\}, \alpha_i \in \{0, \frac{\pi}{2}\} \Rightarrow \beta_i = 0$*, and where* $\alpha_2 = 0 \Rightarrow \alpha_1 = 0$*.*

Proof. Let us consider such $\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in [0, \pi)$ and $\beta_4, \beta_5, \beta_6 \in [0, 2\pi)$. We first prove that, assuming that they exist, their values are uniquely determined by U.

Let $U_1 \coloneqq$  $\circ\, U^\dagger$, $U_2 \coloneqq$  $\circ\, U^\dagger$ and $U_3 \coloneqq$  $\circ\, U^\dagger$, where $[\![-]\!]_{\mathrm{pp}}$ is defined in Definition 5.11.

By construction, $U_3 = \begin{pmatrix} e^{-i\beta_4} & 0 & 0 \\ 0 & e^{-i\beta_5} & 0 \\ 0 & 0 & e^{-i\beta_6} \end{pmatrix}$, so that

$$U_2 = \begin{pmatrix} e^{-i\beta_4} & 0 & 0 \\ 0 & e^{-i(\beta_3+\beta_5)}\cos(\alpha_3) & -ie^{-i(\beta_3+\beta_6)}\sin(\alpha_3) \\ 0 & -ie^{-i\beta_5}\sin(\alpha_3) & e^{-i\beta_6}\cos(\alpha_3) \end{pmatrix}, \tag{E}$$

and $U_1 =$  $\circ\, U_2$. Since  does not act on the last mode, this implies that $(U_1)_{2,0} = 0$.[30] That is, by definition of U_1, $ie^{i\beta_1}\sin(\alpha_1)U_{0,1}^\dagger + \cos(\alpha_1)U_{0,2}^\dagger = 0$.

- If $U_{0,1}, U_{0,2} \neq 0$, then this equality implies that $\cos(\alpha_1) \neq 0$ and $\sin(\alpha_1) \neq 0$ (indeed, if $\cos(\alpha_1) = 0$ then $\sin(\alpha_1) = \pm 1$ and conversely, which in both cases prevents the equality from being satisfied). Hence, β_1 is the unique angle in $[0, \pi)$ such that $\frac{ie^{i\beta_1}U_{0,1}^\dagger}{U_{0,2}^\dagger} \in \mathbb{R}$, namely $\arg(U_{0,1}) - \arg(U_{0,2}) + \frac{\pi}{2} \bmod \pi$. Then α_1 is the unique angle in $[0, \pi) \setminus \{\frac{\pi}{2}\}$ such that $\tan(\alpha_1) = -\frac{U_{0,2}^\dagger}{ie^{i\beta_1}U_{0,1}^\dagger}$.
- If $U_{0,2} = 0$ and $U_{0,1} \neq 0$, then $\sin(\alpha_1) = 0$, which means, since $\alpha_1 \in [0, \pi)$, that $\alpha_1 = 0$. Due to the constraints on the angles, this implies that $\beta_1 = 0$ too.
- If $U_{0,1} = 0$ and $U_{0,2} \neq 0$, then $\cos(\alpha_1) = 0$, which means, since $\alpha_1 \in [0, \pi)$, that $\alpha_1 = \frac{\pi}{2}$. Due to the constraints on the angles, this implies that $\beta_1 = 0$ too.
- If $U_{0,1} = U_{0,2} = 0$, then since U is unitary, it is of the form $U = \begin{pmatrix} e^{i\varphi} & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$, where $*$ denotes any complex number. Then, regardless of α_1 and β_1, U_1 is of the same form: $U_1 = \begin{pmatrix} e^{i\varphi} & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$. Consequently, $U_2 = \begin{pmatrix} e^{i\varphi}\cos(\alpha_2) & * & * \\ ie^{i\varphi}\sin(\alpha_2) & * & * \\ 0 & * & * \end{pmatrix}$. By (E), this implies that $\sin(\alpha_2) = 0$, which means, since $\alpha_2 \in [0, \pi)$, that $\alpha_2 = 0$. Due to the constraints on the angles, this implies that $\alpha_1 = \beta_1 = \beta_2 = 0$ too.

Thus, α_1 and β_1, and in turn U_1, are uniquely determined given U.

[30] We denote by $M_{i,j}$ the entry of indices (i, j) of a matrix M, the index of the first row and column being 0.

Since $(U_1)_{2,0} = 0$, U_1 can be written as $\begin{pmatrix} (U_1)_{0,0} & * & * \\ (U_1)_{1,0} & * & * \\ 0 & * & * \end{pmatrix}$. By (E) we have $(U_2)_{1,0} = 0$, that is, $ie^{i\beta_2}\sin(\alpha_2)(U_1)_{0,0} + \cos(\alpha_2)(U_1)_{1,0} = 0$. Since U_1 is unitary, $|(U_1)_{0,0}|^2 + |(U_1)_{1,0}|^2 = 1$, so that we cannot have $(U_1)_{0,0} = (U_1)_{1,0} = 0$. The other cases are similar to those of α_1 and β_1:

- If $(U_1)_{0,0}, (U_1)_{1,0} \neq 0$, then similarly, the equality implies that $\cos(\alpha_2) \neq 0$ and $\sin(\alpha_2) \neq 0$. Hence, β_2 is the unique angle in $[0, \pi)$ such that $\frac{ie^{i\beta_2}(U_1)_{0,0}}{(U_1)_{1,0}} \in \mathbb{R}$, namely $\arg((U_1)_{1,0}) - \arg((U_1)_{0,0}) + \frac{\pi}{2} \bmod \pi$. Then α_2 is the unique angle in $[0, \pi) \setminus \{\frac{\pi}{2}\}$ such that $\tan(\alpha_2) = -\frac{(U_1)_{1,0}}{ie^{i\beta_2}(U_1)_{0,0}}$.
- If $(U_1)_{1,0} = 0$ and $(U_1)_{0,0} \neq 0$, then $\sin(\alpha_2) = 0$, which means, since $\alpha_2 \in [0, \pi)$, that $\alpha_2 = 0$. Due to the constraints on the angles, this implies that $\beta_2 = 0$ too.
- If $(U_1)_{0,0} = 0$ and $(U_1)_{1,0} \neq 0$, then $\cos(\alpha_2) = 0$, which means, since $\alpha_2 \in [0, \pi)$, that $\alpha_2 = \frac{\pi}{2}$. Due to the constraints on the angles, this implies that $\beta_2 = 0$ too.

Thus, α_2 and β_2, and in turn U_2, are also uniquely determined given U.

Furthermore, (E) implies that

- If $(U_2)_{1,1}, (U_2)_{2,1} \neq 0$, then β_3 is the unique angle in $[0, \pi)$ such that $\frac{e^{i\beta_3}(U_2)_{1,1}}{i(U_2)_{2,1}} \in \mathbb{R}$, namely, $\arg((U_2)_{2,1}) - \arg((U_2)_{1,1}) + \frac{\pi}{2} \bmod \pi$, and α_3 is the unique angle in $[0, \pi)$ such that $\tan(\alpha_3) = \frac{i(U_2)_{2,1}}{e^{i\beta_3}(U_2)_{1,1}}$.
- If $(U_2)_{2,1} = 0$ and $(U_2)_{1,1} \neq 0$ then $\sin(\alpha_3) = 0$, which means, since $\alpha_3 \in [0, \pi)$, that $\alpha_3 = 0$. Due to the constraints on the angles, this implies that $\beta_3 = 0$ too.
- If $(U_2)_{1,1} = 0$ and $(U_2)_{2,1} \neq 0$, then $\cos(\alpha_3) = 0$, which means, since $\alpha_3 \in [0, \pi)$, that $\alpha_3 = \frac{\pi}{2}$. Due to the constraints on the angles, this implies that $\beta_3 = 0$ too.

Thus, α_3 and β_3, and in turn U_3, are also uniquely determined given U.

Finally, since $U_3 = \begin{pmatrix} e^{-i\beta_4} & 0 & 0 \\ 0 & e^{-i\beta_5} & 0 \\ 0 & 0 & e^{-i\beta_6} \end{pmatrix}$, we necessarily have $\beta_4 = -\arg((U_3)_{0,0})$, $\beta_5 = -\arg((U_3)_{1,1})$ and $\beta_6 = -\arg((U_3)_{2,2})$. This finishes proving the uniqueness.

Conversely, it is easy to see that the unique possible values given above for α_1, α_2, α_3, β_1, β_2, β_3, β_4, β_5 and β_6 are well-defined for any unitary U and satisfy the desired properties, which proves the existence. □

Remark 5.14. *It is possible to generalise the proof of Lemma 5.13 to extend the result to an arbitrary number of modes (namely, to prove that any unitary $n \times n$ matrix is represented in a unique way by a circuit with the same shape and conditions on the angles as in Figure 5.10). This provides an alternative proof of Proposition 5.37.*

$\mathrm{LO_v}$-circuits are more expressive than $\mathrm{LO_{PP}}$-ones, they not only act on the polarisation but the use of detectors and sources allows for the representation of non-unitary evolutions: For any $\mathrm{LO_v}$-circuit $D : n \to m$, $[\![D]\!]$ is sub-unitary[31]. $\mathrm{LO_v}$-circuits are actually universal for sub-unitary transformations:

Theorem 5.15 (Universality of $\mathrm{LO_v}$)**.** *For every sub-unitary map $U : \mathbb{C}^{M_n} \to \mathbb{C}^{M_m}$ (i.e. such that $U^\dagger U \sqsubseteq I$) there exists a circuit $D : n \to m$ s.t. $[\![D]\!] = U$.*

Proof. The proof relies on the normal forms developed in Section 5.4 and on the universality of $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuits (Proposition 5.37). It is given at the end of Section 5.4. □

[31] U is sub-unitary (see for instance [119]) iff $U^\dagger U \sqsubseteq I$, where $\sqsubseteq$ is the Löwner partial order, i.e. $I - U^\dagger U$ is positive semi-definite. Equivalently, U is sub-unitary iff it is a sub-matrix of a unitary matrix.

5.2 Equational Theory

Two distinct $\mathrm{LO_v}$-circuits may represent the same quantum evolution: for instance, composing two negations is equivalent to the identity. In order to characterise equivalences of $\mathrm{LO_v}$-circuits, we introduce a set of equations, shown in Figure 5.4. They capture basic properties of $\mathrm{LO_v}$-circuits, such as: detectors and sources essentially absorbing the other generators (Equations (5.8) to (5.14)); parameters forming a monoid (Equations (5.1) to (5.3)); and various commutation properties (Equations (5.15) and (5.16)). Equations (5.4) to (5.7) are the axioms of the PBS-calculus that are relevant here (see Figure 3.4), and capture the behaviour of PBS and negations in the absence of other generators. Notice that there are two equations acting on 3 modes: Equation (5.6) and Equation (5.18). Equation (5.6) can be seen as related to the Yang-Baxter Equation [86] (see Equation (A.1) and its proof, and note that the right-hand side can be flipped upside down by deformation), while Equation (5.18) is a property of decompositions into Euler angles, generalised with additional phases. Indeed, in 3-dimensional space, the two sides of this equation correspond — if one ignores the phases — to two distinct decompositions in elementary rotations. Finally, Equation (5.17) captures the fact that a beam splitter performs the same operation as a wave plate, on the position instead of on the polarisation, and therefore can be simulated using wave plates, together with some PBS and negations that essentially serve to swap the polarisation with the position.

Definition 5.16 ($\mathrm{LO_v}$-calculus)**.** *Two* $\mathrm{LO_v}$*-circuits* D_1, D_2 *are equivalent according to the rules of the* $\mathrm{LO_v}$-calculus*, denoted* $\mathrm{LO_v} \vdash D_1 = D_2$*, if one can transform* D_1 *into* D_2 *using the equations given in Figure 5.4. More precisely,* $\mathrm{LO_v} \vdash \cdot = \cdot$ *is defined as the smallest congruence which satisfies the equations of Figure 5.4 in addition to the axioms of PROP.*

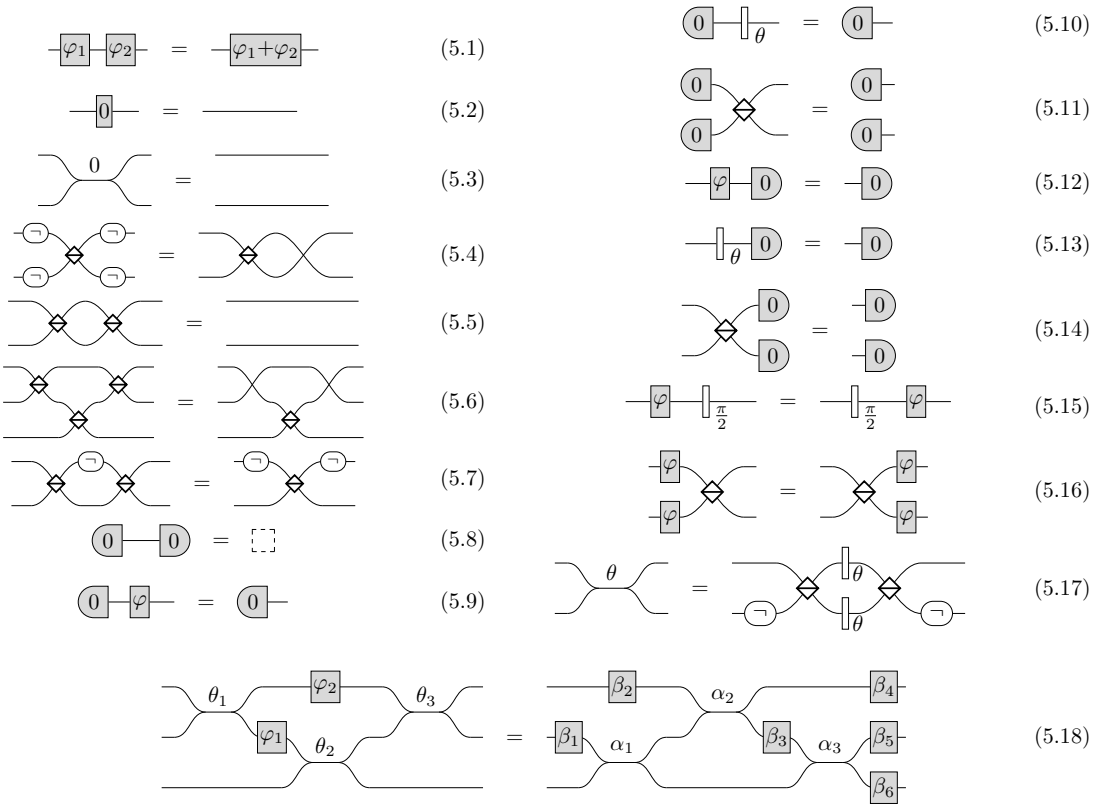


Figure 5.4: Axioms of the $\mathrm{LO_v}$-calculus. The equations are valid for arbitrary parameters $\varphi, \varphi_i, \theta, \theta_i \in \mathbb{R}$. In Equation (5.18), the angles on the left-hand side can take any value while the right-hand side is given by Lemma 5.13 (where U is the $[\![.]\!]_{\mathrm{pp}}$-semantics of the left-hand side of the equation).

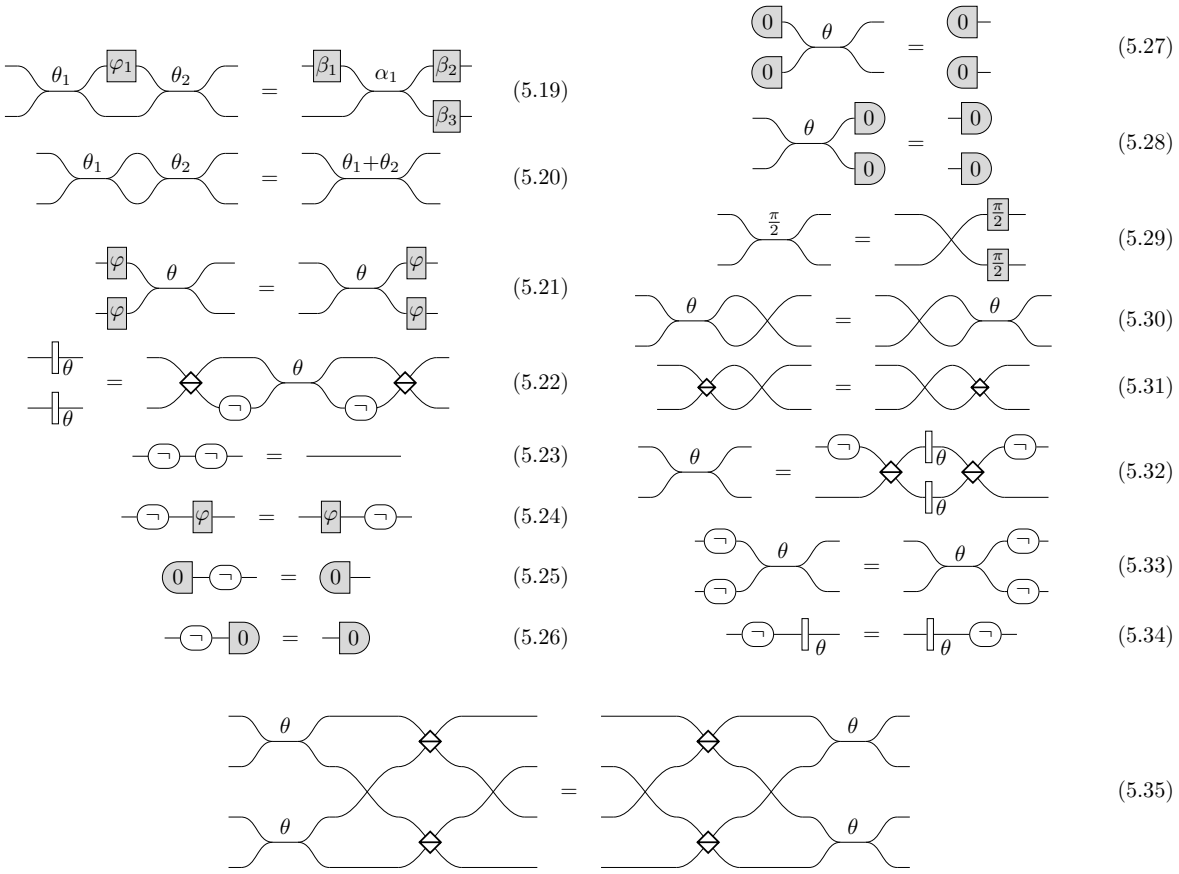


Figure 5.5: Useful consequences of the axioms of the $\mathrm{LO_v}$-calculus. In Equation (5.19), the angles on the left-hand side can take any value, and the right-hand side is given by Lemma 5.12.

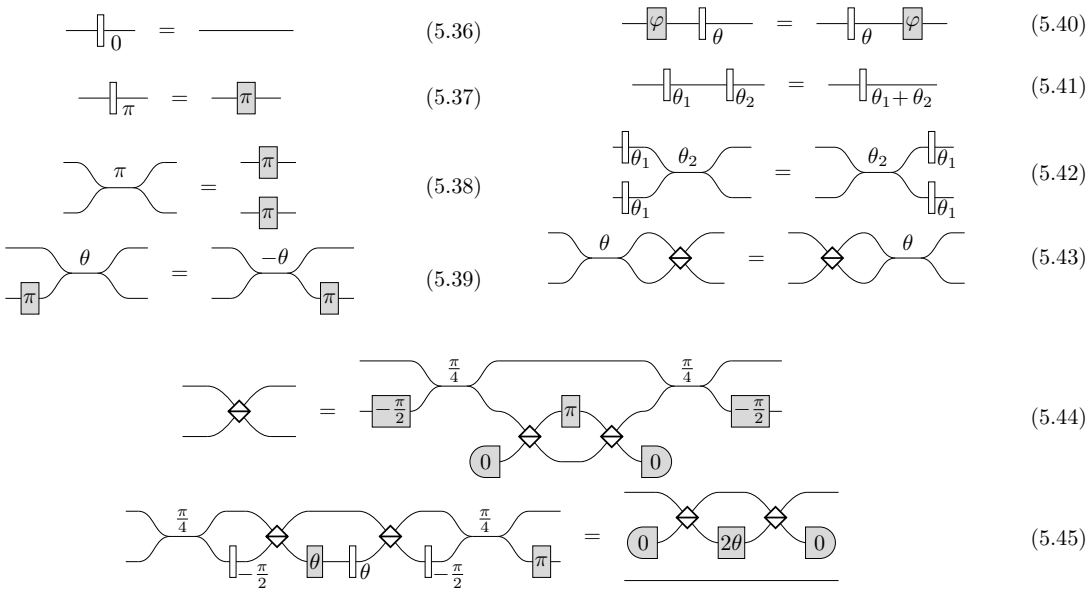


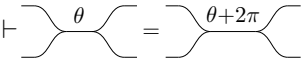
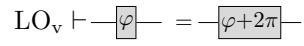
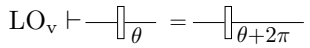
Figure 5.6: Interesting consequences of the axioms of the $\mathrm{LO_v}$-calculus.

Proposition 5.17 (Soundness)**.** *For any two* $\mathrm{LO_v}$*-circuits* D_1, D_2*, if* $\mathrm{LO_v} \vdash D_1 = D_2$ *then* $[\![D_1]\!] = [\![D_2]\!]$*.*

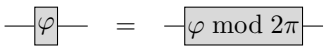
Proof. Since semantic equality is a congruence, it suffices to check that for every equation of Figure 5.4 both sides have the same semantics, which follows from Definition 5.6 and Lemma 5.13. □

Example 5.18. *The* 2π*-periodicity of the parameters is proved using the equational theory, as Proposition 5.19. Figure 5.5 shows some other equations that will be useful in the rest of this chapter, in particular for proving that the equational theory is complete (Theorem 5.22), and that we derive explicitly from the axioms (the derivations are given in Appendix C.1). Figure 5.6 shows some additional interesting properties that are not directly used in the proofs; the fact that these are consequences of the axioms of Figure 5.4 will follow from the completeness result.*

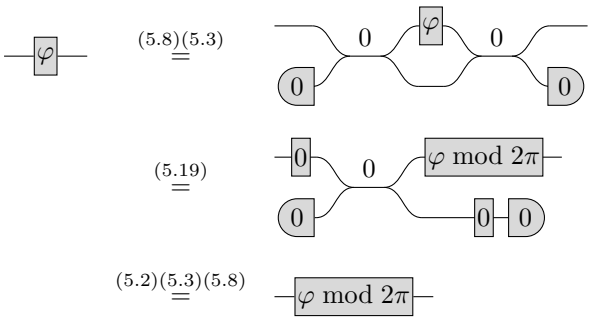
Proposition 5.19. *The rules of the* $\mathrm{LO_v}$*-calculus imply that the parameters are* 2π*-periodic, i.e. for any* $\theta, \varphi \in \mathbb{R}$*:*

$\mathrm{LO_v} \vdash$  $\mathrm{LO_v} \vdash$  $\mathrm{LO_v} \vdash$ 

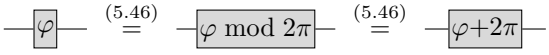
Proof. We actually prove a stronger version of the 2π-periodicity for the phase shifter:

 (5.46)

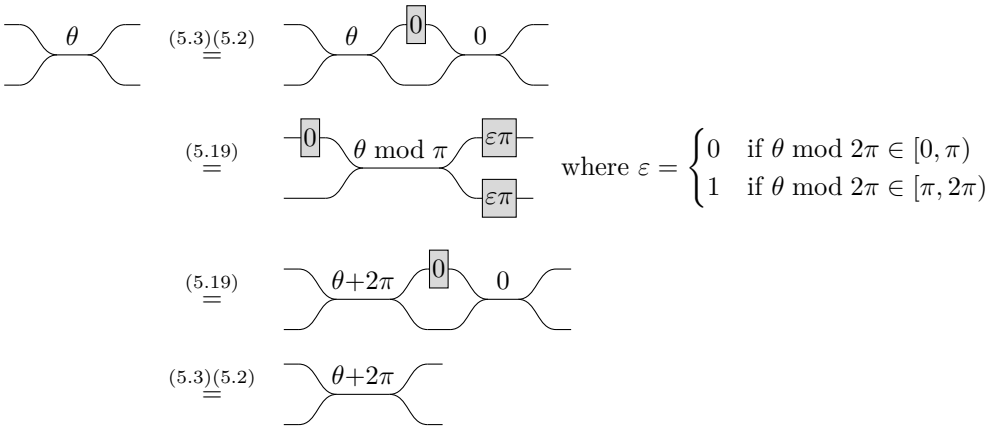
as follows:



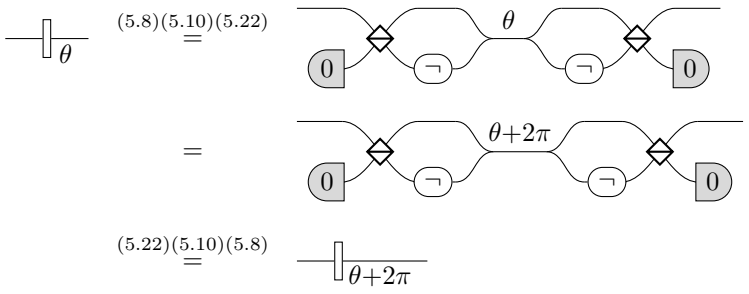
Then, the equality of Proposition 5.19 follows straightforwardly:



To prove the 2π-periodicity for the beam splitter, we proceed as follows:

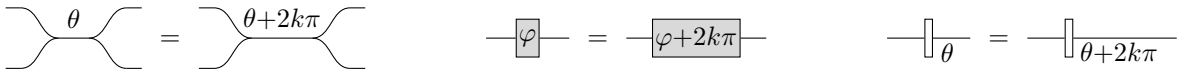


Finally, the 2π-periodicity for the wave plate follows from that for the beam splitter as follows:



□

Remark 5.20. *Note that we could also prove the following stronger equations, for any $k \in \mathbb{Z}$, with the same sequence of rewriting steps, that is, in a bounded number of steps:*



Lemma 5.21. *The equations of Figure 5.5 are consequences of the axioms of the* $\mathrm{LO_v}$*-calculus.*

Proof. The derivations are given in Appendix C.1. □

We now state one of our main results: the completeness of the $\mathrm{LO_v}$-calculus.

Theorem 5.22 (Completeness)**.** *For any two* $\mathrm{LO_v}$*-circuits D_1, D_2, if $[\![D_1]\!] = [\![D_2]\!]$ then* $\mathrm{LO_v} \vdash D_1 = D_2$.

The proof of Theorem 5.22 is given in Section 5.4. As a step towards proving the theorem, we first consider the fragment of the $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuits.

5.3 Polarisation-Preserving Circuits

This section gives a universal normal form for any $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit. We prove the uniqueness of that form by introducing a strongly normalising and confluent polarisation-preserving rewriting system: PPRS.

Definition 5.23. *The rewriting system* PPRS *is defined on* $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$*-circuits with the rules of Figure 5.7.*

First, note that the rewriting system PPRS is sound with respect to the $\mathrm{LO_v}$ equational theory:

Lemma 5.24. *If D_1 rewrites to D_2 using the* PPRS *rewriting system then* $\mathrm{LO_v} \vdash D_1 = D_2$.

Proof. It suffices to show for each rule of Figure 5.7 that it is sound with respect to the equational theory, that is, that we can transform the left-hand side into the right-hand side using the axioms of the $\mathrm{LO_v}$-calculus.

The soundness of Rules (5.56) and (5.57) is a direct consequence of Proposition 5.19. Note that in both cases, transforming the left-hand side into the right-hand side using the equations of Figure 5.4 only requires a bounded number of rewriting steps (see Remark 5.20).

The soundness of Rule (5.58) is a direct consequence of Equation (5.1).

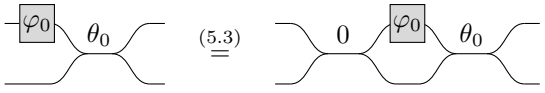
The soundness of Rule (5.59) is a direct consequence of Equation (5.2).

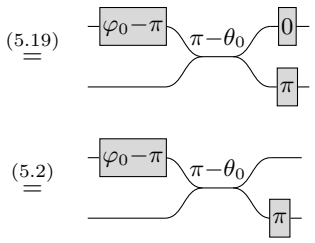
The soundness of Rule (5.60) is a direct consequence of Equation (5.3).

The soundness of Rule (5.61) is a direct consequence of Equations (5.2), (5.1) and (5.21).

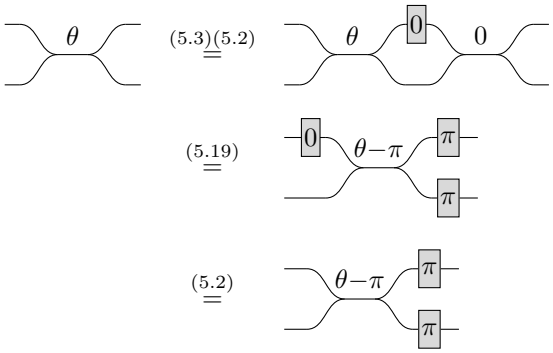
The soundness of Rule (5.62) is a direct consequence of Equation (5.29), (5.1) and (5.2).

To prove the soundness of Rule (5.63), if $\varphi \in [\pi, 2\pi)$ and $\theta \in (0, \pi)$, then we have:





To prove the soundness of Rule (5.64), if $\theta \in [\pi, 2\pi)$ then we have:



The soundness of Rule (5.65) is a direct consequence of Equations (5.18) and (5.2).
The soundness of Rule (5.66) is a direct consequence of Equations (5.19) and (5.2). □

Theorem 5.25. *The rewriting system* PPRS *is strongly normalising.*

Proof. Given a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit $D : n \to n$, let us consider the tuple (a, b, c, d, e), defined as follows.

- a is the number of beam splitters in D with angle not in $[0, \pi)$
- b is the number of beam splitters in D with angle not in $[0, 2\pi)$
- $c = \sum_{i=0}^{n-2} (n-i)c(i)$ where $c(i)$ is the number of beam splitters in D between positions i and $i+1$
- To define d, let us define the *depth* of a phase shifter p of D, denoted $d(p)$, as the maximal number of beam splitters that a photon starting from p and going to the right would be able to traverse before reaching an output port, if it were allowed to choose each time whether to be reflected or transmitted. Then $d \coloneqq \sum_{p \text{ phase shifter of } D} w(p) \cdot 9^{d(p)}$, where, given a phase shifter $p = \boxed{\varphi}$ of D,

$$w(p) \coloneqq \begin{cases} 4 & \text{if } p \text{ belongs to a pattern of the form } \boxed{\varphi}\ \boxed{\varphi_1}\cdots\boxed{\varphi_k}\ \theta \\ 3 & \text{if } p \text{ does not belong to such a pattern and } \varphi \notin [0, \pi) \\ 2 & \text{if } p \text{ does not belong to such a pattern and } \varphi \in [0, \pi) \end{cases}.$$

- e is the number of phase shifters in D with angle not in $[0, 2\pi)$.

Since $\mathbb{N}^5$ is well-ordered with respect to the lexicographic order, to prove that the rewriting system is strongly normalising, it suffices to prove that each of the rewriting rules strictly decreases the tuple (a, b, c, d, e) with respect to this order.

- Rule (5.56) strictly decreases e without increasing any component of the tuple.
- Rule (5.57) strictly decreases b without increasing a.

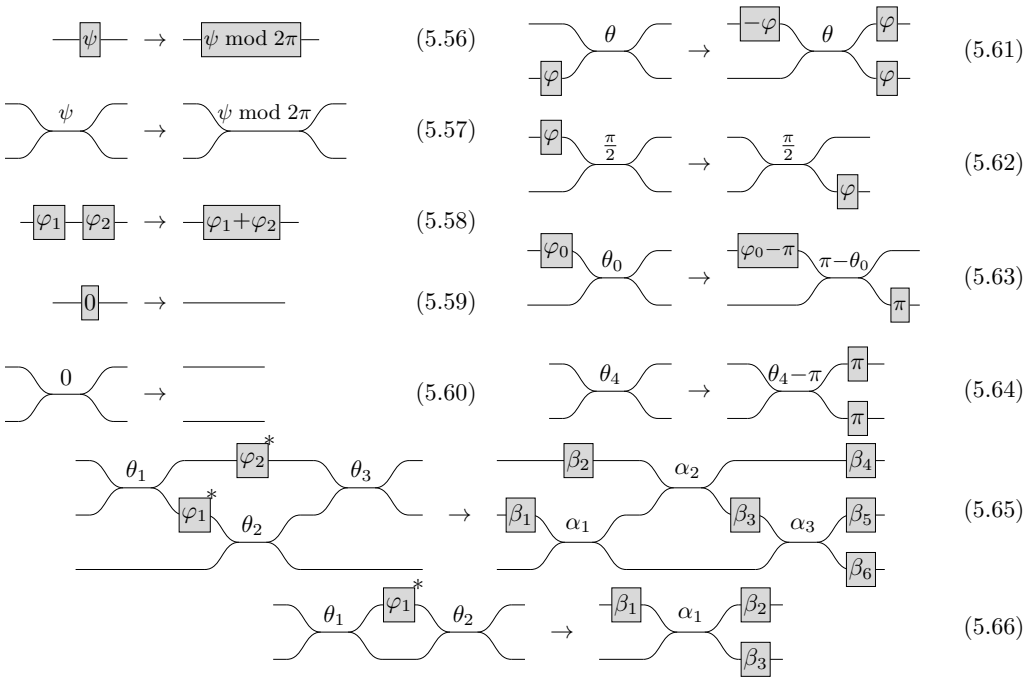
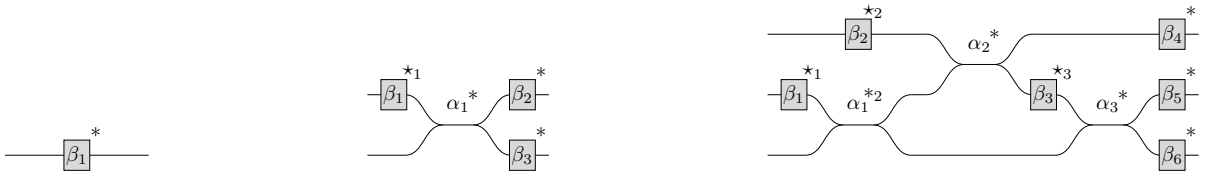


Figure 5.7: Rewriting rules of PPRS. $\psi \in \mathbb{R} \setminus [0, 2\pi)$, $\varphi, \varphi_1, \varphi_2 \in (0, 2\pi)$, $\varphi_0, \theta_4 \in [\pi, 2\pi)$, $\theta, \theta_0, \theta_1, \theta_2, \theta_3 \in (0, \pi)$, and $\theta_0 \neq \frac{\pi}{2}$. $-\boxed{\varphi}^{*}-$ denotes either $-\boxed{\varphi}-$ or $-\!-\!-$. In Rules (5.65) and (5.66), the angles on the left-hand side can take any value while the right-hand side is given by Lemma 5.13 and Lemma 5.12 respectively.

- Rule (5.58) does not change a, b or c since it does not affect the beam splitters; and strictly decreases d. Indeed, it transform two phase shifters p_1, p_2 of same depth into a phase shifter p_{12} with same depth as p_1 and p_2; if $w(p_{12}) = 4$ then this means that one had $w(p_1) = w(p_2) = 4$, so that d has strictly decreased since $w(p_{12}) < w(p_1)+w(p_2)$; and if $w(p_{12}) \in \{2, 3\}$ then since $w(p_1)+w(p_2) \geq 4$, one also has $w(p_{12}) < w(p_1) + w(p_2)$, so that d has strictly decreased.
- Rule (5.59) does not increase a, b or c since it does not affects the beam splitters; and it strictly decreases d since it removes a phase shifter.
- Rule (5.60) does not increase a or b since it only removes a beam splitter, and strictly decreases c.
- Rule (5.61) does not change a, b or c since it does not affect the beam splitters, and it strictly decreases d. Indeed, removes a phase shifter p on the bottom left of a beam splitter, which decreases d by $4 \cdot 9^{d(p)}$, adds a phase shifter of depth $d(p)$ on the top left of this beam splitter, which increases d by at most $3 \cdot 9^{d(p)}$, and adds two phase shifters of depth at most $d(p) - 1$, which increases d twice by at most $4 \cdot 9^{d(p)-1}$. In total, d has decreased by at least $4 \cdot 9^{d(p)} - 3 \cdot 9^{d(p)} - 8 \cdot 9^{d(p)-1} = 9^{d(p)-1}$.
- Rule (5.62) does not change a, b or c since it does not affect the beam splitters, and it strictly decreases d since it moves a phase shifter to a place where it has strictly lower depth.
- Rule (5.63) does not change a, b or c since it affects the beam splitters only by changing the angle of one of them and keeps this angle in $(0, \pi)$, and it strictly decreases d. Indeed, it takes a phase shifter p with angle not in $[0, \pi)$ on the top left of a beam splitter, and puts its angle in $[0, \pi)$, which decreases d by $9^{d(p)}$. It also adds a phase shifter of depth at most $d(p) - 1$, which increases d by at most $4 \cdot 9^{d(p)-1}$. In total, d has decreased by at least $5 \cdot 9^{d(p)-1}$.
- Rule (5.64) strictly decreases a.



(a) For $n = 1$ (b) For $n = 2$ (c) For $n = 3$

Figure 5.8: Normal forms of PPRS for $n \in \{1, 2, 3\}$. $*$ means that the phase shifter or beam splitter is replaced by (an) identity wire(s) when the angle is zero. $*_i$ represents the identity in the preceding case and also when $\alpha_i = 0$. $\star_i$ represents the identity in the preceding two cases and also when $\alpha_i = \frac{\pi}{2}$. The α_i are in $[0, \pi)$ as well as the phases with a $\star_i$, all other phases are in $[0, 2\pi)$.

- Rule (5.65) decreases c by 1, and does not increase a or b since it only outputs beam splitters with angle in $[0, \pi)$.
- Rule (5.66) does not increase a or b since it can only output a beam splitter with angle in $[0, \pi)$, and it strictly decreases c. □

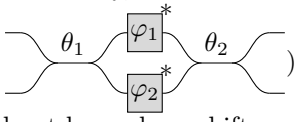
As PPRS is terminating, every $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit can be reduced to at least one normal form. The next step is to show that the normal forms are unique, this is the purpose of Theorem 5.27. To this end, it is useful to first characterise the normal forms of circuits on at most three modes:

Lemma 5.26. *For any* $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$*-circuit of size* $n \in \{1, 2, 3\}$*,* PPRS *terminates to a unique normal form with the shape shown in Figure 5.8.*

Proof. First, we show that the normal forms are necessarily of the form given in Figure 5.8.

In a normal form, because of Rule (5.56), all phase shifters have angle in $[0, 2\pi)$; because of Rules (5.57) and (5.64), all beam splitters have angle in $[0, \pi)$; because of Rules (5.59) and (5.60), there is no phase shifters or beam splitters with angle 0; because of Rule (5.62), there is no phase shifter on the top left of a $\frac{\pi}{2}$-angled beam splitter; and because of Rule (5.63), all phase shifters on the top left of a beam splitter have angle in $[0, \pi)$. Thus, if a normal form is of one of the three forms given in Figure 5.8, then the conditions on the angles are satisfied.

Because of Rule (5.58), a normal form cannot contain two consecutive phase shifters. This implies in particular that the normal forms have the claimed shape for $n = 1$.

Additionally, a normal form also cannot contain two consecutive beam splitters (i.e. a pattern of the form 

). Indeed, because of Rule (5.61), in such a pattern in a normal form, there would not be a phase shifter on the bottom wire, so that the pattern would be reducible by Rule (5.66). Thus, in the case where $n = 2$, a normal form contains at most one beam splitter. Because of Rule (5.61), such a beam splitter does not have any phase shifter on its bottom left, and because of Rule (5.58), there is at most one phase shifter on each of its other three ports. Because of Rule (5.62), there is no phase shifter on the bottom right if the angle of the beam splitter is $\frac{\pi}{2}$. Moreover, if the normal form does not contain a beam splitter, then because of Rule (5.58) there is at most one phase shifter on each of the two wires. Thus, in all cases, the normal forms have the claimed shape for $n = 2$.

In the case where $n = 3$, since there cannot be two consecutive beam splitters in a normal form, the beam spitters are alternatively between the top two wires and the bottom two wires. Because of Rules (5.61) and (5.58), if there is a beam splitter between the top two wires, then one betwen the bottom two wires, and then again one between the top two wires, those three beam splitter necessarily match the left-hand side of Rule (5.65). Hence, a normal form contains at most three beam splitters: at most one on the top and two on the bottom. Additionally, if the one on the top is not here, then since there cannot be two consecutive beam splitters, there is only one on the bottom. Finally, Rules (5.61) and (5.58) guarantee that the phase shifters are such that the normal form has the shape given in Figure 5.8c.

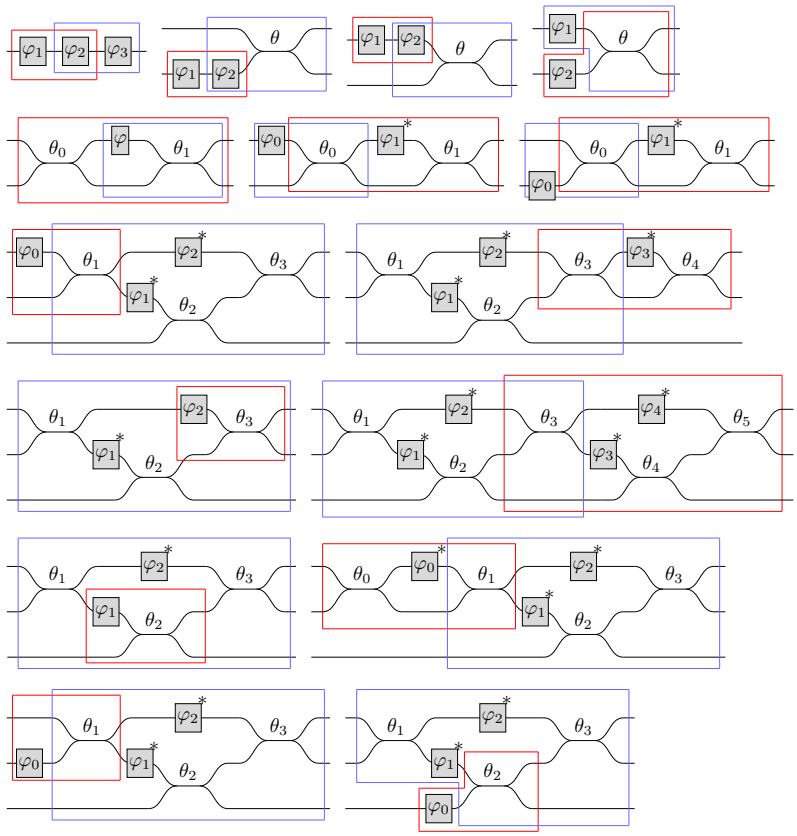


Figure 5.9: Non-trivial critical peaks (more precisely, those not involving single-generator patterns).

Now, we want to show that the normal forms are unique (that is, that the normal form of any circuit is unique). Lemma 5.24 and Proposition 5.17 imply that the rewriting rules preserve the semantics, hence it suffices to show that the circuits of Figure 5.8 are uniquely determined by their semantics. One can check that given any circuit of the form given in Figure 5.8b (resp. Figure 5.8c), there is a (unique) way of adding 0-angled phase shifters and beam splitters that gives us a circuit of the form of Lemma 5.12 (resp. Lemma 5.13) with the conditions on the angles satisfied. Then the uniqueness for $n = 2$ and $n = 3$ follows from the uniqueness given by Lemma 5.12 and Lemma 5.13 respectively. For $n = 1$, the proof is straightforward. □

Theorem 5.27. PPRS *is globally confluent.*

Proof. Since PPRS is strongly normalising, by Newman's lemma [125], it suffices to prove that PPRS is locally confluent.

First, note that the trivial critical pairs, in which the two rewriting rules are applied to disjoint patterns, can be closed in a straightforward way. Indeed, after doing any of the two transformations involved, the other one can be done independently, and the final result does not depend on which transformation was applied first.

Additionally, the non-trivial critical pairs (see Figure 5.9) all involve at most three (spatial) modes.

Indeed, first, two overlapping patterns necessarily share at least one spatial mode, so that if they both involve at most two modes, then their union involves at most three modes. This implies that any non-trivial critical pair involving at least four modes must arise from at least one instance of Rule (5.65).

If the other rewriting step of the critical pair is not an instance of Rule (5.65), it would involve at most two modes. For the union with the instance of Rule (5.65) to involve four modes, it must involve exactly

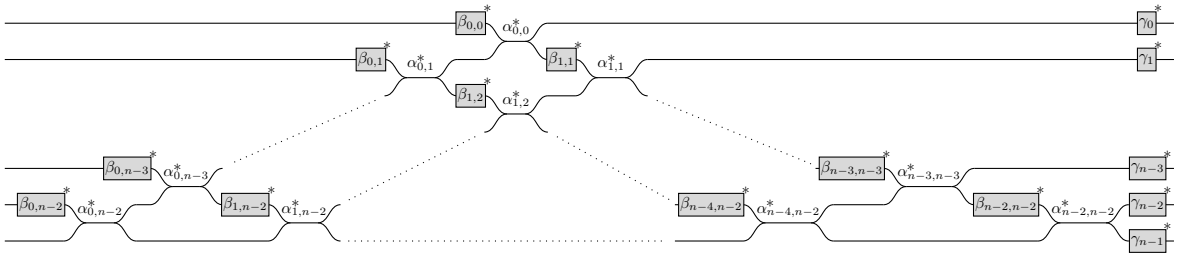


Figure 5.10: General scheme of a PPRS triangular normal form. The stars mean that any phase shifter or beam splitter with angle 0 is replaced by the identity. The conditions on the angles are the following: $\alpha_{i,j}, \beta_{i,j} \in [0, \pi)$; $\gamma_i \in [0, 2\pi)$; $\alpha_{i,j} = 0 \Rightarrow \forall j' > j, \alpha_{i,j'} = 0$; $\alpha_{i,j} \in \{0, \frac{\pi}{2}\} \Rightarrow \beta_{i,j} = 0$.

two modes and the two patterns must share only one mode. Consequently, their union is composed only of phase shifters. Since in the left-hand side of Rule (5.65) there is at most one phase shifter on each mode, the union of the two patterns must be a single phase shifter.[32] Moreover, for the two patterns to share not more than one mode, it must be on the top mode of one pattern and on the bottom mode of the other pattern. Namely, since the left-hand side of Rule (5.65) does not have a phase shifter on the bottom mode, it must be on the top mode of the associated pattern and on the bottom mode of the other pattern. The only rule in which the left-hand side involves two modes and has a phase shifter on the bottom mode is Rule (5.61), but this phase shifter cannot belong to a pattern corresponding to the left-hand side of Rule (5.65) since it would be both on the top left and on the bottom left of a beam splitter at the same time, which is not possible.

Hence, any non-trivial critical pair involving at least four modes must arise from two instances of Rule (5.65). Since the left-hand side of this rule does not have a phase shifter on the bottom mode, the two patterns cannot share only one mode and must share at least two modes. Then since their union involves at least four modes, they share exactly two modes. These two modes are the top two of one pattern and the bottom two of the other pattern. In the left-hand side of Rule (5.65), there are at most two generators that act only on the bottom two modes and therefore can be in the intersection of the two patterns: the phase shifter labeled with φ_1 if present, and the beam splitter labelled with θ_2. If the phase shifter labeled with φ_1 is in the intersection of the two patterns then it necessarily correspond to the phase shifter labeled with φ_2 in the other pattern, but this is not possible since on is on the top right of a beam splitter whereas the other is on the bottom right of a beam splitter. Therefore, the two patterns necessarily overlap by one beam splitter, which is the bottom one in one pattern and one of the two top ones in the other pattern. But in the left-hand side of Rule (5.65), the bottom beam splitter is connected by its top wires to the bottom of another beam splitter on each side, whereas each of the two top ones is connected by at least one of its top wires to the top wire of another beam splitter, hence the two patterns cannot overlap this way.

Thus, all non-trivial critical pairs involve at most three spatial modes. It follows from Lemma 5.26 that any critical pair on at most three wires can be closed, which gives us the local confluence. □

We now characterise the normal forms of PPRS in the general case.

Definition 5.28. *A* PPRS triangular normal form *is a circuit with a triangular shape similar to Figure 5.1a, but with all* 0*-angled generators replaced with identities and with additional conditions on the angles, as described in Figure 5.10.*

Figure 5.11 shows an example: the figure on the left is the "full" circuit with 0-angled beam splitters while on the right is the corresponding PPRS triangular normal form.

Lemma 5.29. *A* $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$*-circuit is irreducible if and only if it is a PPRS triangular normal form.*

Proof. First we prove that PPRS triangular normal forms are irreducible by checking that none of the rules of Figure 5.7 can be applied in a PPRS triangular normal form.

[32] Note that two patterns that overlap only by identities can be considered disjoint.

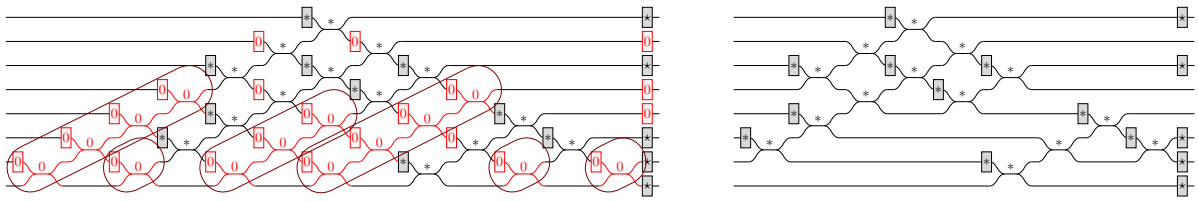


Figure 5.11: An example of a PPRS triangular normal form. In the figure on the left, the beam splitters and phase shifters with angle 0 in the corresponding triangular form are shown in red. In the figure on the right, they are replaced with identities.

- In a PPRS triangular normal form, the angles of all generators are in $(0, 2\pi)$ (indeed, in Figure 5.10, $\forall i, j,\ \alpha_{i,j}, \beta_{i,j}, \gamma_i \in [0, 2\pi)$, and all generators with angle 0 are replaced by the identity). Hence, one cannot apply Rules (5.56),(5.57),(5.59) and (5.60).

- For each beam splitter replaced by the identity in the scheme of Figure 5.10, the conditions on the angles imply that the phase shifter on its top left is replaced by the identity too. Hence, in a PPRS triangular normal form, any phase shifter must be either on the top left of a beam splitter, or on the far right of the circuit. In both cases, there cannot be another phase shifter on its right. Hence, there are no consecutive phase shifters, so that Rule (5.58) cannot be applied. Moreover, this also implies that a phase shifter cannot be on the bottom left of a beam splitter, so that Rule (5.61) cannot be applied either.

- The conditions on the angles imply that there is no phase shifter on the top left of a $\frac{\pi}{2}$-angled beam splitter. Hence, Rule (5.62) cannot be applied.

- The angles of the beam splitters, and of the phase shifters on the top left of beam splitters, are in $(0, \pi)$. Hence, Rules (5.63) and (5.64) cannot be applied.

- The triangular shape, together with the fact that $\alpha_{i,j} = 0 \Rightarrow \alpha_{i,j+1} = 0$ in Figure 5.10, imply that any beam splitter must be connected by its top right either directly to the output (possibly through a phase shifter), or to the bottom left of another beam splitter. In the left hand sides of Rules (5.65) and (5.66), the top right of the leftmost beam splitter is connected to the top left of another beam splitter, which is incompatible with this property. Hence, one cannot find these patterns in a PPRS triangular normal form, so that Rules (5.65) and (5.66) cannot be applied.

Now we want to prove that any irreducible circuit is a PPRS triangular normal form. First, note that any irreducible circuit satisfies the following properties:

- There are no consecutive phase shifters. This is due to Rule (5.58).

- All angles are in $(0, 2\pi)$. This is due to Rules (5.56),(5.57),(5.59) and (5.60).

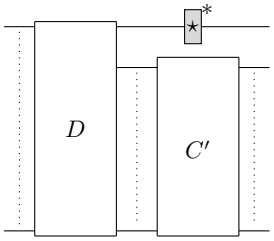
- The angles of the beam splitters, and of the phase shifters on the top left of beam splitters, are in $(0, \pi)$. This is due to Rules (5.63) and (5.64).

- There is no phase shifter on the top left of a $\frac{\pi}{2}$-angled beam splitter. This is due to Rule (5.62).

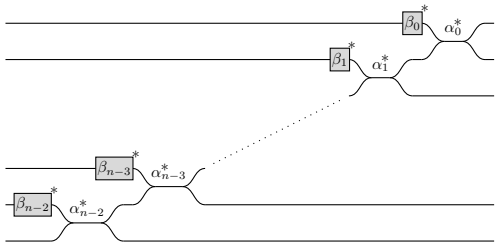
- There is no phase shifter on the bottom left of a beam splitter. This is due to Rule (5.61).

- There are not two consecutive beam splitters on the same modes. This is due to Rule (5.66) and to the fact that there is no phase shifter on the bottom left of a beam splitter.

Second, we can remark that a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit of size $n \geq 2$ is a PPRS triangular normal form if and only if it is of the form



where C' is a PPRS triangular normal form of size $n-1$, and D is of the form



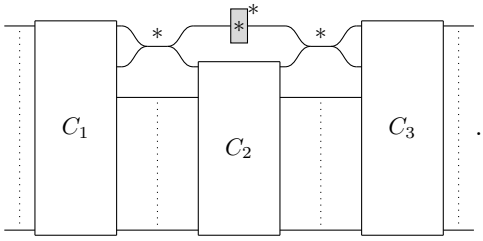
where, as in Figure 5.10, the stars mean that any phase shifter or beam splitter with angle 0 is replaced by the identity, and $\forall i,\ \alpha_i, \beta_i \in [0, \pi),\ \alpha_i = 0 \Rightarrow \alpha_{i+1} = 0,$ and $\alpha_i \in \{0, \frac{\pi}{2}\} \Rightarrow \beta_i = 0$. We will call such a circuit a *PS-BS-diagonal.*

We now prove by induction on n that any irreducible circuit of size n is a PPRS triangular normal form.

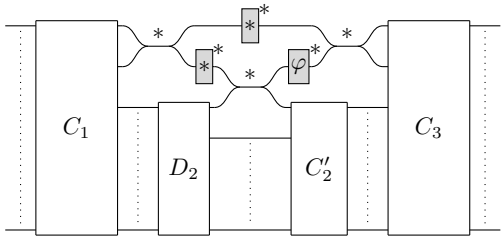
If $n \in \{1, 2, 3\}$, then the result follows directly from Lemma 5.26.

Given $n \geq 3$, let us assume that the result holds for circuits of size at most n, and consider an irreducible $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit C of size $n+1$.

First, C contains at most one beam splitter between the top two wires. Indeed, by contradiction, assume that it contains two beam splitters or more between the top two wires. Then by deformation, C can be written in the form



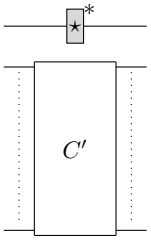
Since C is irreducible, C_2 is irreducible too, so that by induction hypothesis it is a PPRS triangular normal form. Since there cannot be two consecutive beam splitters in C, there must be a beam splitter between the top two wires in C_2. Thus by deformation, C can be written in the form



where D_2 is a PS-BS-diagonal and C_2' is a PPRS triangular normal form. If $\varphi \neq 0$ (that is, if the phase shifter is present), then C can be reduced using Rule (5.61). If $\varphi = 0$ (that is, if the phase shifter is not present), then C can be reduced using Rule (5.65). In both cases, this contradicts the fact that C is

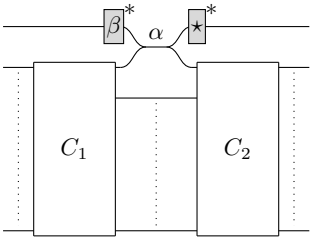
irreducible.

Thus, C contains at most one beam splitter between the top two wires. If it contains no beam splitter between these wires, then it is of the form

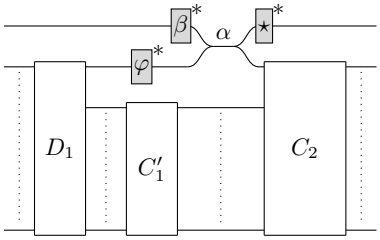


with C' irreducible. By induction hypothesis, C' is a PPRS triangular normal form. Note that the identity circuit is a PS-BS-diagonal (with $\forall i,\ \alpha_i = \beta_i = 0$), so that C is a PPRS normal form.

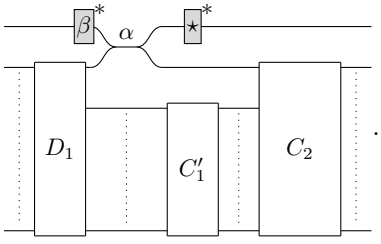
If C contains a beam splitter between the top two wires, then by deformation it can be written in the form



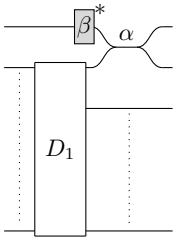
with C_1 and C_2 irreducible. Note that since C is irreducible, α cannot be equal to 0, and $\alpha = \frac{\pi}{2} \Rightarrow \beta = 0$. By induction hypothesis, C_1 is a PPRS triangular normal form, so that C can be further decomposed as



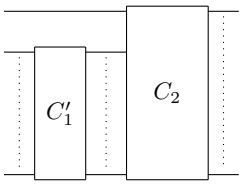
where D_1 is a PS-BS-diagonal and C_1' is a PPRS triangular normal form. Since there cannot be a phase shifter on the bottom left of a beam splitter, one has $\varphi = 0$, so that up to deformation,

$C =$ 

.

Since $\alpha \neq 0$ and $\alpha = \frac{\pi}{2} \Rightarrow \beta = 0$, 

necessarily satisfies the conditions to be a PS-BS-

diagonal. Moreover, 

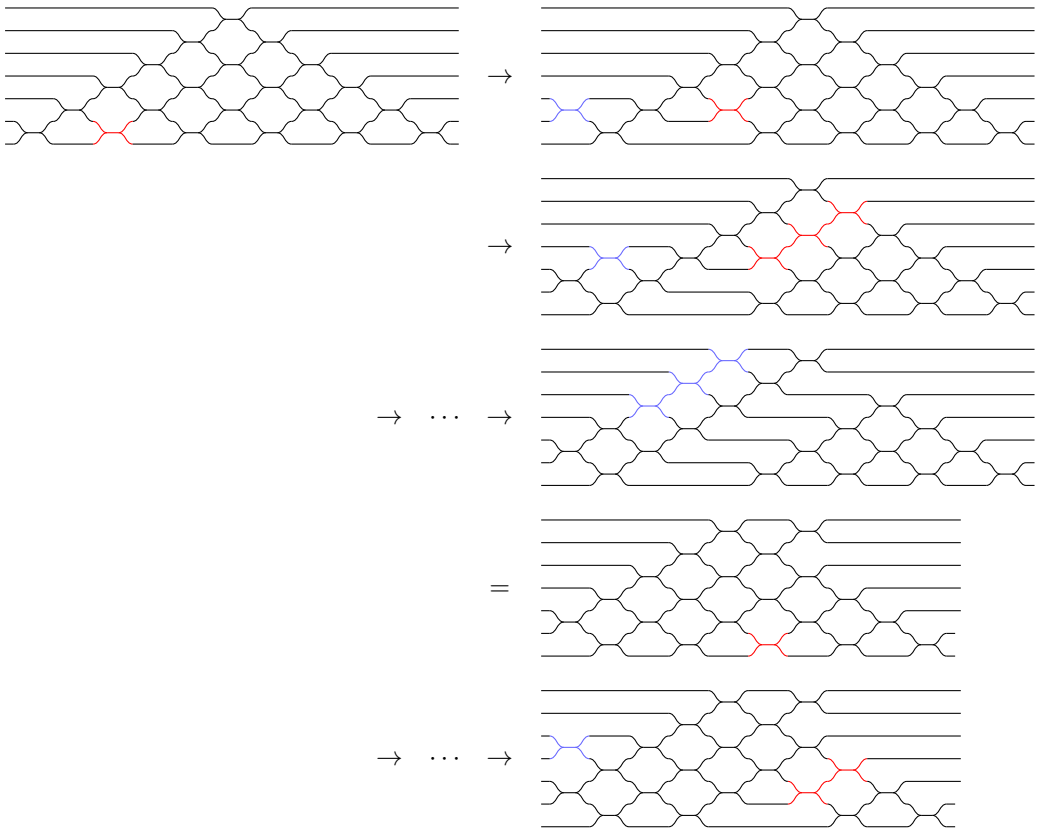
is irreducible as it is a sub-circuit of C, so that by induction hypothesis it is a PPRS triangular normal form. Hence, C is a PPRS triangular normal form. □

Theorem 5.30. *Any* $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$*-circuit, with the rules of* PPRS*, converges to a unique* PPRS *triangular normal form.*

Proof. Since PPRS is globally confluent and terminating, every circuit is reduced to a unique normal form. It follows from Lemma 5.29 that this normal form is a PPRS triangular normal form. □

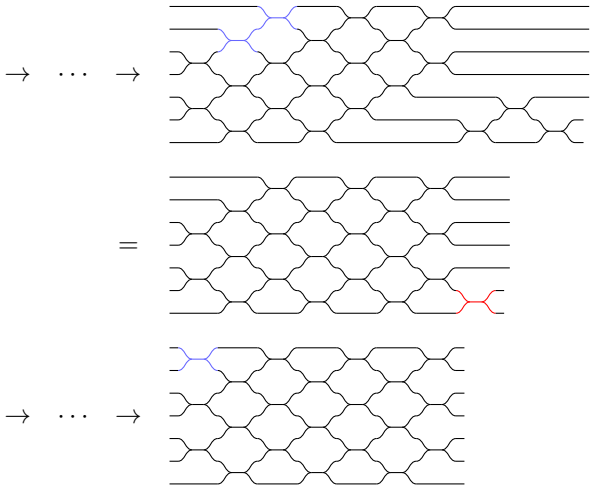
Remark 5.31. *By using Equation* (5.18) *(together with Equations* (5.1), (5.2) *and* (5.21)*) and by adding 0-angled beam splitters if necessary, one can turn any circuit in PPRS triangular normal form into a circuit in the rectangular form of [41] shown in Figure 5.1b.*

More precisely, if necessary, one adds 0-angled beam splitters in the PPRS triangular normal form to obtain a triangular shape, as in Figure 5.1a. Then, for example with 7 spatial modes, one proceeds as follows:[33]



[33]Here we only show how the beam splitters move along the process. We interpret Equation (5.18) as sliding one of the beam splitters through the two others while changing the parameters and adding some phase shifters. Before and after each move it may be necessary to manipulate the phase shifters with the help of Equations (5.1), (5.2) and (5.21). The beam splitters represented in red are just to be moved, and the beam splitters represented in blue have just been moved.

Note that we apply Equation (5.18) from right to left. Indeed, note that the upside-down version of Equation (5.18) is sound. This implies that by manipulating the phases, any pattern of three beam splitters of the shape of the right-hand side of Equation (5.18) and with angles in $[0, \pi)$ can be made to satisfy the required conditions, and that there exists a left-hand side with the angles of the beam splitters in $[0, \pi)$. In practice, one would in fact rather use a generalised version of Equation (5.18) with fewer conditions, which can be derived from the axioms of the LO_{V}-calculus (or of the $\mathrm{LO}_{\mathrm{PP}}$-calculus defined below) due to their completeness.



This leads us to a rectangular form of [41] (see Figure 5.1b).

We can now prove the completeness for the polarisation-preserving fragment.

Theorem 5.32. *For any* $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$*-circuits* C_1,C_2 *such that* $[\![C_1]\!]_{\mathrm{pp}} = [\![C_2]\!]_{\mathrm{pp}}$*, their normal forms are equal, i.e.* $N_1 = N_2$*, where* N_1 *(resp.* N_2*) is the unique normal form of* C_1 *(resp.* C_2*) given by Theorem 5.30.*

Proof. As the rewriting system preserves the semantics, it is sufficient to prove that $[\![N_1]\!]_{\mathrm{pp}} = [\![N_2]\!]_{\mathrm{pp}} \Rightarrow N_1 = N_2$.

Let id_n denote the identity circuit with n identity wires. First, we show by induction on n that $[\![N]\!]_{\mathrm{pp}} = [\![id_n]\!]_{\mathrm{pp}} \Rightarrow N = id_n$ for any PPRS triangular normal form $N\colon n \to n$.

For $n = 1$, $N =$ —$\boxed{\beta_1}^{*}$—. The semantics imposes $\beta_1 = 0$. Therefore $N = id_1$.

Let us consider the case where N is of size $n+1$. With the notations of Figure 5.10 for the angles, one has $\langle 0|\,[\![N]\!]_{\mathrm{pp}}\,|0\rangle = e^{i(\beta_{0,0}+\gamma_0)}\cos(\alpha_{0,0})$. Since $\langle 0|\,[\![id_{n+1}]\!]_{\mathrm{pp}}\,|0\rangle = 1$, this implies that $\alpha_{0,0} = 0$. In turn, the conditions on the angles imply that $\beta_{0,0} = 0$. Hence $\gamma_0 = 0$ too. Again by the conditions on the angles, one has $\forall i, \alpha_{0,i} = \beta_{0,i} = 0$. Thus, N is of the form $id_1 \oplus N'$ where N' is a PPRS triangular normal form. By induction hypothesis, $N' = id_n$, so that $N = id_{n+1}$, which concludes the induction.

Let P be an inverse circuit of N_1 and N_2, that is, a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit such that $[\![P]\!]_{\mathrm{pp}} = [\![N_1]\!]_{\mathrm{pp}}^{-1}$. The existence of such a circuit follows from [114]. As $[\![N_1P]\!]_{\mathrm{pp}} = [\![PN_2]\!]_{\mathrm{pp}} = [\![id_n]\!]_{\mathrm{pp}}$, the term N_1PN_2 can both be reduced to N_1 (by reducing PN_2 first) and N_2 (by reducing N_1P first). By Theorem 5.30, $N_1 = N_2$. □

It follows directly from Theorems 5.30 and 5.32 that one can obtain a complete equational theory for $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuits by turning the rules of Figure 5.7 into equations. This equational theory can be simplified, moreover it can be extended into a complete equational theory for $\mathrm{LO_{PP}}$-circuits by observing that the swap is equivalent to a $\frac{\pi}{2}$-angled beam splitter, up to a global phase.

Definition 5.33 ($\mathrm{LO_{PP}}$-calculus)**.** *Two* $\mathrm{LO_{PP}}$*-circuits* D_1, D_2 *are equivalent according to the rules of the* $\mathrm{LO_{PP}}$-calculus*, denoted* $\mathrm{LO_{PP}} \vdash D_1 = D_2$*, if one can transform* D_1 *into* D_2 *using the equations given in Figure 5.12. More precisely,* $\mathrm{LO_{PP}} \vdash \cdot = \cdot$ *is defined as the smallest congruence which satisfies the equations of Figure 5.12 in addition to the axioms of PROP.*

Remark 5.34. *The equations of Figure 5.12 are consequences of the axioms of the* $\mathrm{LO_v}$*-calculus. Indeed, Equations* (5.B) *and* (5.D) *correspond respectively to Equations* (5.3) *and* (5.1)*; Equation* (5.G) *is a particular case of Equation* (5.18) *(up to Equation* (5.2)*); Equations* (5.E) *and* (5.F) *correspond respectively to Equations* (5.21) *and* (5.19)*; Equation* (5.A) *follows directly from Equation* (5.2) *and Proposition 5.19; and Equation* (5.C) *follows directly from Equations* (5.29), (5.1) *and* (5.2).

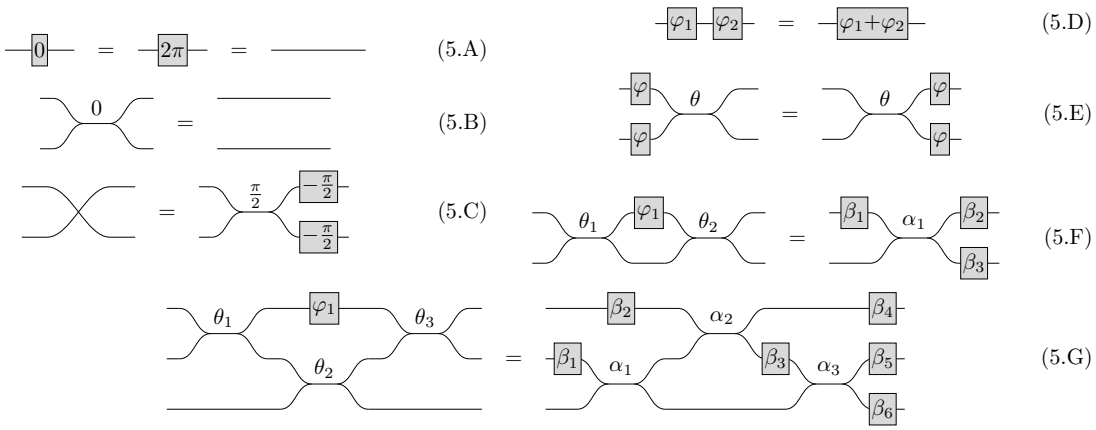


Figure 5.12: Axioms of the $\mathrm{LO}_{\mathrm{PP}}$-calculus. The equations are valid for arbitrary parameters $\varphi, \varphi_i, \theta, \theta_i \in \mathbb{R}$. In Equations (5.F) and (5.G), the angles on the left-hand side can take any value while the right-hand side is given by Lemma 5.13 and Lemma 5.12 respectively.

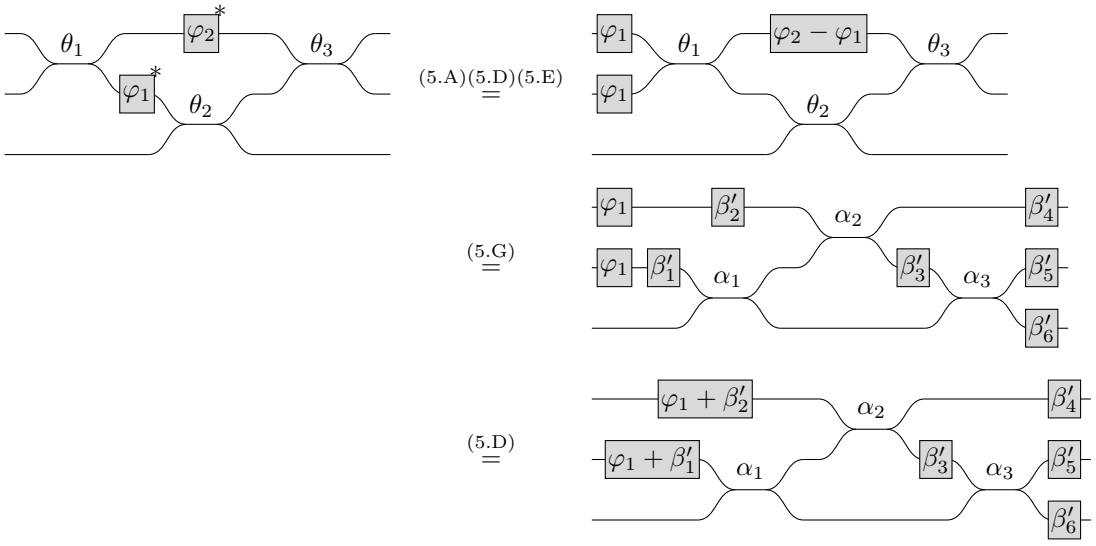
Corollary 5.35. *The equational theory given by Figure 5.12 is sound and complete: for any two* $\mathrm{LO}_{\mathrm{PP}}$*-circuits* D_1 *and* D_2*,* $[\![D_1]\!]_{\mathrm{pp}} = [\![D_2]\!]_{\mathrm{pp}}$ *iff* $\mathrm{LO}_{\mathrm{PP}} \vdash D_1 = D_2$*.*

Proof. The soundness follows directly from the fact that the equations of Figure 5.12 are consequences of those of the $\mathrm{LO_v}$-calculus, together with the soundness of the latter.

Regarding completeness, first, using Equation (5.C) one can transform any circuit into a swap-free circuit. Then it remains to show that every rule of Figure 5.7 is sound with respect to the equational theory given by Figure 5.12.

For Rules (5.56) to (5.64) and (5.66), it suffices to remark that in the proof of Lemma 5.24 we only use Equations (5.1), (5.2), (5.3), (5.21) and (5.19) — which correspond to Equations (5.D), (5.A), (5.B), (5.E) and (5.F) respectively — Equation (5.29) — which is a direct consequence of Equations (5.C), (5.A) and (5.D) — and Proposition 5.19 in the cases of a phase shifter and of a beam splitter — which follow from Equations (5.A), (5.B), (5.D) and (5.F).

Regarding Rule (5.65), its LHS can be transformed as follows:



Note that the angles in the resulting circuit are not necessarily those of the RHS of Rule (5.65). However, it can be reduced to a normal form using the PPRS rewriting system, and one can remark that the reduction cannot use Rule (5.65) (indeed, using this rule would require a second beam splitter

between the two top wires, but no rule in PPRS allows for creating beam splitters or to move them to the top). Moreover, one can check that the conditions on the angles in Rule (5.65) are the same as in a PPRS triangular normal form on 3 modes, so that up to using Equations (5.A) and (5.B), the normal form corresponds to the RHS of Rule (5.65). Hence, the soundness of Rule (5.65) with respect to the equational theory of Figure 5.12 follows from that of the other rules. □

Remark 5.36. *Note that Equation* (5.G) *is slightly simplified compared to Equation* (5.18)*, with one phase shifter less. We have just proved that Equation* (5.18) *can be derived from the equations of Figure 5.12. However, this does not imply* a priori *that we can replace Equation* (5.18) *by Equation* (5.G) *in the axioms of the* $\mathrm{LO_v}$*-calculus while preserving the completeness. Indeed, the derivation uses Equation* (5.E) *(a.k.a. Equation* (5.21)*), whose proof itself uses Equation* (5.18) *with two non-zero phases (see Appendix C.1). Such a simplification nonetheless becomes possible if one generalises Equation* (5.15) *into Equation* (5.40)*, since one can then derive Equation* (5.21) *using Equations* (5.17)*,* (5.24) *(which follows from Equations* (5.1) *and* (5.40)*) and* (5.16)*.*

Finally, we can now show that PPRS triangular normal forms give a unique representation of any unitary:

Proposition 5.37 (Universality and uniqueness in the polarisation-preserving fragment)**.** *For any unitary* $U : \mathbb{C}^n \to \mathbb{C}^n$*, there exists a unique circuit* T *in* PPRS *triangular normal form such that* $[\![T]\!]_{\mathrm{pp}} = U$*.*

Proof. This follows directly from [114], Theorems 5.30 and 5.32, Lemma 5.24 together with Proposition 5.17, and the fact that all PPRS triangular normal forms are irreducible. □

5.4 Completeness of the $\mathrm{LO_v}$-Calculus

To prove the completeness of the $\mathrm{LO_v}$-calculus (Theorem 5.22), we introduce the following notion of normal form.

Definition 5.38 (Normal form)**.** *A circuit in normal form* $N : n \to m$ *is a circuit of the form shown in Figure 5.13, where* T *is a PPRS triangular normal form (Definition 5.28). If* $n' = m' = 0$*, then* N *is said to be in* pure normal form*.*

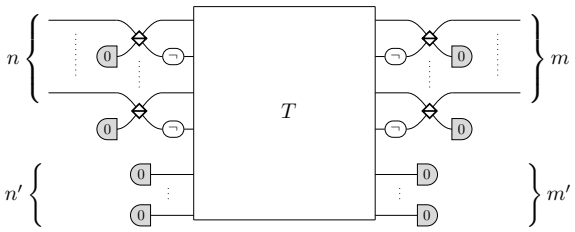


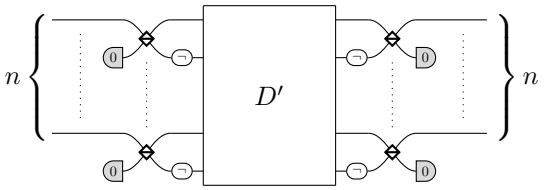
Figure 5.13: Shape of a circuit in normal form as of Definition 5.38.

Lemma 5.39 (Uniqueness of the pure normal form)**.** *If two circuits* N_1 *and* N_2 *in pure normal form are such that* $[\![N_1]\!] = [\![N_2]\!]$*, then* $N_1 = N_2$*.*

Proof. Let T_1 (resp. T_2) be the $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit associated with N_1 (resp N_2) as in Figure 5.13. Note that $[\![T_i]\!]_{\mathrm{pp}} \circ \mu = \mu \circ [\![N_i]\!]$ where $\mu : \mathbb{C}^{M_n} \to \mathbb{C}^{2n}$ is the isomorphism $|\mathbf{V}, k\rangle \mapsto |2k\rangle$ and $|\mathbf{H}, k\rangle \mapsto |2k+1\rangle$. Thus $[\![N_1]\!] = [\![N_2]\!]$ implies $[\![T_1]\!]_{\mathrm{pp}} = [\![T_2]\!]_{\mathrm{pp}}$ so that the result follows from Proposition 5.37. □

Lemma 5.40. *For any circuit* D *without vacuum state sources or detectors there exists a circuit in pure normal form* N *such that* $\mathrm{LO_v} \vdash D = N$*.*

Proof. By Theorem 5.30 and Lemma 5.24, it suffices to prove that any circuit $D : n \to n$ without $\boxed{0}\!-$ or $-\boxed{0}$ can be put in the form



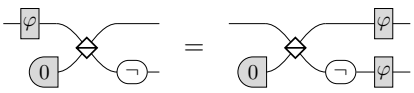
(E′)

where D' is a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit, by using the equations of Figure 5.4.

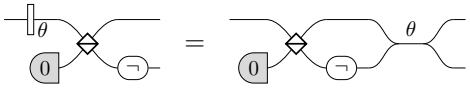
Note that any circuit $D : n \to n$ without $\boxed{0}\!-$ or $-\boxed{0}$ can be written as $d_k \circ \cdots \circ d_1$, with the d_i of the form $id_\ell \oplus g \oplus id_{\ell'}$, where $id_\ell := \ell\{\ \vdots\ \}$ (with $id_0 = [\,]$), $g \in \{\theta, \boxed{\varphi}, \boxed{\theta}, \}$ and $\ell + \ell' = n - 1$ or $n - 2$ depending on the type of g (if $k = 0$ then we take the product $d_k \circ \cdots \circ d_1$ to be the identity circuit id_n).

By Equations (5.23), (5.5) and (5.8), id_n is equivalent to the circuit of the form (E′) with $D' = id_{2n}$, which is indeed a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit. It remains to prove that for any circuit D of the form (E′) with D' a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit, any $g \in \{\theta, \boxed{\varphi}, \boxed{\theta}, \}$ and any ℓ, the circuit $D \circ (id_\ell \oplus g \oplus id_{\ell'})$ can be put again in the form (E′) with D' being a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit.

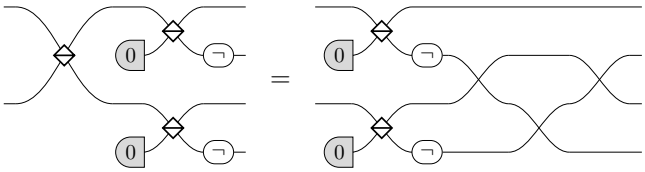
The generator g passes through the left part of D as follows:



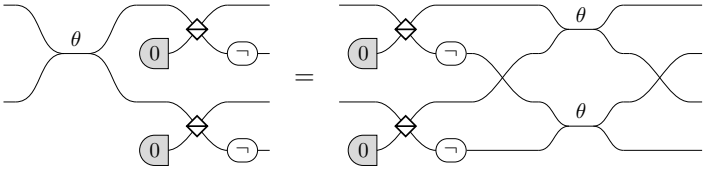
(5.67)



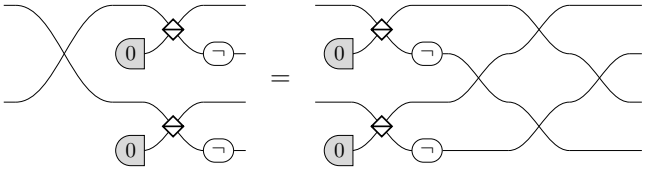
(5.68)



(5.69)



(5.70)



(5.71)

Then, using Equation (5.C) (and Remark 5.34), we can remove the swaps in order to turn the middle part into a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit, which finishes the proof.

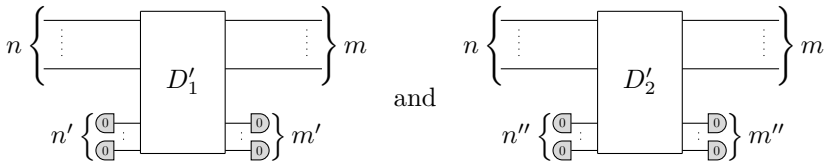
It remains to prove Equations (5.67) to (5.71) using the axioms of the $\mathrm{LO_v}$-calculus. The derivations are given in Appendix C.2. □

The completeness for circuits without vacuum state sources or detectors follows directly from Lemmas 5.39 and 5.40:

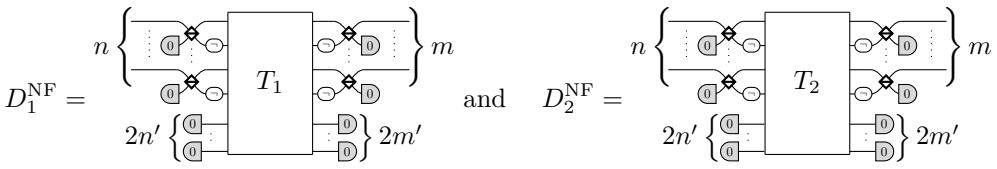
Proposition 5.41. *Given any two circuits D_1 and D_2 without any $\boxed{0}\!-$ or $-\boxed{0}$, if $[\![D_1]\!] = [\![D_2]\!]$ then $\mathrm{LO_v} \vdash D_1 = D_2$.*

Proof. By Lemma 5.40, there exist two circuits in pure normal form N_1 and N_2 such that $\mathrm{LO_v} \vdash D_1 = N_1$ and $\mathrm{LO_v} \vdash D_2 = N_2$. By soundness (Proposition 5.17), one has $[\![N_1]\!] = [\![D_1]\!] = [\![D_2]\!] = [\![N_2]\!]$, so that by Lemma 5.39, $N_1 = N_2$. The result follows by transitivity. □

Proof of Theorem 5.22. We now have the required material to to finish the proof of Theorem 5.22. Let $D_1, D_2 : n \to m$ be any two $\mathrm{LO_v}$-circuits such that $[\![D_1]\!] = [\![D_2]\!]$. By deformation, we can write them as



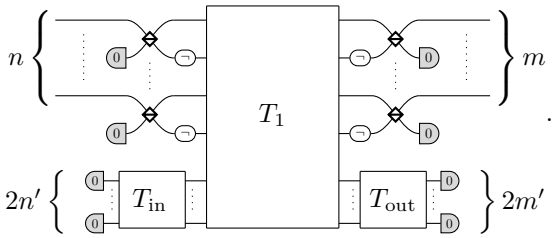
where D_1', D_2' do not contain $\boxed{0}$– or –$\boxed{0}$. Up to using Equation (5.8), we can assume that $n'' = n'$. Since circuits without vacuum state sources and detectors necessarily have the same number of input wires as of output wires, this implies that $m'' = m'$. By Lemma 5.40, we can put D_1' and D_2' in pure normal form. Then by using Equations (5.11), (5.14), (5.25) and (5.26), we get two circuits in normal form



with T_1 and T_2 in PPRS triangular normal form.

$[\![D_1]\!] = [\![D_2]\!]$ implies that $\pi \circ [\![T_1]\!]_{\mathrm{pp}} \circ \iota = \pi \circ [\![T_2]\!]_{\mathrm{pp}} \circ \iota$ where $\iota : \mathbb{C}^{2n} \to \mathbb{C}^{2(n+n')}$ is the injection $|k\rangle \mapsto |k\rangle$ and $\pi : \mathbb{C}^{2(m+m')} \to \mathbb{C}^{2m}$ is the projector s.t. $\pi\,|k\rangle = |k\rangle$ when $k < 2m$ and $\pi\,|k\rangle = 0$ otherwise. By using basic linear algebra, one can show that this implies that there exists two unitaries Q, Q' s.t. $[\![T_2]\!]_{\mathrm{pp}} = (I \oplus Q') \circ [\![T_1]\!]_{\mathrm{pp}} \circ (I \oplus Q)$ (see Lemma C.36 in Appendix C.3).

By Proposition 5.37, there exist two circuits T_{in} and T_{out} in PPRS triangular normal form such that $[\![T_{\mathrm{in}}]\!]_{\mathrm{pp}} = Q$ and $[\![T_{\mathrm{out}}]\!]_{\mathrm{pp}} = Q'$. By Equations (5.9), (5.12), (5.27) and (5.28), we can make T_{in} and T_{out} appear, turning D_1^{NF} into



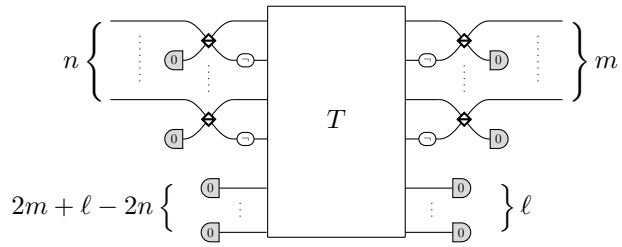
.

Since by construction, the middle part (made of T_{in}, T_1 and T_{out}) has the same semantics as T_2, by Proposition 5.41 (or by Corollary 5.35 and Remark 5.34), we can transform it into T_2 using the axioms of the $\mathrm{LO_v}$-calculus, which means transforming D_1^{NF} into D_2^{NF}. The result follows by transitivity. □

Proof of Theorem 5.15. Finally, we can now also prove the universality of $\mathrm{LO_v}$-circuits. Let $U : \mathbb{C}^{M_n} \to \mathbb{C}^{M_m}$ be a sub-unitary map i.e. a map U s.t. $U^\dagger U \sqsubseteq I_n$. We show in the following how to construct a $\mathrm{LO_v}$-circuit C s.t. $[\![C]\!] = U$. First note that $V : \mathbb{C}^{2n} \to \mathbb{C}^{2m} = \mu_m \circ U \circ \mu_n^\dagger$ is also a sub-unitary map, where $\mu_n : \mathbb{C}^{M_n} \to \mathbb{C}^{2n}$ is such that $\mu_n\,|\mathbf{V}, k\rangle = |2k\rangle$ and $\mu_n\,|\mathbf{H}, k\rangle = |2k+1\rangle$.

Since $I_n - V^\dagger V$ is semi-definite positive there exists $A : \mathbb{C}^{2n} \to \mathbb{C}^\ell$ s.t. $A^\dagger A = I_n - V^\dagger V$. As a consequence the matrix $W : \mathbb{C}^{2n} \to \mathbb{C}^{2m+\ell} = \begin{pmatrix} V \\ A \end{pmatrix}$ is an isometry since $W^\dagger W = V^\dagger V + A^\dagger A = I_{2n}$. W can be turned into a unitary matrix by adding columns to W, i.e. $\exists B, D$ s.t. $U' : \mathbb{C}^{2m+\ell} \to \mathbb{C}^{2m+\ell} =$

$\begin{pmatrix} V & B \\ A & D \end{pmatrix}$ is unitary. By Proposition 5.37, there exists a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit T s.t. $[\![T]\!]_{\mathrm{pp}} = U'$. Let C be the following LO_{v}-circuit:



By construction, $[\![C]\!] = U$. □

5.5 Discussion About the Trace

Note that we have defined LO_{v}-circuits as a PROP without a trace. In this section, we discuss two ways of enriching LO_{v}-circuits with a trace while giving it a semantics.

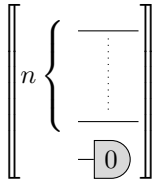
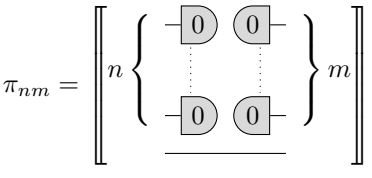
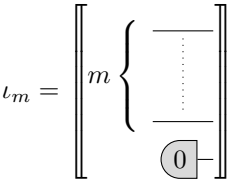
5.5.1 Instant-Travel Model

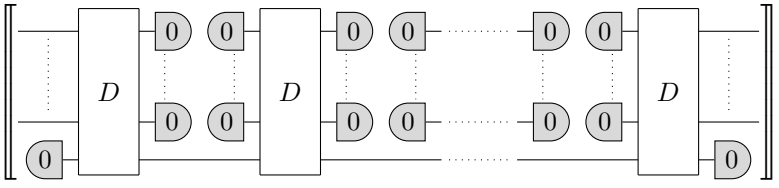
5.5.1.1 Definition

If we were to add a trace to LO_{v}-circuits, the most obvious way to give it a semantics is by adapting the formula of Definition 3.11: $[\![Tr(D)]\!] = \mathcal{T}([\![D]\!])$, where, for any sub-unitary $f\colon \mathbb{C}^{M_{m+1}} \to \mathbb{C}^{M_{n+1}}$,

$$\mathcal{T}(f) \coloneqq \sum_{k=0}^{\infty} \pi_{<n} \circ (f \circ \pi_{nm})^k \circ f \circ \iota_m$$

where $\pi_{<n} = \begin{array}{ccc} \mathbb{C}^{M_{n+1}} & \to & \mathbb{C}^{M_n} \\ |c,p\rangle & \mapsto & \begin{cases} |c,p\rangle & \text{if } p < n \\ 0 & \text{if } p = n \end{cases} \end{array}$, $\pi_{nm} = \begin{array}{ccc} \mathbb{C}^{M_{n+1}} & \to & \mathbb{C}^{M_m+1} \\ |c,p\rangle & \mapsto & \begin{cases} 0 & \text{if } p < n \\ |c,m\rangle & \text{if } p = n \end{cases} \end{array}$ and $\iota_m = \begin{array}{ccc} \mathbb{C}^{M_m} & \to & \mathbb{C}^{M_{m+1}} \\ |c,p\rangle & \mapsto & |c,p\rangle \end{array}$.

In other words, $\pi_{<n} =$  , $\pi_{nm} =$  , $\iota_m =$  and

$[\![Tr(D)]\!] = \sum_{k=0}^{\infty}$ 

It follows from a result of [16] that if f is unitary, then $\mathcal{T}(f)$ is well-defined and unitary. If f is only sub-unitary, then similarly as in the proof of Theorem 5.15, we can build a unitary matrix of the form $\begin{pmatrix} A & B \\ C & f \end{pmatrix}$. That is, we can write f as $\bar{\pi}_{(n+1)}^{(N+1)} \circ U \circ \bar{\iota}_{(m+1)}^{(N+1)}$, where $U\colon \mathbb{C}^{N+1} \to \mathbb{C}^{N+1}$ is unitary, $\bar{\pi}_{(n)}^{(N)} = \begin{array}{ccc} \mathbb{C}^{M_N} & \to & \mathbb{C}^{M_n} \\ |c,p\rangle & \mapsto & \begin{cases} |c,p+n-N\rangle & \text{if } p \geq N-n \\ 0 & \text{if } p < N-n \end{cases} \end{array}$ and $\bar{\iota}_{(m)}^{(N)} = \begin{array}{ccc} \mathbb{C}^{M_m} & \to & \mathbb{C}^{M_N} \\ |c,p\rangle & \mapsto & |c,p+N-m\rangle \end{array}$. Then

$$\begin{aligned}\mathcal{T}(f) &= \sum_{k=0}^{\infty} \pi_{<n} \circ \left(\bar{\pi}^{(N+1)}_{(n+1)} \circ U \circ \bar{\iota}^{(N+1)}_{(m+1)} \circ \pi_{nm}\right)^k \circ \bar{\pi}^{(N+1)}_{(n+1)} \circ U \circ \bar{\iota}^{(N+1)}_{(m+1)} \circ \iota_m \\ &= \sum_{k=0}^{\infty} \pi_{<n} \circ \bar{\pi}^{(N+1)}_{(n+1)} \circ \left(U \circ \bar{\iota}^{(N+1)}_{(m+1)} \circ \pi_{nm} \circ \bar{\pi}^{(N+1)}_{(n+1)}\right)^k \circ U \circ \bar{\iota}^{(N+1)}_{(m+1)} \circ \iota_m.\end{aligned}$$

Noting that $\pi_{<n} \circ \bar{\pi}^{(N+1)}_{(n+1)} = \bar{\pi}^{(N)}_{(n)} \circ \pi_{<N}$, $\bar{\iota}^{(N+1)}_{(m+1)} \circ \pi_{nm} \circ \bar{\pi}^{(N+1)}_{(n+1)} = \pi_{NN}$ and $\bar{\iota}^{(N+1)}_{(m+1)} \circ \iota_m = \iota_N \circ \bar{\iota}^{(N)}_{(m)}$, this gives us

$$\mathcal{T}(f) = \sum_{k=0}^{\infty} \bar{\pi}^{(N)}_{(n)} \circ \pi_{<N} \circ (U \circ \pi_{NN})^k \circ U \circ \iota_N \circ \bar{\iota}^{(N)}_{(m)}.$$

Since U is unitary, it is clear given the result of [16] that this series is convergent and equal to $\bar{\pi}^{(N)}_{(n)} \circ \mathcal{T}(U) \circ \bar{\iota}^{(N)}_{(m)}$, which is sub-unitary.

Thus, defining $[\![Tr(D)]\!] = \mathcal{T}([\![D]\!])$ gives a well-defined semantics to the trace, which preserves the fact that the semantics of any circuit is sub-unitary. Additionally, if the semantics of a circuit is unitary (which is the case for instance if it contain neither  nor), then the semantics of its trace is still unitary.

Moreover, it is easy to see that if the semantics of a circuit D does not act on the polarisation, that is, if $[\![D]\!] = I_{\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}} \otimes f$ for some $f\colon \mathbb{C}^n \to \mathbb{C}^m$, then this is also the case of $Tr(D)$, and $[\![Tr(D)]\!]_{\mathrm{pp}} = \mathcal{T}_{\mathrm{pp}}([\![D]\!]_{\mathrm{pp}})$, where $\mathcal{T}_{\mathrm{pp}}$ is defined analogously as $\mathcal{T}$. This implies that one can also make the PROP of $\mathrm{LO_{PP}}$-circuits into a traced PROP and give this semantics to the trace.

5.5.1.2 Complete Equational Theories

With this semantics, the completeness result of Theorem 5.22 can be extended to the traced PROP of $\mathrm{LO_v}$-circuits by adding the two axioms of Figure 5.14 to those of Figure 5.4. Analogously, the completeness result of Corollary 5.35 can be extended to the traced PROP of $\mathrm{LO_{PP}}$-circuits by adding the two axioms of Figure 5.15 to those of Figure 5.12. Indeed, to show these extended completeness results, it suffices

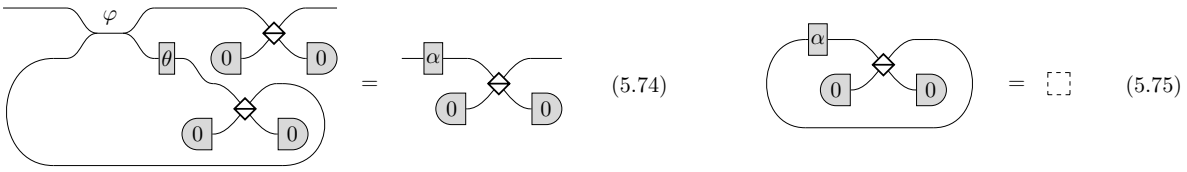
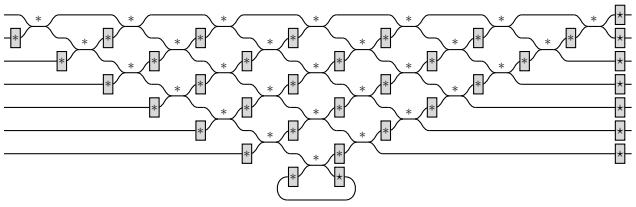


Figure 5.14: Additional axioms to the $\mathrm{LO_v}$-calculus for traced $\mathrm{LO_v}$-circuits. In Equation (5.74), $\alpha = \arg\left(2\cos(\varphi) - \cos(\theta)(1+\cos^2(\varphi)) - \mathrm{i}\sin(\theta)\sin^2(\varphi)\right)$ (and by convention, $\alpha = 0$ if $\theta = \varphi = 0$ and $\alpha = \pi$ if $\theta = \varphi = \pi$).

Figure 5.15: Additional axioms to the $\mathrm{LO_{PP}}$-calculus for traced $\mathrm{LO_{PP}}$-circuits. In Equation (5.78), $\alpha = \arg\left(2\cos(\varphi) - \cos(\theta)(1+\cos^2(\varphi)) - \mathrm{i}\sin(\theta)\sin^2(\varphi)\right)$ (and by convention, $\alpha = 0$ if $\theta = \varphi = 0$ and $\alpha = \pi$ if $\theta = \varphi = \pi$).

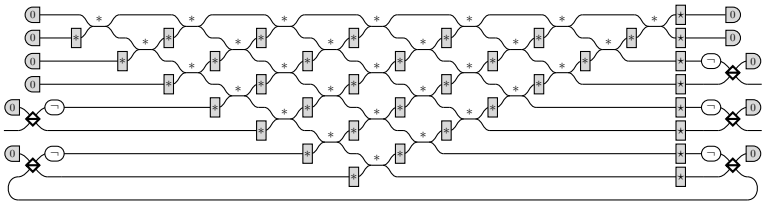
to prove that any circuit can be transformed into a trace-free circuit using the equations of Figures 5.4 and 5.14 (resp. Figures 5.12 and 5.15). By induction, it suffices to prove that given a trace-free circuit D, $Tr(D)$ can be transformed into a trace-free circuit.

In the case of a $\mathrm{LO}_{\mathrm{PP}}$-circuit, it follows from Corollary 5.35 and Proposition 5.37 that using the equations of Figure 5.12, D can be transformed into a PPRS triangular normal form flipped upside down. This gives us a circuit of the form

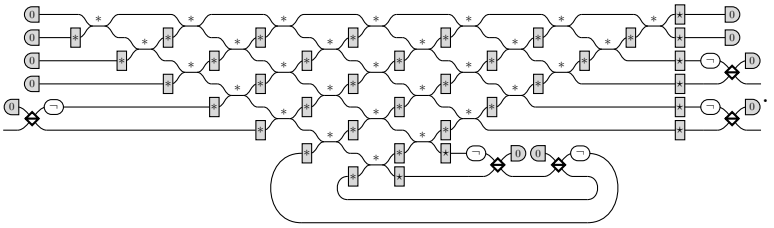


(with possibly missing beam splitters and phase shifters), from which the trace can be removed using Equation (5.1) (together with deformation) and Equation (5.78) or (5.79).

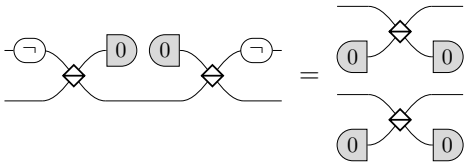
In the case of a general LO_{v}-circuit, the proof is similar. By proceeding in a similar way as in the proof of Theorem 5.22 (but with all circuits flipped upside down), on can transform D into a normal form flipped upside down. Then $Tr(D)$ looks like, for instance:



which can be deformed into

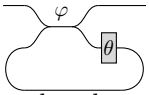


After using the following equality, which is a consequence of the axioms of the LO_{v}-calculus:

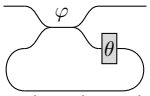


one can then, twice, apply Equation (5.74) or (5.75), together with some additional transformations by the axioms of the LO_{v}-calculus, to remove the two traces.

5.5.1.3 Physical Interpretation

Intuitively, a photon in a circuit with traces follows several (possibly infinitely many) paths in superposition, each path being from an input wire to an output wire and containing an arbitrary number of travels through trace wires. For instance in the circuit  , there is one possible path for each natural integer, corresponding to the number of times the photon takes the feedback loop, and a photon entering this circuit follows all these paths in superposition (except if φ is a multiple of π). Namely, the amplitude corresponding to passing n times through the feedback loop is $\cos(\varphi)$ if $n = 0$, and $-\sin^2(\varphi)\cos^{n-1}(\varphi)e^{ni\theta}$ if $n \neq 0$.

Intuitively, the semantics assumes that the travelling time is the same for all possible paths. Physically, this can mean that the travelling time through loops is negligible, which may not be a realistic assumption, especially in cases where the photon loops an unbounded number of times. In particular, one can notice the discontinuity in the value of α given by Equation (5.78) when $\theta = 0$: one has $\alpha = \pi$ if $\varphi \neq 0$ but $\alpha = 0$ if $\varphi = 0$. Intuitively, when $\theta = 0$ and φ approaches 0, in order to approximate the final state of the photon, one has to take into account a number of values of n (corresponding to the number of times the photon takes the feedback loop) that approaches infinity, which eventually breaks the assumption that the travelling time is negligible. The situation is similar when $\theta = \pi$: then one has $\alpha = 0$ if $\varphi \neq \pi$ but $\alpha = \pi$ if $\varphi = \pi$.

With the diagrams considered in Chapters 3, 4 and 7, since there is only one path for each basis state of the photon, it is always possible to correct the differences in the time taken by the photon in the different paths of a physical implementation, by adding elements such as  at the output. Unfortunately, such a correction is clearly not possible in traced $\mathrm{LO_v}$-circuits, for instance in 

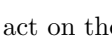
. Correction might however be possible in the case where the photon is purely monochromatic, since in this case a difference in travelling time would become equivalent to a difference in phase, which could be corrected using a phase shifter. As with the negligible time hypothesis above, any defect in the monochromality would (at least in theory) become apparent if θ and φ come close enough to 0 or π.

Finally, this semantics might make sense in the context of an experiment in which the time when the photon exits the circuit does not matter.

5.5.2 Delayed Trace

The semantics of the trace given in the previous section can be made more realistic by taking into account the time that the photon takes to go into a feedback loop and traverse the circuit again. We briefly present here a possible way to formalise this, although the study of such a formalism is essentially left for future work.

We consider time as an additional degree of freedom of the photon, so that its state space is now $\mathbb{C}^{M_n} \otimes \mathbb{C}^{\mathbb{R}}$. We also consider an additional generator 

, for any $\tau \in \mathbb{R}_{>0}$, which delays the photon by τ: $\left[\!\!\left[\right.\right.$ 

$\left.\right]\!\!\right] := |c, p, t\rangle \mapsto |c, p, t + \tau\rangle$. The semantics of the other generators is the same as before on the polarisation and the position, and they do not act on the time. The semantics of the sequential and parallel compositions is adapted in the straightforward way, and the semantics of the trace is defined in the same way as in the previous section, with $\pi_{<n}$, π_{nm} and ι_m not acting on the time. Now we impose an additional restriction on diagrams, namely that there must be a delay generator at the beginning of every trace loop. For instance, in Figure 5.16, the diagram on the right is valid while the diagram on the left is not.

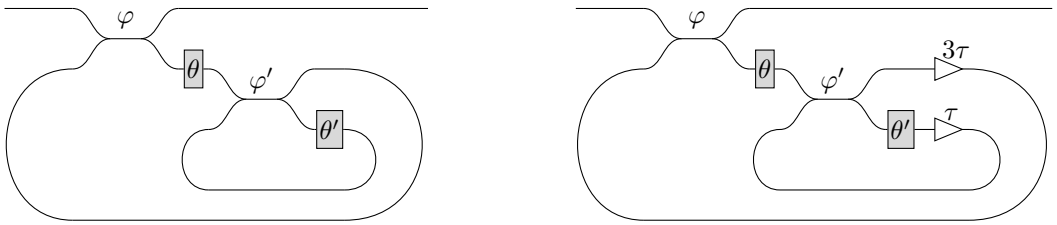


Figure 5.16: [*Left*] A circuit with instant-travel traces. [*Right*] The same circuit with delayed traces, with a different delay for each trace.

As a possible variant of this formalism, instead of requiring that every trace is preceded by a delay generator, one can slightly change the semantics of the trace so that it already includes a fixed delay. Note that then, strictly speaking, circuits do not form a traced PROP anymore, since the yanking axiom is not sound with respect to the modified semantics. Indeed,  is then equivalent to a delay generator.

Other, straightforward, possible variants consist in considering discrete time and/or preventing time from going arbitrarily far in the past, for instance by working in $\mathbb{Z}$, $\mathbb{R}_{>0}$ or $\mathbb{N}$ instead of $\mathbb{R}$.

Note that the idea of using a delayed trace and delay generators is similar to the approach of [26], although the structures considered are different (indeed, [26] considers circuits with discard maps, similar to those of Section 2.3, in which in particular different wires represent different quantum systems instead of different positions of the same quantum system).

As a final remark, note that in this chapter, we have not considered the travelling time of a photon in a circuit without a trace. Indeed, in practice it is always possible to choose the length of the different wires so that all paths take the same time to follow.

Chapter 6

A Complete Equational Theory for Quantum Circuits

Quantum circuits currently form the *de facto* standard for representing low-level, logical operations on a quantum memory. They are used for everything: resource estimation [69], optimisation [9, 57, 92, 101, 100, 103], satisfaction of hardware constraints [91, 104], *etc.*

However, as ubiquitous to quantum computing as they are, the graphical language of quantum circuits has never been fully formalised. In particular, a *complete equational theory* has been a longstanding open problem for 30 years [1]. It would make it possible to directly prove properties such as circuit equivalence without having to rely on ad-hoc sets of equations. So far, complete equational theories were only known for non-universal fragments (that is, not able to represent arbitrary unitaries, even approximately), such as circuits acting on at most two qubits [19, 48], the stabiliser fragment [99, 113], the CNot-dihedral fragment [8], or fragments of reversible circuits [82, 43, 42].

A seemingly promising approach to developing a complete equational theory for quantum circuits has been to rely on other graphical languages for quantum computing. Arguably the strongest candidate has been the ZX-calculus [44, 45],[34] equipped with complete equational theories [83, 76, 84, 85, 127]. The ZX-calculus shares the same underlying mathematical representation for states: wires correspond to Hilbert spaces and parallel composition to the tensor operation. Nonetheless, the completeness of the ZX-calculus does not lead *a priori* to a complete equational theory for quantum circuits. The reason lies in the expressiveness of the ZX-calculus and the *non-unitarity* of some of its generators. Any quantum circuit can be straightforwardly seen as a ZX-diagram. On the other hand, a ZX-diagram does not necessarily represent a unitary map, and even when it does, extracting a corresponding quantum circuit is known to be a hard task in general [57, 52].

A related approach, used for instance for the fragment of Clifford+T circuits [65, 70, 19], has been to rely on decompositions of unitary matrices into elementary operations. This approach is related to the first one in that those decompositions can be made into a graphical language. This language has a structure of PROP, as the ZX-calculus, but with the difference that the parallel composition stands for the direct sum instead of the tensor product.

In this chapter, we introduce the first complete equational theory for quantum circuits, by following the second approach. Specifically, we rely on the complete axiomatisation of the $\mathrm{LO}_{\mathrm{PP}}$-calculus found in Chapter 5. Thus the elementary unitary operations are those performed by the beam splitters and the phase shifters.

The key difference between $\mathrm{LO}_{\mathrm{PP}}$-circuits and ZX-diagrams, that allows us to derive a complete equational theory for quantum circuits from the $\mathrm{LO}_{\mathrm{PP}}$-calculus but not from the ZX-calculus, is that unlike ZX-generators, the generators of $\mathrm{LO}_{\mathrm{PP}}$-circuits are unitary, making it possible to write a translation not only of quantum circuits into $\mathrm{LO}_{\mathrm{PP}}$-circuits but also the other way.

The complete equational theory for quantum circuits is derived from that for (polarisation-preserving)[35]

[34] or its variants like ZH [14] and ZW [76], sharing several similar properties.

[35] In this chapter we will not consider other kinds of linear optical circuits than polarisation-preserving ones.

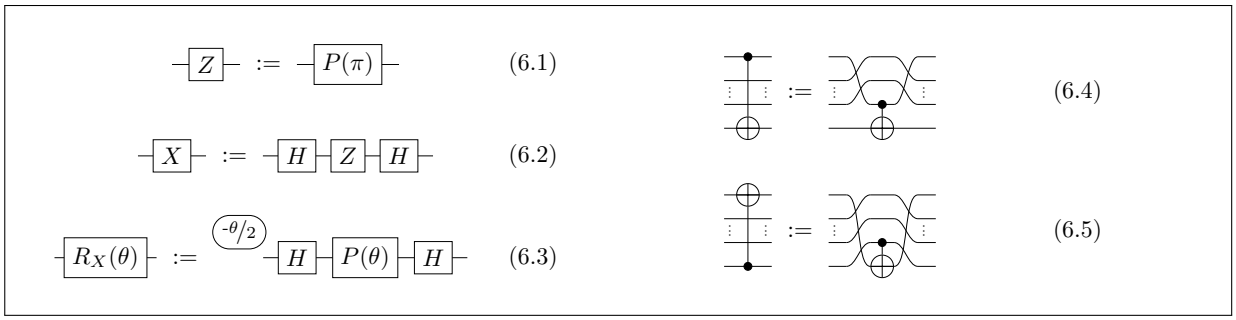


Figure 6.1: Usual abbreviations of quantum circuits.

linear optical circuits as follows: equipped with maps for encoding (from quantum circuits to linear optical circuits) and decoding (from linear optical circuits to quantum circuits), one can roughly speaking prove completeness for quantum circuits as long as their equational theory is powerful enough to derive a finite number of equations, those corresponding to the decoding of the equations of the complete equational theory for linear optical circuits.

Due to the difference in its interpretation in both kinds of circuits, the parallel composition is not preserved by the encoding nor the decoding maps. The translations are actually based on a sequentialisation of circuits, since the translation of a local gate (acting on at most two wires) is translated as a piece of circuit acting potentially on all wires. Technically, this forces us to work with *raw circuits*,[36] that is, circuits not considered up to the axioms of PROP, as a circuit may lead to *a priori* distinct translations depending on the choice of the sequentialisation. Moreover, a single linear optical generator like a phase shifter (which consists in applying a phase on a particular basis state) is decoded as a piece of circuit that can be interpreted as a multi-controlled gate acting on all qubits. As we choose to stick with the usual generators of quantum circuits acting on at most two qubits, multi-controlled gates are inductively defined and we introduce an equational theory powerful enough to prove the basic algebra of multi-controlled gates, necessary to finalise the proof of completeness.

The chapter is structured as follows. We first introduce a set of "structural" relations for quantum circuits generated by the standard elementary gates: Hadamard, Phase-rotations, and CNot. We define multi-controlled gates using these elementary gates, and show that the basic algebra of multi-controlled gates can be derived from the structural relations. In addition to the structural equations, we introduce Euler-angle-based equations. We then proceed to the proof of completeness, based on a back-and-forth translation from quantum circuits to linear optical circuits.

6.1 Quantum Circuits

6.1.1 Quantum Circuits: Syntax and Semantics

We consider quantum circuits defined on the following standard set of generators: Hadamard, Control-Not, and Phase-gates, together with global phases.

Definition 6.1. *Let* **QC** *be the PROP generated by* $\boxed{H}: 1 \to 1$, $\oplus: 2 \to 2$, *and for any* $\varphi \in \mathbb{R}$, $\boxed{P(\varphi)}: 1 \to 1$ *and* $\textcircled{\varphi}: 0 \to 0$.

A quantum circuit $C: n \to n$ with n inputs and n outputs is called a n-qubit circuit. Given an n-qubit circuit C, the corresponding unitary map $[\![C]\!]$ acts on the Hilbert space $\mathbb{C}^{\{0,1\}^n} = \mathrm{span}(|x\rangle, x \in \{0,1\}^n)$:

Definition 6.2 (Semantics)**.** *For any n-qubit quantum circuit C, let $[\![C]\!] : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$ be the linear map inductively defined as follows: $[\![C_2 \circ C_1]\!] = [\![C_2]\!] \circ [\![C_1]\!]$, $[\![C_1 \otimes C_3]\!] = [\![C_1]\!] \otimes [\![C_3]\!]$, and $\forall x, y \in \{0,1\}$,*

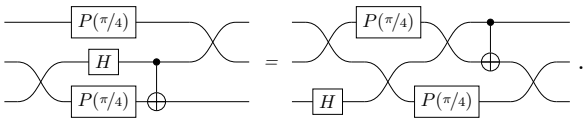
[36] *Raw terms* are for instance similarly used [109] as an intermediate step in the definition of PROP.

$\forall \varphi \in \mathbb{R}$,

$$[\![-\boxed{H}-]\!] = |x\rangle \mapsto \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}, \qquad [\![-\boxed{P(\varphi)}-]\!] = |x\rangle \mapsto e^{ix\varphi} |x\rangle, \qquad [\![—]\!] = |x\rangle \mapsto |x\rangle,$$

$$\left[\!\!\left[\begin{array}{c} \bullet \\ \oplus \end{array} \right]\!\!\right] = |x, y\rangle \mapsto |x, x \oplus y\rangle,^{37} \qquad [\![\times]\!] = |x, y\rangle \mapsto |y, x\rangle, \qquad [\![\textcircled{\varphi}]\!] = 1 \mapsto e^{i\varphi}, \qquad [\![\boxed{}]\!] = 1 \mapsto 1.$$

Remark 6.3. *As before, the axioms of PROP guarantee that circuits can be depicted graphically without ambiguity, and moreover, that they are defined up to deformation. For instance:*



As before too, the semantics is well-defined, that is, two circuits (or more precisely, using the vocabulary introduced in Section 6.2.1, two raw *circuits) equal up to deformation have the same semantics.*

Proposition 6.4 (Universality [15])**.** *For any unitary map U acting on $\mathbb{C}^{\{0,1\}^n}$, there exists an n-qubit circuit C such that $[\![C]\!] = U$.* □

We use standard shortcuts in the description of quantum circuits, given in Figure 6.1. In textual description, we sometimes use CNot, $s(\varphi)$, X, $P(\varphi)$, *etc.* to denote respectively $\left[\!\!\left[\begin{array}{c} \bullet \\ \oplus \end{array} \right]\!\!\right]$, $[\![\textcircled{\varphi}]\!]$, $[\![-\boxed{X}-]\!]$, $[\![-\boxed{P(\varphi)}-]\!]$, *etc.* Moreover, when the parameters (e.g. φ) are not specific values they can take arbitrary ones. We write $R_X(\theta)$ for the so-called X-rotation [105],[38] whereas the standard phase gate $P(\varphi)$ is a Z-rotation only up to a global phase. As a consequence, they have a slightly different behaviour: P is 2π-periodic: $[\![P(2\pi)]\!] = I$, whereas R_X is 4π-periodic, and we instead have $[\![R_X(2\pi)]\!] = -I$.

6.1.2 Structural Equations

We introduce a set QC_0 of *structural equations* on quantum circuits in Figure 6.2. These equations are structural in the sense that the transformations on the parameters are only based on the fact that $\mathbb{R}$ is an additive group. In particular, these equations are valid for any reasonable[39] restriction on the angles.

We write $\mathrm{QC}_0 \vdash C_1 = C_2$ when C_1 can be transformed into C_2 using the equations of Figure 6.2.[40]

Proposition 6.5. *The structural equations of Figure 6.2 are sound, i.e. if $\mathrm{QC}_0 \vdash C_1 = C_2$ then $[\![C_1]\!] = [\![C_2]\!]$.*

Proof. By inspection of the equations of Figure 6.2. □

Equations (6.a) to (6.l) are fairly standard in quantum computing. Equation (6.m), which is used for instance in [5], describes two equivalent ways to define a controlled-Z gate. Note that this equation cannot be derived from the other axioms as it is the only equation on 2 qubits which does not preserve the parity of the number of CNots plus the number of swaps. Equations (6.n) and (6.o) are more involved and account for some specific commutation properties of controlled gates (see Proposition 6.27 and Proposition 6.30).

The axioms of QC_0, i.e. the equations given in Figure 6.2, are sufficient to derive standard elementary circuit identities like those given in Figure 6.3.

One can also prove that some particular circuits, called phase-gadgets [51], can be flipped vertically:

[37] Where $x \oplus y \coloneqq x + y \bmod 2$.

[38] $[\![R_X(\theta)]\!] = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$

[39] I.e. which forms an additive group and contains $\pi/2$.

[40] More formally, $\mathrm{QC}_0 \vdash \cdot = \cdot$ is defined as the smallest congruence which satisfies the equations of Figure 6.2 (together with the axioms of PROP).

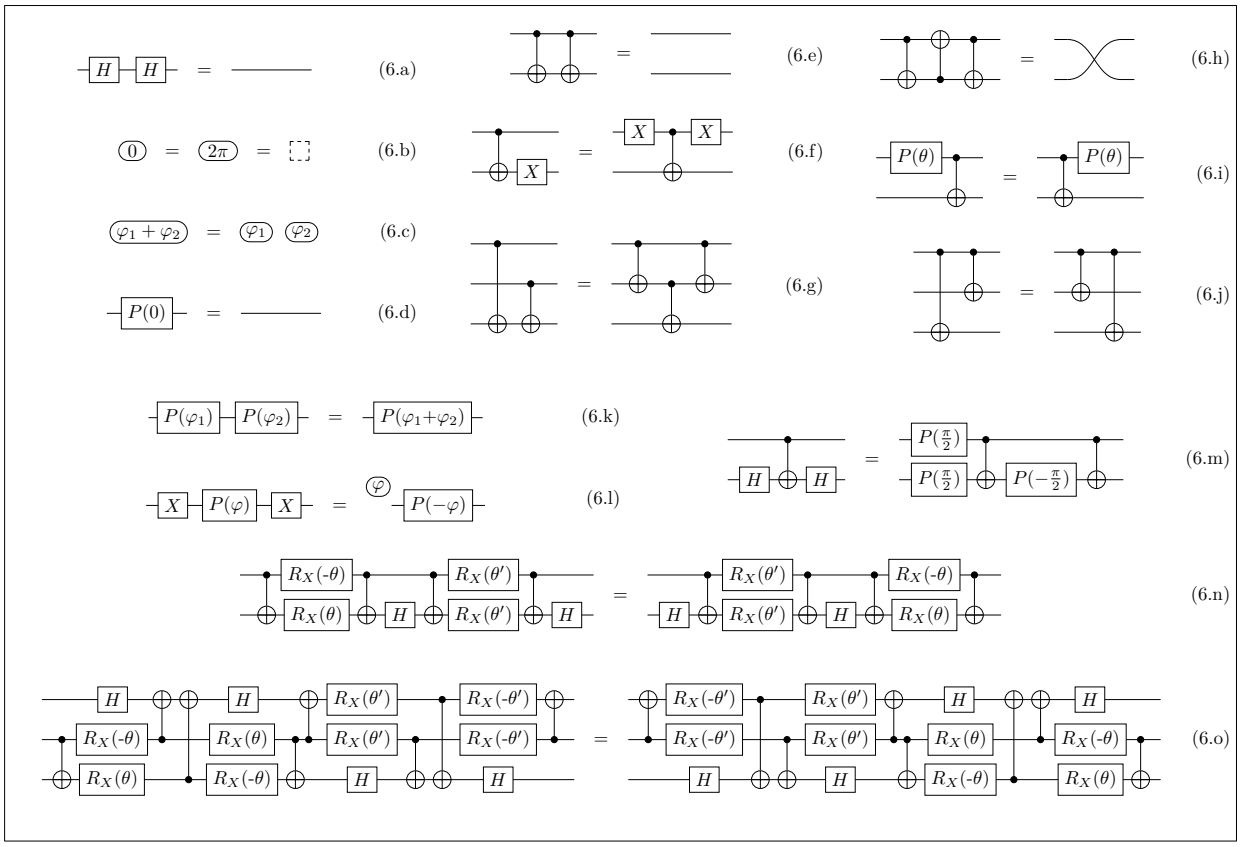


Figure 6.2: **Axioms of $\mathbf{QC}_0$:** Structural equations on quantum circuits. The equations are defined for any $\varphi, \varphi_1, \varphi_2, \theta, \theta' \in \mathbb{R}$.

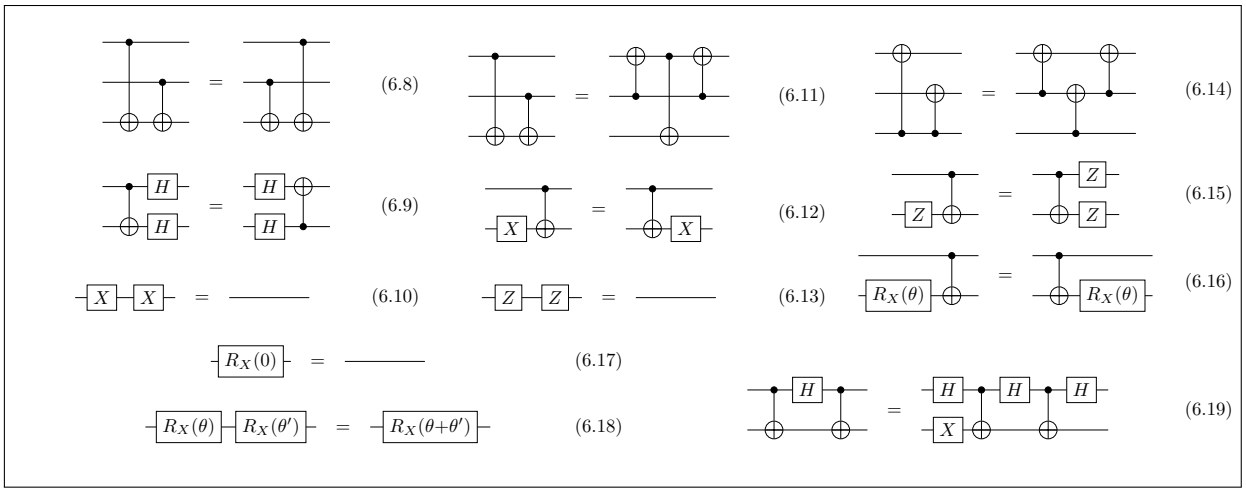
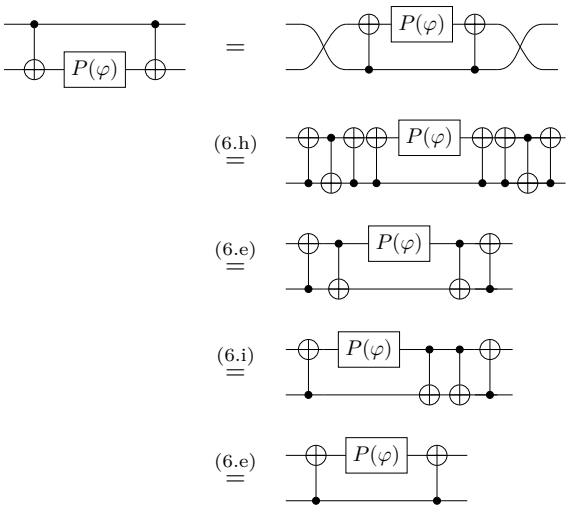


Figure 6.3: Standard circuit identities that can be derived from the axioms of QC_0, given in Figure 6.2 . The proofs are given in Appendix D.1.

$$\mathrm{QC}_0 \vdash \quad = \tag{6.6}$$

$$\mathrm{QC}_0 \vdash \quad = \tag{6.7}$$

For instance, Equation (6.6) is derived as follows:



The other derivations are given in Appendix D.1.

Combining Equation (6.6) and Equation (6.i), one can easily prove the following equation, used for instance in [103] in the context of circuit optimisation:

$$\mathrm{QC}_0 \vdash \quad =$$

When $\varphi = -\varphi' = \alpha/2$ the above circuits are two equivalent standard implementations of a controlled-Z-rotation of angle α. We show in the next section how the basic algebra of (multi-)controlled gates can be derived.

6.1.3 Controlled Gates

Multi-controlled gates are useful to describe more elaborate quantum circuits. We use the notations "λ" and "Λ" for controls. Given a 1-qubit gate G, $\lambda^1 G$ is a 2-qubit positively controlled gate: if the control qubit (the top one) is in state $|1\rangle$ (resp. $|0\rangle$) then G (resp. the identity) is applied on the target qubit (the bottom one). $\lambda^2 G$ is a 3-qubit positively controlled gate, where the two upper qubits are controls: they both need to be in state $|1\rangle$ for the gate G to fire on the bottom qubit. We also consider more general multi-controlled gates $\Lambda^{x_1 \cdots x_k} G$ with positive (when $x_i = 1$) and negative (when $x_i = 0$) controls: if the first qubit is in the state $|x_1\rangle$ (resp. $|\overline{x_1}\rangle$) then $\Lambda^{x_2 \cdots x_k} G$ (resp. the identity) is applied on the remaining qubits. Finally, $\Lambda^x_y G$ denotes a multi-controlled gate with control qubits on both sides — above and below — of the target qubit.

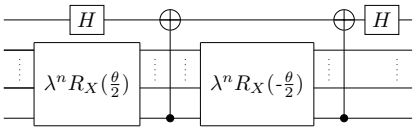
We will follow a standard construction for multi-controls using a decomposition into elementary 1- and 2-qubit gates (see for instance [15]). Note that we do not aim here at defining *all* controlled operators: as this construction is the main apparatus for the completeness result, we only focus on the operations $s(\varphi)$, X, $R_X(\theta)$ and $P(\varphi)$. Other controlled operations can then be derived if needed.

We first define in Definition 6.6 circuits implementing regular, all-positive multi-controlled gates $\lambda^n G$. We then present in Definition 6.7 how to handle positive and negative controls. In Definition 6.8 we finally introduce controlled gates with controls both above and below the gate G.

Definition 6.6 (Positively multi-controlled gates)**.** *For all $n \in \mathbb{N}$ and $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$, we define a quantum circuit $\lambda^n G$.*[41] *This circuit acts on n wires when $G = s(\varphi)$ and $n+1$ otherwise. We define each circuit $\lambda^n G$ as follows.*

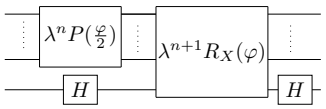
- *$\lambda^n R_X(\theta)$ is defined by induction:*

$$\lambda^0 R_X(\theta) \coloneqq R_X(\theta), \qquad \lambda^{n+1} R_X(\theta) \coloneqq$$



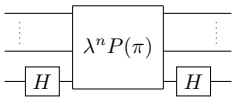
- *$\lambda^n P(\varphi)$ is defined by induction using $\lambda^n R_X(\varphi)$:*

$$\lambda^0 P(\varphi) \coloneqq P(\varphi), \qquad \lambda^{n+1} P(\varphi) \coloneqq$$



- *$\lambda^n X$ is a simple macro:*

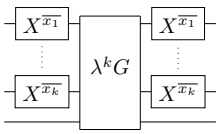
$$\lambda^n X \coloneqq$$



- *Finally, $\lambda^0 s(\varphi) \coloneqq s(\varphi)$ and $\lambda^{n+1} s(\varphi) \coloneqq \lambda^n P(\varphi)$.*

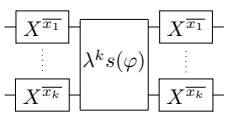
Definition 6.7 (Multi-controlled gates)**.** *For any k-length list of booleans $x = x_1, \ldots, x_k$ ($x_i \in \{0,1\}$), for any $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$ we define the quantum circuit $\Lambda^x G$ as*

$$\Lambda^x G \coloneqq$$



when $G \in \{X, R_X(\theta), P(\varphi)\}$, and

$$\Lambda^x s(\varphi) \coloneqq$$

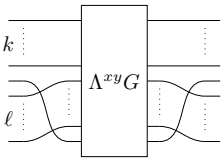


[41] Note that G spans non-elementary gates. The constructor λ is not considered as a gate operator, and the fact that the circuit $\lambda^n G$ happens to be related to G is a corollary of its definition, as discussed further in the chapter.

where $\overline{x} = 1 - x$, $-\boxed{X^1}- = -\boxed{X}-$, *and* $-\boxed{X^0}- = ——$.

Definition 6.8 (General multi-controlled gates)**.** *Given two lists of booleans* $x \in \{0,1\}^k$ *and* $y \in \{0,1\}^\ell$, *if* xy *is the concatenation of* x *and* y *we define the two quantum circuits*

- *for any* $G \in \{X, R_X(\theta), P(\varphi)\}$

$\Lambda^x_y G \coloneqq$ 

- $\Lambda^x_y s(\varphi) \coloneqq \Lambda^{xy} s(\varphi)$.

One can double check using the semantics that $\Lambda^x_y G$ is actually a multi-controlled gate:

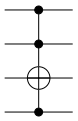
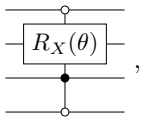
Proposition 6.9. *For any* $x, u \in \{0,1\}^k$, $y, v \in \{0,1\}^\ell$, $a \in \{0,1\}$ *and* $G \in \{X, R_X(\theta), P(\varphi)\}$,

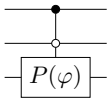
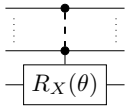
$$\left[\!\left[\Lambda^x_y G\right]\!\right] |u, a, v\rangle = \begin{cases} |u\rangle \otimes (\left[\!\left[G\right]\!\right] |a\rangle) \otimes |v\rangle & \text{if } uv = xy, \\ |u, a, v\rangle & \text{otherwise,} \end{cases}$$

and

$$\left[\!\left[\Lambda^x_y s(\varphi)\right]\!\right] |u, v\rangle = \begin{cases} e^{i\varphi} |u, v\rangle & \text{if } uv = xy, \\ |u, v\rangle & \text{otherwise.} \end{cases}$$

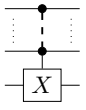
We use the standard bullet-based graphical notation for multi-controlled gates: the i^{th} control is black (resp. white) when $x_i = 1$ (resp. $x_i = 0$), and the j^{th} from the end control is black (resp. white) when $y_{\ell-j+1} = 1$ (resp. $= 0$), e.g.:

$\Lambda^{11}_1 X :$  , $\Lambda^0_{10} R_X(\theta) :$  ,

$\Lambda^{10} P(\varphi) :$  , $\Lambda^{1\ldots1} R_X(\theta) :$  .

To avoid ambiguity with CNot we will not use the $\bigoplus$ notation in the particular case of $\Lambda^1 X$ and $\Lambda_1 X$:

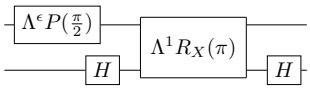
$\Lambda^1 X :$  , $\Lambda_1 X :$  ,

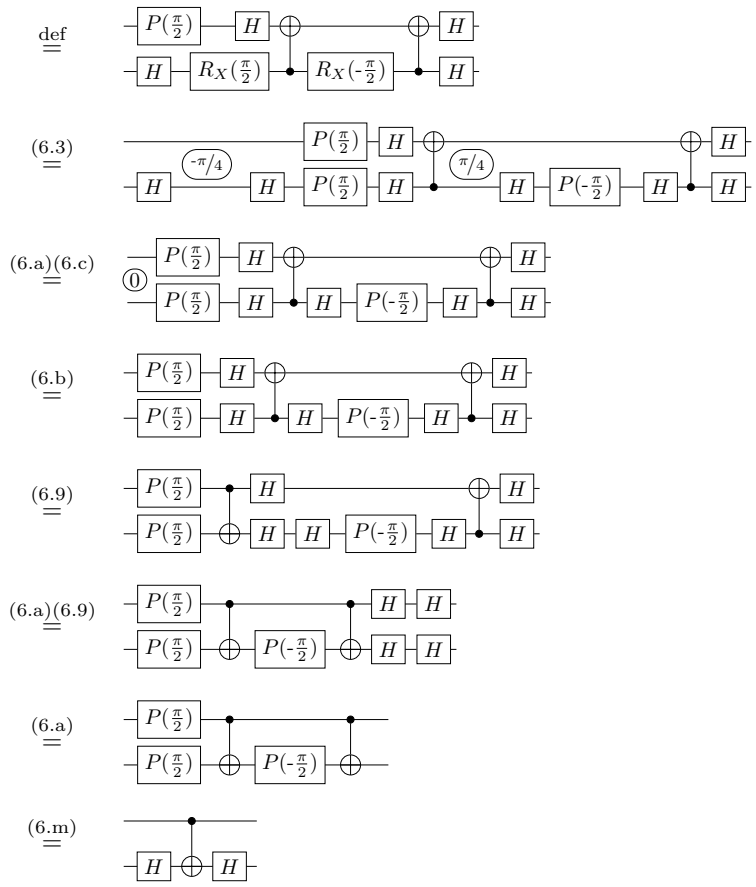
$\Lambda^{1\ldots1} X :$  (if there can be exactly one control).

Note however that $\Lambda^1 X$ is provably equivalent to CNot:

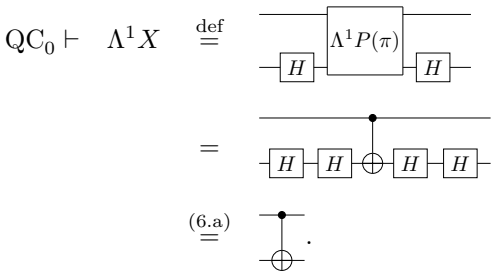
Proposition 6.10. $\mathrm{QC}_0 \vdash \Lambda^1 X =$  .

Proof. First, we can notice that

$\mathrm{QC}_0 \vdash \quad \Lambda^1 P(\pi) \quad \overset{\text{def}}{=}$ 



It follows that



□

6.1.4 Properties of Multi-Controlled Gates

In this section, we will prove basic properties of multi-controlled gates, namely: that one can swap positive (or negative) controls together (Proposition 6.17), and positive controls with phase gates (Proposition 6.18); that combining a positive and a negative control of the same gate gives the gate itself (Proposition 6.26); and that two multi-controlled gates commute whenever there is a control and an anti-control on the same qubit (Propositions 6.27 and 6.30).

A large part of the proofs of this section will be by induction on the number of control qubits of the multi-controlled gates. Note that their definition is explicitly inductive only in the case with only positive controls, this is why we first make the inductive properties of more general multi-controlled gates explicit:

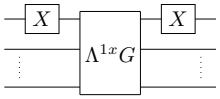
6.1.4.1 Inductive Properties for Multi-Controls

The following technical lemmas highlight the inductive properties of the circuits $\Lambda^x G$.

Lemma 6.11 (Base case for the inductive properties)**.** *For all $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$, if ϵ is the empty list, $\Lambda^\epsilon G = G$.*

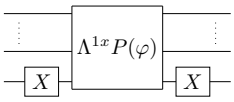
Proof. In the case of an empty list, in Definition 6.7 there are no gates $X^{\overline{x_i}}$, and $\Lambda^\epsilon G = \lambda^0 G$. We can then check in Definition 6.6 that each $\lambda^0 G$ is G: by definition this is true for $R_X(\theta)$, $s(\varphi)$ and $P(\theta)$. For X we fall back on the definition of X as $HP(\pi)H = HZH$. □

Lemma 6.12 (Inductive properties for $\Lambda^{0x} G$)**.** *For all $x \in \{0,1\}^k$, and $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$,*

$\Lambda^{0x} G =$ 

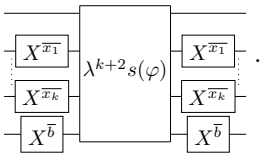
Proof. This is directly derived from the definition of $\Lambda^x G$: the $X^{\overline{x_1}}$'s on the top wire are X for $\Lambda^{0x} G$ and the identity for $\Lambda^{1x} G$, while the $X^{\overline{x_i}}$'s on the lower wires are the same. □

Lemma 6.13 (Inductive properties for $\Lambda^x s(\varphi)$)**.** *Suppose that x is a k-length list of booleans. We then have $\Lambda^1 s(\varphi) = P(\varphi)$, $\Lambda^{1x1} s(\varphi) = \Lambda^{1x} P(\varphi)$, and*

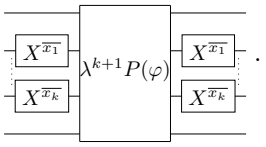
$\Lambda^{1x0} s(\varphi) =$ 

Proof. By definition, $\Lambda^1 s(\varphi)$ is $\lambda^1 s(\varphi)$: there are no $X^{\overline{x_i}}$ since the list only contains a single 1. By definition, $\lambda^1 s(\varphi)$ is $\lambda^0 P(\varphi)$, which is $P(\varphi)$.

Suppose now that x is a k-length list of booleans, and b is a single boolean. Consider $\Lambda^{1xb} s(\varphi)$: by definition it is

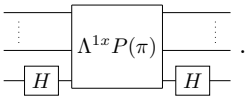


By definition, $\lambda^{k+2} s(\varphi) = \lambda^{k+1} P(\varphi)$. Now, $\Lambda^{1x} P(\varphi)$ is

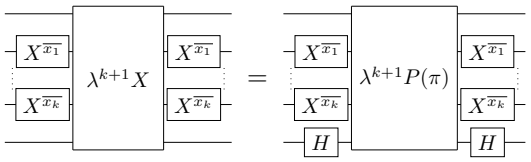


We directly recover $\Lambda^{1x1} s(\varphi)$, i.e. when $b = 1$, and the case $b = 0$ since this just amounts to add the two gates $X^{\overline{0}} = X^1 = X$ on the bottom wire. □

Lemma 6.14 (Inductive properties of $\Lambda^x X$)**.** *Suppose that x is a k-length list of booleans. Then*

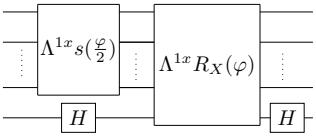
$\Lambda^{1x} X =$ 

Proof. By definition,

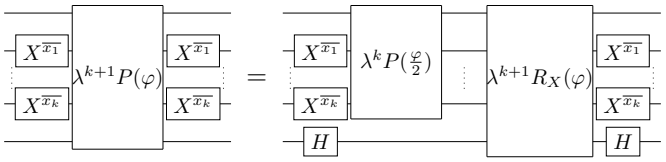
$\Lambda^{1x} X =$ 

which is exactly the right-hand side of the desired equation. □

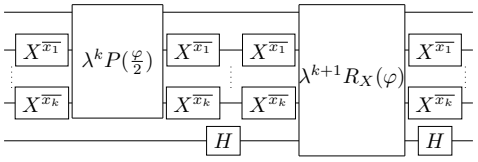
Lemma 6.15 (Inductive properties of $\Lambda^x P(\varphi)$)**.** *Suppose that x is a k-length list of booleans. Then*

$\mathrm{QC}_0 \vdash \Lambda^{1x} P(\varphi) =$ 

Proof. By definition,

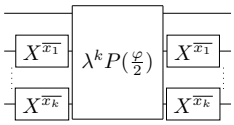
$\Lambda^{1x} P(\varphi) =$ 

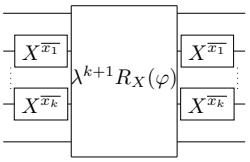
Since XX is the identity according to Equation (6.10), this is equal to



.

We can conclude by noting that

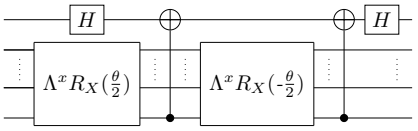
$\Lambda^{1x} s(\frac{\varphi}{2}) =$ 

and $\Lambda^{1x} R_X(\varphi) =$ 

.

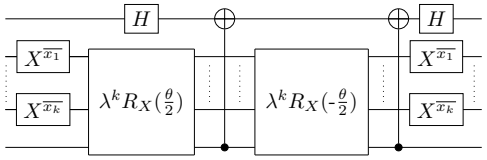
□

Lemma 6.16 (Inductive properties of $\Lambda^x R_X(\varphi)$)**.** *Suppose that x is a k-length list of booleans. Then*

$\mathrm{QC}_0 \vdash \Lambda^{1x} R_X(\theta) =$ 

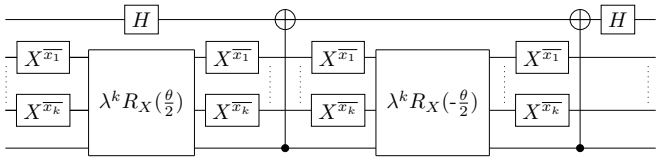
.

Proof. By definition of $\Lambda^{1x} R_X(\theta)$ and $\lambda^{k+1} R_X(\theta)$, we have:

$\Lambda^{1x} R_X(\theta) =$ 

.

Using Equation (6.10), we infer that

$\Lambda^{1x} R_X(\theta) =$ 

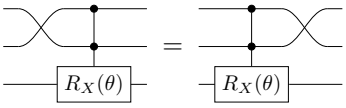
.

We can then conclude by using the definition of $\Lambda^x R_X(\frac{\theta}{2})$ and $\Lambda^x R_X(-\frac{\theta}{2})$ (and the deformation of circuits coming from the PROP structure). □

Since these lemmas are essentially consequences of the definitions (except for the use of Equation (6.10) in Lemmas 6.15 and 6.16), in the following we will mostly keep their uses implicit.

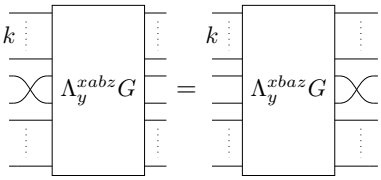
6.1.4.2 Swapping Controls Together and With Phase Gates

In a multi-qubit controlled gate, all control qubits play a similar role. This can be expressed as the following commutation property:

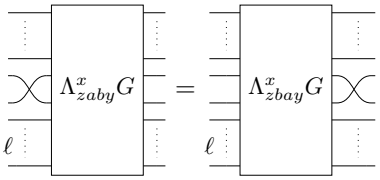


This property is provable in QC_0, considering three cases depending on whether the exchanged control qubits are either above or below the target qubit:

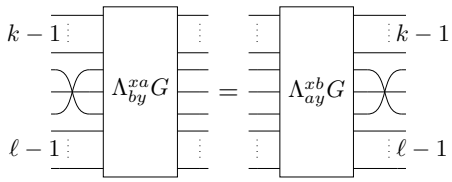
Proposition 6.17. *For any $x \in \{0,1\}^k, y \in \{0,1\}^\ell, z \in \{0,1\}^m$, $a, b \in \{0,1\}$ and any $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$,*

$$\mathrm{QC}_0 \vdash$$ 

(6.20)

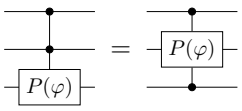
$$\mathrm{QC}_0 \vdash$$ 

(6.21)

$$\mathrm{QC}_0 \vdash$$ 

(6.22)

A peculiar property of controlled phase gates (and hence controlled scalars) is that the target qubit is actually equivalent to the control qubits, e.g.:



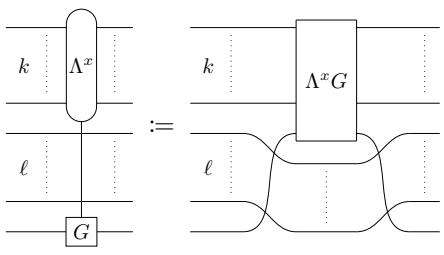
This property is also provable in QC_0:

Proposition 6.18. *For any $x \in \{0,1\}^k, y \in \{0,1\}^\ell$,*

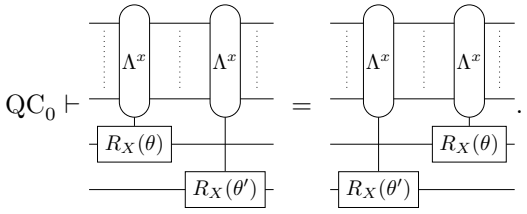
$$\mathrm{QC}_0 \vdash \Lambda_{y1}^{x} P(\varphi) = \Lambda^{x1y} P(\varphi) \tag{6.23}$$

Ancillary Lemmas To prove Propositions 6.17 and 6.18, we need to first prove a few ancillary lemmas.

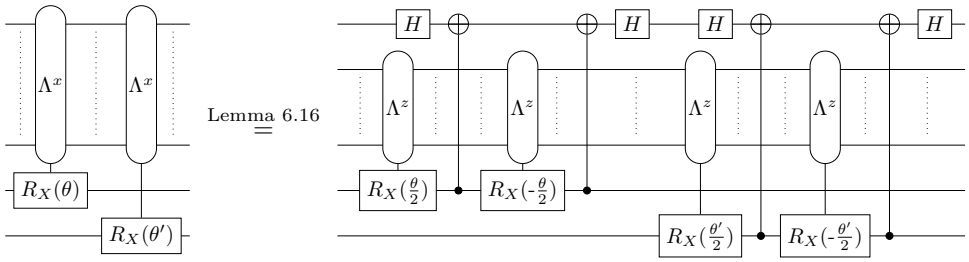
To state these lemmas, it is convenient to introduce a graphical notation of multi-controlled gate which allows for more flexibility in the position of the target qubit, relatively to the control qubits:



Lemma 6.19. *For any $x \in \{0,1\}^k$,*

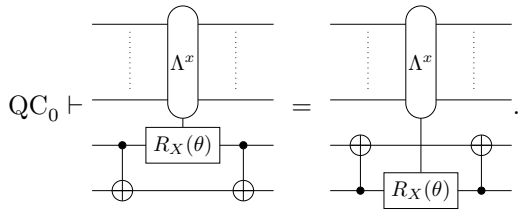


Proof. We proceed by induction on k. If $k = 0$, then the equality is a consequence of the topological rules.[42] If $k \geq 1$, by Equation (6.10) we can assume without loss of generality that $x = 1z$ with $z \in \{0,1\}^{k-1}$. One has

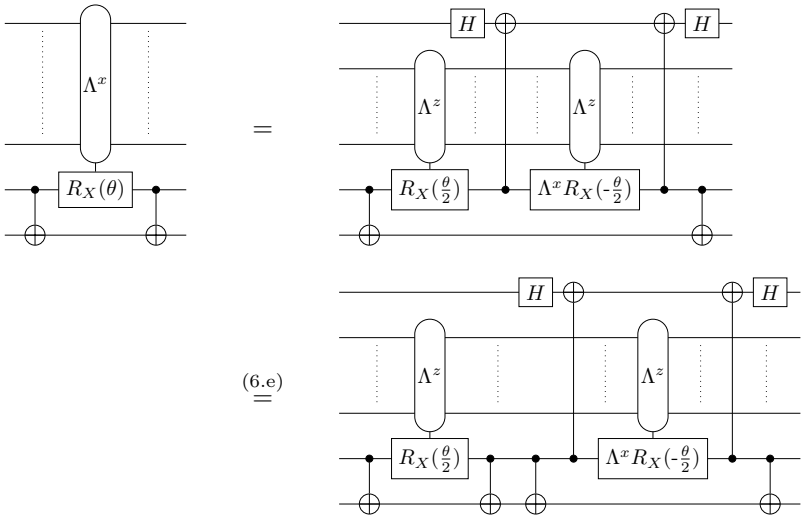


then it is easy to see that the two parts commute by induction hypothesis and Equations (6.8) and (6.a), together with topological rules. □

Lemma 6.20. *For any $x \in \{0,1\}^k$,*

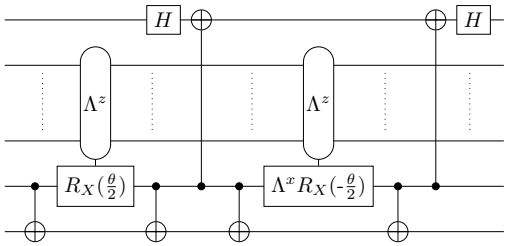


Proof. We proceed by induction on k. If $k = 0$, then the result is just Equation (6.7). If $k \geq 1$, then we can assume without loss of generality that $x = 1z$ with $z \in \{0,1\}^{k-1}$. One has

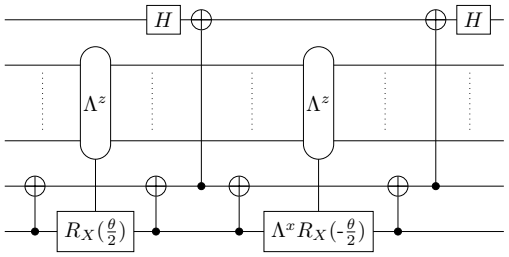


[42] The topological rules are the rules that allow us to deform the circuits, that is, the axioms of PROP.

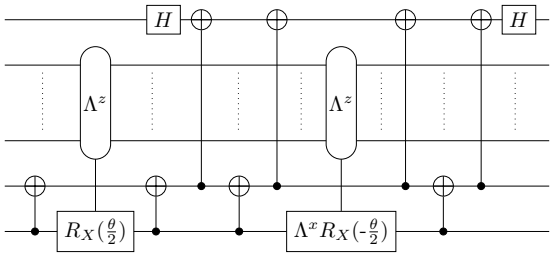
(6.j) =



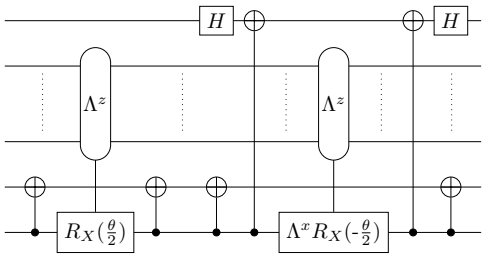
induction hypothesis =



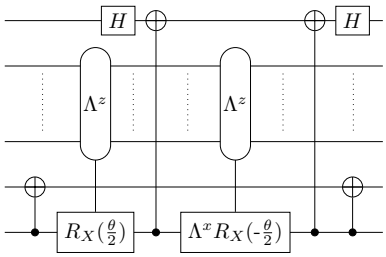
(6.e) =



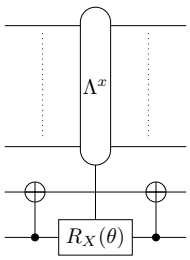
(6.14)(6.j) =



(6.e) =

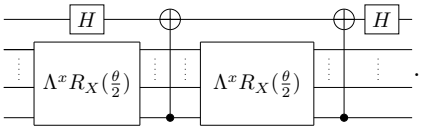


=

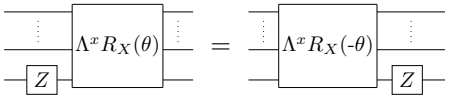


□

Lemma 6.21. *For any $x \in \{0,1\}^k$,*

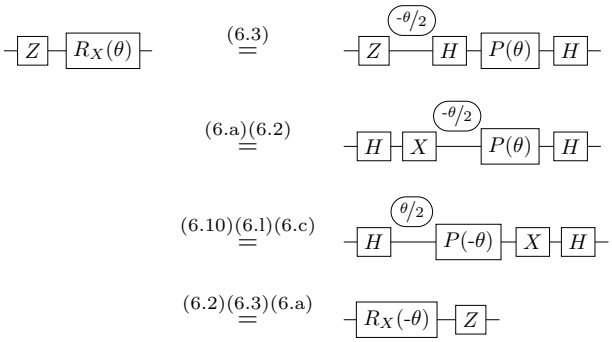
$\mathrm{QC}_0 \vdash \Lambda^{0x} R_X(\theta) =$ 

Proof. The proof relies on the following property:

$\mathrm{QC}_0 \vdash$  (6.24)

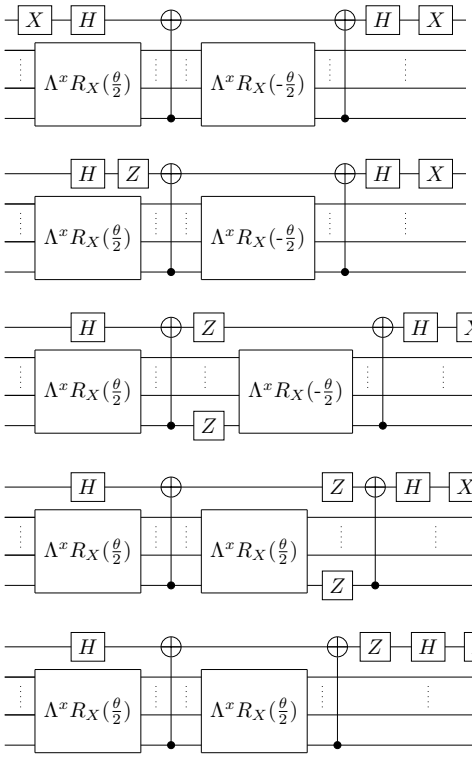
that we prove by induction on the length of x as follows:

If $x = \epsilon$, then

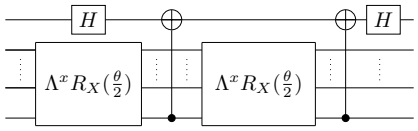


If $x \neq \epsilon$, then the commutation is a direct consequence of the induction hypothesis and Equation (6.i).

Given this property, the result can be deduced as follows:

$\Lambda^{0x} R_X(\theta) =$ 

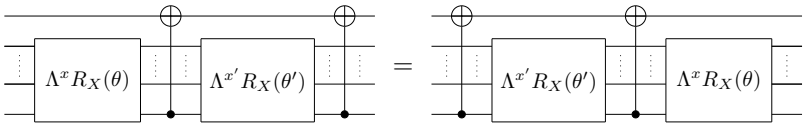
(6.2)(6.a)(6.13) =



□

Lemma 6.22. *For any $x, x' \in \{0,1\}^k$,*

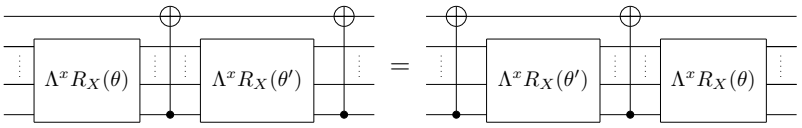
$\mathrm{QC}_0 \vdash$



(6.25)

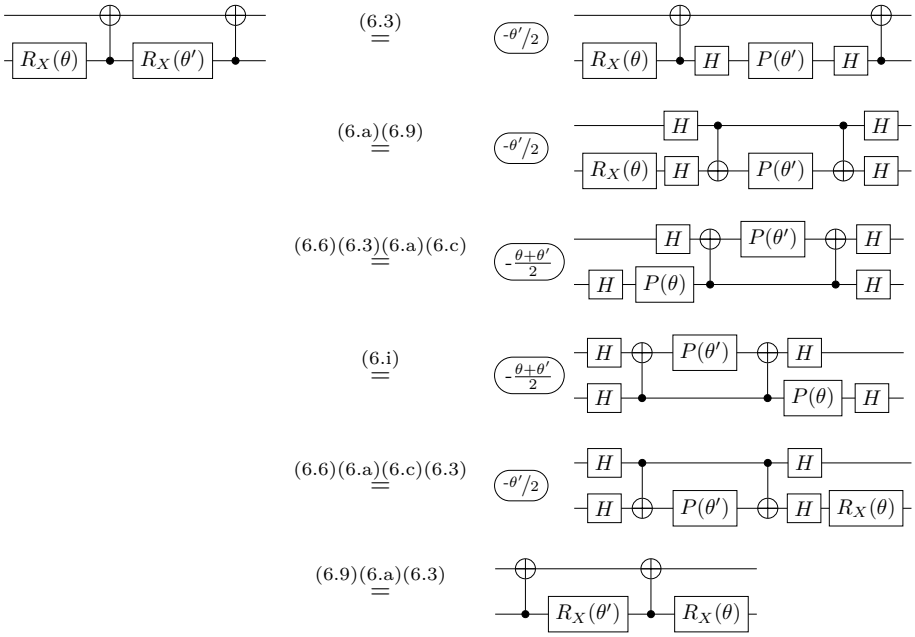
In the proof of Propositions 6.17 and 6.18 (and in a few other later proofs), we will more precisely use the particular case of Equation (6.25) where $x = x'$:

$\mathrm{QC}_0 \vdash$

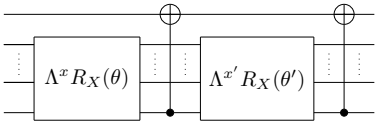


(6.26)

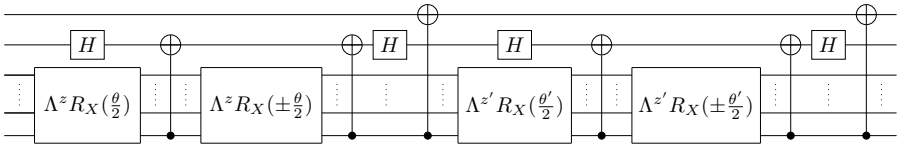
Proof of Equation (6.25). The proof is by induction on x.
If $x = \epsilon$ (i.e. $k = 0$),



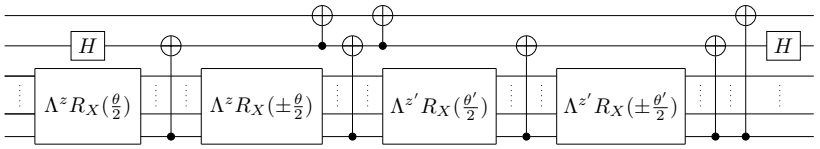
If $k \geq 1$, then we can write $x = az$ and $x' = a'z'$ with $a, a' \in \{0,1\}$. One has (where the $\pm$ signs correspond respectively to $(-1)^a$ and $(-1)^{a'}$):



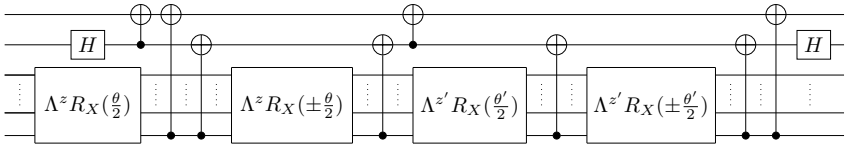
Lemma 6.21 =



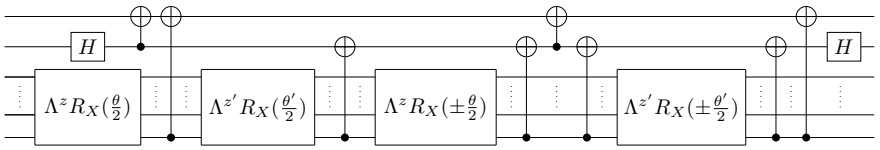
(6.a)(6.j)(6.14) =



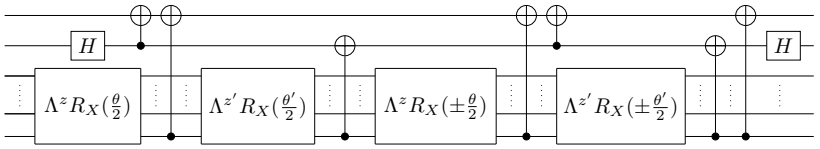
(6.e)(6.14) =



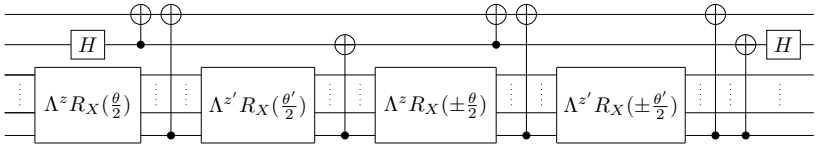
induction hypothesis =



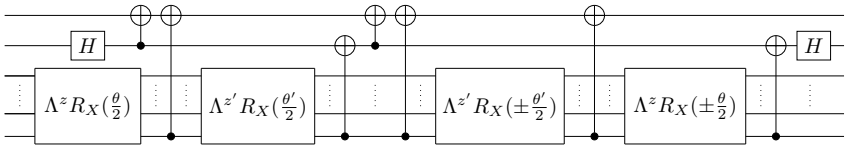
(6.g) =



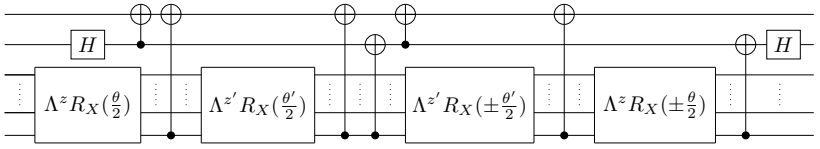
(6.8)(6.j) =



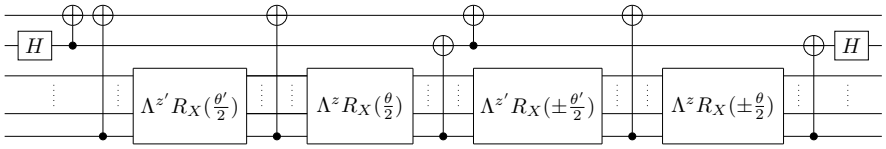
induction hypothesis =



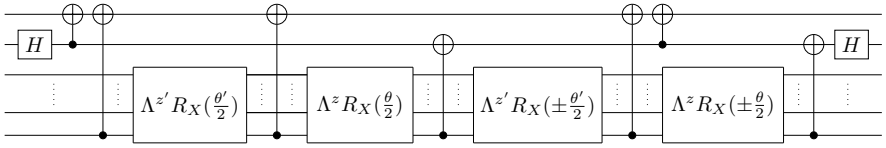
(6.8)(6.j) =



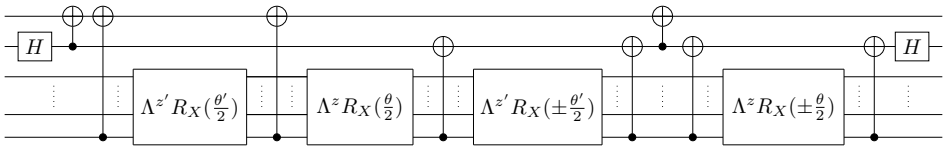
induction hypothesis =

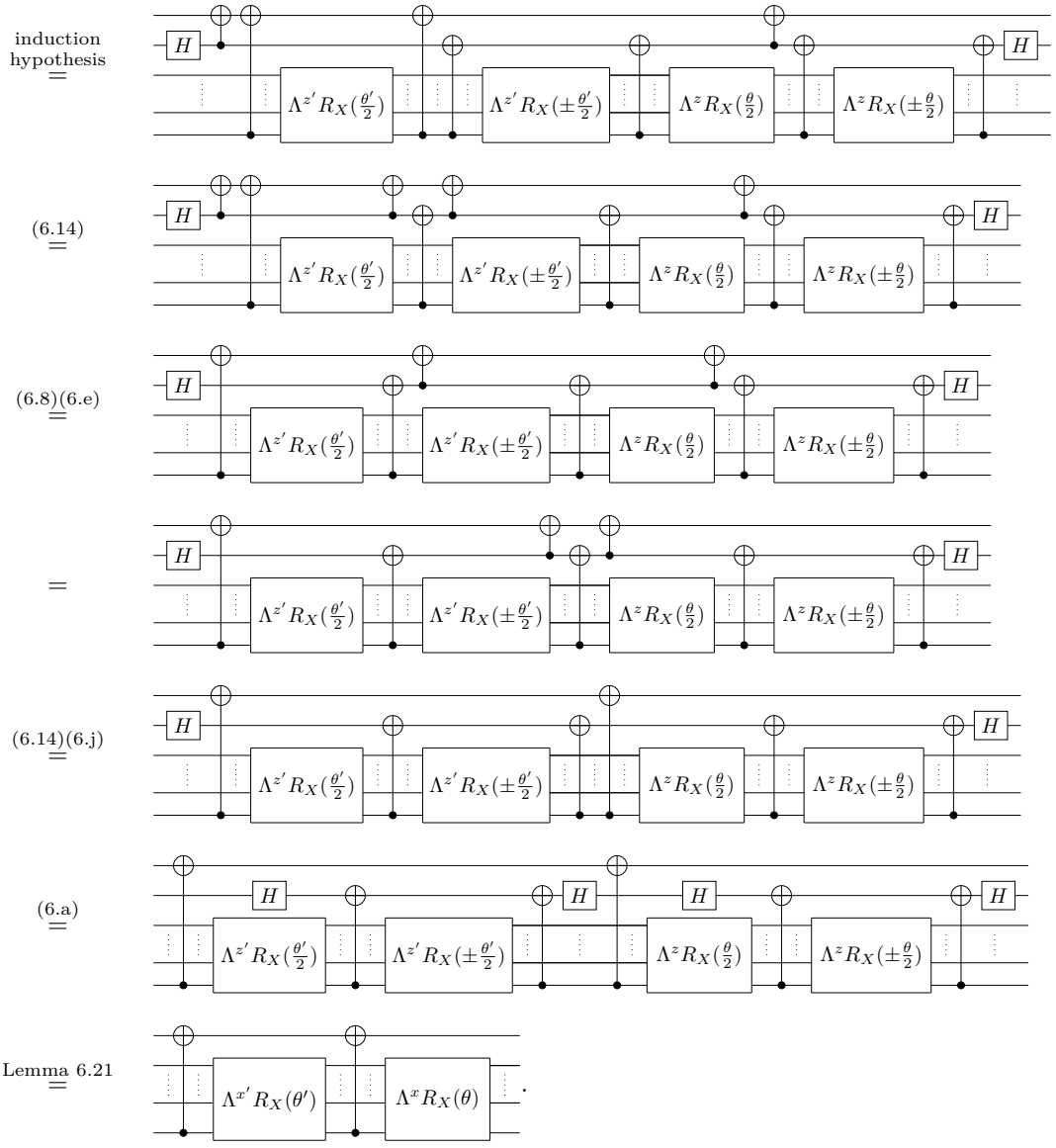


(6.8) =



(6.g) =



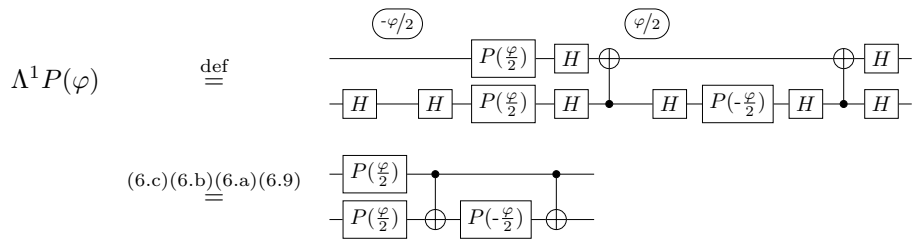


□

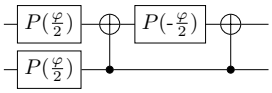
Proof of Propositions 6.17 and 6.18. First, we consider the case $G = R_X(\theta)$ of Equations (6.20)-(6.22), for which the proof is a direct induction based on Equation (6.26).

Next, we prove Equation (6.23) in the case $y = \epsilon$.

We can assume without loss of generality that $x = 1^k$. If $k = 0$, then



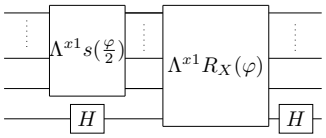
$\overset{(6.6)}{=}$



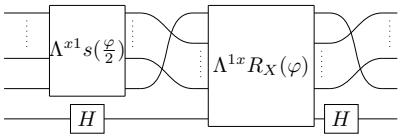
$\overset{(6.c)(6.b)(6.a)(6.9)}{=} \Lambda_1^{\epsilon} P(\varphi).$

If $k \geq 1$, then one has

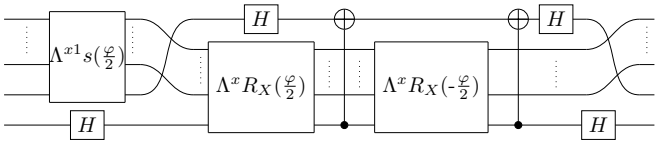
$\Lambda^{x1} P(\varphi) \overset{\text{def}}{=}$



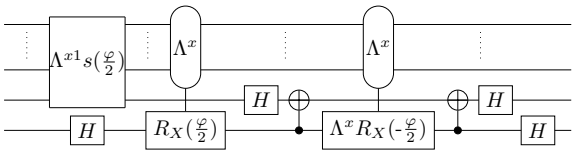
$\overset{\text{Equations (6.20)-(6.22) (case } G = R_X(\theta))}{=}$



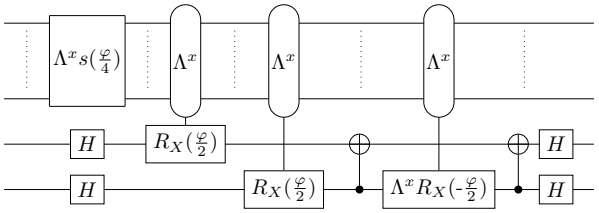
$\overset{\text{def}}{=}$



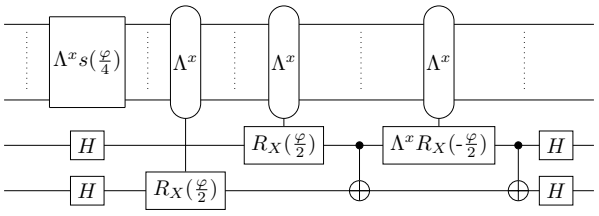
$=$



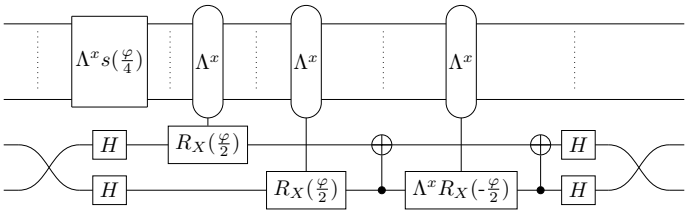
$\overset{\text{def,(6.a)}}{=}$



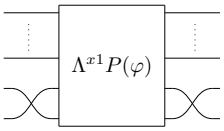
$\overset{\text{Lemmas 6.19 and 6.20}}{=}$



$=$



$=$



$= \quad \Lambda^x_1 P(\varphi).$

Now, we can prove Equations (6.20)-(6.22) in the case $G = s(\varphi)$ (the cases $G = P(\varphi)$ and $G = X$ are direct consequences of this case). Without loss of generality we can assume $y = \epsilon$ and consider only Equation (6.20).

The proof is by induction on the number r of input qubits of $\Lambda^{xabz} s(\varphi)$. If $z = \epsilon$, which is necessarily the case in the base case $r = 2$, then the result is a direct consequence of the case $y = \epsilon$ of Equation (6.23). If $z \neq \epsilon$, then using Definitions 6.6 and 6.7 (in particular the case of $\lambda^{n+1} P(\varphi)$ in Definition 6.6), the result is a direct consequence of the induction hypothesis and the case $G = R_X(\theta)$ of Equations (6.20)-(6.22).

Finally, using the definition of $\Lambda^x_{y1} P(\varphi)$ in terms of $\Lambda^{xy1} P(\varphi)$, the general case of Equation (6.23) follows directly from the case $y = \epsilon$ and Equations (6.20)-(6.22). □

6.1.4.3 Monoid Structure

The gates $P(\varphi)$ form a monoid, i.e. $P(\varphi + \varphi') = P(\varphi) \circ P(\varphi')$ (Equation (6.k)) and $P(0) = ——$ (Equation (6.d)). Notice that $R_X(\theta)$ and $s(\varphi)$ also form monoids. It is provable in QC_0 that their multi-controlled versions enjoy the same property:

Proposition 6.23. *For any $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$,*

$$\mathrm{QC}_0 \vdash \Lambda^x_y R_X(\theta') \circ \Lambda^x_y R_X(\theta) = \Lambda^x_y R_X(\theta + \theta'), \qquad \mathrm{QC}_0 \vdash \Lambda^x_y R_X(0) = id_{k+\ell+1},$$

$$\mathrm{QC}_0 \vdash \Lambda^x_y P(\varphi') \circ \Lambda^x_y P(\varphi) = \Lambda^x_y P(\varphi + \varphi'), \qquad \mathrm{QC}_0 \vdash \Lambda^x_y P(0) = id_{k+\ell+1},$$

$$\mathrm{QC}_0 \vdash \Lambda^x_y s(\varphi') \circ \Lambda^x_y s(\varphi) = \Lambda^x_y s(\varphi + \varphi'), \qquad \mathrm{QC}_0 \vdash \Lambda^x_y s(0) = id_{k+\ell},$$

where $id_k \coloneqq —^{\otimes k}$ is the identity circuit on k qubits (see Figure 6.5 below).

Remark 6.24. *Note that Proposition 6.23 does not imply the periodicity of controlled gates. The latter is proven in Proposition 6.39 with the help of the rules of Figure 6.4.*

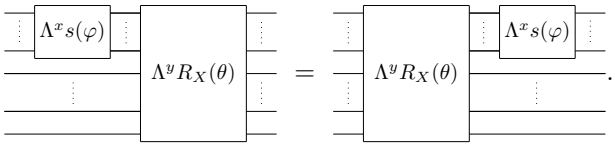
Proof of Proposition 6.23. First, proving that multi-controlled gates with angle 0 are equivalent to the identity is straightforward by induction.

To prove the rest of the proposition, we first prove that $\mathrm{QC}_0 \vdash \Lambda^{1\cdots1} R_X(\theta') \circ \Lambda^{1\cdots1} R_X(\theta) = \Lambda^{1..1} R_X(\theta + \theta')$. The proof is by induction: we unfold the two multi-controlled gates, use Equation (6.26) to put the multi-controlled gates with angles $\theta/2$ and $\theta'/2$ side by side, and merge them using the induction hypothesis. We use again Equation (6.26) to allow the combination of the multi-controlled gates with angle $-\theta/2$ and $-\theta'/2$, closing the case.

The cases with more general controls are derived from this one using Definitions 6.7 and 6.8.

It remains to treat the $\Lambda^x P$ and $\Lambda^x s$ cases. Those cases are a direct consequence of the following lemma:

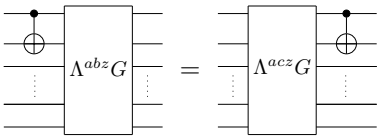
Lemma 6.25. *For any $x \in \{0,1\}^k$ and $y \in \{0,1\}^\ell$ with $\ell \geq k$,*

$\mathrm{QC}_0 \vdash$ 

To prove the previous lemma, we do a proof by induction on k. However, to prove the induction step for $k \geq 2$, we use $\mathrm{QC}_0 \vdash \Lambda^{1^{k-2}} s(\varphi) \circ \Lambda^{1^{k-2}} s(\varphi') = \Lambda^{1^{k-2}} s(\varphi + \varphi')$ and $\mathrm{QC}_0 \vdash \Lambda^{1^{k-2}} s(0) = id_{k-1}$, which are the statements of Proposition 6.23.

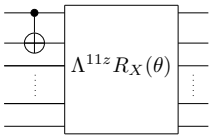
Therefore, we need to do a common induction proof for both the $\Lambda^x P$ and $\Lambda^x s$ cases of Proposition 6.23 and for Lemma 6.25. The plan of the proof is the following. First we prove an ancillary equation (Equation (6.27)) which is derived from previous lemmas. Then we proceed with the induction proof: for $k \geq 2$, the induction step of Lemma 6.25 is proved with the help of Proposition 6.23 with $k-2$ control qubits, while the induction step of Proposition 6.23 is proved with the help of Lemma 6.25 with x of size k, and of the $\Lambda^x R_X$ case which is already proven.

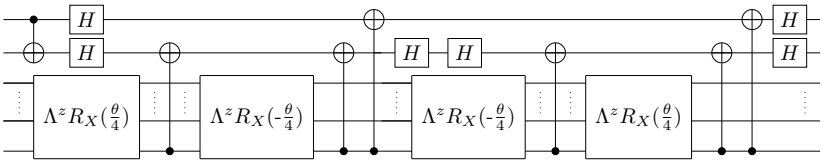
First we prove the following property, which is true for any $a, b \in \{0,1\}$, $z \in \{0,1\}^m$ and $G \in \{s(\varphi), P(\varphi), R_X(\theta), X\}$:

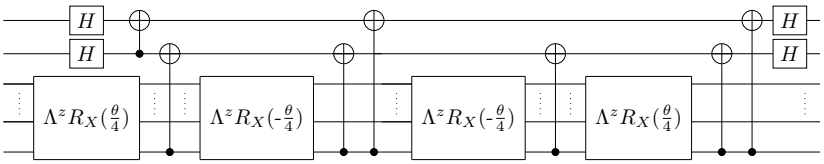
$\mathrm{QC}_0 \vdash$ 

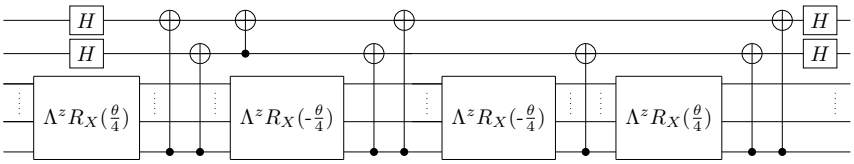
$$\text{where } c = \begin{cases} b & \text{if } a = 0 \\ \bar{b} & \text{if } a = 1 \end{cases} \tag{6.27}$$

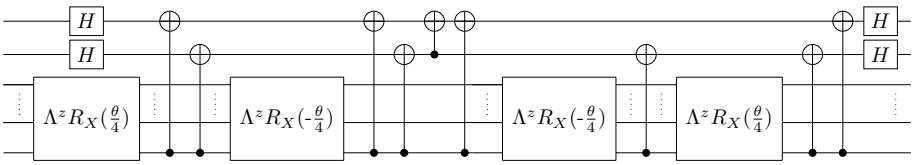
To prove Equation (6.27), by Equations (6.10), (6.12) and (6.f) we can assume without loss of generality that $a = b = 1$. If $G = R_X(\theta)$, then



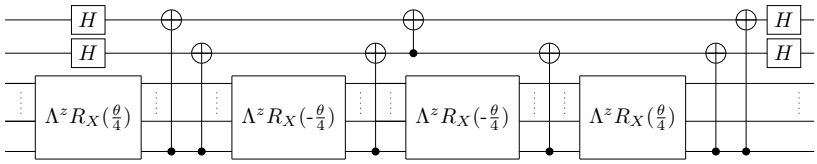
$=$ 

$\overset{(6.9)(6.a)}{=}$ 

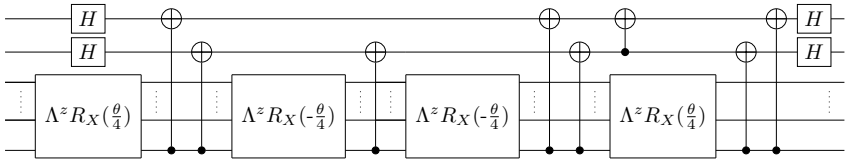
$\overset{(6.e)(6.14)}{=}$ 

$\overset{(6.e)(6.14)}{=}$ 

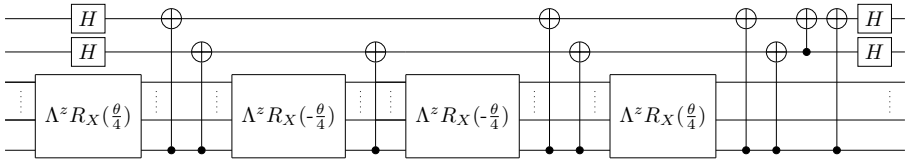
(6.8)(6.j)(6.e) =



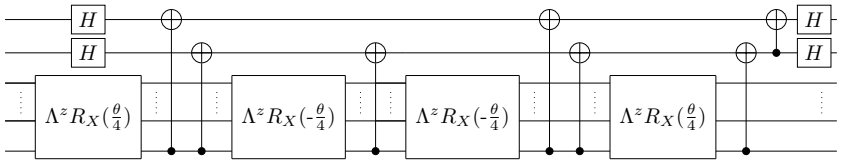
(6.e)(6.14) =



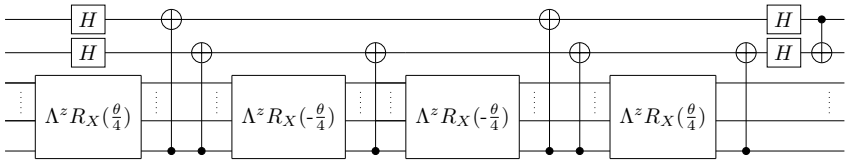
(6.e)(6.14) =



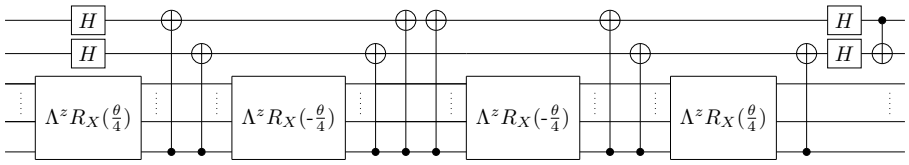
(6.8)(6.j)(6.e) =



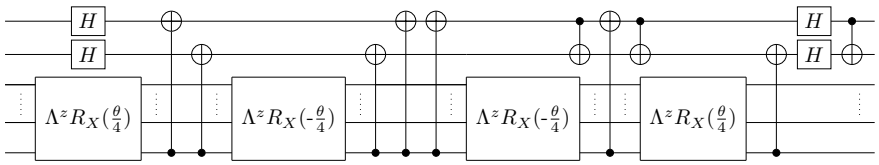
(6.9) =



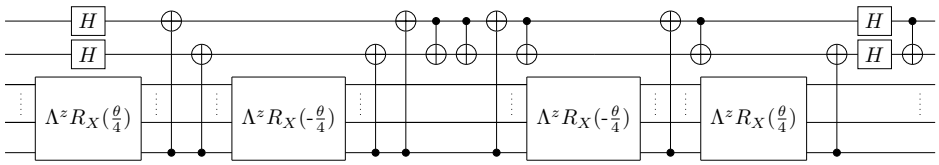
(6.e) =



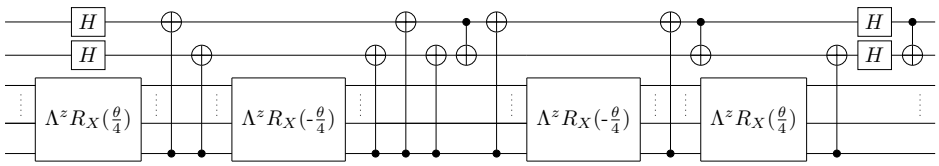
(6.14) =

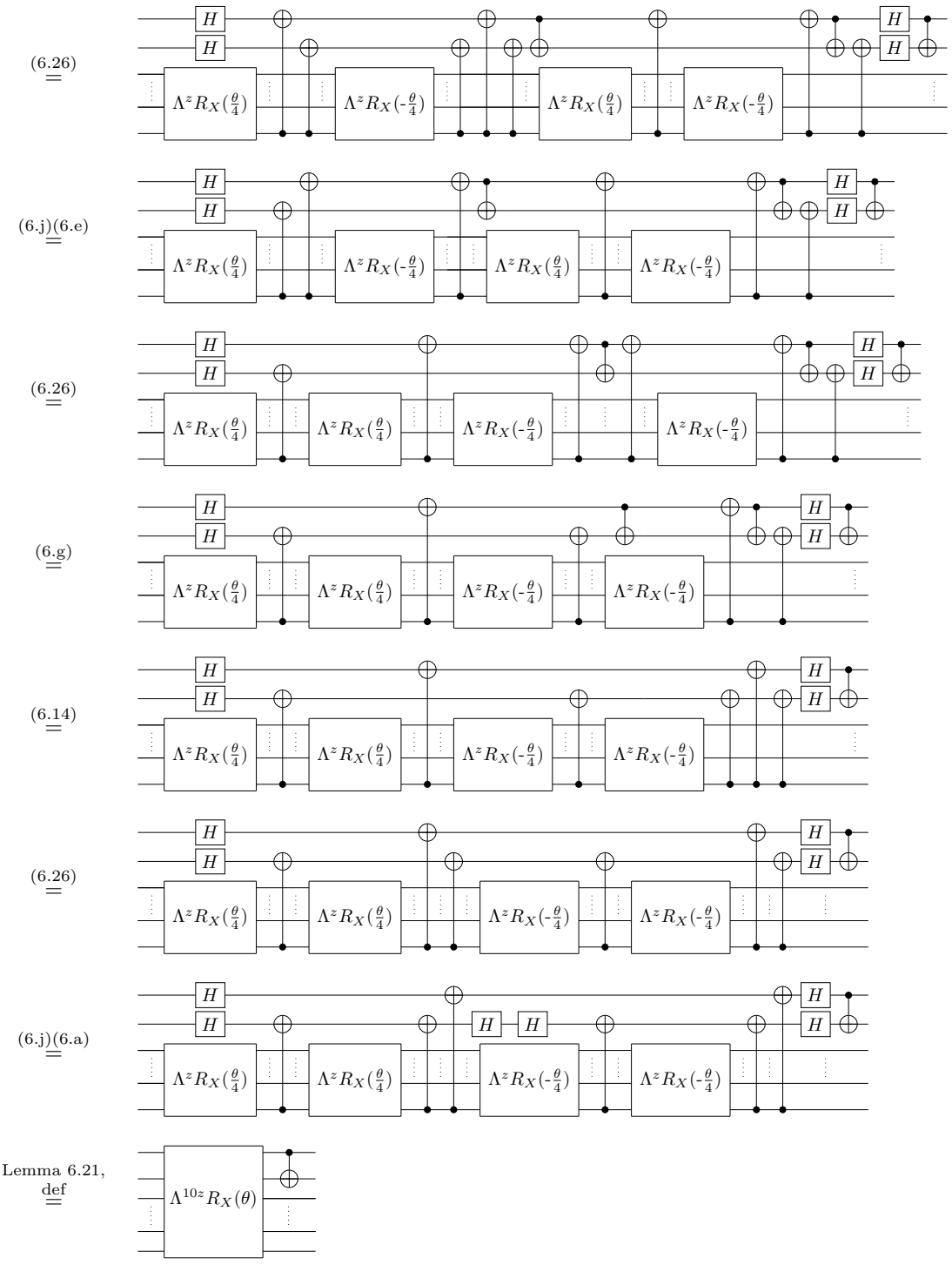


(6.e) =

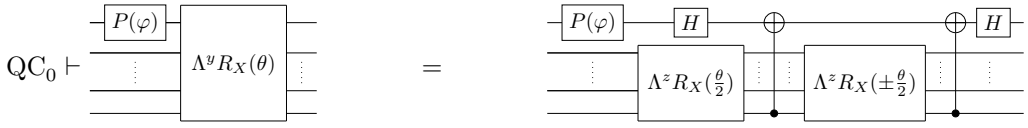


(6.14)(6.j)(6.8) =

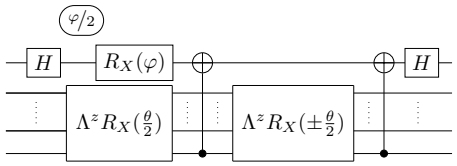




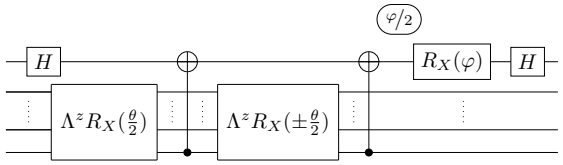
Now, to prove Proposition 6.23 and Lemma 6.25, by Equation (6.10) we can assume without loss of generality that $x = 1^k$. We proceed by induction on k. If $k = 0$, then Proposition 6.23 is a consequence of Equations (6.b), (6.c), (6.d) and (6.k), and Lemma 6.25 is a consequence of the topological rules. If $k = 1$, then $\Lambda^x s(\varphi) = P(\varphi)$. Let $y = az$ with $a \in \{0, 1\}$. By Lemma 6.21, one has



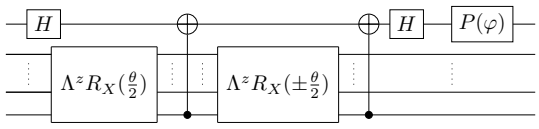
(6.a)(6.b)(6.c)(6.3) =



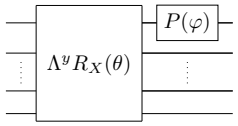
(6.16) =



(6.3)(6.c)(6.b)(6.a) =



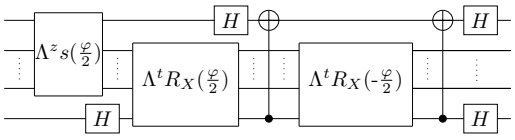
Lemma 6.21 =



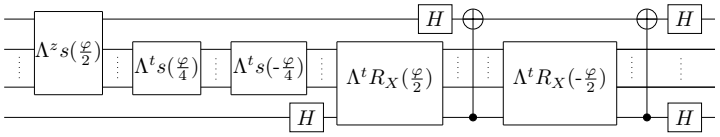
where the $\pm$ sign is $(-1)^a$. The case of $k = 1$ for Proposition 6.23 is then a direct consequence of the previous result, the case with R_X, Definition 6.6 (case $\lambda^n P(\varphi)$) and Equations (6.a), (6.d) and (6.k).

If $k \geq 2$, let $z = 1^{k-1}$ and $t = 1^{k-2}$. To prove Lemma 6.25, one has

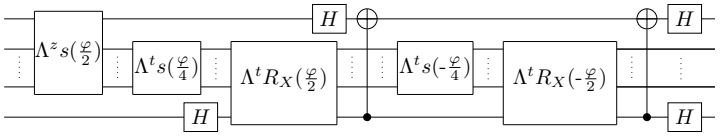
$\Lambda^x s(\varphi)$ =



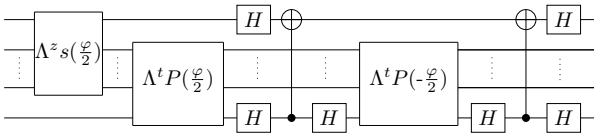
induction hypothesis of Proposition 6.23 =



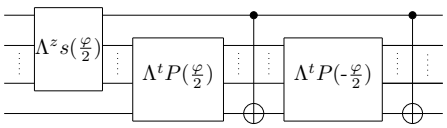
induction hypothesis of Lemma 6.25 =



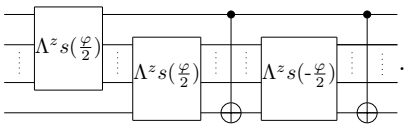
(6.a), def =



(6.9)(6.a) =



def =

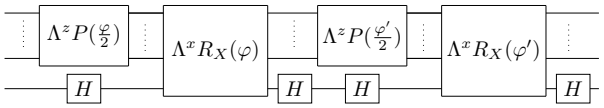


.

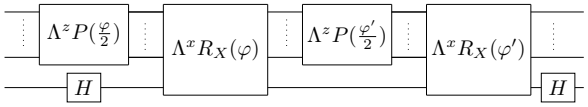
Hence, the commutation with $\Lambda^y R_X(\theta)$ follows by induction hypothesis and Equation (6.27), together with Proposition 6.17.

Then to prove the $\Lambda^x P$ case of Proposition 6.23, one has

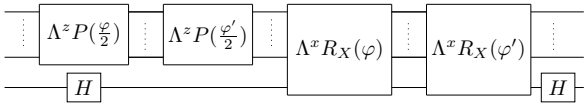
$\Lambda^x P(\varphi') \circ \Lambda^x P(\varphi) \quad =$



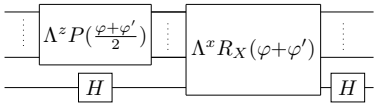
(6.a) $=$



induction hypothesis of Lemma 6.25 $=$



$\Lambda^x R_X$ case and induction hypothesis of Proposition 6.23 $=$

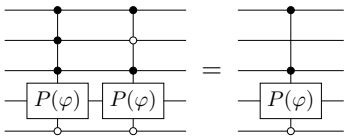


$= \quad \lambda^x P(\varphi + \varphi').$

Finally, the $\Lambda^x s$ case is a direct consequence of the $\Lambda^z P$ case. □

6.1.4.4 Complementarity of Control and Anti-Control

Combining a control and anti-control on the same qubit makes the evolution independent of this qubit, as in the following example in which the evolution is independent of the second qubit:[43]



Such simplifications can be derived in QC_0:

Proposition 6.26. *For any $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$, and $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$,*

$$\mathrm{QC}_0 \vdash \Lambda_y^{0x} G \circ \Lambda_y^{1x} G = \text{——} \otimes \Lambda_y^x G.$$

Proof. Without loss of generality, we can assume that $y = \epsilon$.

The case where $G = s(\varphi)$ and $x = \epsilon$ follows directly from Equations (6.l), (6.k) and (6.d). The cases where $G = s(\varphi)$ and $x \neq \epsilon$ follow directly from the case $G = P(\varphi)$, together with Equation (6.10).

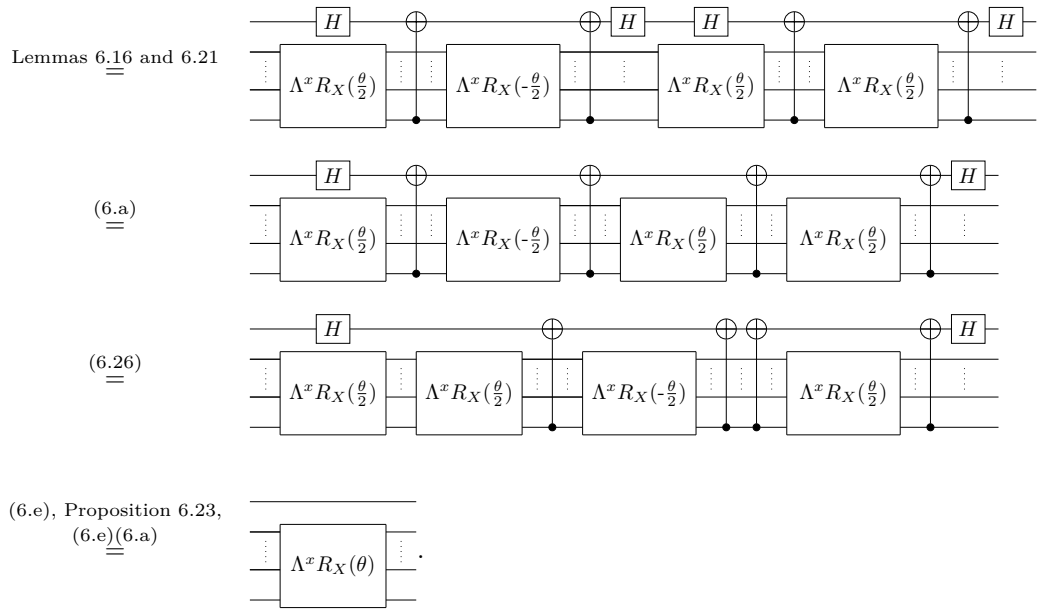
By Equations (6.10) and (6.a), the case $G = X$ follows directly from the case $G = P(\pi)$.

The case $G = P(\varphi)$ follows from the case $G = R_X(\theta)$ by a straightforward induction, using Lemmas 6.15 and 6.25 and Equation (6.a).

Thus, it suffices to treat the case where $G = R_X(\theta)$. One has

$$\Lambda^{0x} R_X(\theta) \circ \Lambda^{1x} R_X(\theta)$$

[43] Note that in the above example we implicitly use Proposition 6.17 to swap the first two qubits and apply Proposition 6.26. As a consequence, the resulting multi-controlled gate acts on non-adjacent qubits. Similarly to the CNot case (see Equations (6.4) and (6.5)), we use some syntactic sugar to represent such multi-controlled gates acting on non-adjacent qubits.

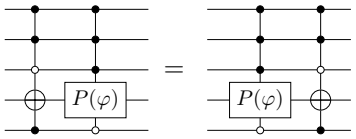


□

Proposition 6.26 shows how control and anti-control can be combined on the first qubit of a multi-controlled gate. Note, however, that it can be generalised to any control qubit thanks to Proposition 6.17.

6.1.4.5 Controlled and Anti-Controlled Gates Commute (Same Target)

Another useful property of multi-controlled gates is that they commute when there is a control and anti-control on the same qubit, as in the following example in which their controls differ on the third (and last) qubit:



When the target qubit is the same, such a commutation property can be derived in QC_0, using in particular Equation (6.n):

Proposition 6.27. *For any $x, x' \in \{0,1\}^k$, $y, y' \in \{0,1\}^\ell$, and $G, G' \in \{X, R_X(\theta), P(\varphi)\}$, if $xy \neq x'y'$*[44] *then*

$$\mathrm{QC}_0 \vdash \Lambda^x_y G \circ \Lambda^{x'}_{y'} G' = \Lambda^{x'}_{y'} G' \circ \Lambda^x_y G\,.$$

Ancillary Lemmas To prove Proposition 6.27, we need to first prove two ancillary lemmas.

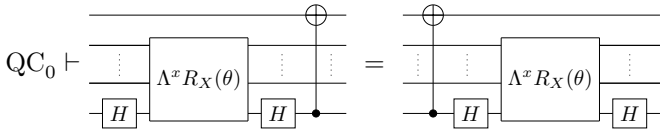
Lemma 6.28. *For any $x \in \{0,1\}^k$,*

$$\mathrm{QC}_0 \vdash \Lambda^x X \;=\; \Lambda^x s(\tfrac{\pi}{2}) \;\; \Lambda^x R_X(\pi) \tag{6.28}$$

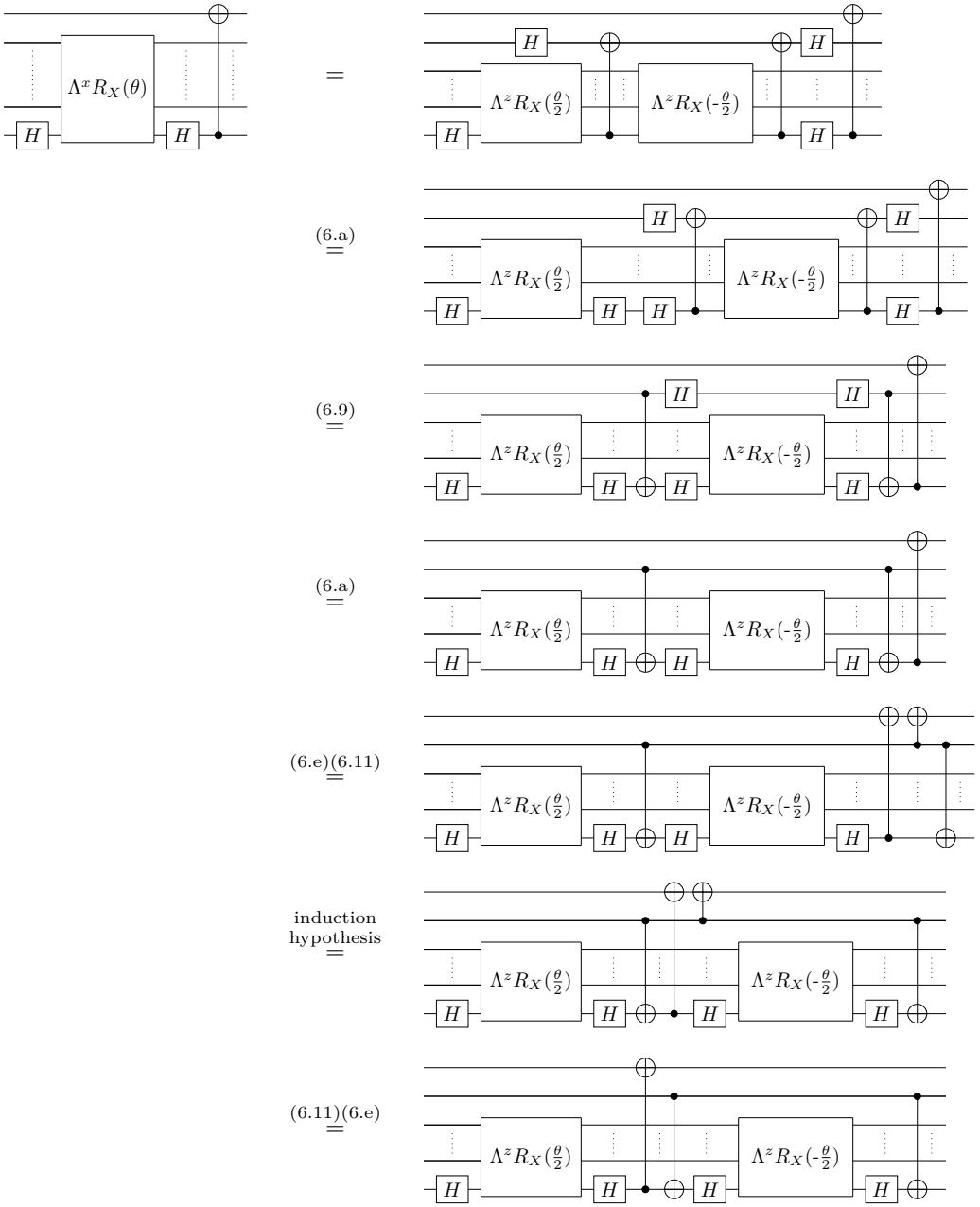
Proof. If $x = \epsilon$, then Equation (6.28) is a direct consequence of Lemma 6.11 and Equations (6.2), (6.b), (6.c) and (6.3). If $x \neq \epsilon$, then Equation (6.28) is a direct consequence of Lemmas 6.12, 6.14 and 6.15 and Equations (6.10) and (6.a). □

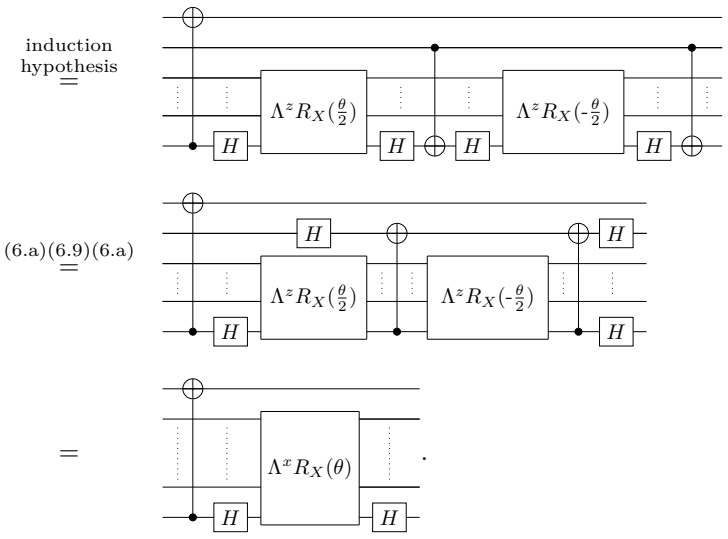
[44] $xy \neq x'y'$ iff $\exists i, x_i \neq x'_i \vee y_i \neq y'_i$.

Lemma 6.29. *For any $x \in \{0,1\}^k$,*



Proof. We proceed by induction on k. If $k = 0$ then the result is a direct consequence of Equations (6.3), (6.a) and (6.i). If $k \geq 1$, then without loss of generality we can assume that $x = 1z$ with $z \in \{0,1\}^{k-1}$. One has





□

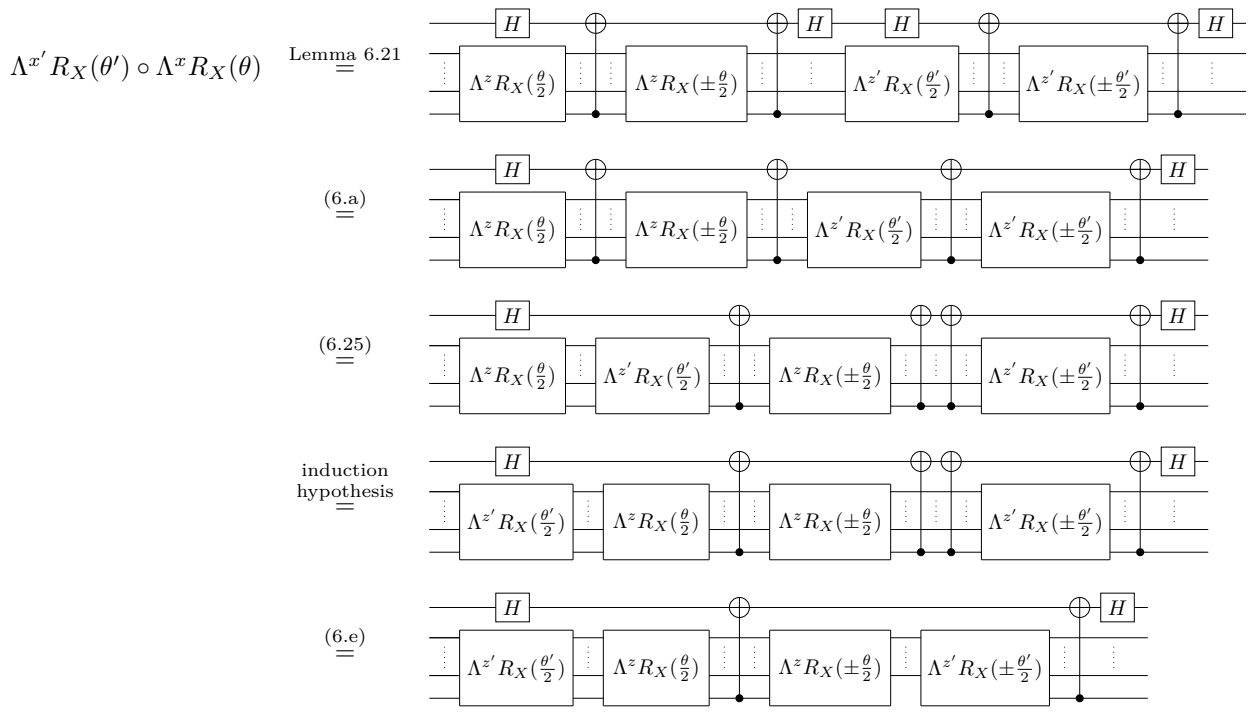
Proof of Proposition 6.27. We assume without loss of generality that $y = y' = \epsilon$.

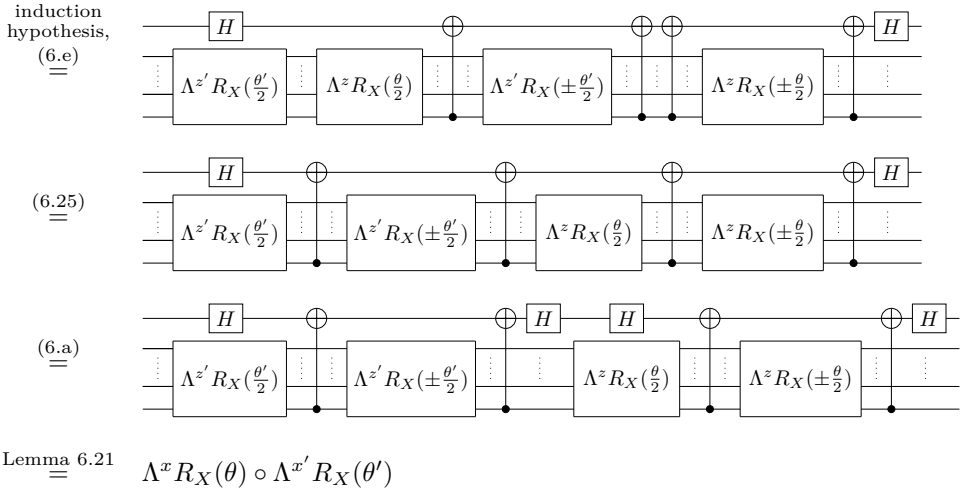
First, for the case where $G = R_X(\theta)$ and $G' = R_X(\theta')$, we prove by induction on k that for any $x, x' \in \{0,1\}^k$,

$$\mathrm{QC}_0 \vdash \Lambda^x R_X(\theta) \circ \Lambda^{x'} R_X(\theta') = \Lambda^{x'} R_X(\theta') \circ \Lambda^x R_X(\theta). \tag{6.29}$$

The desired result corresponds to Equation (6.29) with $x \neq x'$. Notice that when $x = x'$, Equation (6.29) is already a consequence of Proposition 6.23.

If $k = 0$, then Equation (6.29) is a direct consequence of Equation (6.18). If $k \geq 1$, then we can write $x = az$ and $x' = a'z'$ with $a, a' \in \{0,1\}$. One has (where the $\pm$ signs correspond respectively to $(-1)^a$ and $(-1)^{a'}$):





If $G = P(\theta)$ and $G' = P(\theta')$, we prove by induction on k that for any $z, z' \in \{0,1\}^k$,

$$\mathrm{QC}_0 \vdash \Lambda^z s(\varphi) \circ \Lambda^{z'} s(\varphi') = \Lambda^{z'} s(\varphi') \circ \Lambda^z s(\varphi). \tag{6.30}$$

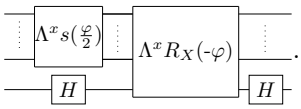
The result corresponds to the case where $z = x1$ and $z' = x'1$ with $x \neq x'$. Notice that the case where $x = x'$ is already a consequence of Proposition 6.23.

If $k = 0$, then Equation (6.30) is a consequence of the topological rules.

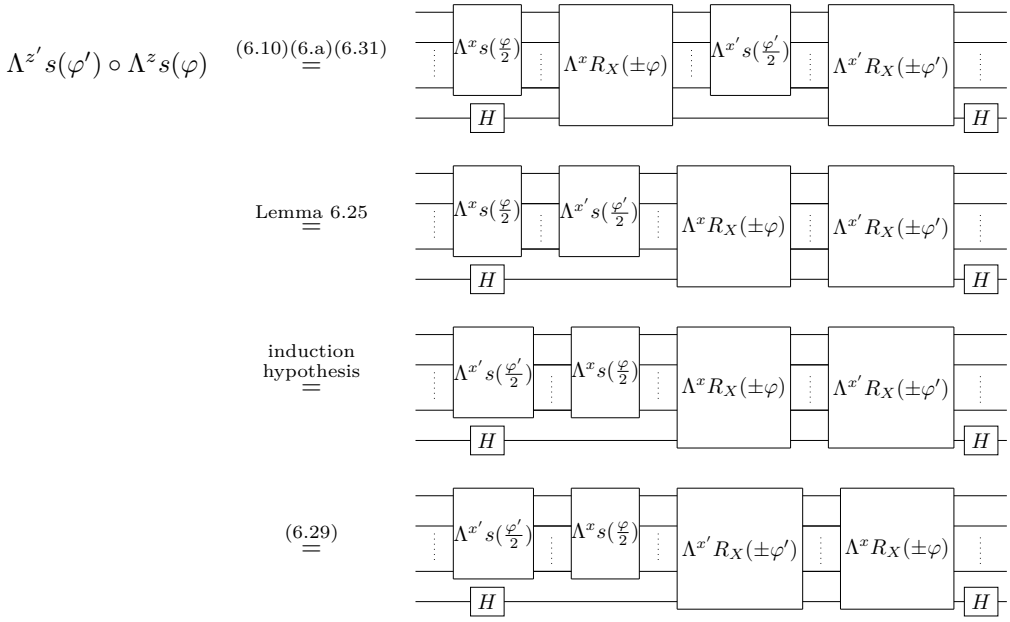
If $k = 1$, then it is a consequence of Equations (6.k) and (6.l).

If $k \geq 2$, note first that by Equations (6.2), (6.a), (6.24), and (6.13) (or (6.l), (6.a), (6.c) and (6.3) if $m = 0$), for any $x \in \{0,1\}^m$,

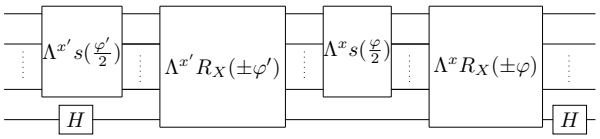
$$\mathrm{QC}_0 \vdash \Lambda^{x0} s(\varphi) \;=\; \tag{6.31}$$



Let $z = xa$ and $z' = x'a'$ with $a, a' \in \{0,1\}$ and $x, x' \in \{0,1\}^{k-1}$. One has (with the $\pm$ signs being $(-1)^{1-a}$ and $(-1)^{1-a'}$ respectively):

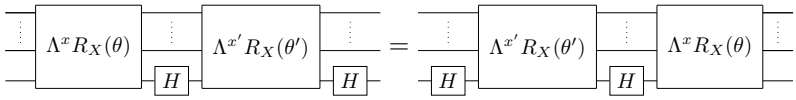


Lemma 6.25 $=$



(6.10)(6.a)(6.31) $=$ $\Lambda^z s(\varphi) \circ \Lambda^{z'} s(\varphi')$.

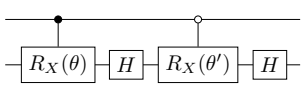
For the case where $G = R_X(\theta)$ and $G' = P(\theta')$, we prove by induction on $k \geq 1$ that for any $x, x' \in \{0,1\}^k$ with $x \neq x'$,

$$\mathrm{QC}_0 \vdash$$ 

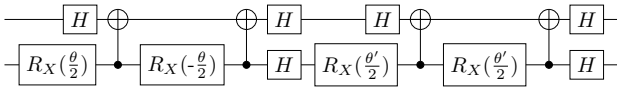
(6.32)

Note that by Lemma 6.25 (and the definition of $\Lambda^x P(\theta')$), Equation (6.32) is equivalent to the desired result.

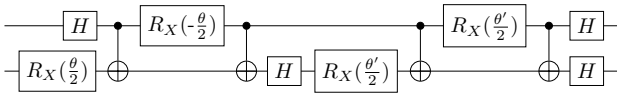
If $k = 1$, then without loss of generality we can assume that $x = 1$ and $x' = 0$. One has



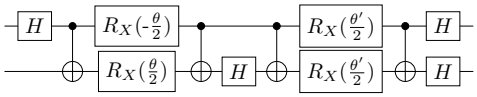
Lemma 6.21 $=$



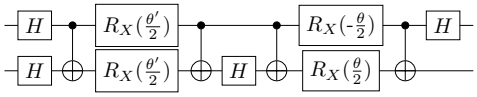
(6.a)(6.7) $=$



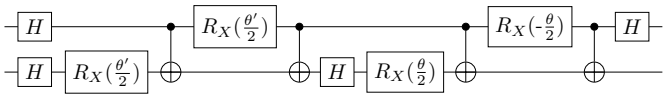
(6.16) $=$



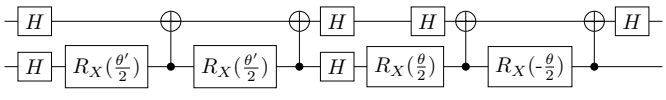
(6.n) $=$



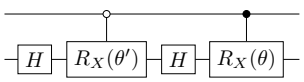
(6.16) $=$



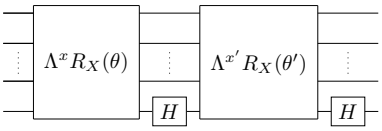
(6.7)(6.a) $=$



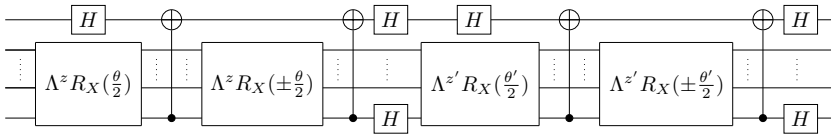
Lemma 6.21 $=$



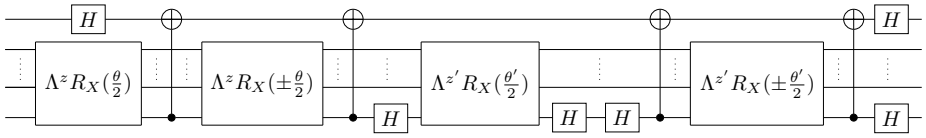
If $k \geq 2$, then by Proposition 6.17, we can assume without loss of generality that we can write $x = az$ and $x' = az'$ with $a, a' \in \{0,1\}$ and $z \neq z'$. One has (where the $\pm$ signs correspond respectively to $(-1)^a$ and $(-1)^{a'}$):



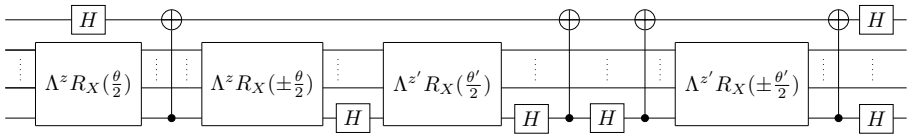
Lemma 6.21 =



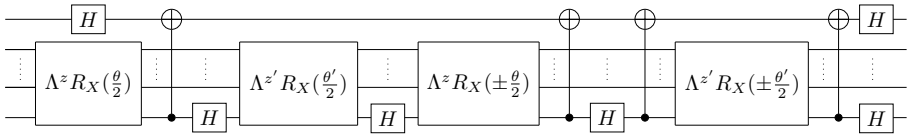
(6.a) =



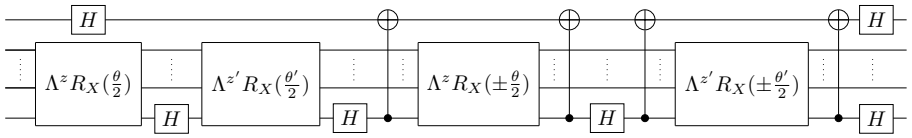
Lemma 6.29 =



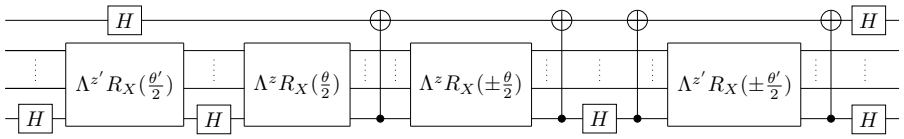
induction hypothesis =



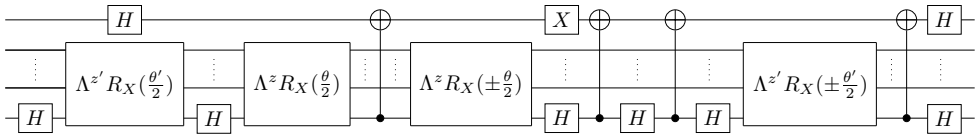
Lemma 6.29 =



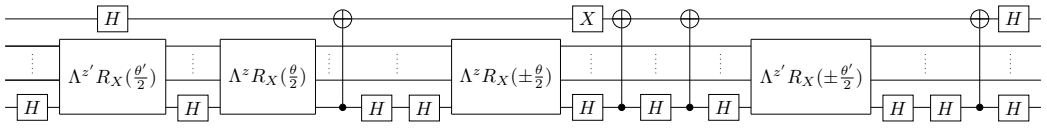
induction hypothesis =



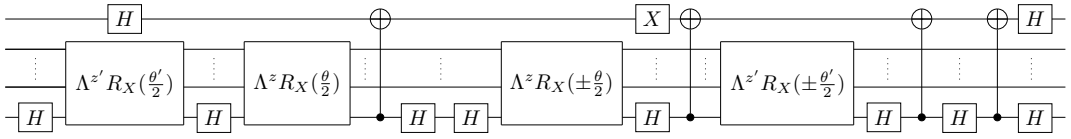
(6.19) =



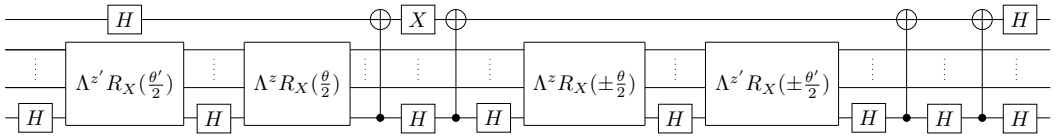
(6.a) =



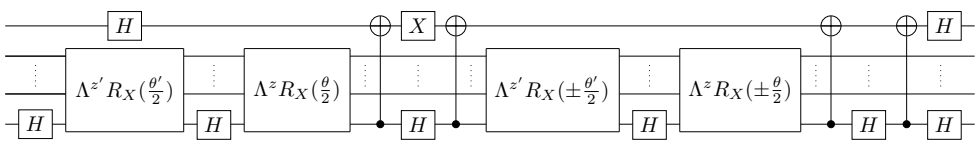
Lemma 6.29, (6.a) =



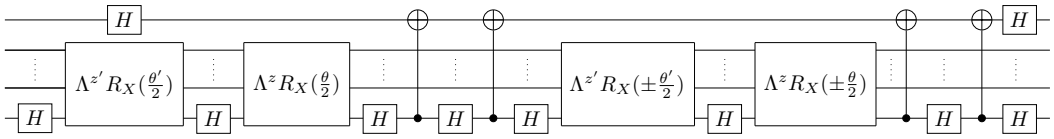
Lemma 6.29 =



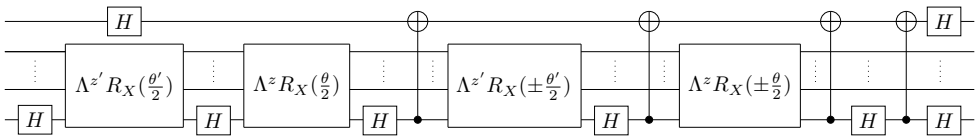
induction hypothesis, (6.a) =



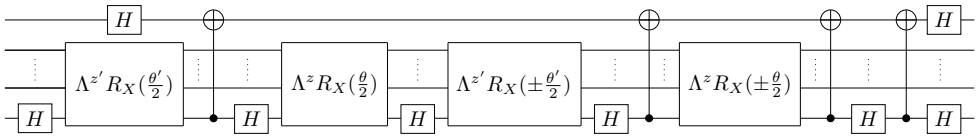
(6.12)(6.19)
(6.10)
=



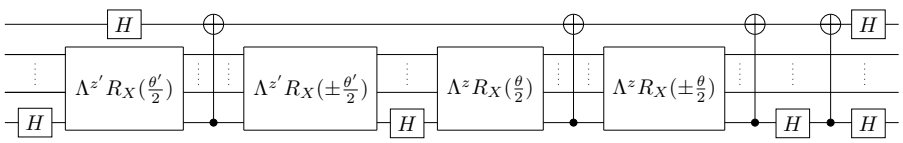
Lemma 6.29,
(6.a)
=



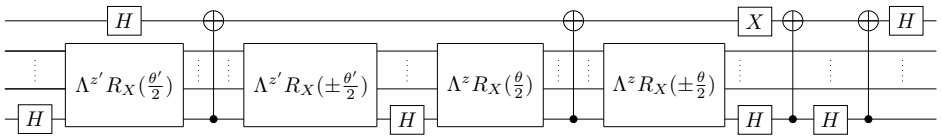
Lemma 6.29
=



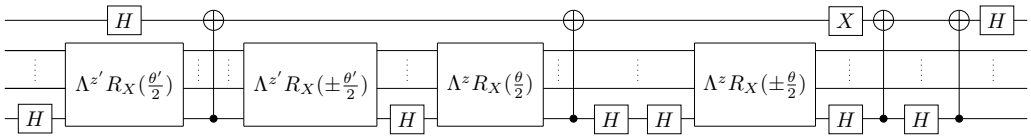
induction
hypothesis,
(6.a)
=



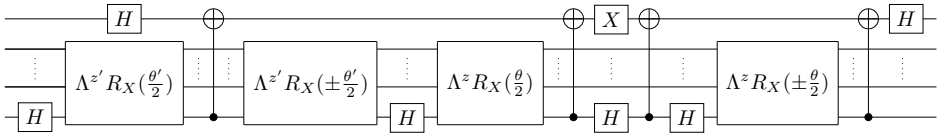
(6.19)(6.a)
=



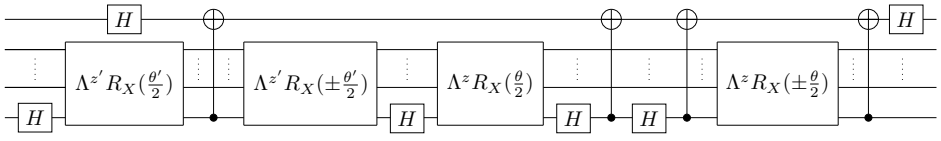
(6.a)
=



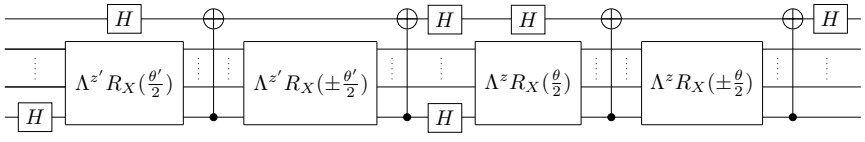
Lemma 6.29,
(6.a)
=



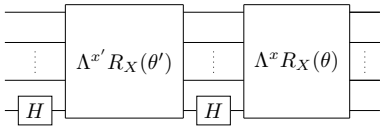
(6.12)(6.19)
(6.10)(6.a)
=



Lemma 6.29,
(6.a)
=



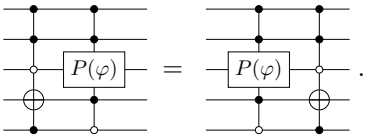
Lemma 6.21
=



If $G = X$ or $G' = X$, then by Equation (6.28), the result follows from the preceding cases together with Lemma 6.25 and Equation (6.30). □

6.1.4.6 Controlled and Anti-Controlled Gates Commute (Different Targets)

Controlled and anti-controlled gates also commute when the target qubits are not the same in both gates, as in:



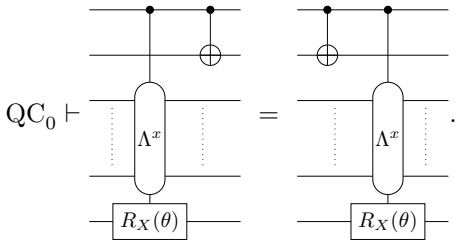
This property can also be derived in QC_0, using in particular Equation (6.o):

Proposition 6.30. *For any $a, b \in \{0,1\}$, $x, x' \in \{0,1\}^k$, $y, y' \in \{0,1\}^\ell$, $z, z' \in \{0,1\}^m$ and $G, G' \in \{X, R_X(\theta), P(\varphi)\}$, if $xyz \neq x'y'z'$ then*

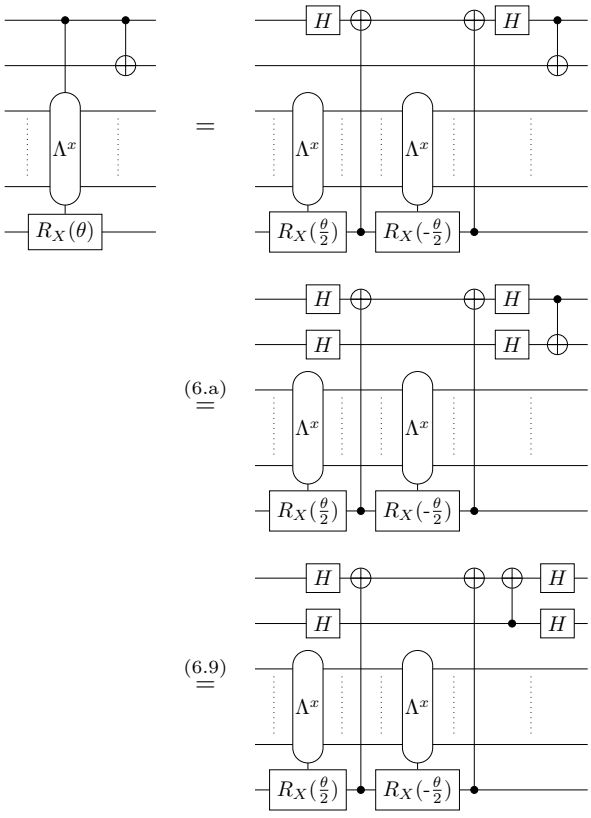
$$\mathrm{QC}_0 \vdash \Lambda^x_{yaz} G \circ \Lambda^{x'by'}_{z'} G' = \Lambda^{x'by'}_{z'} G' \circ \Lambda^x_{yaz} G$$

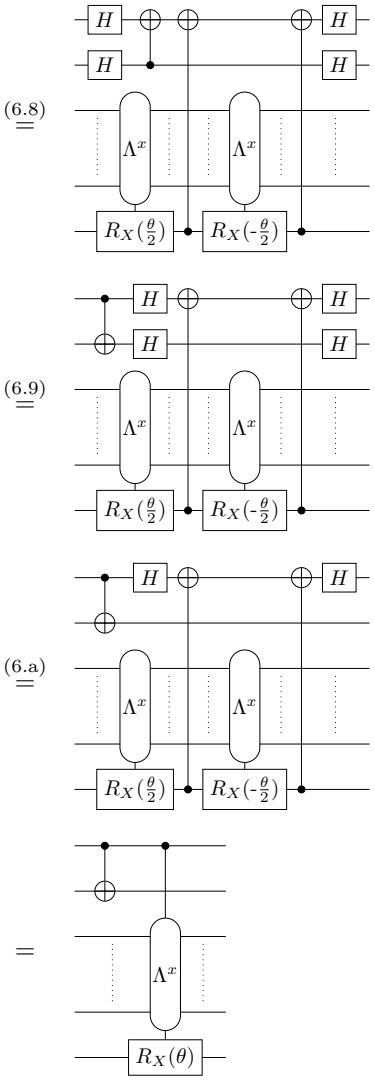
Ancillary Lemmas To prove Proposition 6.30, we need a few additional ancillary lemmas.

Lemma 6.31. *For any $x \in \{0,1\}^k$,*



Proof.





□

Lemma 6.32. *For any $x \in \{0,1\}^k$ and $y \in \{0,1\}^\ell$,*

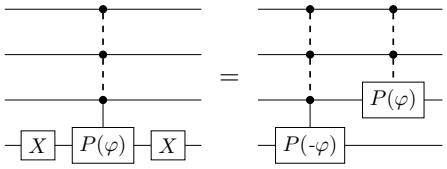
$$\mathrm{QC}_0 \vdash (id_k \otimes X \otimes id_\ell) \circ \Lambda^x_y X = \Lambda^x_y X \circ (id_k \otimes X \otimes id_\ell)$$

and

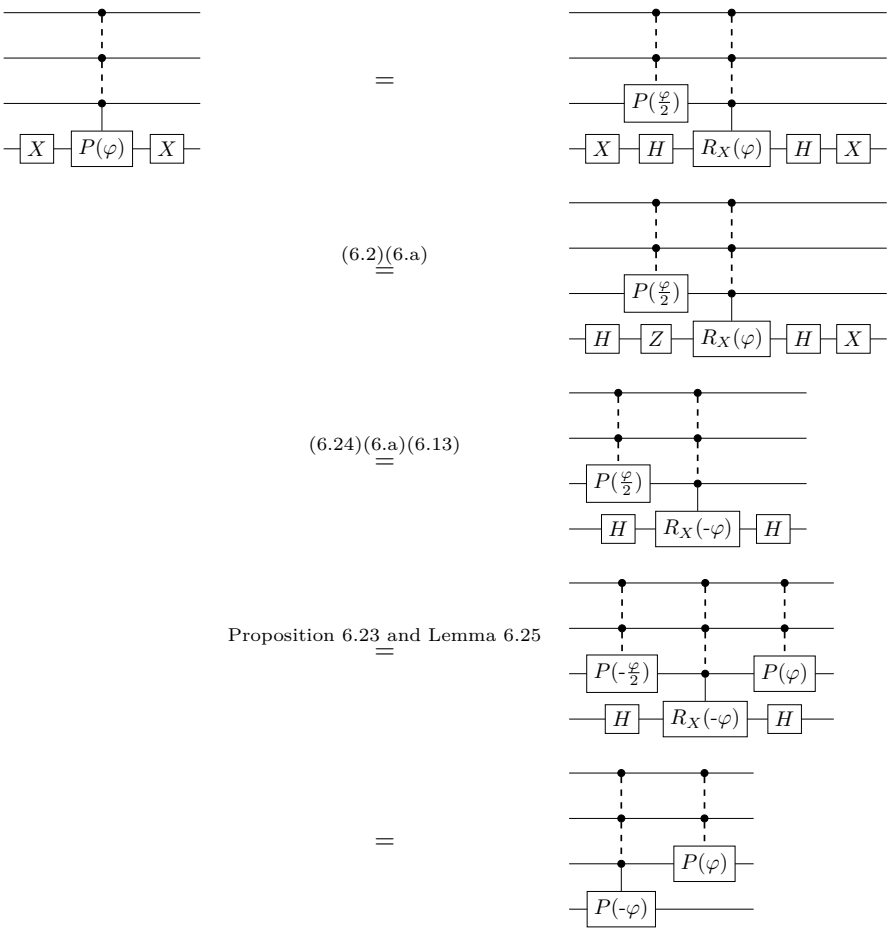
$$\mathrm{QC}_0 \vdash (id_k \otimes X \otimes id_\ell) \circ \Lambda^x_y R_X(\theta) = \Lambda^x_y R_X(\theta) \circ (id_k \otimes X \otimes id_\ell)$$

Proof. The case of $\Lambda^x_y X$ is a direct consequence of Propositions 6.26 and 6.27. Indeed, using Proposition 6.26, $(id_k \otimes X \otimes id_\ell)$ can be decomposed into a product of multi-controlled gates of the form $\Lambda^{x'}_{y'} X$ with $x' \in \{0,1\}^k$ and $y' \in \{0,1\}^\ell$. Then these multi-controlled gates commute with $\Lambda^x_y X$, trivially in the case where $x'y' = xy$, and by Proposition 6.27 in the other cases. For the case of $\Lambda^x_y R_X(\theta)$, note that by Equations (6.1) to (6.3), (6.b) and (6.c), one has $-\boxed{X}- = -\overset{(\pi/2)}{\boxed{R_X(\pi)}}-$. Then $s(\frac{\pi}{2})$ commutes by the topological rules, while the commutation of $(id_k \otimes R_X(\pi) \otimes id_\ell)$ is a direct consequence of Propositions 6.26, 6.27 and 6.23: using Proposition 6.26, it can be decomposed into a product of multi-controlled gates of the form $\Lambda^{x'}_{y'} R_X(\pi)$ with $x' \in \{0,1\}^k$ and $y' \in \{0,1\}^\ell$. Then these multi-controlled gates commute with $\Lambda^x_y R_X(\theta)$, by Proposition 6.27 in the cases where $x'y' \neq xy$, and by Proposition 6.23 in the case where $x'y' = xy$. □

Lemma 6.33.

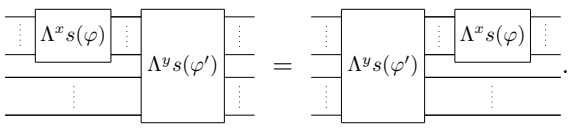
$\mathrm{QC}_0 \vdash$ 

Proof.



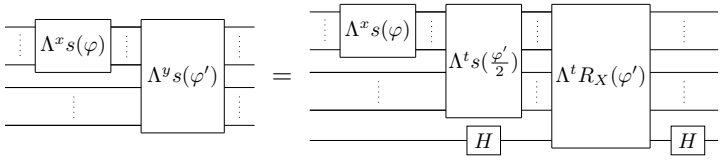
□

Lemma 6.34. *For any $x \in \{0,1\}^k$ and $y \in \{0,1\}^\ell$ with $\ell \geq k$,*

$\mathrm{QC}_0 \vdash$ 

.

Proof. We proceed by induction on $\ell - k$. If $\ell = k$ then the result is a consequence of Proposition 6.23 or 6.27 (or just of the topological rules if $k = \ell = 0$). If $\ell \geq k+1$, then without loss of generality, we can assume that $y = t1$ for some $t \in \{0,1\}^{\ell-1}$. Then by Lemma 6.15 (together with Lemma 6.12 and Equation (6.10)),

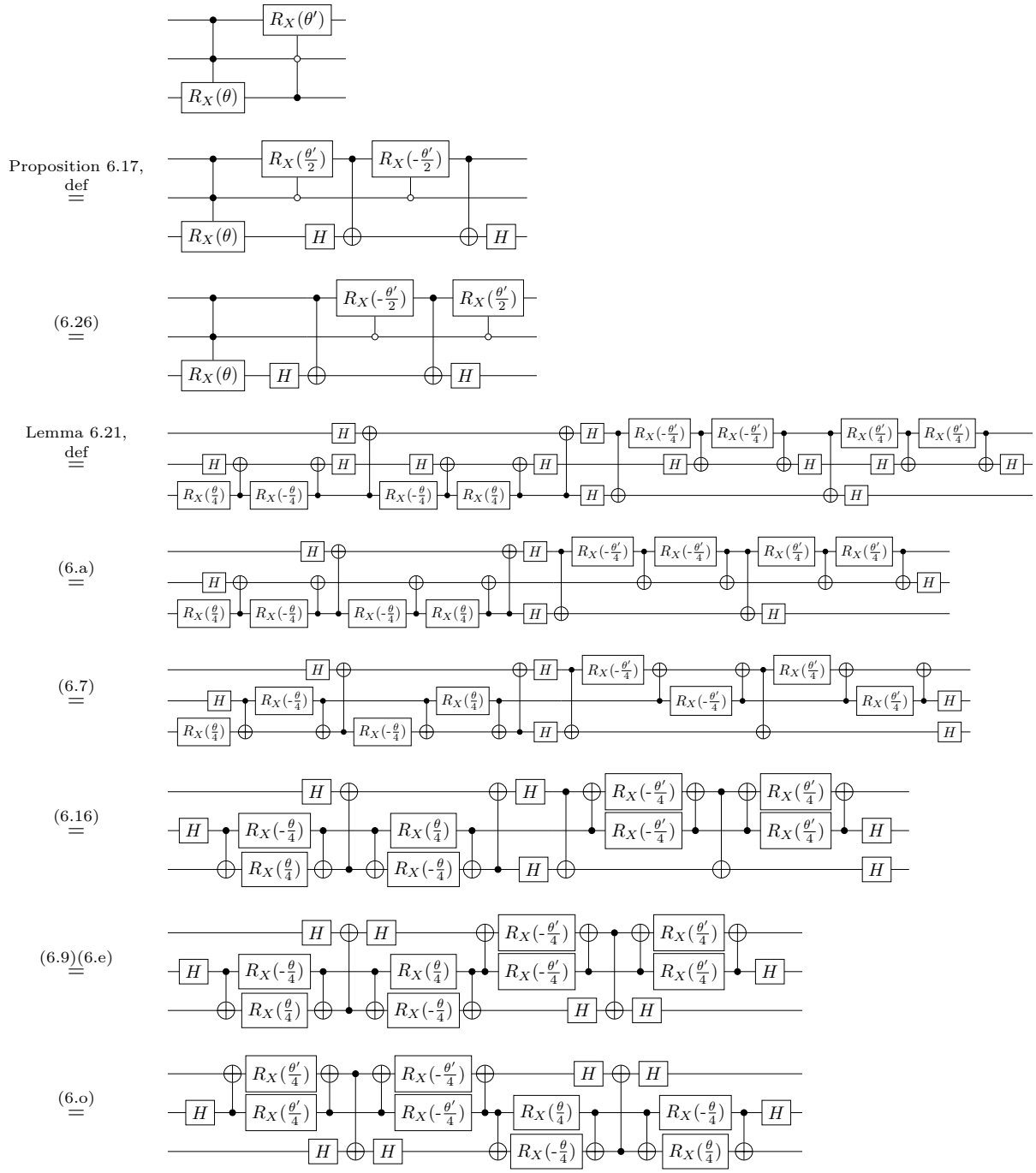
$\mathrm{QC}_0 \vdash$ 

so that the commutation follows by induction hypothesis and Lemma 6.25. □

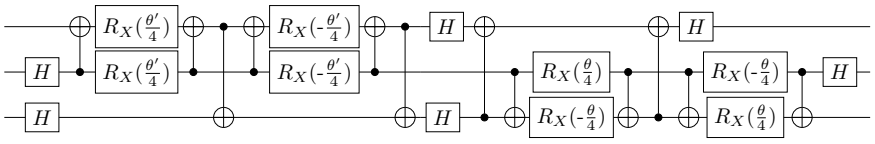
Proof of Proposition 6.30. If $G = R_X(\theta)$ and $G' = P(\varphi)$ (or conversely), then by Proposition 6.18, the result is a consequence of Lemma 6.32 and Proposition 6.27.

If $G = P(\varphi)$ and $G' = P(\varphi')$, then by Proposition 6.18, the result is a consequence of Lemmas 6.33 and 6.34 (together with Equation (6.10)) and Proposition 6.27.

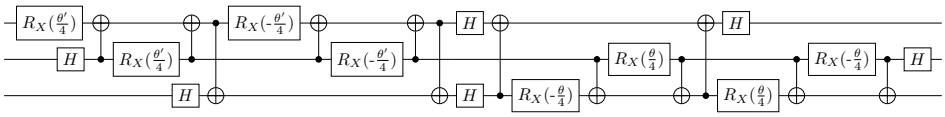
Now we treat the case where $G = R_X(\theta)$ and $G' = R_X(\theta')$. By Lemma 6.32, we can assume without loss of generality that $a = b = 1$. By definition of Λ_u^t and Proposition 6.17, we can also assume without loss of generality that $k = m = 0$. Then the hypothesis $xyz \neq x'y'z'$ becomes $y \neq y'$. We proceed by induction on ℓ. If $\ell = 1$, then without loss of generality we can assume that $y = 1$ and $y' = 0$. One has



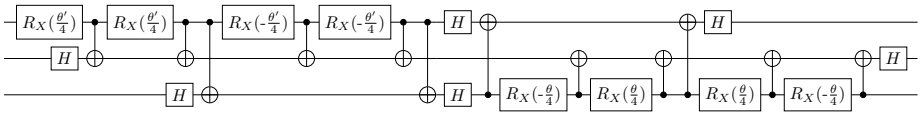
(6.e)(6.9) =



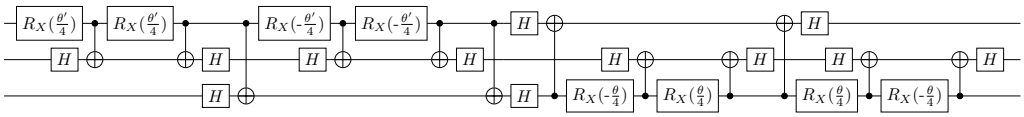
(6.16) =



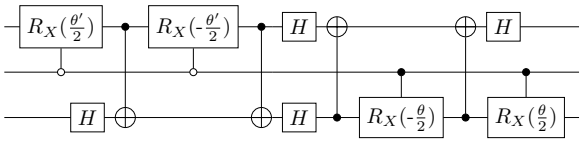
(6.7) =



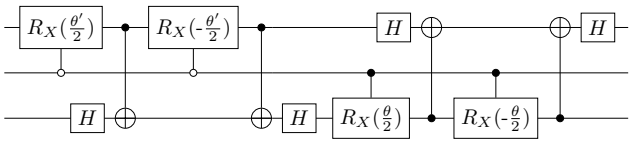
(6.a) =



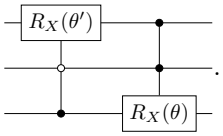
Lemma 6.21, def =



(6.26) =

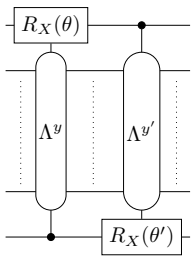


Proposition 6.17, def =

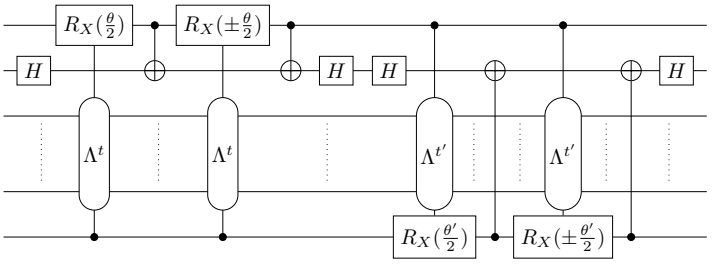


.

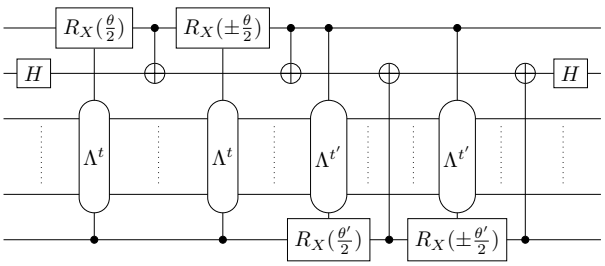
If $\ell \geq 2$, by Proposition 6.17 we can assume without loss of generality that $y = at$ and $y' = a't'$ with $a, a' \in \{0, 1\}$ and $t \neq t'$. One has (with the $\pm$ signs being $(-1)^a$ and $(-1)^{a'}$ respectively):



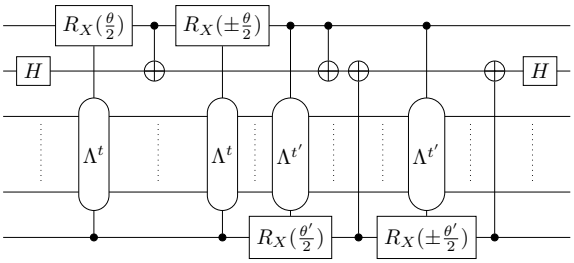
Proposition 6.17, Lemma 6.21 =



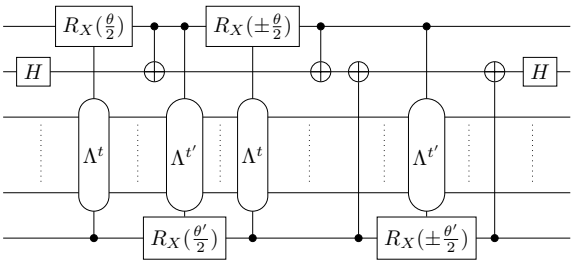
(6.a) =



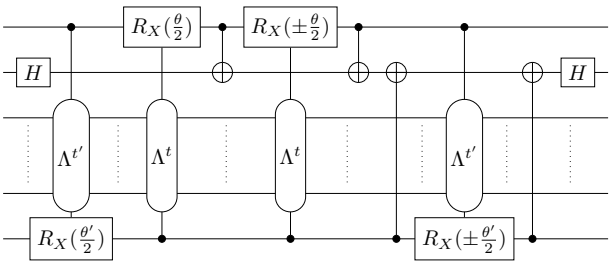
Lemma 6.31 =



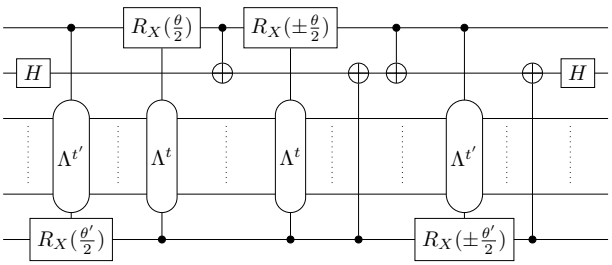
induction hypothesis =



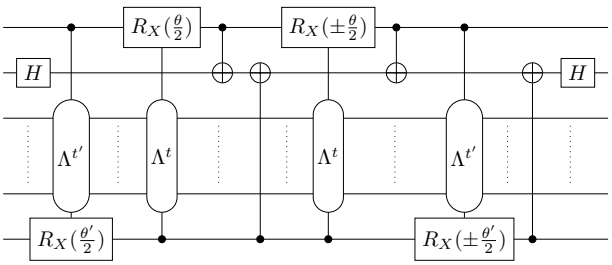
Lemma 6.31, induction hypothesis =



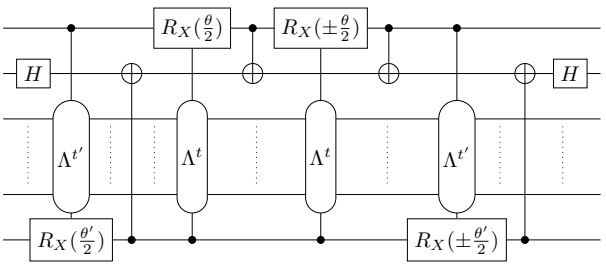
(6.8) =



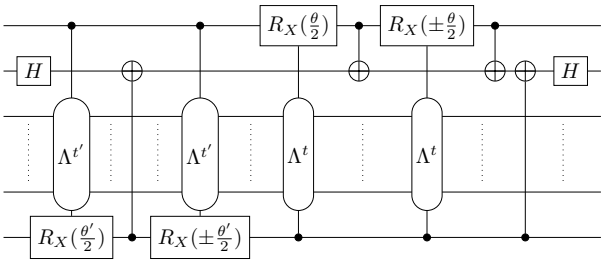
Proposition 6.17, Lemma 6.31 =



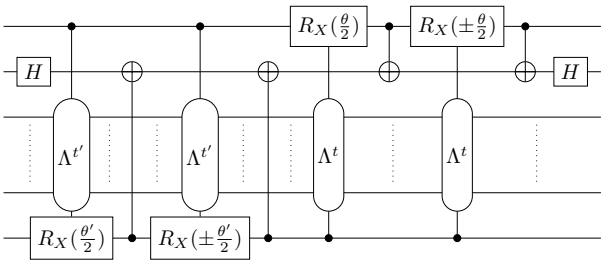
(6.8), Proposition 6.17, Lemma 6.31 =



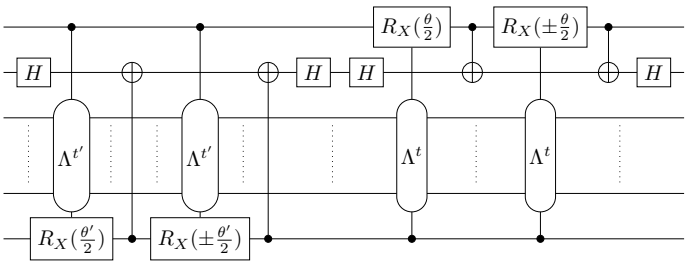
Lemma 6.31, induction hypothesis =



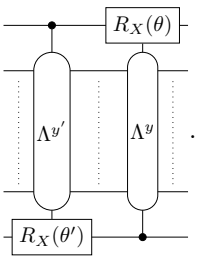
(6.8), Proposition 6.17, Lemma 6.31 =



(6.a) =



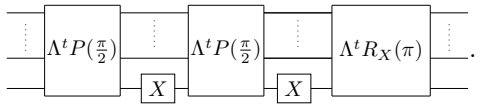
Proposition 6.17, Lemma 6.21 =



.

It remains to treat the cases where G or $G' = X$. First, note that for any $t \in \{0,1\}^p$, using Equation (6.28) and Proposition 6.26 (together with Proposition 6.17), and then Proposition 6.18, one can decompose $\Lambda^t X$ as follows:

$\mathrm{QC}_0 \vdash \Lambda^t X \;=$



.

In the cases where G or $G' = X$, one can use this decomposition, and make the multi-controlled parts commute using the preceding cases. The non-controlled X gates commute with the control dots by changing their colour, with the help of Equation (6.10). This does not alter the fact that the multi-controlled gates commute, since the X gates are not on the same wire as the control dots of different colours. And since the decomposition produces each time two X gates on the same wire, any control dot gets changed twice, so that it is the same at the end as at the beginning. □

6.1.5 Euler Angles and Periodicity

QC_0 is not complete. In particular equations based on Euler angles, which require non-trivial calculations on the angles, cannot be derived. As a consequence we add to the equational theory the three rules shown in Figure 6.4, leading to the equational theory QC. We write $\mathrm{QC} \vdash C_1 = C_2$ when C_1 can be rewritten into C_2 using equations of Figure 6.2 and Figure 6.4 (together with the deformation rules).

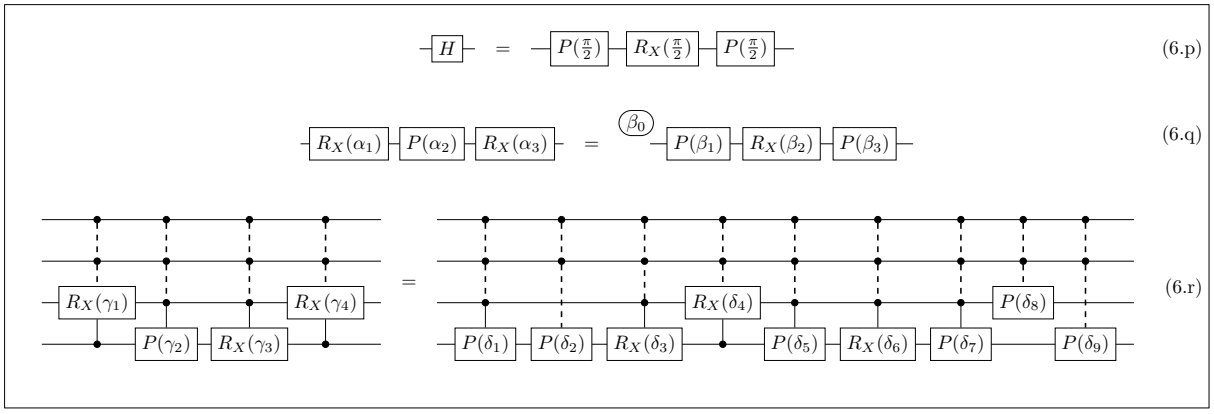
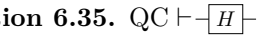
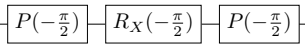
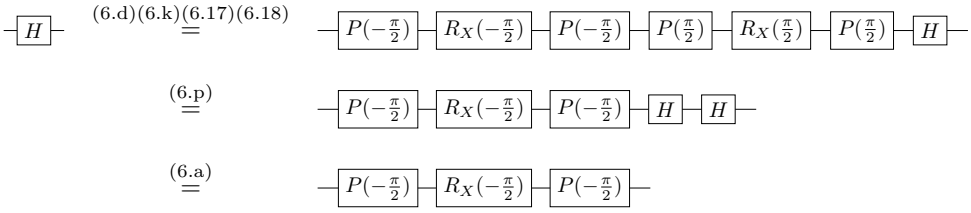


Figure 6.4: **Non-structural equations.** In Equations (6.q) and (6.r) the LHS circuit has arbitrary parameters which uniquely determine the parameters of the RHS circuit. Equation (6.q) is nothing but the well-known Euler-decomposition rule which states that any unitary can be decomposed, up to a global phase, into basic X- and Z-rotations. Thus for any $\alpha_i \in \mathbb{R}$, there exist $\beta_j \in \mathbb{R}$ such that Equation (6.q) is sound. We make the angles β_j unique by assuming that $\beta_1 \in [0, \pi)$, $\beta_0, \beta_2, \beta_3 \in [0, 2\pi)$ and if $\beta_2 \in \{0, \pi\}$ then $\beta_1 = 0$. Equation (6.p) is the particular Euler decomposition of H. Equation (6.r) reads as follows: the equation is defined for any $n \geq 2$ input qubits, in such a way that all gates are controlled by the first $n-2$ qubits. Equation (6.r) can be seen as a generalisation of the Euler rule, using multi-controlled gates. Similarly to Equation (6.q), for any $\gamma_i \in \mathbb{R}$, there exist $\delta_j \in \mathbb{R}$ such that Equation (6.r) is sound. We ensure that the angles δ_j are uniquely determined by assuming that $\delta_1, \delta_2, \delta_5 \in [0, \pi)$, $\delta_3, \delta_4, \delta_6, \delta_7, \delta_8, \delta_9 \in [0, 2\pi)$, if $\delta_3 = 0$ then $\delta_2 = 0$, if $\delta_3 = \pi$ then $\delta_1 = 0$, if $\delta_4 = 0$ then $\delta_1 = \delta_3$ $(= \delta_2) = 0$, if $\delta_4 = \pi$ then $\delta_2 = 0$, if $\delta_4 = \pi$ and $\delta_3 = 0$ then $\delta_1 = 0$, and if $\delta_6 \in \{0, \pi\}$ then $\delta_5 = 0$.

The Euler decomposition of H (Equation (6.p)) is not unique:

Proposition 6.35. $\mathrm{QC} \vdash$  $=$ 

Proof.



□

More generally the Euler angles are not unique, but can be made unique by adding some constraints on the angles, like choosing them in the appropriate intervals (see Figure 6.4).

Proposition 6.36. *Equations* (6.q) *and* (6.r) *are sound. Moreover, the choice of parameters in the RHS-circuits to make the equations sound is unique (under the constraints given in Figure 6.4).*

Proof. The proof is inspired by the proofs of Lemmas 5.12 and 5.13.

Soundness and Uniqueness of Equation (6.q)**.**

Given any $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, let $U \coloneqq$ 

. We have to prove that there exist unique $\beta_0, \beta_1, \beta_2, \beta_3$ satisfying the conditions of Figure 6.4 such that 

$= U$. We are going to prove that assuming that such β_j exist, their values are uniquely determined by U. Since we are going to do so by giving explicit expressions of the unique possible value of each β_j in terms of the entries of U, it will then be easy to check that these expressions indeed define angles with the desired properties.

One has

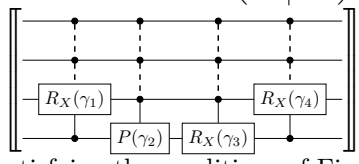
$$U = \left[\!\!\left[\begin{array}{l} \beta_0 \\ \hline P(\beta_1) \\ \hline R_X(\beta_2) \\ \hline P(\beta_3) \end{array} \right]\!\!\right] = e^{i\beta_0} \begin{pmatrix} \cos\left(\frac{\beta_2}{2}\right) & -ie^{i\beta_1}\sin\left(\frac{\beta_2}{2}\right) \\ -ie^{i\beta_3}\sin\left(\frac{\beta_2}{2}\right) & e^{i(\beta_1+\beta_3)}\cos\left(\frac{\beta_2}{2}\right) \end{pmatrix}$$

If U has a null entry, then since it is unitary, it is either diagonal or anti-diagonal. If it is diagonal, then $\sin\left(\frac{\beta_2}{2}\right) = 0$, which, since $\beta_2 \in [0, 2\pi)$, implies that $\beta_2 = 0$, which by the constraint on β_1 and β_2, implies that $\beta_1 = 0$. Consequently, $\beta_0 = \arg(U_{0,0})$ and $\beta_3 = \arg\left(\frac{U_{1,1}}{U_{0,0}}\right)$. If U is anti-diagonal, then $\cos\left(\frac{\beta_2}{2}\right) = 0$, which, since $\beta_2 \in [0, 2\pi)$, implies that $\beta_2 = \pi$, which by the constraint on β_1 and β_2, implies that $\beta_1 = 0$. Consequently, $\beta_0 = \arg\left(\frac{U_{0,1}}{-i}\right)$ and $\beta_3 = \arg\left(\frac{U_{1,0}}{U_{0,1}}\right)$.

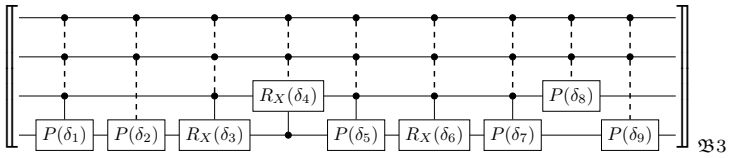
If U has no null entry, then one has $\beta_2 \neq \pi$ and $\frac{ie^{-i\beta_1}U_{0,1}}{U_{0,0}} = \tan\left(\frac{\beta_2}{2}\right)$. Hence, β_1 is the unique angle in $[0, \pi)$ such that $\frac{ie^{-i\beta_1}U_{0,1}}{U_{0,0}} \in \mathbb{R}$, namely $\arg\left(\frac{iU_{0,1}}{U_{0,0}}\right) \bmod \pi$. In turn, β_2 is the unique angle in $[0, 2\pi) \setminus \{\pi\}$ such that $\tan\left(\frac{\beta_2}{2}\right) = \frac{ie^{-i\beta_1}U_{0,1}}{U_{0,0}}$. Finally, one has $e^{i\beta_3} = \frac{\cos(\frac{\beta_2}{2})U_{1,0}}{-i\sin(\frac{\beta_2}{2})U_{0,0}}$, so that $\beta_3 = \arg\left(\frac{\cos(\frac{\beta_2}{2})U_{1,0}}{-i\sin(\frac{\beta_2}{2})U_{0,0}}\right)$, and $e^{i\beta_0} = \frac{U_{0,0}}{\cos(\frac{\beta_2}{2})}$, so that $\beta_0 = \arg\left(\frac{U_{0,0}}{\cos(\frac{\beta_2}{2})}\right)$.

Soundness and Uniqueness of Equation (6.r)**.**

Let $B_n \colon \{0, ..., 2^n - 1\} \to \{0,1\}^n$ be any bijection such that $B_n(1...101) = 2^n - 3$, $B_n(1...111) = 2^n - 2$ and $B_n(1...110) = 2^n - 1$,[45] and let $\mathfrak{B}_n \colon \mathbb{C}^{2^n} \to \mathbb{C}^{\{0,1\}^n}$ be the linear map $|k\rangle \mapsto |B_n(k)\rangle$. Given any n-qubit quantum circuit C such that $\mathfrak{B}_n^{-1} \circ [\![C]\!] \circ \mathfrak{B}_n$ is of the form $\left(\begin{array}{c|c} I & 0 \\ \hline 0 & U \end{array}\right)$ with $U \in \mathbb{C}^{3\times 3}$, let $[\![C]\!]_{\mathfrak{B}3} \coloneqq U$.

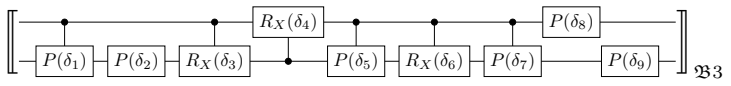
Given any $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \mathbb{R}$, let $U \coloneqq$ 

. We have to prove that there exist unique $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6, \delta_7, \delta_8, \delta_9$ satisfying the conditions of Figure 6.4 such that



$= U,$

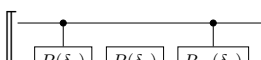
or equivalently,

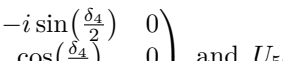


$= U.$

[45] The reason for this choice is that it coincides with the Gray code (see Definition 6.40) in the 2-qubit case while for any number of qubits it ensures that the semantics of the two sides of Equation (6.r) is of the form $\left(\begin{array}{c|c} I & 0 \\ \hline 0 & U \end{array}\right)$ with $U \in \mathbb{C}^{3\times 3}$.

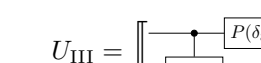
We are going to prove that assuming that such δ_j exist, their values are uniquely determined by U. Since we are going to do so by giving explicit expressions of the unique possible value of each δ_j in terms of the entries of U, it will then be easy to check that these expressions indeed define angles with the desired properties.

Let $U_{123} \coloneqq$  $= \begin{pmatrix} e^{i\delta_2} & 0 & 0 \\ 0 & e^{i(\delta_1+\delta_2)}\cos\left(\frac{\delta_3}{2}\right) & -i\sin\left(\frac{\delta_3}{2}\right) \\ 0 & -ie^{i(\delta_1+\delta_2)}\sin\left(\frac{\delta_3}{2}\right) & \cos\left(\frac{\delta_3}{2}\right) \end{pmatrix}$, $U_4 \coloneqq$ $=$

$\begin{pmatrix} \cos\left(\frac{\delta_4}{2}\right) & -i\sin\left(\frac{\delta_4}{2}\right) & 0 \\ -i\sin\left(\frac{\delta_4}{2}\right) & \cos\left(\frac{\delta_4}{2}\right) & 0 \\ 0 & 0 & 1 \end{pmatrix}$ and $U_{56} \coloneqq$  $= \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\delta_5}\cos\left(\frac{\delta_6}{2}\right) & -i\sin\left(\frac{\delta_6}{2}\right) \\ 0 & -ie^{i\delta_5}\sin\left(\frac{\delta_6}{2}\right) & \cos\left(\frac{\delta_6}{2}\right) \end{pmatrix}$.

Let also $U_{\mathrm{I}} \coloneqq U_{123} \circ U^\dagger$, $U_{\mathrm{II}} \coloneqq U_4 \circ U_{\mathrm{I}}$ and $U_{\mathrm{III}} \coloneqq U_{56} \circ U_{\mathrm{II}}$.

By construction,

$$U_{\mathrm{III}} = \text{  }^\dagger = \begin{pmatrix} e^{-i\delta_9} & 0 & 0 \\ 0 & e^{-i(\delta_7+\delta_8+\delta_9)} & 0 \\ 0 & 0 & e^{-i\delta_8} \end{pmatrix} \tag{E$_1$}$$

so that

$$U_{\mathrm{II}} = U_{56}^\dagger \circ U_{\mathrm{III}} = \begin{pmatrix} e^{-i\delta_9} & 0 & 0 \\ 0 & e^{-i(\delta_5+\delta_7+\delta_8+\delta_9)}\cos\left(\frac{\delta_6}{2}\right) & ie^{-i(\delta_5+\delta_8)}\sin\left(\frac{\delta_6}{2}\right) \\ 0 & ie^{-i(\delta_7+\delta_8+\delta_9)}\sin\left(\frac{\delta_6}{2}\right) & e^{-i\delta_8}\cos\left(\frac{\delta_6}{2}\right) \end{pmatrix} \tag{E$_2$}$$

and $U_{\mathrm{I}} = U_4^\dagger \circ U_{\mathrm{II}}$. Since U_4 acts as the identity on the last entry, this implies that $(U_{\mathrm{I}})_{2,0} = 0$.[46] That is, by definition of U_{I},

$$-ie^{i(\delta_1+\delta_2)}\sin\left(\tfrac{\delta_3}{2}\right)U_{0,1}^\dagger + \cos\left(\tfrac{\delta_3}{2}\right)U_{0,2}^\dagger = 0. \tag{E$_3$}$$

By direct calculation using the definitions of U_{I} and U_{II}, one gets $(U_{\mathrm{I}})_{0,0} = e^{i\delta_2}U_{0,0}^\dagger$ and $(U_{\mathrm{I}})_{1,0} = e^{i(\delta_1+\delta_2)}\cos\left(\frac{\delta_3}{2}\right)U_{0,1}^\dagger - i\sin\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger$, so that $(U_{\mathrm{II}})_{1,0} = -i\sin\left(\frac{\delta_4}{2}\right)(U_{\mathrm{I}})_{0,0} + \cos\left(\frac{\delta_4}{2}\right)(U_{\mathrm{I}})_{1,0} = -i\sin\left(\frac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + \cos\left(\frac{\delta_4}{2}\right)(e^{i(\delta_1+\delta_2)}\cos\left(\frac{\delta_3}{2}\right)U_{0,1}^\dagger - i\sin\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger)$. That is, since by (E$_2$), $(U_{\mathrm{II}})_{1,0} = 0$:

$$-i\sin\left(\tfrac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + \cos\left(\tfrac{\delta_4}{2}\right)\left(e^{i(\delta_1+\delta_2)}\cos\left(\tfrac{\delta_3}{2}\right)U_{0,1}^\dagger - i\sin\left(\tfrac{\delta_3}{2}\right)U_{0,2}^\dagger\right) = 0 \tag{E$_4$}$$

- If $U_{0,1} = U_{0,2} = 0$, then since U is unitary, $U_{0,0} \neq 0$ and (E$_4$) becomes $-i\sin\left(\frac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger = 0$, that is $\sin\left(\frac{\delta_4}{2}\right) = 0$. Since $\delta_4 \in [0, 2\pi)$, this implies that $\delta_4 = 0$, which by the conditions of Figure 6.4, implies that $\delta_1 = \delta_2 = \delta_3 = 0$.

- If $(U_{0,1}, U_{0,2}) \neq (0, 0)$, then $e^{i(\delta_1+\delta_2)}\cos\left(\frac{\delta_3}{2}\right)U_{0,1}^\dagger - i\sin\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger \neq 0$. Indeed, if this expression was equal to 0, by (E$_3$) this would mean that the non-zero vector $\begin{pmatrix} e^{i(\delta_1+\delta_2)}U_{0,1}^\dagger \\ U_{0,2}^\dagger \end{pmatrix}$ is in the kernel of the matrix $\begin{pmatrix} \cos\left(\frac{\delta_3}{2}\right) & -i\sin\left(\frac{\delta_3}{2}\right) \\ -i\sin\left(\frac{\delta_3}{2}\right) & \cos\left(\frac{\delta_3}{2}\right) \end{pmatrix}$, whereas this matrix is invertible. Then:

  - If $U_{0,0} = 0$, then (E$_4$) implies that $\cos\left(\frac{\delta_4}{2}\right) = 0$, which, since $\delta_4 \in [0, 2\pi)$, implies that $\delta_4 = \pi$. By the conditions of Figure 6.4, this implies that $\delta_2 = 0$. Then:
    - If $U_{0,2} = 0$, then $U_{0,1} \neq 0$, and (E$_3$) implies that $\sin\left(\frac{\delta_3}{2}\right) = 0$, that is, since $\delta_3 \in [0, 2\pi)$, that $\delta_3 = 0$. By the conditions of Figure 6.4, together with the fact that $\delta_4 = \pi$, this implies that $\delta_1 = 0$.
    - If $U_{0,1} = 0$, then $U_{0,2} \neq 0$, and (E$_3$) implies that $\cos\left(\frac{\delta_3}{2}\right) = 0$, that is, since $\delta_3 \in [0, 2\pi)$, that $\delta_3 = \pi$. By the conditions of Figure 6.4, this implies that $\delta_1 = 0$.

[46] Where we denote by $M_{i,j}$ the entry of indices (i, j) of any matrix M, the index of the first row and column being 0.

* If $U_{0,1}, U_{0,2} \neq 0$, then (E_3), on the one hand, implies that $\delta_3 \neq \pi$, and on the other hand, is equivalent to

$$\tan\left(\tfrac{\delta_3}{2}\right) = \frac{e^{-i\delta_1}U_{0,2}^\dagger}{iU_{0,1}^\dagger}.$$

Hence, δ_1 is the unique angle in $[0,\pi)$ such that $\frac{e^{-i\delta_1}U_{0,2}^\dagger}{iU_{0,1}^\dagger} \in \mathbb{R}$. In turn, δ_3 is the unique angle in $[0,2\pi)$ such that $\tan\left(\frac{\delta_3}{2}\right) = \frac{e^{-i\delta_1}U_{0,2}^\dagger}{iU_{0,1}^\dagger}$.

– If $U_{0,0} \neq 0$, then (E_4) can be simplified into

$$-i\tan\left(\tfrac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + e^{i(\delta_1+\delta_2)}\cos\left(\tfrac{\delta_3}{2}\right)U_{0,1}^\dagger - i\sin\left(\tfrac{\delta_3}{2}\right)U_{0,2}^\dagger = 0. \tag{E_5}$$

* If $U_{0,2} = 0$, then $U_{0,1} \neq 0$, and (E_3) implies that $\sin\left(\frac{\delta_3}{2}\right) = 0$, that is, since $\delta_3 \in [0,2\pi)$, that $\delta_3 = 0$. By the conditions of Figure 6.4, this implies that $\delta_2 = 0$. Then (E_5) becomes

$$-i\tan\left(\tfrac{\delta_4}{2}\right)U_{0,0}^\dagger + e^{i\delta_1}U_{0,1}^\dagger = 0$$

that is,

$$\tan\left(\tfrac{\delta_4}{2}\right) = \frac{e^{i\delta_1}U_{0,1}^\dagger}{iU_{0,0}^\dagger}.$$

Hence, δ_1 is the unique angle in $[0,\pi)$ such that $\frac{e^{i\delta_1}U_{0,1}^\dagger}{iU_{0,0}^\dagger} \in \mathbb{R}$. In turn, δ_4 is the unique angle in $[0,2\pi)$ such that $\tan\left(\frac{\delta_4}{2}\right) = \frac{e^{i\delta_1}U_{0,1}^\dagger}{iU_{0,0}^\dagger}$.

* If $U_{0,1} = 0$, then $U_{0,2} \neq 0$, and (E_3) implies that $\cos\left(\frac{\delta_3}{2}\right) = 0$, that is, since $\delta_3 \in [0,2\pi)$, that $\delta_3 = \pi$. By the conditions of Figure 6.4, this implies that $\delta_1 = 0$. Then (E_5) becomes

$$-i\tan\left(\tfrac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger - iU_{0,2}^\dagger = 0$$

that is,

$$\tan\left(\tfrac{\delta_4}{2}\right) = -\frac{e^{-i\delta_2}U_{0,2}^\dagger}{U_{0,0}^\dagger}.$$

Hence, δ_2 is the unique angle in $[0,\pi)$ such that $\frac{e^{-i\delta_2}U_{0,2}^\dagger}{U_{0,0}^\dagger} \in \mathbb{R}$. In turn, δ_4 is the unique angle in $[0,2\pi)$ such that $\tan\left(\frac{\delta_4}{2}\right) = -\frac{e^{-i\delta_2}U_{0,2}^\dagger}{U_{0,0}^\dagger}$.

* If $U_{0,1}, U_{0,2} \neq 0$, then (E_3), on the one hand, implies that $\delta_3 \notin \{0,\pi\}$, and on the other hand, is equivalent to

$$e^{i(\delta_1+\delta_2)} = \frac{\cos\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger}{i\sin\left(\frac{\delta_3}{2}\right)U_{0,1}^\dagger}. \tag{E_6}$$

Then by substituting in (E_5), we get

$$-i\tan\left(\tfrac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + \frac{\cos^2\left(\frac{\delta_3}{2}\right)U_{0,2}^\dagger}{i\sin\left(\frac{\delta_3}{2}\right)} - i\sin\left(\tfrac{\delta_3}{2}\right)U_{0,2}^\dagger = 0$$

which can be simplified into

$$-i\tan\left(\tfrac{\delta_4}{2}\right)e^{i\delta_2}U_{0,0}^\dagger + \frac{U_{0,2}^\dagger}{i\sin\left(\frac{\delta_3}{2}\right)} = 0$$

which is equivalent to

$$\tan\left(\tfrac{\delta_4}{2}\right) = -\frac{e^{-i\delta_2}U^\dagger_{0,2}}{\sin\left(\tfrac{\delta_3}{2}\right)U^\dagger_{0,0}}. \tag{E$_7$}$$

Hence, δ_2 is the unique angle in $[0,\pi)$ such that $\dfrac{e^{-i\delta_2}U^\dagger_{0,2}}{U^\dagger_{0,0}} \in \mathbb{R}$. Then (E$_6$) can be rephrased into

$$\tan\left(\tfrac{\delta_3}{2}\right) = \frac{e^{-i(\delta_1+\delta_2)}U^\dagger_{0,2}}{iU^\dagger_{0,1}}.$$

Hence, δ_1 is the unique angle in $[0,\pi)$ such that $\frac{e^{-i(\delta_1+\delta_2)}U^\dagger_{0,2}}{iU^\dagger_{0,1}} \in \mathbb{R}$. In turn, δ_3 is the unique angle in $[0,2\pi)$ such that $\tan\left(\frac{\delta_3}{2}\right) = \frac{e^{-i(\delta_1+\delta_2)}U^\dagger_{0,2}}{iU^\dagger_{0,1}}$. Finally, δ_4 is the unique angle in $[0,2\pi)$ satisfying (E$_7$).

Thus, assuming that the δ_j exist, since U_{I} and U_{II} only depend on δ_1, δ_2, δ_3, δ_4 and U, they are uniquely determined by U. Then (E$_2$) implies that

- If $(U_{\mathrm{II}})_{1,2} = 0$, then $\sin\left(\frac{\delta_6}{2}\right) = 0$, which means, since $\delta_6 \in [0,2\pi)$, that $\delta_6 = 0$. By the conditions of Figure 6.4, this implies that $\delta_5 = 0$.
- If $(U_{\mathrm{II}})_{2,2} = 0$, then $\cos\left(\frac{\delta_6}{2}\right) = 0$, which means, since $\delta_6 \in [0,2\pi)$, that $\delta_6 = \pi$. By the conditions of Figure 6.4, this implies that $\delta_5 = 0$.
- If $(U_{\mathrm{II}})_{1,2} = 0, (U_{\mathrm{II}})_{2,2} \neq 0$, then

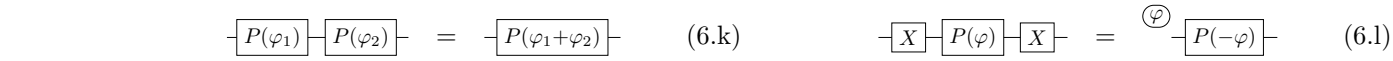
  $$\tan\left(\tfrac{\delta_6}{2}\right) = \frac{e^{i\delta_5}(U_{\mathrm{II}})_{1,2}}{i(U_{\mathrm{II}})_{2,2}}.$$

  Hence, δ_5 is the unique angle in $[0,\pi)$ such that $\frac{e^{i\delta_5}(U_{\mathrm{II}})_{1,2}}{i(U_{\mathrm{II}})_{2,2}} \in \mathbb{R}$. In turn, δ_6 is the unique angle in $[0,2\pi)$ such that $\tan\left(\frac{\delta_6}{2}\right) = \frac{e^{i\delta_5}(U_{\mathrm{II}})_{1,2}}{i(U_{\mathrm{II}})_{2,2}}$.

Thus, assuming that the δ_j exist, since U_{III} only depends on δ_5, δ_6 and U_{II}, it is uniquely determined by U. Then by (E$_1$), $\delta_8 = \arg((U_{\mathrm{III}})^\dagger_{2,2})$, $\delta_9 = \arg((U_{\mathrm{III}})^\dagger_{0,0})$ and $\delta_7 = \arg\left(\frac{(U_{\mathrm{III}})_{0,0}(U_{\mathrm{III}})_{2,2}}{(U_{\mathrm{III}})_{1,1}}\right)$. □

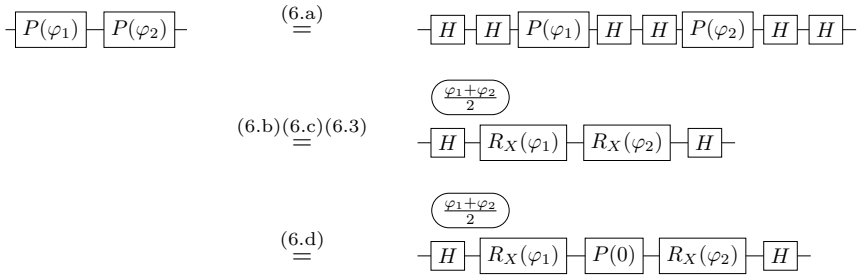
Note that Equation (6.q) subsumes Equations (6.k) and (6.l), which can now be derived using the other axioms of QC:

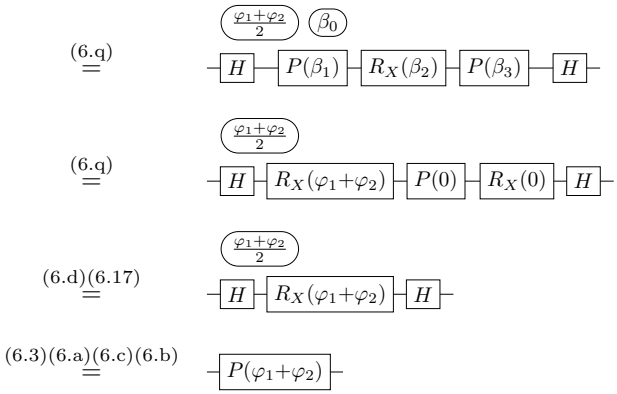
Proposition 6.37. *The following two equations of* QC*,*



can be derived from the other axioms of QC*.*

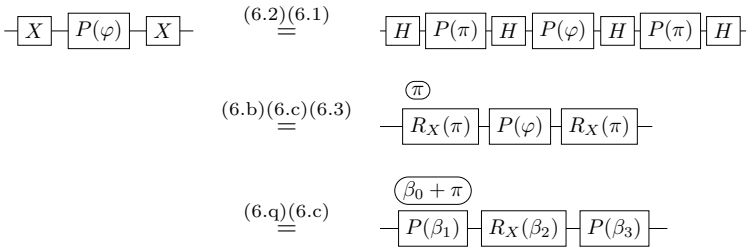
Proof. Proof of Equation (6.k):

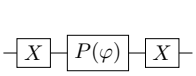
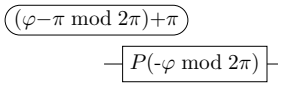
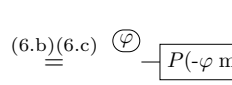


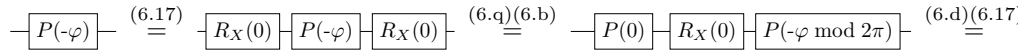


The first use of Equation (6.q) is valid since Equation (6.q) is applied from left to right. The second use of Equation (6.q) is valid since it preserves the semantics. Note that one can show that $\beta_1 = \beta_3 = 0$, $\beta_2 = \varphi_1 + \varphi_2 \bmod 2\pi$ and $\beta_0 = \begin{cases} 0 & \text{if } (\varphi_1 + \varphi_2 \bmod 4\pi) \in [0, 2\pi) \\ \pi & \text{if } (\varphi_1 + \varphi_2 \bmod 4\pi) \in [2\pi, 4\pi) \end{cases}$.

Proof of Equation (6.l):



One has $\beta_1 = \beta_2 = 0$, $\beta_3 = -\varphi \bmod 2\pi$ and $\beta_0 = \varphi - \pi \bmod 2\pi$. Indeed, this choice of angles satisfies the conditions of Equation (6.q) and is sound with respect to the semantics (moreover Proposition 6.36 guarantees that this is the only possible choice). Thus, by Equations (6.d) and (6.17), this implies that one can transform  into   . Finally,



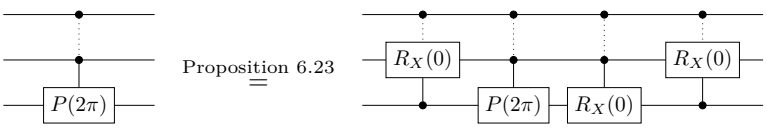
which terminates the proof. □

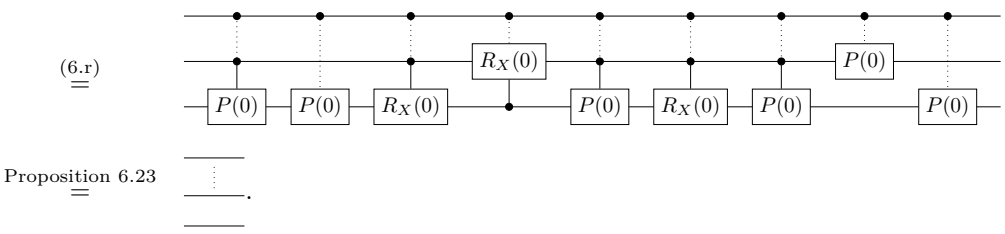
The introduction of the additional equations of Figure 6.4 allows us to prove some extra properties about multi-controlled gates, like periodicity (for those with a parameter) in Proposition 6.39 and the fact that a multi-controlled X gate is self-inverse.

Proposition 6.38. *For any $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$,*

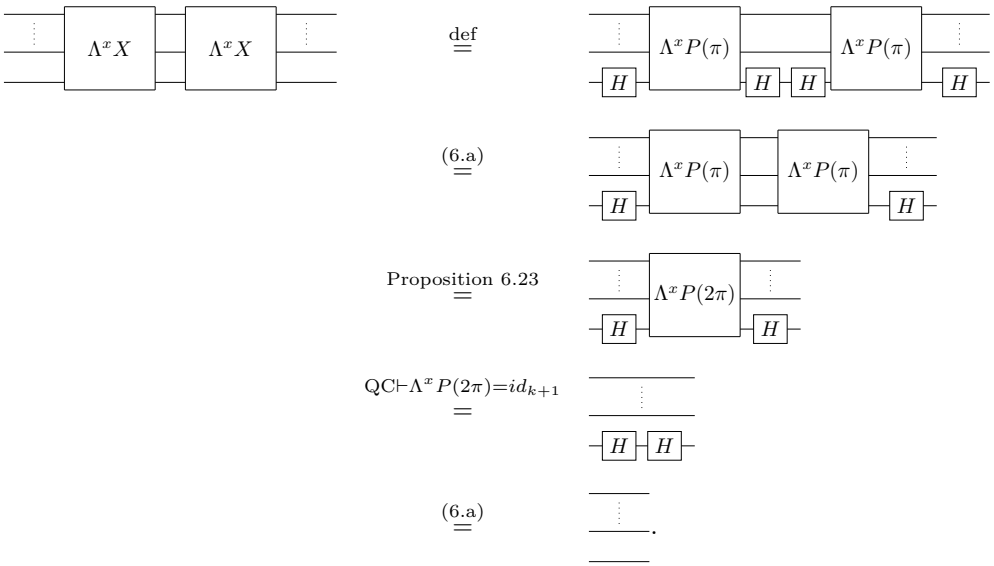
$$\mathrm{QC} \vdash \Lambda^x_y X \circ \Lambda^x_y X = id_{k+\ell+1}$$

Proof. The case $x = y = \epsilon$ is a direct consequence of Equation (6.10). For the other cases, without loss of generality we can assume that $y = \epsilon$ and $x = 1^k$. First, we can show that $\mathrm{QC} \vdash \Lambda^x P(2\pi) = id_{k+1}$ as follows:





It follows that:



□

Proposition 6.39. *For any $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$, $\theta \in \mathbb{R}$,*

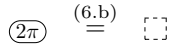
$$\mathrm{QC} \vdash \Lambda^x_y R_X(\theta + 4\pi) = \Lambda^x_y R_X(\theta), \qquad \mathrm{QC} \vdash \Lambda^x_y P(\theta + 2\pi) = \Lambda^x_y P(\theta), \qquad \mathrm{QC} \vdash \Lambda^x_y s(\theta + 2\pi) = \Lambda^x_y s(\theta).$$

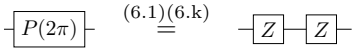
Proof. Because of the additivity given by Proposition 6.23, it is sufficient to show that for any $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$,

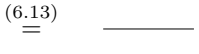
$$\mathrm{QC} \vdash \Lambda^x_y R_X(4\pi) = id_{k+\ell+1}, \qquad \mathrm{QC} \vdash \Lambda^x_y P(2\pi) = id_{k+\ell+1}, \qquad \mathrm{QC} \vdash \Lambda^x_y s(2\pi) = id_{k+\ell}.$$

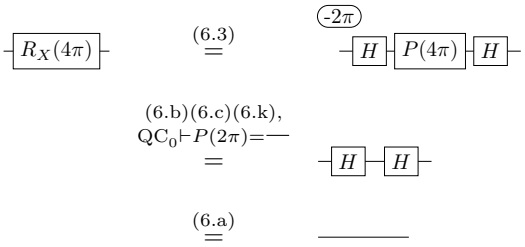
Additionally, by Equation (6.10) and Definitions 6.7 and 6.8, we can assume without loss of generality that $y = \epsilon$ and $x = 1^k$.

First, note that the case where $x = \epsilon$ only needs QC_0:





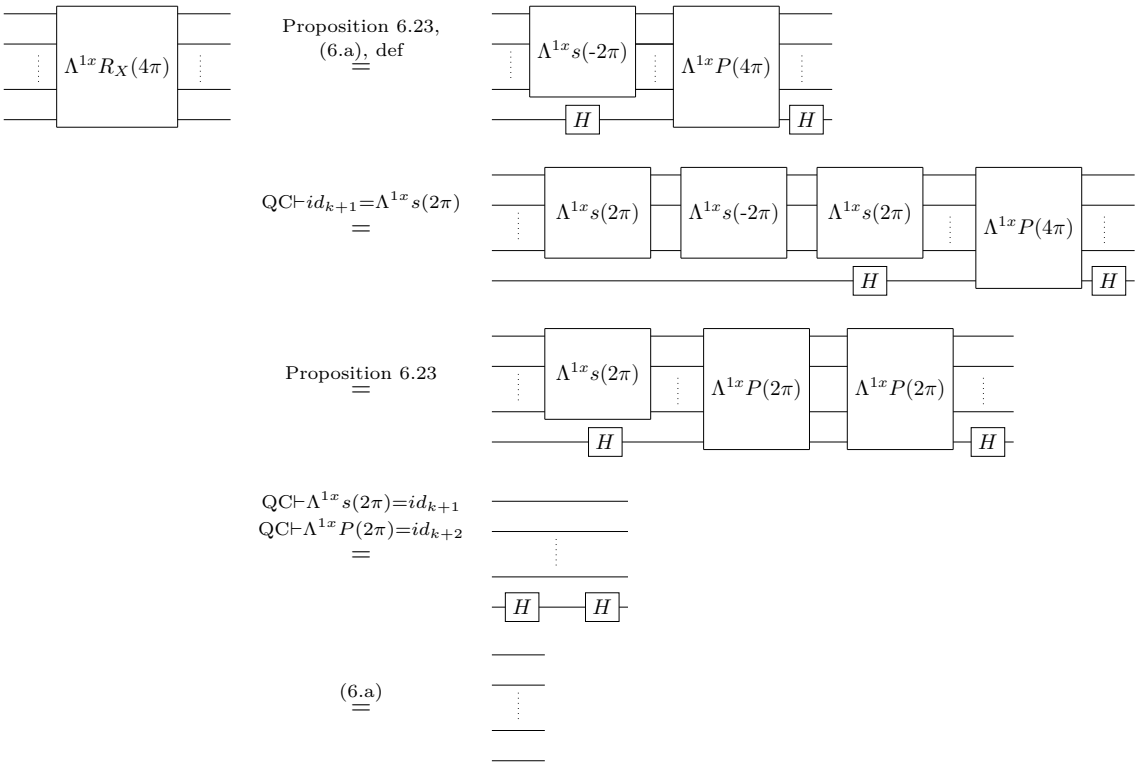




For the case where $k \geq 1$, note first that we have already proved that $\mathrm{QC} \vdash \Lambda^x P(2\pi) = id_{k+1}$, in the proof of Proposition 6.38.

As $\Lambda^{x1} s(2\pi) = \Lambda^x P(2\pi)$, this also proves that for any $x = 1^k$, $\mathrm{QC} \vdash \Lambda^x s(2\pi) = id_k$.

Finally:



□

6.2 Completeness

In this section we prove the main result of this chapter, namely the completeness of QC. To this end, a back and forth encoding of quantum circuits into $\mathrm{LO}_{\mathrm{PP}}$-circuits is introduced.

6.2.1 Forgetting the Monoidal Structure

The proof of completeness for quantum circuits is based on a back and forth translation from linear optical circuits. While both kinds of circuits form a PROP, so both have a monoidal structure, these monoidal structures do not coincide. The monoidal product of quantum circuits corresponds to the tensor product, whereas that of linear optical circuits is a direct sum. Hence the translations do not preserve the monoidal structure.

As a consequence there is a technical issue around defining the translation directly on circuits. We instead define the transformations on *raw* circuits, that is, circuits not considered up to the axioms of PROP, which are just terms built inductively from the generators (including $\boxed{\ }$, — and $\times$) using the sequential and parallel compositions $\circ$ and $\otimes$ (resp. $\circ$ and $\oplus$), in a similar way as in the first part of Definition 1.4. The collection of raw quantum (resp. $\mathrm{LO_{PP}}$) circuits is denoted by $\mathbf{QC^{raw}}$ (resp. $\mathbf{LO^{raw}_{PP}}$). Note that we recover the standard circuits by considering the raw circuits up to the equivalence relation $\equiv$ given by the axioms of PROP: $\mathbf{QC} = \mathbf{QC^{raw}}/\equiv$ and $\mathbf{LO_{PP}} = \mathbf{LO^{raw}_{PP}}/\equiv$. As this will be useful in the following, we give these axioms in Figure 6.5 in the form of an equational theory for raw circuits.

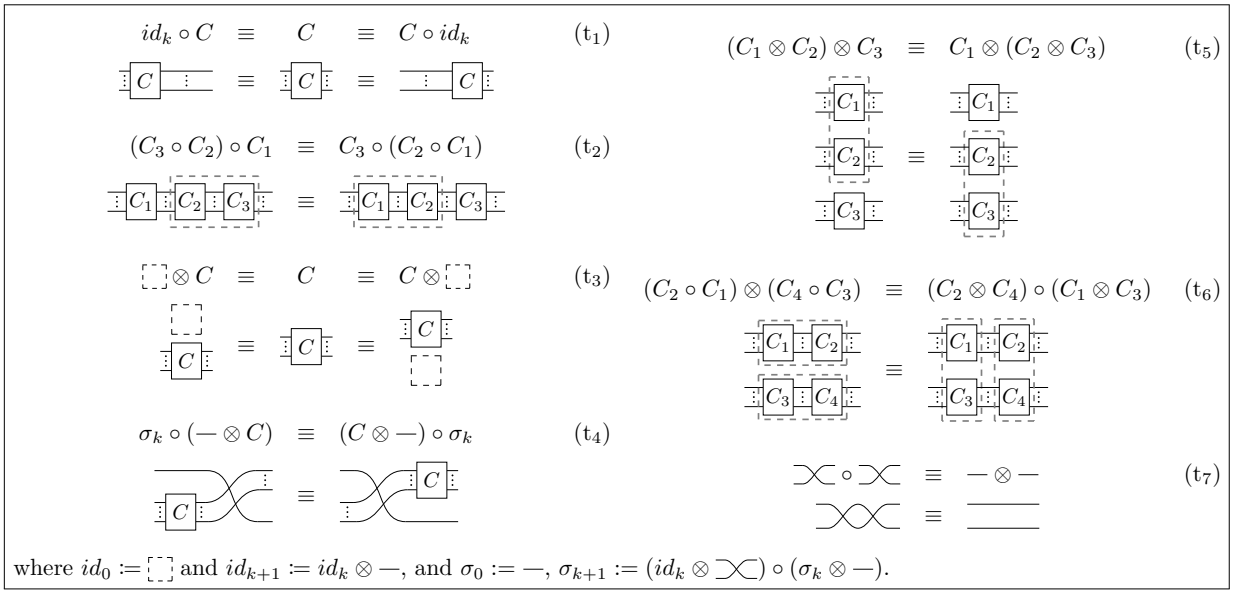
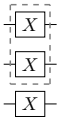
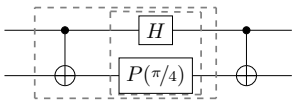
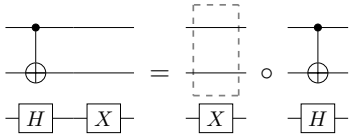


Figure 6.5: Definition of $\equiv$ for raw circuits (either raw quantum circuits or raw optical circuits). Here the symbol $\otimes$ stands for either $\otimes$ or $\oplus$.

To avoid ambiguity in the graphical representation of raw circuits one can use boxes like  for $(\boxed{X} \otimes \boxed{X}) \otimes \boxed{X}$ or  for $\oplus \circ ((\boxed{H} \otimes \boxed{P(\pi/4)}) \circ \oplus)$. We also use a box-free graphical representation that we interpret as a layer-by-layer description of a raw circuit, more precisely we associate with any box-free graphical representation, a raw circuit of the form $C = (\ldots((L_1 \circ L_2) \circ L_3) \circ \ldots) \circ L_k$ where $L_i = (\ldots((g_{i,1} \otimes g_{i,2}) \otimes g_{i,3}) \otimes \ldots) \otimes g_{i,\ell_i}$.

For instance, $((id_1 \otimes id_1) \otimes X) \circ (CNot \otimes H)$ is



Similarly, although the sequential and parallel composition are not associative, we sometimes use parenthesis-free notations for products: namely, $C_1 \circ C_2 \circ C_3 \circ \ldots \circ C_k$ and $C_1 \otimes C_2 \otimes C_3 \otimes \ldots \otimes C_k$ denote respectively $(\ldots((C_1 \circ C_2) \circ C_3) \circ \ldots) \circ C_k$ and $(\ldots((C_1 \otimes C_2) \otimes C_3) \otimes \ldots) \otimes C_k$.

We extend the notation $\mathrm{QC} \vdash \cdot = \cdot$ and $\mathrm{LO_{PP}} \vdash \cdot = \cdot$ to raw circuits. For any raw quantum circuits (resp. raw optical circuits) C_1, C_2, we write $\mathrm{QC} \vdash C_1 = C_2$ (resp. $\mathrm{LO_{PP}} \vdash C_1 = C_2$) if C_1 and C_2 are equivalent by the congruence defined in Figure 6.2, Figure 6.4 and Figure 6.5 (resp. Figure 5.12 and

Figure 6.5).[47]

Note that there exists a derivation between two circuits if and only if there exists a derivation between two of their representative raw circuits. Indeed, intuitively the only difference is that the derivation on raw circuits is more fine-grained as the equivalence relation $\equiv$ is made explicit.

6.2.2 Encoding Quantum Circuits Into Optical Ones

We are now ready to define the encoding of (raw) quantum circuits into (raw) linear optical circuits. For dimension reasons, an n-qubit system is encoded into 2^n modes. One can naturally choose to encode $|x\rangle$, with $x \in \{0,1\}^n$, into the mode $|\underline{x}\rangle$ where $\underline{x} = \sum_{i=1}^{n} x_i 2^{n-i}$ is the usual binary encoding. Alternatively, we use Gray codes to produce circuits with a simpler connectivity, in particular two adjacent modes encode basis qubit states which differ on exactly one qubit.

Definition 6.40 (Gray code)**.** *Let $\mathfrak{G}_n : \mathbb{C}^{2^n} \to \mathbb{C}^{\{0,1\}^n}$ be the map $|k\rangle \mapsto |G_n(k)\rangle$ where $G_n(k)$ is the Gray code of k, inductively defined by $G_0(0) = \epsilon$ and*

$$G_n(k) = \begin{cases} 0G_{n-1}(k) & \text{if } k < 2^{n-1}, \\ 1G_{n-1}(2^n - 1 - k) & \text{if } k \geq 2^{n-1}. \end{cases}$$

For instance G_3 is defined as follows:

$$\begin{array}{lll} 0 \mapsto 000 & \qquad & 4 \mapsto 110 \\ 1 \mapsto 001 & & 5 \mapsto 111 \\ 2 \mapsto 011 & & 6 \mapsto 101 \\ 3 \mapsto 010 & & 7 \mapsto 100 \end{array}$$

In order to get around the fact that the encoding an n-qubit circuit into a 2^n-mode optical circuit cannot preserve the parallel composition, we proceed by "sequentialising" the circuit: roughly speaking, an n-qubit circuit is seen as a sequential composition of layers, each layer being an n-qubit circuit made of an elementary gate g acting on at most two qubits in parallel with the identity on all other qubits, *e.g.* $id_k \otimes g \otimes id_l$. The encoding of such a layer, denoted $E_{k,l}(g)$, is a 2^n-mode optical circuit acting non-trivially on potentially all the modes.

For instance, consider a 3-qubit layer which consists in applying $P(\varphi)$ on the second qubit. Its semantics is $|x,y,z\rangle \mapsto e^{i\varphi y} |x,y,z\rangle$. Such a circuit is encoded into an 8-mode optical circuit $E_{1,1}(P(\varphi))$ made of 4 phase shifters acting on the modes $p \in [2,5]$ (those s.t. $G_3(p) = x1z$). Indeed, the semantics of $E_{1,1}(P(\varphi))$ is $|p\rangle \mapsto \begin{cases} e^{i\varphi} |p\rangle & \text{if } p \in [2,5] \\ |p\rangle & \text{otherwise} \end{cases}$.

The encoding map is formally defined as follows:

Definition 6.41 (Encoding)**.** *Let $E : \mathbf{QC}^{\mathbf{raw}} \to \mathbf{LO}^{\mathbf{raw}}_{\mathbf{PP}}$ be defined as follows: for any n-qubit circuit C, $E(C) = E_{0,0}(C)$ where $E_{k,\ell}$ is inductively defined as:*

- *$E_{k,\ell}(C_1 \otimes C_2) = E_{k+n_1,\ell}(C_2) \circ E_{k,\ell+n_2}(C_1)$, where C_1 (resp. C_2) is acting on n_1 (resp. n_2) qubits;*
- *$E_{k,\ell}(C_2 \circ C_1) = E_{k,\ell}(C_2) \circ E_{k,\ell}(C_1)$;*

Let us define $\sigma_{k,n,\ell}$ as a $2^{k+n+\ell}$-mode linear optical circuit made only of swaps (that is, without any *or* *) such that $\mathfrak{G}_n \circ [\![\sigma_{k,n,\ell}]\!]_{\mathrm{pp}} \circ \mathfrak{G}_n^{-1}(|x,y,z\rangle) = |x,z,y\rangle$[48] for any $x \in \{0,1\}^k$, $y \in \{0,1\}^n$ and $z \in \{0,1\}^\ell$. We then define*

$$E_{k,\ell}(\text{}) = \sigma_{k,\ell,2} \circ \sigma_{k+\ell,1,1} \circ \sigma_{k,2,\ell},$$
$$E_{k,\ell}(\text{  }) = (—)^{\oplus 2^{k+\ell}},$$
$$E_{k,\ell}(—) = (—)^{\oplus 2^{k+\ell+1}},$$
$$E_{k,\ell}(\text{  }) = \left(\text{}\right)^{\oplus 2^{k+\ell}},$$

[47] In this context, the circuits depicted in Figures 6.2, 6.4 and 5.12 are interpreted as box-free graphical representations of raw circuits.

[48] Where $[\![\cdot]\!]_{\mathrm{pp}}$ is defined in Definition 5.11.

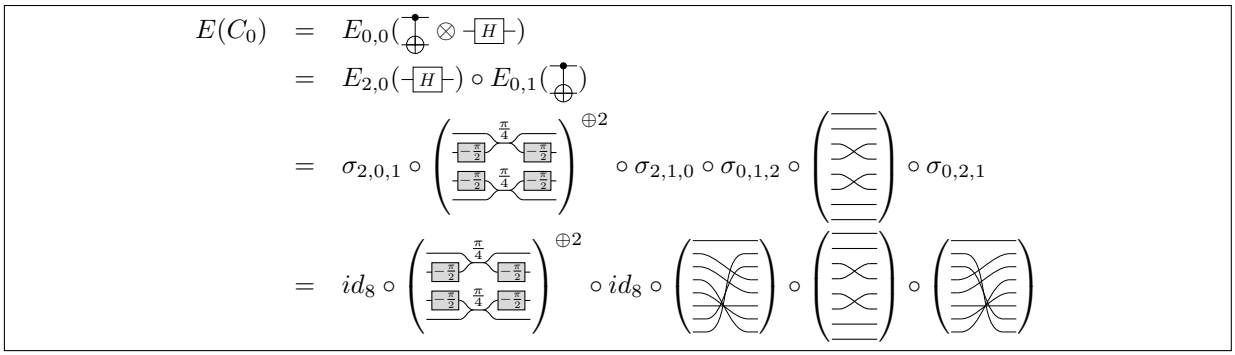
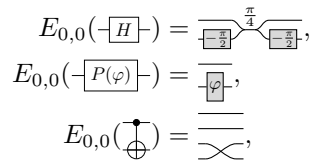


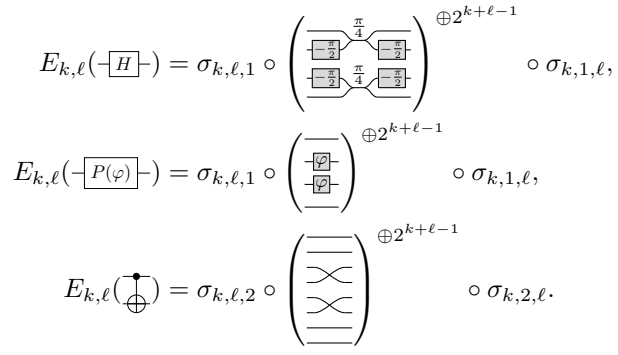
Figure 6.6: Encoding of the circuit discussed in Example 6.43.

where $C^{\oplus n}$ means C n times in parallel: $C^{\oplus 0} =$ [dashed box] and $C^{\oplus n+1} = C^{\oplus n} \oplus C$.

For the remaining generators, we define:



and whenever $(k, \ell) \neq (0, 0)$:

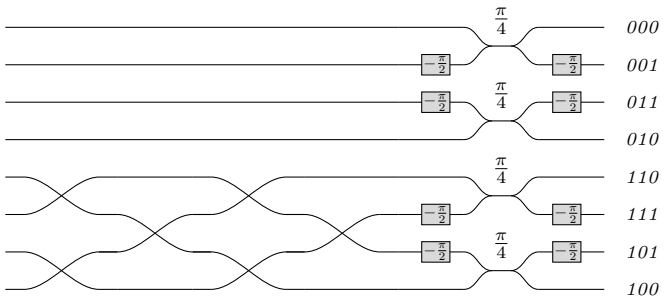


Remark 6.42. *Note that for any n-qubit circuit C, $E_{k,\ell}(C)$ is a $2^{k+n+\ell}$-mode optical circuit. Also note that $\sigma_{k,n,\ell}$ is nothing but a permutation of wires. By Lemma 6.56 — which is independent of the definition of E — any actual circuit satisfying the above property ($\mathfrak{G}_n \circ [\![\sigma_{k,n,\ell}]\!]_{\mathrm{pp}} \circ \mathfrak{G}_n^{-1}(|x, y, z\rangle) = |x, z, y\rangle$) is convenient for our purposes. A formal definition of $\sigma_{k,n,\ell}$ is however given in Definition 6.50.*

Example 6.43. *Consider the simple circuit $C_0 =$*  *. The encoding is as shown in Figure 6.6.*[49]

[49]Note that we have made an abuse of notation in the two last steps in Figure 6.6, by writing the sequential products without parentheses even though this does not comply with the convention given in Section 6.2.1. In the following, we will similarly omit parentheses whenever this does not create ambiguity, in order to lighten the notations.

Using the topological rules (Figure 6.5), one can simplify $E(C_0)$ into the circuit C_1:



The encoding of quantum circuits into linear optical circuits preserves the semantics, up to Gray codes.

Proposition 6.44. *For any n-qubit quantum circuit C,*

$$\mathfrak{G}_n \circ [\![E(C)]\!]_{\mathrm{pp}} = [\![C]\!] \circ \mathfrak{G}_n$$

Proof. By induction. □

6.2.3 Decoding

Regarding the decoding, i.e. the translation back from linear optical circuits to quantum circuits, we use the same sequentialisation approach. Note that such a decoding is defined only for optical circuits with a power of two number of modes.

The decoding of a 2^n-mode layer $id_k \oplus g \oplus id_l$ is a n-qubit circuit denoted $D_{k,n}(g)$. For instance consider a 16-mode layer which consists in applying $-\boxed{\varphi}-$ on the fourth mode. Its semantics is $|p\rangle \mapsto \begin{cases} e^{i\varphi}|p\rangle & \text{if } p = 3 \\ |p\rangle & \text{otherwise} \end{cases}$. Such a circuit is decoded into a 4-qubit circuit $D_{3,4}(-\boxed{\varphi}-)$ implementing the multi-controlled phase $\Lambda^{G_4(3)}s(\varphi)$, whose semantics is $|x,y,z,t\rangle \mapsto \begin{cases} e^{i\varphi}|x,y,z,t\rangle & \text{if } xyzt = G_4(3) \\ |x,y,z,t\rangle & \text{otherwise} \end{cases}$.

The decoding map is formally defined as follows:

Definition 6.45 (Decoding)**.** *Let $D : \mathbf{LO}_{\mathbf{PP}}^{\mathbf{raw}} \to \mathbf{QC}^{\mathbf{raw}}$ be defined as follows: for any 2^n-mode circuit C, $D(C) = D_{0,n}(C)$ where for any n, k, ℓ with $k + \ell \leq 2^n$ and $C : \ell \to \ell$, $D_{k,n}(C)$ is inductively defined as follows:*

- $D_{k,n}(C_1 \oplus C_2) = D_{k+\ell_1,n}(C_2) \circ D_{k,n}(C_1)$*, where C_1 is acting on ℓ_1 modes;*
- $D_{k,n}(C_2 \circ C_1) = D_{k,n}(C_2) \circ D_{k,n}(C_1)$*;*

The generators are treated as follows:

$$D_{k,n}(\text{⌜⌝⌞⌟}) = id_n, \qquad D_{k,n}(-) = id_n, \qquad D_{k,n}(-\boxed{\varphi}-) = \Lambda^{G_n(k)}s(\varphi),$$
$$D_{k,n}(\text{⤫}) = \Lambda^{x_{k,n}}_{y_{k,n}}X, \qquad D_{k,n}(\overset{\theta}{\text{⤫}}) = \Lambda^{x_{k,n}}_{y_{k,n}}R_X(-2\theta),$$

where $x_{2k,n} \coloneqq G_{n-1}(k)$, $y_{2k,n} \coloneqq \epsilon$, $x_{2k+1,n} \coloneqq w$ and $y_{2k+1,n} \coloneqq 1.0^q$, where $q \in \{0, ..., n-2\}$ and $w \in \{0,1\}^{n-q-2}$ are such that $G_n(2k+1) = wa1.0^q$ for some $a \in \{0,1\}$.

The definition of $x_{k,n}$ and $y_{k,n}$ is based on the following elementary properties of Gray codes, which will be useful in the following:

Proposition 6.46 (Useful elementary properties of Gray codes)**.**

- *Let $n \in \mathbb{N}$, $i \in \{0, ..., n\}$ and $k = a2^i + b$, where $a \in \{0, ..., 2^{n-i} - 1\}$ and $b \in \{0, ..., 2^i - 1\}$. Then*

$$G_n(k) = \begin{cases} G_{n-i}(a)G_i(b) & \text{if } a \text{ is even} \\ G_{n-i}(a)G_i(2^i - 1 - b) & \text{if } a \text{ is odd.} \end{cases}$$

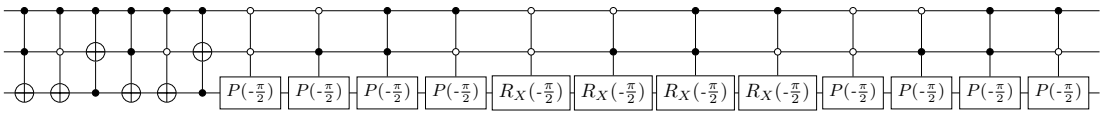
- *For any $n \geq 1$ and $k \in \{0, ..., 2^{n-1} - 1\}$, there exists $a \in \{0, 1\}$ such that*

$$G_n(2k) = G_{n-1}(k)a \quad \text{and} \quad G_n(2k+1) = G_{n-1}(k)\bar{a}.$$

- *For any $n \geq 2$ and $k \in \{0, ..., 2^{n-1} - 1\}$, there exist $a \in \{0, 1\}$, $q \in \{0, ..., n-2\}$ and $w \in \{0, 1\}^{n-q-2}$ such that*

$$G_n(2k+1) = wa1.0^q \quad \text{and} \quad G_n(2k+2) = w\bar{a}1.0^q.$$

Example 6.47. *We consider the optical circuit C_1 obtained in Example 6.43. We can show that*

$D(C_1) \equiv$ 

Similarly to the encoding function, the decoding function preserves the semantics up to Gray codes.

Proposition 6.48. *For any 2^n-mode optical circuit C,*

$$[\![D(C)]\!] \circ \mathfrak{G}_n = \mathfrak{G}_n \circ [\![C]\!]_{\mathrm{pp}}.$$

Proof. The proof is by induction. □

6.2.4 Quantum Circuit Completeness

The proof of completeness is based on the encoding/decoding of quantum circuits into optical circuits. Intuitively, given two quantum circuits representing the same unitary map, one can encode them as linear optical circuits. Since the encoding preserves the semantics and $\mathrm{LO}_{\mathrm{PP}}$ is complete, there exists a derivation proving the equivalence of the encoded circuits. In order to lift this proof to quantum circuits, it remains to prove that the decoding of an encoded quantum circuit is provably equivalent to the original quantum circuit (Lemma 6.49), and that each axiom of $\mathrm{LO}_{\mathrm{PP}}$ can be mimicked in QC (Lemma 6.61). Notice that since the encoding/decoding is defined on raw circuits, an extra step in the proof consists in showing that the axioms of $\equiv$ can also be mimicked in QC (Lemma 6.56).

6.2.4.1 $D(E(C))$ is equivalent to C

Examples 6.43 and 6.47 point out that composing encoding and decoding does not lead, in general, to the original circuit, the decoded circuit being made of multi-controlled gates. However, we show that the equivalence with the initial circuit can always be derived in QC:

Lemma 6.49. *For any n-qubit raw quantum circuit C,*

$$\mathrm{QC} \vdash D(E(C)) = C.$$

Proof. We prove by structural induction on C that

$$\forall k, \ell, \ \mathrm{QC} \vdash D(E_{k,\ell}(C)) = id_k \otimes C \otimes id_\ell.$$

For any two n-qubit raw circuits C_1, C_2, one has

$$D(E_{k,\ell}(C_2 \circ C_1)) = D(E_{k,\ell}(C_2)) \circ D(E_{k,\ell}(C_1))$$

and for any m-qubit raw circuit C_3,

$$D(E_{k,\ell}(C_1 \otimes C_3)) = D(E_{k+n,\ell}(C_3)) \circ D(E_{k,\ell+m}(C_1)).$$

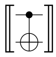
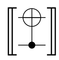
Hence, it remains the base cases, which are proved as Lemma 6.53 below. □

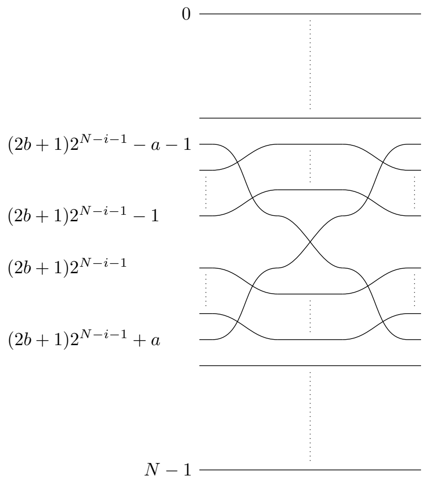
Auxiliary Lemmas. We are going to address the base cases of the induction in three steps, taking the form of three auxiliary lemmas. To state these auxiliary lemmas, we need to first give an explicit definition of $\sigma_{k,n,\ell}$:

Definition 6.50. *$\sigma_{k,n,\ell}$ is defined by $\sigma_{k,0,\ell} \coloneqq (-)^{\oplus 2^{k+\ell}}$ and $\forall n \geq 2,\ \sigma_{k,n,\ell} \coloneqq \sigma^n_{k,1,\ell+n-1}$, with*

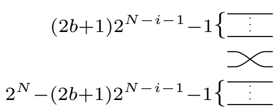
$$\sigma_{k,1,\ell} = \prod_{j=k+1}^{k+\ell} \mathcal{P}_j \mathcal{Q}_j \mathcal{P}_j$$

where

- *given a family of N-mode circuits $C_A, ..., C_B$,* $\displaystyle\prod_{i=A}^{B} C_i \coloneqq (\ldots((C_B \circ C_{B-1}) \circ C_{B-2}) \circ \ldots) \circ C_A,$
- $M \coloneqq k + \ell + 1$
- *$\mathcal{P}_j$ is a raw optical circuit such that $\mathfrak{G}_n \circ [\![\mathcal{P}_j]\!]_{\mathrm{pp}} \circ \mathfrak{G}_n^{-1} = id_{j-1} \otimes$*  *$\otimes\, id_{M-j-1}$, defined as* $\displaystyle\mathcal{P}_j \coloneqq \prod_{\substack{b=0 \\ b \bmod 4 \in \{1,2\}}}^{2^j-1} \ \prod_{a=0}^{2^{M-j-1}-1} \upsilon_{M,j,b,a}$
- *$\mathcal{Q}_j$ is a raw optical circuit such that $\mathfrak{G}_n \circ [\![\mathcal{Q}_j]\!]_{\mathrm{pp}} \circ \mathfrak{G}_n^{-1} = id_{j-1} \otimes$*  *$\otimes\, id_{M-j-1}$, defined as* $\displaystyle\mathcal{Q}_j \coloneqq \prod_{b=0}^{2^{j-1}-1} \ \prod_{a=0}^{2^{M-j-3}-1} \upsilon_{M,j-1,b,a}$
- *$\upsilon_{N,i,b,a}$ is a raw optical circuit such that $\upsilon_{N,i,b,a} \equiv$*



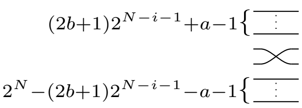
. It is defined for any $N \geq 1$, $i \in \{0, ..., N-1\}$, $b \in \{0, ..., 2^i - 1\}$ and $a \in \{0, ..., 2^{N-i-1} - 1\}$, by finite induction on a by

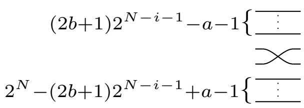
$\upsilon_{N,i,b,0} \coloneqq$ 

,

and for $a \in \{1, ..., 2^{N-i-1} - 1\}$,

$$\upsilon_{N,i,b,a} \coloneqq s_{-a} \circ s_{+a} \circ \upsilon_{N,i,b,a-1} \circ s_{+a} \circ s_{-a},$$

where $s_{+a} \coloneqq$ 

and $s_{-a} \coloneqq$ 

.

The three steps of the proof of the base cases of Lemma 6.49 are the following (note that Lemma 6.53 corresponds exactly to the base cases of Lemma 6.49):

Lemma 6.51. *For any $N \geq 1$, $i \in \{0, ..., N-1\}$, $b \in \{0, ..., 2^i - 1\}$ and $a \in \{0, ..., 2^{N-i-1} - 1\}$,*

$$\mathrm{QC} \vdash D(\upsilon_{N,i,b,a}) = \Lambda^{G_i(b)}_{G_{N-i-1}(2^{N-i-1}-a-1)} X$$

where $\upsilon_{N,i,b,a}$ is defined in Definition 6.50, and given $n \in \mathbb{N}$ and $k \in \{0, ..., 2^n - 1\}$, $G_n(k) \in \{0,1\}^n$ is the n-bit Gray code of k, defined in Definition 6.40. Note that $G_{N-i-1}(2^{N-i-1} - a - 1)$ differs from $G_{N-i-1}(a)$ by only the first bit.

Lemma 6.52. *For any $k, \ell, n \in \mathbb{N}$,*

$$\mathrm{QC} \vdash D(\sigma_{k,n,\ell}) = id_k \otimes \sigma_{n,\ell}.$$

where $\sigma_{0,0} \coloneqq$  *and $\sigma_{n,\ell} \coloneqq \sigma^n_{n+\ell-1}$, where $\sigma_{n+\ell-1}$ is defined in Figure 6.5.*

Lemma 6.53. *For any $g \in \{$*  *$, —, s(\varphi),$*  *,* *,*  *,*  *$\}$,*

$$\mathrm{QC} \vdash D(E_{k,\ell}(g)) = id_k \otimes g \otimes id_\ell.$$

To prove these lemmas, it is convenient to introduce the following notation:

Definition 6.54. *Given $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$ and $G \in \{s(\varphi), X, R_X(\theta), P(\varphi)\}$, we define*

$$\bar{\Lambda}^x_y G \coloneqq \prod_{\substack{x' \in \{0,1\}^k \\ y' \in \{0,1\}^\ell \\ x'y' \neq xy}} \Lambda^{x'}_{y'} G$$

where the product denotes a sequential composition taken in an arbitrary order.

Proof of Lemma 6.51. We proceed by induction on a.

It follows from the definition of D and the properties of the Gray code that

$$D(\upsilon_{N,i,b,0}) \overset{\text{def}}{=} D\left(\begin{array}{r} (2b+1)2^{N-i-1}-1\{ \\ \\ 2^N-(2b+1)2^{N-i-1}-1\{ \end{array} \right.$$

$$\left.\begin{array}{l} \\ \\ \\ \end{array}\right) \equiv \Lambda^{G_i(b)}_{G_{N-i-1}(2^{N-i-1}-1)} X.$$

Assuming for some $a \in \{1, ..., 2^{N-i-1} - 1\}$ that $\mathrm{QC}_0 \vdash D(\upsilon_{N,i,b,a-1}) = \Lambda^{G_i(b)}_{G_{N-i-1}(2^{N-i-1}-a)} X$, by definition of $\upsilon_{N,i,b,a}$, one has

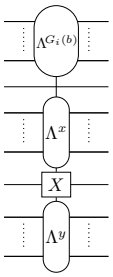
$$\mathrm{QC}_0 \vdash D(\upsilon_{N,i,b,a}) = D(s_{-a}) \circ D(s_{+a}) \circ \left(\Lambda^{G_i(b)}_{G_{N-i-1}(2^{N-i-1}-a)} X\right) \circ D(s_{+a}) \circ D(s_{-a}).$$

Because of the properties of Gray codes, $G_{N-i-1}(2^{N-i-1} - a - 1)$ differs from $G_{N-i-1}(2^{N-i-1} - a)$ by only one bit. That is, there exist $k, \ell \geq 0$ with $k + \ell = N - i - 2$, $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$ and $\alpha \in \{0,1\}$, such that

$$G_{N-i-1}(2^{N-i-1} - a - 1) = x\alpha y \quad \text{and} \quad G_{N-i-1}(2^{N-i-1} - a) = x\bar{\alpha}y$$

where $\bar{\alpha} \coloneqq 1 - \alpha$.

It follows from the definition of D and the properties of the Gray codes that $D(s_{-a}) \equiv \Lambda_y^{G_i(b).0x} X$ and $D(s_{+a}) \equiv \Lambda_y^{G_i(b).1x} X$. Hence, by Propositions 6.17, 6.26 and 6.27, $\mathrm{QC}_0 \vdash D(s_{-a}) \circ D(s_{+a}) =$

$D(s_{+a}) \circ D(s_{-a}) =$ 

$\overset{\text{def}}{=} (\sigma_{1,i} \otimes id_{N-i-1}) \circ \left(- \otimes \Lambda_y^{G_i(b)x} X\right) \circ (\sigma_{i,1} \otimes id_{N-i-1})$, so that

$$\mathrm{QC} \vdash D(\upsilon_{N,i,b,a}) = (\sigma_{1,i} \otimes id_{N-i-1}) \circ \left(- \otimes \Lambda_y^{G_i(b)x} X\right) \circ \left(\Lambda^{\epsilon}_{G_i(b)x\bar{\alpha}y} X\right) \circ \left(- \otimes \Lambda_y^{G_i(b)x} X\right) \circ (\sigma_{i,1} \otimes id_{N-i-1})$$

with

$$\mathrm{QC} \vdash$$

$$\left(- \otimes \Lambda_y^{G_i(b)x} X\right) \circ \left(\Lambda^{\epsilon}_{G_i(b)x\bar{\alpha}y} X\right) \circ \left(- \otimes \Lambda_y^{G_i(b)x} X\right)$$

$$\overset{\text{Propositions 6.38, 6.27 and 6.26}}{=}$$

$$(id_{i+k+1} \otimes X \otimes id_\ell) \circ \left(- \otimes \bar{\Lambda}_y^{G_i(b)x} X\right) \circ \left(\Lambda^{\epsilon}_{G_i(b)x\bar{\alpha}y} X\right) \circ \left(- \otimes \bar{\Lambda}_y^{G_i(b)x} X\right) \circ (id_{i+k+1} \otimes X \otimes id_\ell)$$

$$\overset{\text{Propositions 6.26 and 6.27}}{=}$$

$$(id_{i+k+1} \otimes X \otimes id_\ell) \circ \left(- \otimes \bar{\Lambda}_y^{G_i(b)x} X\right) \circ \left(- \otimes \bar{\Lambda}_y^{G_i(b)x} X\right) \circ \left(\Lambda^{\epsilon}_{G_i(b)x\bar{\alpha}y} X\right) \circ (id_{i+k+1} \otimes X \otimes id_\ell)$$

$$\overset{\text{Propositions 6.27 and 6.38}}{=}$$

$$(id_{i+k+1} \otimes X \otimes id_\ell) \circ \left(\Lambda^{\epsilon}_{G_i(b)x\bar{\alpha}y} X\right) \circ (id_{i+k+1} \otimes X \otimes id_\ell)\,.$$

In other words,

$$\mathrm{QC} \vdash D(\upsilon_{N,i,b,a}) = (id_{i+k+1} \otimes X \otimes id_\ell) \circ \left(\Lambda^{G_i(b)}_{x\bar{\alpha}y} X\right) \circ (id_{i+k+1} \otimes X \otimes id_\ell)\,.$$

By definition of $\Lambda^{G_i(b)}_{x\bar{\alpha}y} X$ and Equation (6.10), this implies that

$$\mathrm{QC} \vdash D(\upsilon_{N,i,b,a}) = \Lambda^{G_i(b)}_{x\alpha y} X$$

which, since $x\alpha y = G_{N-i-1}(2^{N-i-1} - a - 1)$, is the desired property. □

Remark 6.55. *By defining $\upsilon_{N,i,b,a}$ in a less natural way using not only — and*  *but also* *and*  *, one could avoid using Proposition 6.38 and get the stronger result that $\mathrm{QC}_0 \vdash D(\upsilon_{N,i,b,a}) = \Lambda^{G_i(b)}_{G_{N-i-1}(2^{N-i-1}-a-1)} X$, which would in turn imply that the equalities of Lemmas 6.52 and 6.53, and therefore that of Lemma 6.49, can also be taken modulo QC_0 instead of* QC.

Proof of Lemma 6.52. First, if $n = 1$, by definition (see Definitions 6.45 and 6.50), one has

$$D(\sigma_{k,1,\ell}) = \prod_{j=k+1}^{k+\ell} P_j Q_j P_j$$

where, with $M \coloneqq k+\ell+1$, $P_j \coloneqq \prod_{\substack{b=0 \\ b \bmod 4 \in \{1,2\}}}^{2^j-1} \prod_{a=0}^{2^{M-j-1}-1} D(\upsilon_{M,j,b,a})$ and $Q_j \coloneqq \prod_{b=0}^{2^{j-1}-1} \prod_{a=0}^{2^{M-j-3}-1} D(\upsilon_{M,j-1,b,a})$.

By Lemma 6.51, this implies that for all j,

$$\mathrm{QC} \vdash P_j = \prod_{\substack{b=0 \\ b \bmod 4 \in \{1,2\}}}^{2^j-1} \prod_{a=0}^{2^{M-j-1}-1} \Lambda^{G_j(b)}_{G_{M-j-1}(2^{M-j-1}-a-1)} X$$

It is easy to check that when a goes from 0 to $2^{M-j-1}-1$, $G_{M-j-1}(2^{M-j-1}-a-1)$ takes all possible values in $\{0,1\}^{M-j-1}$, once each, and that when b takes all possible values between 0 and 2^j-1 that are congruent to 1 or 2 modulo 4, $G_j(b)$ takes, once each, all values in $\{0,1\}^j$ in which the last bit has value 1. Hence, it follows from Propositions 6.26, 6.27 and 6.10 that

$$\mathrm{QC} \vdash P_j = id_{j-1} \otimes$$  $$\otimes\, id_{M-j-1}.$$

Again by Lemma 6.51, for all j,

$$\mathrm{QC} \vdash Q_j = \prod_{b=0}^{2^{j-1}-1} \prod_{a=0}^{2^{M-j-3}-1} \Lambda^{G_{j-1}(b)}_{G_{M-j}(2^{M-j}-a-1)} X$$

Similarly, it is easy to check that when b goes from 0 to $2^{j-1}-1$, $G_{j-1}(b)$ takes all values in $\{0,1\}^{j-1}$, once each, and that when a goes from 0 to 2^{M-j-3}, $G_{M-j}(2^{M-j}-a-1)$ takes, once each, all values in $\{0,1\}^{M-j}$ in which the first bit has value 1. Hence, it follows from Propositions 6.26, 6.27 and 6.10 that

$$\mathrm{QC} \vdash Q_j = id_{j-1} \otimes$$  $$\otimes\, id_{M-j-1}.$$

Thus,

$$\mathrm{QC} \vdash D(\sigma_{k,1,\ell}) = \prod_{j=k+1}^{k+\ell} id_{j-1} \otimes$$  $$\otimes\, id_{M-j-1}.$$

By Equation (6.h), this implies that

$$\mathrm{QC} \vdash D(\sigma_{k,1,\ell}) = \prod_{j=k+1}^{k+\ell} id_{j-1} \otimes$$  $$\otimes\, id_{M-j-1} \equiv id_k \otimes \sigma_{1,\ell}. \tag{6.33}$$

Finally, if $n > 1$, then

$$\begin{aligned} D(\sigma_{k,n,\ell}) &\overset{\text{def}}{=} D(\sigma^n_{k,1,\ell+n-1}) \\ &\overset{\text{def}}{=} D(\sigma_{k,1,\ell+n-1})^n \\ &\overset{(6.33)}{=} (id_k \otimes \sigma_{1,\ell+n-1})^n \\ &\equiv id_k \otimes \sigma_{n,\ell}. \end{aligned}$$

□

Proof of Lemma 6.53. If $g =$  or — then the result follows directly from the definitions.

If $g = s(\varphi)$, then it follows from the definitions of $E_{k,\ell}$ and D that

$$D(E_{k,\ell}(s(\varphi))) = \prod_{x \in \{0,1\}^{k+\ell}} \Lambda^x s(\varphi)$$

where we use the notation $\prod_{x\in\{0,1\}^{k+\ell}}$ to denote the product without specifying the order of the factors. By Propositions 6.26 and 6.27, this implies that

$$\mathrm{QC} \vdash D(E_{k,\ell}(s(\varphi))) = id_{k+\ell} \otimes s(\varphi)$$

which is equal to $id_k \otimes s(\varphi) \otimes id_\ell$ by the topological rules of quantum circuits.

If $g = -\boxed{P(\varphi)}-$, then it follows from the definitions that if $k = \ell = 0$,

$$D(E_{0,0}(-\boxed{P(\varphi)}-)) = D(\overline{\boxed{\varphi}}) \equiv \Lambda^1 s(\varphi) = P(\varphi).$$

and if $(k,\ell) \neq (0,0)$,

$$D(E_{k,\ell}(-\boxed{P(\varphi)}-)) = D(\sigma_{k,\ell,1}) \circ D\left(\left(\overline{\begin{matrix}\boxed{\varphi}\\ \boxed{\varphi}\end{matrix}}\right)^{\oplus 2^{k+\ell-1}}\right) \circ D(\sigma_{k,1,\ell})$$

with

$$D\left(\left(\overline{\begin{matrix}\boxed{\varphi}\\ \boxed{\varphi}\end{matrix}}\right)^{\oplus 2^{k+\ell-1}}\right) \equiv \prod_{x\in\{0,1\}^{k+\ell}} \Lambda^{x1} s(\varphi) = \prod_{x\in\{0,1\}^{k+\ell}} \Lambda^x P(\varphi).$$

By Propositions 6.26 and 6.27, this product is equal modulo QC_0 to $id_{k+\ell} \otimes P(\varphi)$. Then, Lemma 6.52 together with topological rules of quantum circuits gives us the result.

If $g = -\boxed{H}-$, then it follows from the definitions that if $k = \ell = 0$,

$$D(E_{0,0}(-\boxed{H}-)) = D(\overline{\boxed{-\tfrac{\pi}{2}}\ \overset{\frac{\pi}{4}}{\smile}\ \boxed{-\tfrac{\pi}{2}}}) \equiv \Lambda^1 s(-\tfrac{\pi}{2}) \circ \Lambda^\epsilon_\epsilon R_X(-\tfrac{\pi}{2}) \circ \Lambda^1 s(-\tfrac{\pi}{2})$$

$$= -\boxed{P(-\tfrac{\pi}{2})}-\boxed{R_X(-\tfrac{\pi}{2})}-\boxed{P(-\tfrac{\pi}{2})}-$$

$$\overset{\text{Proposition 6.35}}{=} -\boxed{H}-$$

and if $(k,\ell) \neq (0,0)$,

$$D(E_{k,\ell}(-\boxed{H}-)) = D(\sigma_{k,\ell,1}) \circ D\left(\left(\overline{\begin{matrix}\boxed{-\frac{\pi}{2}}\ \overset{\frac{\pi}{4}}{\smile}\ \boxed{-\frac{\pi}{2}}\\ \boxed{-\frac{\pi}{2}}\ \underset{\frac{\pi}{4}}{\frown}\ \boxed{-\frac{\pi}{2}}\end{matrix}}\right)^{\oplus 2^{k+\ell-1}}\right) \circ D(\sigma_{k,1,\ell})$$

with

$$D\left(\left(\overline{\begin{matrix}\boxed{-\frac{\pi}{2}}\ \overset{\frac{\pi}{4}}{\smile}\ \boxed{-\frac{\pi}{2}}\\ \boxed{-\frac{\pi}{2}}\ \underset{\frac{\pi}{4}}{\frown}\ \boxed{-\frac{\pi}{2}}\end{matrix}}\right)^{\oplus 2^{k+\ell-1}}\right) \equiv \prod_{x\in\{0,1\}^{k+\ell}} \left(\left(\prod_{a\in\{0,1\}} \Lambda^{xa1} s(-\tfrac{\pi}{2})\right) \circ \left(\prod_{a\in\{0,1\}} \Lambda^{xa} R_X(-\tfrac{\pi}{2})\right) \circ \left(\prod_{a\in\{0,1\}} \Lambda^{xa1} s(-\tfrac{\pi}{2})\right)\right).$$

By Propositions 6.26 and 6.27, this product is equal modulo QC_0 to $id_{k+\ell} \otimes -\boxed{P(-\frac{\pi}{2})}\boxed{R_X(-\frac{\pi}{2})}\boxed{P(-\frac{\pi}{2})}-$, which by Proposition 6.35 is equal modulo QC_0 to $-\boxed{H}-$. Then, Lemma 6.52 together with topological rules of quantum circuits gives us the result.

If $g = \overset{\bullet}{\underset{\oplus}{|}}$, then it follows from the definitions that if $k = \ell = 0$,

$$D(E_{0,0}(\overset{\bullet}{\underset{\oplus}{|}})) = D\left(\overline{\times}\right) \equiv \Lambda^1_\epsilon X$$

which is equal to  modulo QC_0 by Proposition 6.10;

and if $(k,\ell) \neq (0,0)$,

$$D(E_{k,\ell}(\;)) = D(\sigma_{k,\ell,2}) \circ D\left(\;\right)^{\oplus 2^{k+\ell-1}} \circ D(\sigma_{k,2,\ell})$$

with

$$D\left(\;\right)^{\oplus 2^{k+\ell-1}} \equiv \prod_{x\in\{0,1\}^{k+\ell}} \Lambda^{x1}X.$$

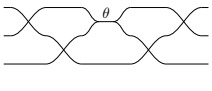
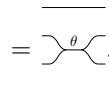
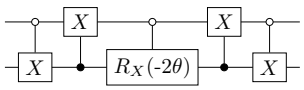
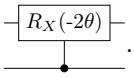
By Propositions 6.26 and 6.27, this product is equal modulo QC_0 to $id_{k+\ell} \otimes \Lambda^1 X$, which by Proposition 6.10 is equal modulo QC_0 to $id_{k+\ell} \otimes$. Then, Lemma 6.52 together with topological rules of quantum circuits gives us the result.

If $g =$  , then it follows from the definitions that

$$D(E_{k,2,\ell}(\;)) = D(\sigma_{k,\ell,2}) \circ D(\sigma_{k+\ell,1,1}) \circ D(\sigma_{k,2,\ell})$$

By Lemma 6.52, this is equal modulo QC to $(id_k \otimes \sigma_{\ell,2}) \circ (id_{k+\ell} \otimes$ $) \otimes (id_k \otimes \sigma_{2,\ell})$, which by the topological rules of quantum circuits, is equal to $id_k \otimes$ $\otimes\, id_\ell$. □

6.2.4.2 Mimicking the Topological Rules

Note that in general, the decoding function does not preserve the topological equivalence. For instance, with the raw circuits $C_1 =$  and $C_2 =$  , we have $C_1 \equiv C_2$ but $D(C_1) =$  and $D(C_2) =$  . Thus, the topological rules also have to be mimicked in QC:

Lemma 6.56. *For any 2^n-mode raw optical circuits C_1, C_2, if $C_1 \equiv C_2$ then* $\mathrm{QC} \vdash D(C_1) = D(C_2)$.

Ancillary Lemma and Useful Definitions The following lemma will be useful to treat one of the cases in the proof of Lemma 6.56:

Lemma 6.57. *For any raw optical circuits $C_1 : \ell_1 \to \ell_1$ and $C_2 : \ell_2 \to \ell_2$, and any k, ℓ, n with $\ell \geq \ell_1$ and $k + \ell \leq 2^n$,*

$$\mathrm{QC}_0 \vdash D_{k+\ell,n}(C_2) \circ D_{k,n}(C_1) = D_{k,n}(C_1) \circ D_{k+\ell,n}(C_2).$$

Proof. We proceed by structural induction on C_1 and C_2.

- If $C_1 = C_1'' \circ C_1'$, then

  $$D_{k+\ell,n}(C_2) \circ D_{k,n}(C_1) = D_{k+\ell,n}(C_2) \circ (D_{k,n}(C_1'') \circ D_{k,n}(C_1'))$$

  while

  $$D_{k,n}(C_1) \circ D_{k+\ell,n}(C_2) = (D_{k,n}(C_1'') \circ D_{k,n}(C_1')) \circ D_{k+\ell,n}(C_2)$$

  so the result follows by Equation (t_2) of quantum circuits and the induction hypothesis.

- The case $C_2 = C_2'' \circ C_2'$ is similar to the previous one.

- If $C_1 = C_1' \oplus C_1''$ with $C_1' : \ell_1' \to \ell_1'$, then

$$D_{k+\ell,n}(C_2) \circ D_{k,n}(C_1) = D_{k+\ell,n}(C_2) \circ (D_{k+\ell_1',n}(C_1'') \circ D_{k,n}(C_1'))$$

  while

$$D_{k,n}(C_1) \circ D_{k+\ell,n}(C_2) = (D_{k+\ell_1',n}(C_1'') \circ D_{k,n}(C_1')) \circ D_{k+\ell,n}(C_2)$$

  so the result follows by Equation (t_2) of quantum circuits and the induction hypothesis.

- The case $C_2 = C_2' \oplus C_2''$ is similar to the previous one.

- If C_1 or C_2 is  or —, then the results follows from Equation (t_1) of quantum circuits.

- If $C_1, C_2 \in \{$  ,  ,  $\}$, then $D_{k,n}(C_1) = \Lambda^{G_n(k)} s(\varphi)$, $\Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\theta)$ or $\Lambda^{x_{k,n}}_{y_{k,n}} X$ and $D_{k+\ell,n}(C_2) = \Lambda^{G_n(k+\ell)} s(\varphi)$, $\Lambda^{x_{k+\ell,n}}_{y_{k+\ell,n}} R_X(-2\theta)$ or $\Lambda^{x_{k+\ell,n}}_{y_{k+\ell,n}} X$. Using the definitions of $G_n(k)$, $x_{k,n}$ and $y_{k,n}$, it is easy to check that in any case, $D_{k,n}(C_1)$ and $D_{k+\ell,n}(C_2)$ satisfy the premises of either Proposition 6.27 or 6.30 and therefore commute.

□

Additionally, it will be useful to slightly generalise the notation of Definition 6.54:

Definition 6.58. *Given $x \in \{0,1\}^k$, $y \in \{0,1\}^\ell$ and $z \in \{0,1\}^m$, we define*

$$\Lambda^{x}_{\substack{y \\ z}} \coloneqq \Lambda^{x1y}_{z} X, \qquad \Lambda^{x}_{\substack{y \\ z}} \coloneqq \Lambda^{x}_{y1z} X, \qquad \bar{\Lambda}^{x}_{\substack{y \\ z}} \coloneqq \prod_{\substack{x' \in \{0,1\}^k \\ y' \in \{0,1\}^\ell \\ z' \in \{0,1\}^m \\ x'y'z' \neq xyz}} \Lambda^{x'1y'}_{z'} X \quad \text{and} \quad \bar{\Lambda}^{x}_{\substack{y \\ z}} \coloneqq \prod_{\substack{x' \in \{0,1\}^k \\ y' \in \{0,1\}^\ell \\ z' \in \{0,1\}^m \\ x'y'z' \neq xyz}} \Lambda^{x'}_{y'1z'} X.$$

Finally, it will be useful, both for the proof of Lemma 6.56 and that of Lemma 6.61 below, to introduce a notion of context and substitution. We actually need to formalise this notion only for optical circuits:

Definition 6.59 (Context)**.** *A N-mode raw context $\mathcal{C}[\cdot]_i$ with $i \in \mathbb{N}$ is inductively defined as follows:*

- *$[\cdot]_i$ is a i-mode raw context,*
- *if $\mathcal{C}[\cdot]_i$ is a N-mode raw context and C is a M-mode raw optical circuit then $\mathcal{C}[\cdot]_i \oplus C$ and $C \oplus \mathcal{C}[\cdot]_i$ are $N+M$-mode raw contexts,*
- *if $\mathcal{C}[\cdot]_i$ is a N-mode raw context and C is a N-mode raw optical circuit then $\mathcal{C}[\cdot]_i \circ C$ and $C \circ \mathcal{C}[\cdot]_i$ are N-mode raw contexts.*

Definition 6.60 (Substitution)**.** *Given a N-mode raw context $\mathcal{C}[\cdot]_i$ and a i-mode raw circuit C, we define the substituted circuit $\mathcal{C}[C]$ as the N-mode raw circuit obtained by replacing the hole $[\cdot]_i$ by C in $\mathcal{C}[\cdot]_i$.*

Proof of Lemma 6.56. To prove Lemma 6.56, it suffices to prove that for each rule of Figure 6.5, of the form $C_1 = C_2$ with $C_1, C_2 \in \mathbf{LO}^{\mathbf{raw}}_{\mathbf{PP}}[i,i]$ (see Definition 1.1), and any 2^n-mode raw context $\mathcal{C}[\cdot]_i$, one has $\mathrm{QC} \vdash D(\mathcal{C}[C_1]) = D(\mathcal{C}[C_2])$. For this purpose, we prove a slightly more general result, namely that for any k, n and any ℓ-mode raw context $\mathcal{C}[\cdot]_i$ with $k + \ell \leq 2^n$, one has $\mathrm{QC} \vdash D_{k,n}(\mathcal{C}[C_1]) = D_{k,n}(\mathcal{C}[C_2])$. We proceed by induction on $\mathcal{C}[\cdot]_i$:

- If $\mathcal{C}[\cdot]_i = C \circ \mathcal{C}'[\cdot]_i$, then $D_{k,n}(\mathcal{C}[C_1]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_1])$ and $D_{k,n}(\mathcal{C}[C_2]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_2])$, so the result follows by induction hypothesis. The case $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \circ C$ is similar.
- If $\mathcal{C}[\cdot]_i = C \oplus \mathcal{C}'[\cdot]_i$ with $C : \ell_1 \to \ell_1$, then $D_{k,n}(\mathcal{C}[C_1]) = D_{k+\ell_1,n}(\mathcal{C}'[C_1]) \circ D_{k,n}(C)$ and $D_{k,n}(\mathcal{C}[C_2]) = D_{k+\ell_1,n}(\mathcal{C}'[C_2]) \circ D_{k,n}(C)$, so the result follows by induction hypothesis. The case $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \oplus C$ is similar.

It remains to prove for each rule of Figure 6.5, of the form $C_1 = C_2$ with $C_1, C_2 \in \mathbf{LO}_{\mathbf{PP}}^{\mathbf{raw}}[i,i]$, that for any k, n with $k + i \leq 2^n$, one has $\mathrm{QC} \vdash D_{k,n}(C_1) = D_{k,n}(C_2)$.

For Equation (t_2), for any $C_1, C_2, C_3 : \ell \to \ell$,

$$D_{k,n}((C_3 \circ C_2) \circ C_1) = (D_{k,n}(C_3) \circ D_{k,n}(C_2)) \circ D_{k,n}(C_1)$$

and

$$D_{k,n}(C_3 \circ (C_2 \circ C_1)) = D_{k,n}(C_3) \circ (D_{k,n}(C_2) \circ D_{k,n}(C_1)).$$

Both are equal according to Equation (t_2) of quantum circuits.

For Equation (t_5), for any optical circuits $C_1 : \ell_1 \to \ell_1$, $C_2 : \ell_2 \to \ell_2$ and $C_3 : \ell_3 \to \ell_3$,

$$D_{k,n}((C_1 \oplus C_2) \oplus C_3) = D_{k+\ell_1+\ell_2,n}(C_3) \circ (D_{k+\ell_1,n}(C_2) \circ D_{k,n}(C_1))$$

and

$$D_{k,n}(C_1 \oplus (C_2 \oplus C_3)) = (D_{k+\ell_1+\ell_2,n}(C_3) \circ D_{k+\ell_1,n}(C_2)) \circ D_{k,n}(C_1).$$

Again, both are equal according to Equation (t_2) of quantum circuits.

For Equation (t_1), for any ℓ-mode optical circuit C, by definition of id_ℓ and $D_{k,n}$,

$$D_{k,n}(id_\ell \circ C) = (id_n \circ (id_n \circ (\cdots \circ (id_n \circ id_n)) \cdots)) \circ D_{k,n}(C)$$

with $\ell + 1$ occurences of id_n in the right-hand side. This is equal to $D_{k,n}(C)$ according to Equation (t_1) of quantum circuits. Similarly, $D_{k,n}(C \circ id_\ell) \equiv D_{k,n}(C)$.

For Equation (t_3), for any ℓ-mode optical circuit C,

$$D_{k,n}(\boxed{\ } \oplus C) = D_{k,n}(C) \circ id_\ell$$

which is equal to $D_{k,n}(C)$ according to Equation (t_1) of quantum circuits. Similarly, $D_{k,n}(C \oplus \boxed{\ }) \equiv D_{k,n}(C)$.

For Equation (t_6), for any optical circuits $C_1, C_2 : \ell \to \ell$ and $C_3, C_4 : m \to m$,

$$D_{k,n}((C_2 \circ C_1) \oplus (C_4 \circ C_3)) = (D_{k+\ell,n}(C_4) \circ D_{k+\ell,n}(C_3)) \circ (D_{k,n}(C_2) \circ D_{k,n}(C_1))$$

and

$$D_{k,n}((C_2 \oplus C_4) \circ (C_1 \oplus C_3)) = (D_{k+\ell,n}(C_4) \circ D_{k,n}(C_2)) \circ (D_{k+\ell,n}(C_3) \circ D_{k,n}(C_1)).$$

The result follows from Equation (t_2) of quantum circuits and Lemma 6.57.

For Equation (t_7), one has

$$D_{k,n}(\supset\!\subset \circ \supset\!\subset) = \Lambda_{y_{k,n}}^{x_{k,n}} X \circ \Lambda_{y_{k,n}}^{x_{k,n}} X$$

which by Proposition 6.38, implies that

$$\mathrm{QC} \vdash D_{k,n}(\supset\!\subset \circ \supset\!\subset) = id_n.$$

On the other hand,

$$D_{k,n}(- \oplus -) = id_n \circ id_n \equiv id_n.$$

For Equation (t_4), we proceed by induction on C.

- If $C = C_1 \circ C_2$, then $\sigma_k \circ (- \oplus (C_1 \circ C_2)) \equiv (\sigma_k \circ (- \oplus C_1)) \circ (- \oplus C_2)$, and the derivation of the equivalence does not use Equation (t_4). Hence it follows from the paragraphs above that

  $$\mathrm{QC} \vdash D_{k,n}(\sigma_k \circ (- \oplus (C_1 \circ C_2))) = D_{k,n}((\sigma_k \circ (- \oplus C_1)) \circ (- \oplus C_2)).$$

  It follows similarly from those paragraphs that

  $$\mathrm{QC} \vdash D_{k,n}(((C_1 \circ C_2) \oplus -) \circ \sigma_k) = D_{k,n}((C_1 \oplus -) \circ ((C_2 \oplus -) \circ \sigma_k)).$$

  The equality modulo QC of the two right-hand sides follows from the induction hypothesis, together with the compatibility of $D_{k,n}$ with Equation (t_2) modulo QC, which is proved above.

- If $C = C_1 \oplus C_2$ with $C_1 : \ell_1 \to \ell_1$ and $C_2 : \ell_2 \to \ell_2$, then

$$\sigma_k \circ (- \oplus (C_1 \oplus C_2)) \equiv (id_{\ell_1} \oplus (\sigma_{\ell_2} \circ (- \oplus C_2))) \circ ((\sigma_{\ell_1} \circ (- \oplus C_1)) \oplus id_{\ell_2})$$

and the derivation of the equivalence does not use Equation (t_4), so that by the paragraphs above (together with Equation (t_1) of quantum circuits),

$$\mathrm{QC} \vdash D_{k,n}(\sigma_k \circ (- \oplus (C_1 \oplus C_2))) = D_{k+\ell_1}(\sigma_{\ell_2} \circ (- \oplus C_2)) \circ D_{k,n}(\sigma_{\ell_1} \circ (- \oplus C_1)).$$

The result follows by applying a similar transformation to the right-hand side of Equation (t_4) and applying the induction hypothesis.

- If $C =$  or —, then the result follows from Equations (t_1) and (t_3) of quantum circuits.

- If $C =$  , let us write $G_n(k)$ as xay with $a \in \{0,1\}$ and $y = \epsilon$ if k is even or $y = 1.0^q$ for some q if k is odd. Note that $G_n(k+1) = x\bar{a}y$. Then by definition of $D_{k,n}$ and Equation (6.23), if $a = 0$ then

$$\mathrm{QC} \vdash D_{k,n}(\sigma_1 \circ (- \oplus$$ $$)) = \Lambda^x_y X \circ \Lambda^x_y P(\varphi)$$

and

$$\mathrm{QC} \vdash D_{k,n}((\text{—}\boxed{\varphi}\text{—} \oplus —) \circ \sigma_1) = (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda^x_y P(\varphi) \circ (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda^x_y X.$$

By Propositions 6.26, 6.27 and 6.38, the following equalities are true modulo QC:

$$\begin{array}{rcl} \Lambda^x_y X \circ \Lambda^x_y P(\varphi) & = & (id_{|x|} \otimes X \otimes id_{|y|}) \circ \bar{\Lambda}^x_y X \circ \Lambda^x_y P(\varphi) \\ & = & (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda^x_y P(\varphi) \circ \bar{\Lambda}^x_y X \\ & = & (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda^x_y P(\varphi) \circ (id_{|x|} \otimes X \otimes id_{|y|}) \circ \Lambda^x_y X \end{array}$$

which gives us the result. The case $a = 1$ is similar.

- If $C =$  , by the properties of the Gray code, exactly one bit differs between $G_n(k)$ and $G_n(k+1)$, as well as between $G_n(k+1)$ and $G_n(k+2)$, and in exactly one of the two cases this is the last bit that differs (namely between $G_n(k)$ and $G_n(k+1)$ if k is even, and between $G_n(k+1)$ and $G_n(k+2)$ if k is odd). Hence we can write $G_n(k)$ as $xayb$ with $a, b \in \{0,1\}$, in such a way that $G_n(k+2) = x\bar{a}y\bar{b}$ and $G_n(k+1) = xay\bar{b}$ or $x\bar{a}yb$ depending on the parity of k. We treat the case where k is even, the case with k odd being similar. Then

$$D_{k,n}(\sigma_2 \circ (- \oplus$$ $$)) \equiv \Lambda^x_{y\bar{b}} X \circ \Lambda^{xay} X \circ \Lambda^x_{y\bar{b}} R_X(-2\theta)$$

and

$$D_{k,n}((\,$$ $$\, \oplus —) \circ \sigma_2) \equiv \Lambda^{xay} R_X(-2\theta) \circ \Lambda^x_{y\bar{b}} X \circ \Lambda^{xay} X$$

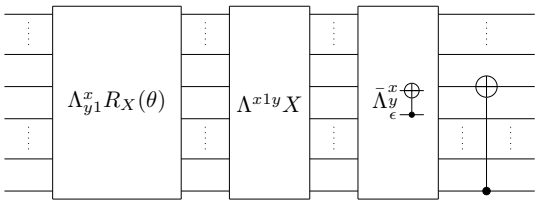
so by Lemma 6.32 and Equation (6.10), it suffices to prove that for any θ,

$$\mathrm{QC} \vdash \Lambda^x_{y1} X \circ \Lambda^{x1y} X \circ \Lambda^x_{y1} R_X(\theta) = \Lambda^{x1y} R_X(\theta) \circ \Lambda^x_{y1} X \circ \Lambda^{x1y} X.$$

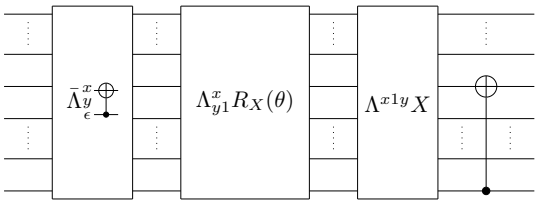
To prove this, one has, modulo QC (together with the topological rules of quantum circuits):

$\Lambda^x_{y1} X \circ \Lambda^{x1y} X \circ \Lambda^x_{y1} R_X(\theta)$

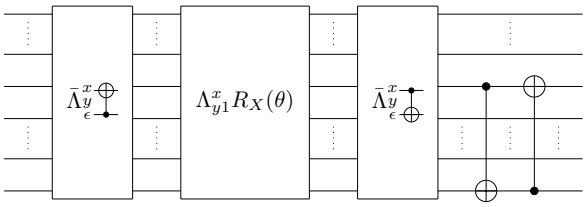
Propositions 6.38, 6.27, 6.17, 6.26 and 6.10 $=$



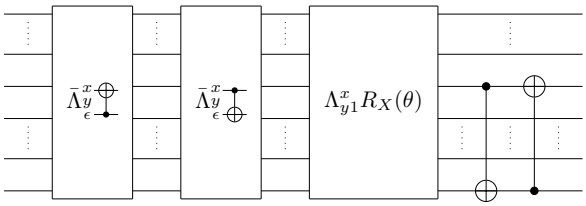
Propositions 6.27 and 6.30
=



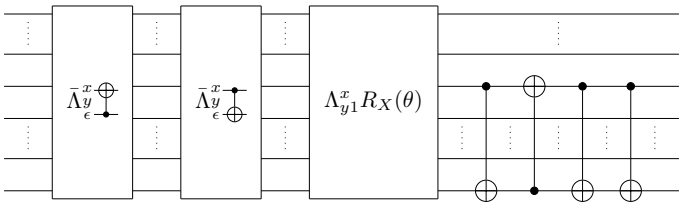
Propositions 6.38, 6.27, 6.17, 6.26 and 6.10
=



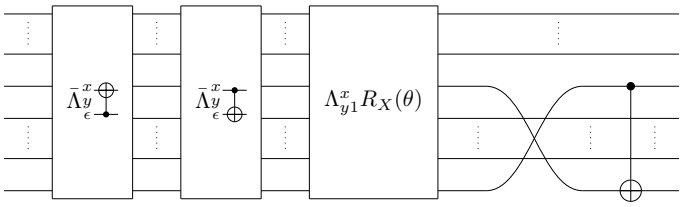
Proposition 6.30
=



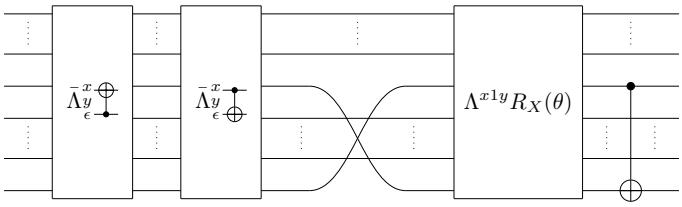
(6.e)
=



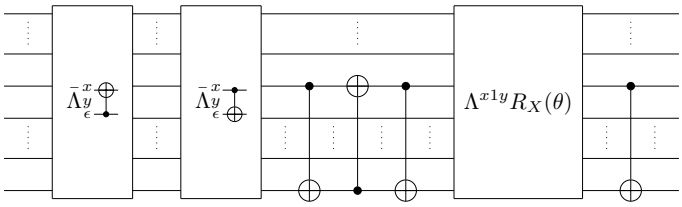
(6.h)
=



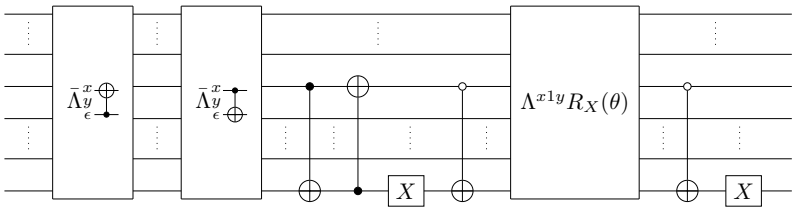
Proposition 6.17
=



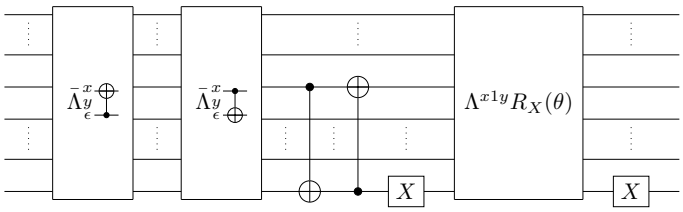
(6.h)
=



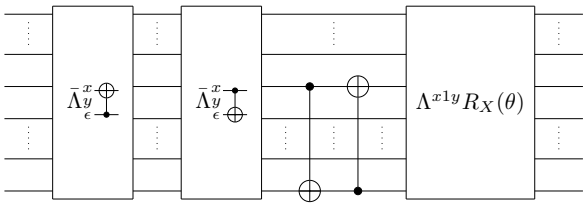
(6.10)(6.f)(6.12)
=



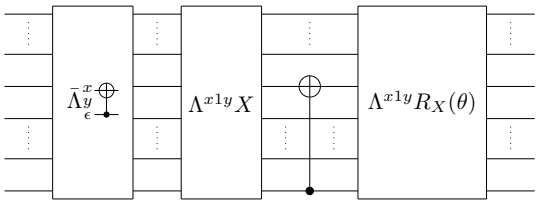
Propositions 6.10, 6.26 and 6.27, (6.10)(6.e)
=



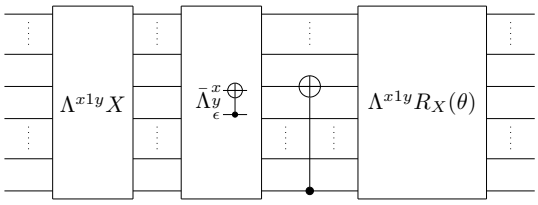
Lemma 6.32, (6.10)
=



Propositions 6.10, 6.17, 6.26, 6.27 and 6.38
=



Proposition 6.30
=



Propositions 6.10, 6.17, 6.26, 6.27 and 6.38
=

$\Lambda^{x1y}R_X(\theta) \circ \Lambda^x_{y1}X \circ \Lambda^{x1y}X.$

- The case $C = \times$ is similar to the preceding one, with $R_X(\theta)$ replaced by X.

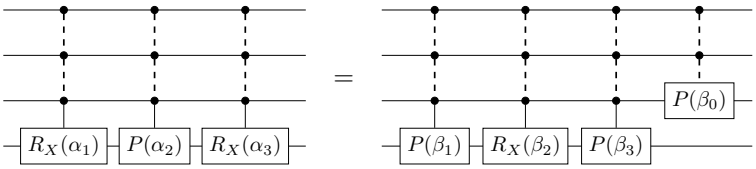
□

6.2.4.3 Mimicking the Rules of QC

Lemma 6.61. *For any 2^n-mode raw optical circuits C_1, C_2, if $\mathrm{LO}_{\mathrm{PP}} \vdash C_1 = C_2$ then $\mathrm{QC} \vdash D(C_1) = D(C_2)$.*

Auxiliary Lemmas We first prove a few additional auxiliary properties, which will be useful in the proof of Lemma 6.61 in particular to prove that the conditions on the angles in Equations (6.q) and (6.r) do not prevent us from getting the result. Namely, multi-controlled versions of Equations (6.q), (6.l) and (6.24), of the fact that $R_X(2\pi)$ is equivalent to a global phase of π, and an equality which is roughly speaking the decoding of Rule 5.63 of PPRS.

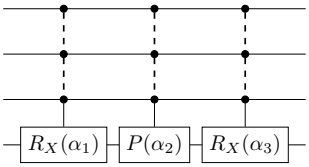
Lemma 6.62. *The following equation can be derived in* QC*:*



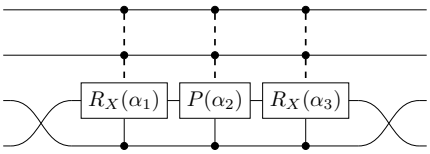
(6.34)

where the angles are the same as in Equation (6.q)*.*

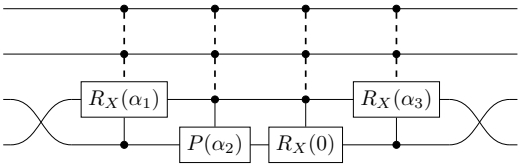
Proof.



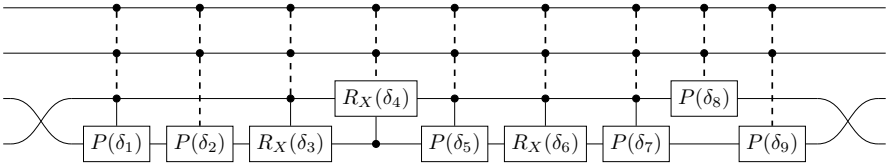
$\equiv$



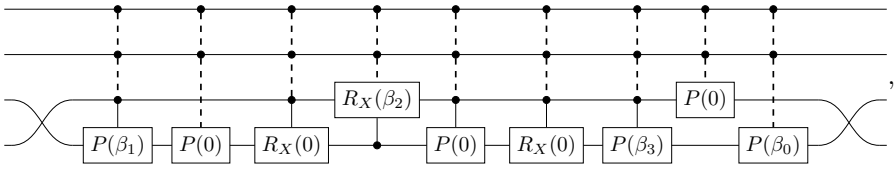
Propositions 6.18 and 6.23 $=$



(6.r) $=$

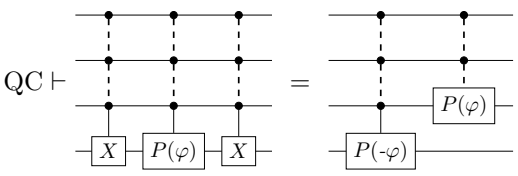


By uniqueness of the right-hand side in Equations (6.q) and (6.r), the δ_i are such that the last circuit is equal to

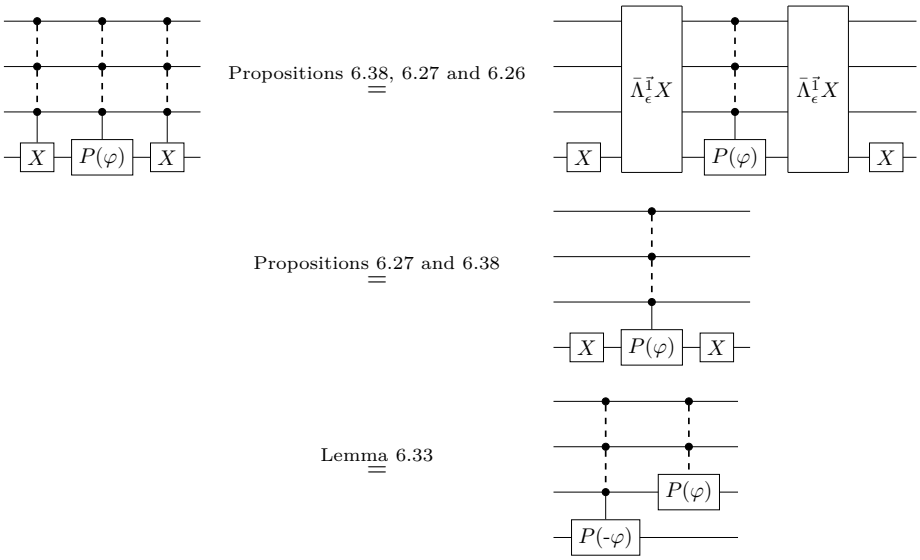


, where the β_j are computed in the same way as in Equation (6.q). It follows from Propositions 6.18 and 6.23 that this is equal modulo QC_0 to the right-hand side of Equation (6.34). □

Lemma 6.63.

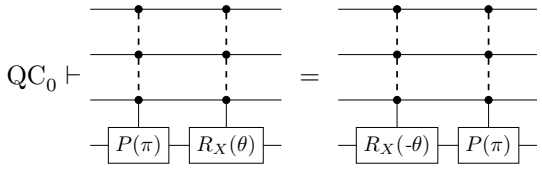


Proof.

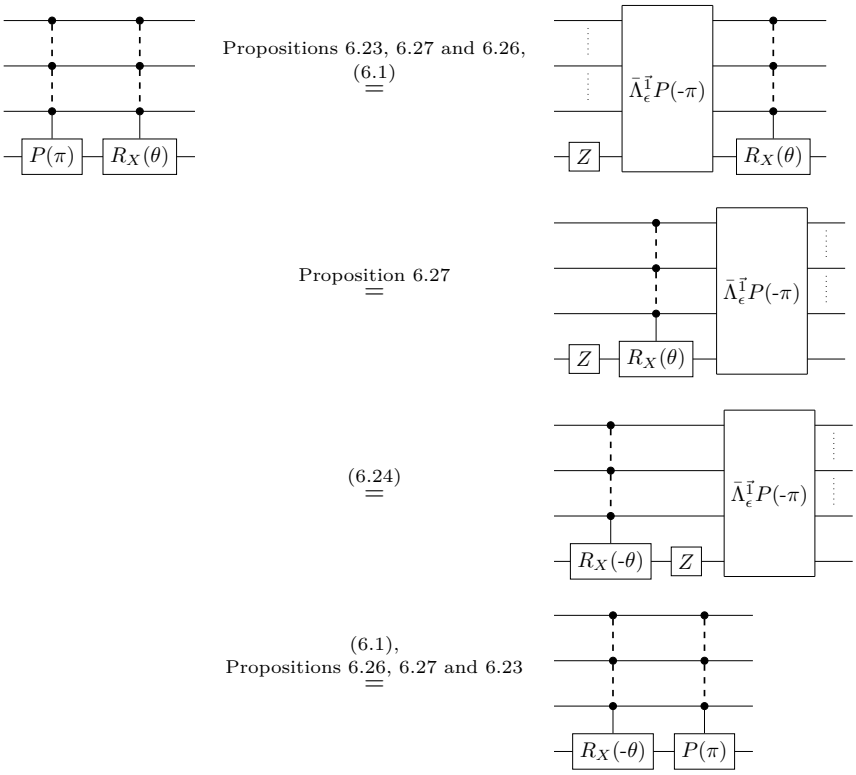


where $\vec{1}$ denotes a list of appropriate length whose elements are all equal to 1. □

Lemma 6.64.



Proof.

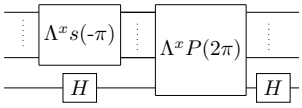


□

Lemma 6.65. *For any $x \in \{0,1\}^k$,*

$$\mathrm{QC} \vdash \Lambda^x R_X(2\pi) = \Lambda^x s(\pi) \otimes —$$

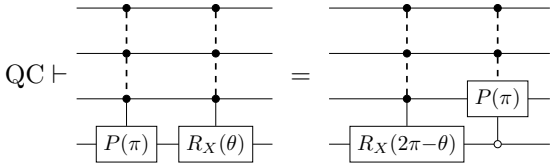
Proof.

$\Lambda^x R_X(2\pi)$ $\overset{\text{(6.10), (6.a), Proposition 6.23 and Lemma 6.15}}{=}$ 

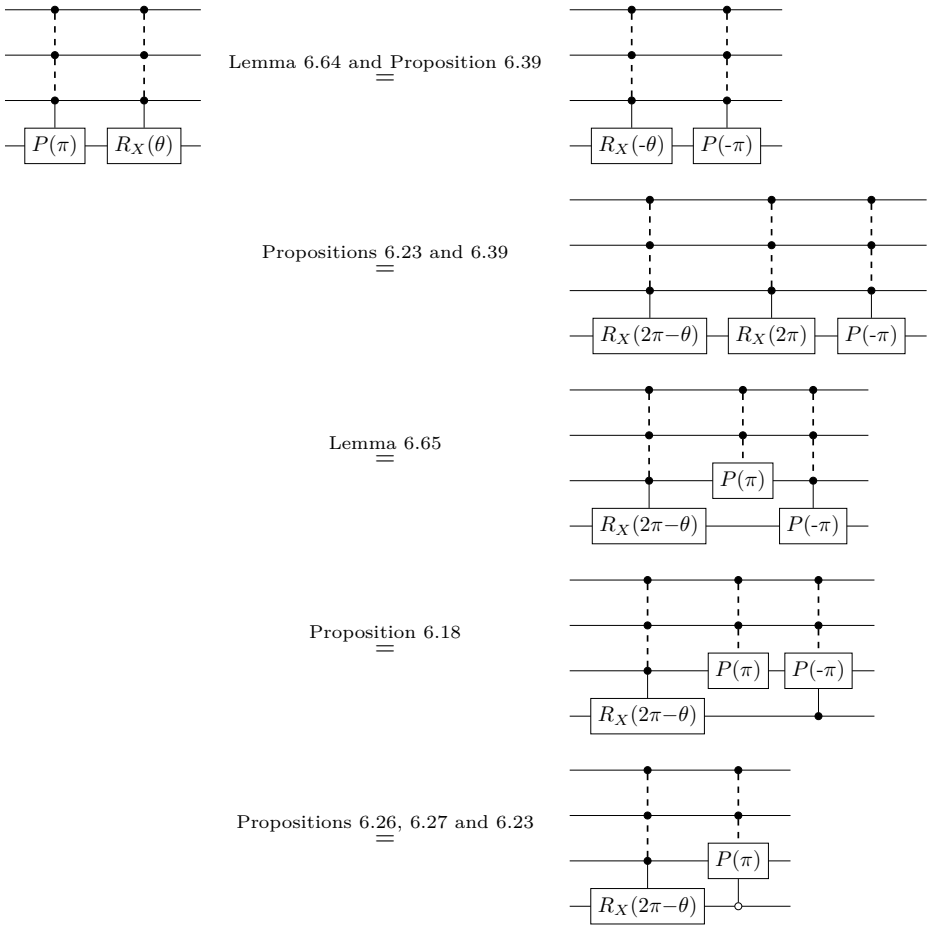
$\overset{\text{Propositions 6.39 and 6.23 and Equation (6.a)}}{=}$ $\Lambda^x s(\pi) \otimes —$

□

Lemma 6.66.



Proof.



Note that in the last step, we have omitted to mention the use of Proposition 6.17 needed to apply Proposition 6.26. In the proof of Lemma 6.61, we will similarly omit it in analogous situations. □

Proof of Lemma 6.61. By Lemma 6.56, to prove Lemma 6.61, it suffices to prove that for each rule of Figure 5.12, of the form $C_1 = C_2$ with $C_1, C_2 \in \mathbf{LO}^{\mathbf{raw}}_{\mathbf{PP}}[i,i]$ (see Footnote 47), and any 2^n-mode raw context $\mathcal{C}[\cdot]_i$, one has QC $\vdash D(\mathcal{C}[C_1]) = D(\mathcal{C}[C_2])$. For this purpose, we prove a slightly more general result, namely that for any k, n and any ℓ-mode raw context $\mathcal{C}[\cdot]_i$ with $k + \ell \leq 2^n$, one has QC $\vdash D_{k,n}(\mathcal{C}[C_1]) = D_{k,n}(\mathcal{C}[C_2])$. We proceed by induction on $\mathcal{C}[\cdot]_i$:

- If $\mathcal{C}[\cdot]_i = C \circ \mathcal{C}'[\cdot]_i$, then $D_{k,n}(\mathcal{C}[C_1]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_1])$ and $D_{k,n}(\mathcal{C}[C_2]) = D_{k,n}(C) \circ D_{k,n}(\mathcal{C}'[C_2])$, so the result follows by induction hypothesis. The case $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \circ C$ is similar.
- If $\mathcal{C}[\cdot]_i = C \oplus \mathcal{C}'[\cdot]_i$ with $C : \ell_1 \to \ell_1$, then $D_{k,n}(\mathcal{C}[C_1]) = D_{k+\ell_1,n}(\mathcal{C}'[C_1]) \circ D_{k,n}(C)$ and $D_{k,n}(\mathcal{C}[C_2]) = D_{k+\ell_1,n}(\mathcal{C}'[C_2]) \circ D_{k,n}(C)$, so the result follows by induction hypothesis. The case $\mathcal{C}[\cdot]_i = \mathcal{C}'[\cdot]_i \oplus C$ is similar.

It remains to prove for each rule of Figure 5.12, of the form $C_1 = C_2$ with $C_1, C_2 \in \mathbf{LO}^{\mathbf{raw}}_{\mathbf{PP}}[i,i]$, that for any k, n with $k + i \leq 2^n$, one has QC $\vdash D_{k,n}(C_1) = D_{k,n}(C_2)$. Again by Lemma 6.56, it suffices to prove that QC $\vdash D_{k,n}(C_1') = D_{k,n}(C_2')$ for arbitrary C_1' and C_2' such that $C_1' \equiv C_1$ and $C_2' \equiv C_2$.

For Equation (5.A), one has $D_{k,n}(-\boxed{0}-) = \Lambda^{G_n(k)} s(0)$, $D_{k,n}(-\boxed{2\pi}-) = \Lambda^{G_n(k)} s(2\pi)$ and $D_{k,n}(-) = id_n$. The three are equal modulo QC by Propositions 6.23 and 6.39.

For Equation (5.B), one has $D_{k,n}(\supset\!\overset{0}{\bullet}\subset) = \Lambda^{x_{k,n}}_{y_{k,n}} R_X(0)$ (where $x_{k,n}$ and $y_{k,n}$ are defined in Definition 6.45) and $D_{k,n}(\cap) = id_n \circ id_n \equiv id_n$. The two are equal modulo QC by Proposition 6.23.

For Equation (5.C), one has $D_{k,n}(\times) = \Lambda^{x_{k,n}}_{y_{k,n}} X$, and $D_{k,n}(\supset\!\overset{\frac{\pi}{2}}{\bullet}\subset\!\begin{smallmatrix}\boxed{-\frac{\pi}{2}}\\ \boxed{-\frac{\pi}{2}}\end{smallmatrix}) = \left(\prod_{j\in\{k,k+1\}} \Lambda^{G_n(j)} s(-\tfrac{\pi}{2})\right) \circ \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-\pi)$. Note that the definitions and the properties of Gray codes imply that

$$\{G_n(k), G_n(k+1)\} = \{x_{k,n}0y_{k,n}, x_{k,n}1y_{k,n}\}. \tag{6.35}$$

Therefore,

$$\begin{aligned}
D_{k,n}(\supset\!\overset{\frac{\pi}{2}}{\bullet}\subset\!\begin{smallmatrix}\boxed{-\frac{\pi}{2}}\\ \boxed{-\frac{\pi}{2}}\end{smallmatrix}) &= \sigma_{1,|x_{k,n}|} \circ \left(\prod_{a\in\{0,1\}} \Lambda^{a x_{k,n} y_{k,n}} s(-\tfrac{\pi}{2})\right) \circ \Lambda^{\epsilon}_{x_{k,n}y_{k,n}} R_X(-\pi) \circ \sigma_{|x_{k,n}|,1} \\
&\overset{\text{Propositions 6.26 and 6.27}}{=} \sigma_{1,|x_{k,n}|} \circ \left(- \otimes \Lambda^{x_{k,n}y_{k,n}} s(-\tfrac{\pi}{2})\right) \circ \Lambda^{\epsilon}_{x_{k,n}y_{k,n}} R_X(-\pi) \circ \sigma_{|x_{k,n}|,1}
\end{aligned}$$

which by Proposition 6.38, Equation (6.28), and Proposition 6.23, is equal modulo QC to $\Lambda^{x_{k,n}}_{y_{k,n}} X$.

For Equation (5.D), one has $D_{k,n}(-\boxed{\varphi_1}\boxed{\varphi_2}-) = \Lambda^{G_n(k)} s(\varphi_2) \circ \Lambda^{G_n(k)} s(\varphi_1)$ and $D_{k,n}(-\boxed{\varphi_1+\varphi_2}-) = \Lambda^{G_n(k)} s(\varphi_1 + \varphi_2)$. Both are equal modulo QC by Proposition 6.23.

For Equation (5.E), one has

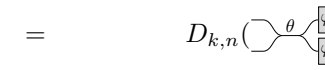
$$\begin{aligned}
D_{k,n}(\begin{smallmatrix}\boxed{\varphi}\\ \boxed{\varphi}\end{smallmatrix}\!\overset{\theta}{\bullet}\subset) &= \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\theta) \circ \left(\prod_{j\in\{k,k+1\}} \Lambda^{G_n(j)} s(\varphi)\right) \\
&\overset{(6.35)}{=} \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\theta) \circ \left(\prod_{a\in\{0,1\}} \Lambda^{x_{k,n} a y_{k,n}} s(\varphi)\right) \\
&= \sigma_{1,|x_{k,n}|} \circ \Lambda^{\epsilon}_{x_{k,n}y_{k,n}} R_X(-2\theta) \circ \left(\prod_{a\in\{0,1\}} \Lambda^{a x_{k,n} y_{k,n}} s(\varphi)\right) \circ \sigma_{|x_{k,n}|,1} \\
&\overset{\text{Propositions 6.26 and 6.27}}{=} \sigma_{1,|x_{k,n}|} \circ \Lambda^{\epsilon}_{x_{k,n}y_{k,n}} R_X(-2\theta) \circ (- \otimes \Lambda^{x_{k,n}y_{k,n}} s(\varphi)) \circ \sigma_{|x_{k,n}|,1}
\end{aligned}$$

$$\overset{\text{Lemma 6.25}}{=} \quad \sigma_{1,|x_{k,n}|} \circ (- \otimes \Lambda^{x_{k,n}y_{k,n}} s(\varphi)) \circ \Lambda^{\epsilon}_{x_{k,n}y_{k,n}} R_X(-2\theta) \circ \sigma_{|x_{k,n}|,1}$$

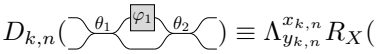
$$\overset{\text{Propositions 6.26 and 6.27}}{=} \quad \sigma_{1,|x_{k,n}|} \circ \left(\prod_{a\in\{0,1\}} \Lambda^{a x_{k,n}y_{k,n}} s(\varphi) \right) \circ \Lambda^{\epsilon}_{x_{k,n}y_{k,n}} R_X(-2\theta) \circ \sigma_{|x_{k,n}|,1}$$

$$= \quad \left(\prod_{a\in\{0,1\}} \Lambda^{x_{k,n}a y_{k,n}} s(\varphi) \right) \circ \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\theta)$$

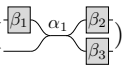
$$\overset{(6.35)}{=} \quad \left(\prod_{j\in\{k,k+1\}} \Lambda^{G_n(j)} s(\varphi) \right) \circ \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\theta)$$

$$= \quad D_{k,n}($$  $$).$$

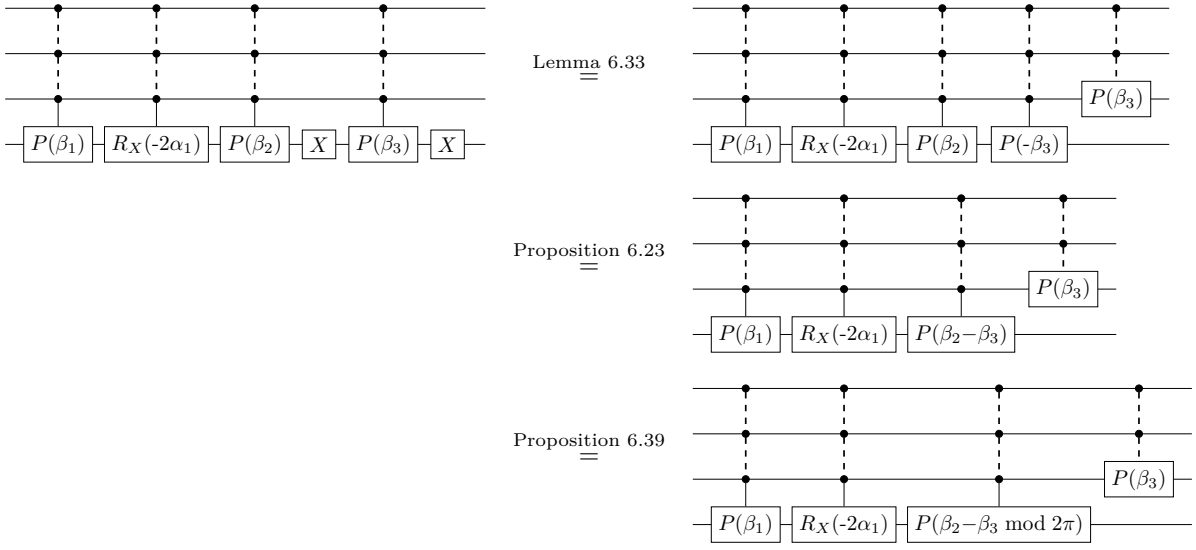
For Equation (5.F), one has

$$D_{k,n}($$  $$) \equiv \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\theta_2) \circ \Lambda^{G_n(k)} s(\varphi_1) \circ \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\theta_1)$$

and

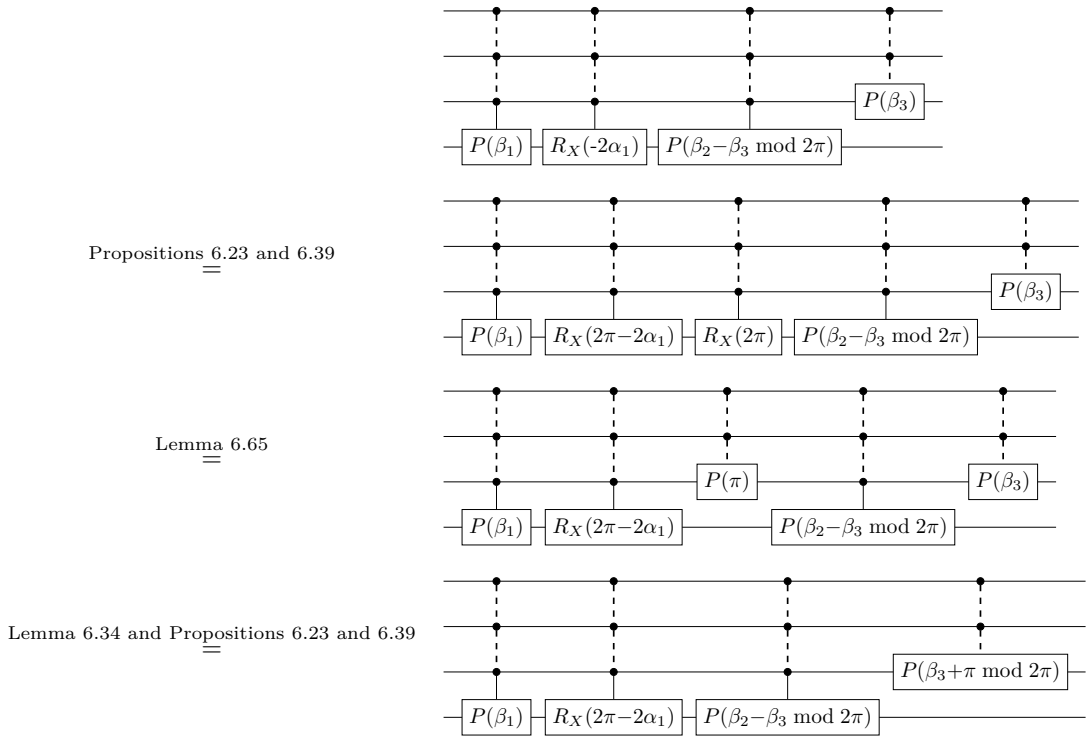
$$D_{k,n}($$  $$) \equiv \Lambda^{G_n(k+1)} s(\beta_3) \circ \Lambda^{G_n(k)} s(\beta_2) \circ \Lambda^{x_{k,n}}_{y_{k,n}} R_X(-2\alpha_1) \circ \Lambda^{G_n(k)} s(\beta_1).$$

Note that for some $a_k \in \{0,1\}$, one has $G_n(k) = x_{k,n}a_k y_{k,n}$ and $G_n(k+1) = x_{k,n}\overline{a}_k y_{k,n}$. Therefore, by Proposition 6.18, for any $\varphi \in \mathbb{R}$, one has $\mathrm{QC} \vdash \Lambda^{G_n(k)} s(\varphi) = \Lambda^{x_{k,n}}_{y_{k,n}} P(\varphi)$ and $\mathrm{QC} \vdash \Lambda^{G_n(k+1)} s(\varphi) = (id_{|x_{k,n}|} \otimes X \otimes id_{|y_{k,n}|}) \circ \Lambda^{x_{k,n}}_{y_{k,n}} P(\varphi) \circ (id_{|x_{k,n}|} \otimes X \otimes id_{|y_{k,n}|})$, or conversely. Thus, up to using Equation (6.10) and possibly Lemma 6.32, it suffices to prove that $\mathrm{QC} \vdash \lambda^{n-1} R_X(-2\theta_2) \circ \lambda^{n-1} P(\varphi_1) \circ \lambda^{n-1} R_X(-2\theta_1) = (id_{n-1} \otimes X) \circ \lambda^{n-1} P(\beta_3) \circ (id_{n-1} \otimes X) \circ \lambda^{n-1} P(\beta_2) \circ \lambda^{n-1} R_X(-2\alpha_1) \circ \lambda^{n-1} P(\beta_1)$. One has



Because of the conditions on the angles in the right-hand side of Equation (5.F), if $\alpha_1 = 0$ then the angles of the last circuit satisfy the conditions so that it matches the right-hand side of Equation (6.34). Hence, since it has the same semantics as $\lambda^{n-1} R_X(-2\theta_2) \circ \lambda^{n-1} P(\varphi_1) \circ \lambda^{n-1} R_X(-2\theta_1)$, both circuits are equal according to Equation (6.34).

If $\alpha_1 \neq 0$, then



Because of the conditions on the angles in the right-hand side of Equation (5.F), one has $\alpha_1 \in (0, \pi)$, so that $2\pi - 2\alpha_1 \in (0, 2\pi)$, and if $2\pi - 2\alpha_1 = \pi$ then $\alpha_1 = \frac{\pi}{2}$, so that $\beta_1 = 0$. Hence, the angles of the last circuit satisfy the conditions so that it matches the right-hand side of Equation (6.34). Again, since it has the same semantics as $\lambda^{n-1}R_X(-2\theta_2) \circ \lambda^{n-1}P(\varphi_1) \circ \lambda^{n-1}R_X(-2\theta_1)$, both circuits are equal according to Equation (6.34).

For Equation (5.G), by the properties of the Gray code, exactly one bit differs between $G_n(k)$ and $G_n(k+1)$, as well as between $G_n(k+1)$ and $G_n(k+2)$, and in exactly one of the two cases this is the last bit that differs (namely between $G_n(k)$ and $G_n(k+1)$ if k is even, and between $G_n(k+1)$ and $G_n(k+2)$ if k is odd). Hence we can write $G_n(k)$ as $xayb$ with $a, b \in \{0, 1\}$, in such a way that $G_n(k+2) = x\bar{a}y\bar{b}$ and $G_n(k+1) = xay\bar{b}$ or $x\bar{a}yb$ depending on the parity of k. We treat the case where k is even, the case with k odd being similar. One has

$$D_{k,n}\left(\begin{array}{c}\theta_1\ \boxed{\varphi_1}\ \theta_3\\ \theta_2\end{array}\right) \equiv \Lambda^{xay}R_X(-2\theta_3) \circ \Lambda^x_{y\bar{b}}R_X(-2\theta_2) \circ \Lambda^{xayb}s(\varphi_1) \circ \Lambda^{xay}R_X(-2\theta_1)$$

and

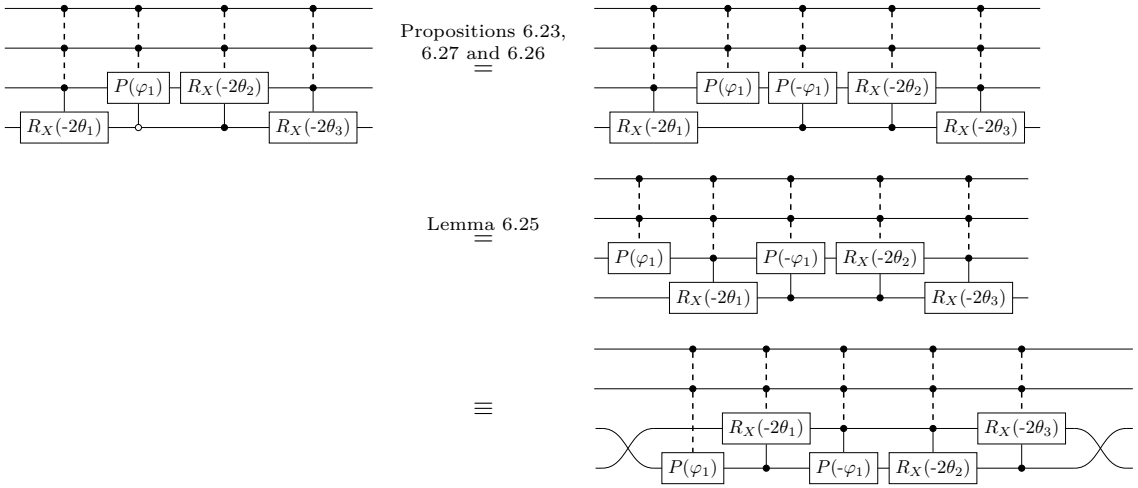
$$D_{k,n}\left(\begin{array}{c}\beta_2\ \ \alpha_2\ \ \beta_4\\ \beta_1\ \alpha_1\ \ \beta_3\ \alpha_3\ \beta_5\\ \beta_6\end{array}\right) \equiv \begin{array}{l}\Lambda^{x\bar{a}y\bar{b}}s(\beta_6) \circ \Lambda^{xay\bar{b}}s(\beta_5) \circ \Lambda^{xayb}s(\beta_4) \circ \Lambda^x_{y\bar{b}}R_X(-2\alpha_3) \circ \Lambda^{xay\bar{b}}s(\beta_3)\\ \circ\Lambda^{xay}R_X(-2\alpha_2) \circ \Lambda^x_{y\bar{b}}R_X(-2\alpha_1) \circ \Lambda^{xayb}s(\beta_2) \circ \Lambda^{xay\bar{b}}s(\beta_1).\end{array}$$

Up to using Equation (6.10), we can assume that the components of x and y are all equal to 1. Up to using additionally Lemma 6.32, we can assume that $a = 1$ and $b = 0$. Finally, up to deforming the circuits and using Proposition 6.17, we can assume that $y = \epsilon$. Thus, it suffices to prove that

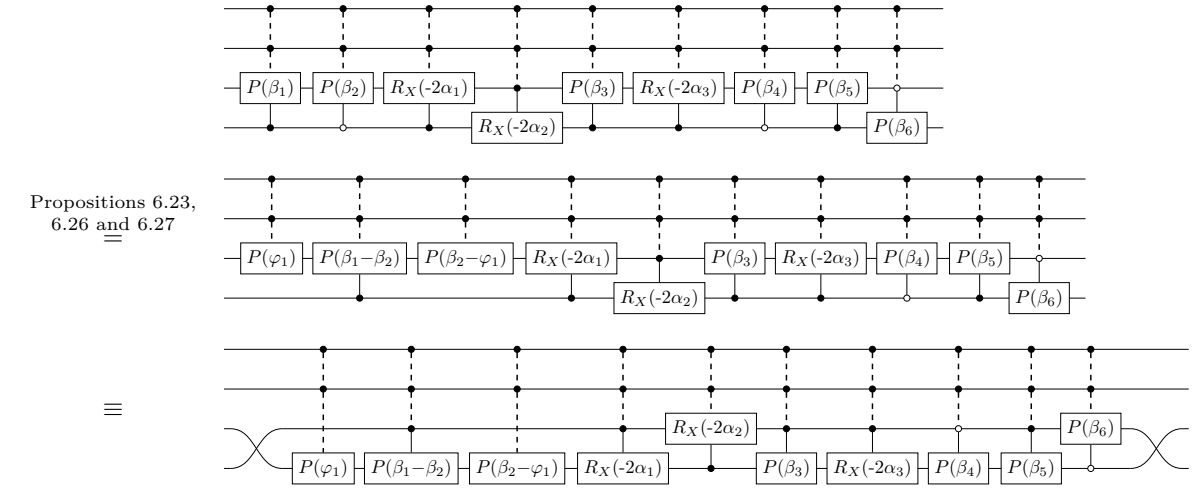
$$\begin{aligned}\mathrm{QC} \vdash \Lambda^{x1}R_X(-2\theta_3) \circ \Lambda^x_1R_X(-2\theta_2) \circ \Lambda^{x10}s(\varphi_1) \circ \Lambda^{x1}R_X(-2\theta_1) = \Lambda^{x01}s(\beta_6) \circ \Lambda^{x11}s(\beta_5) \circ \Lambda^{x10}s(\beta_4)\circ\\ \Lambda^x_1R_X(-2\alpha_3) \circ \Lambda^{x11}s(\beta_3) \circ \Lambda^{x1}R_X(-2\alpha_2) \circ \Lambda^x_1R_X(-2\alpha_1) \circ \Lambda^{x10}s(\beta_2) \circ \Lambda^{x11}s(\beta_1)\end{aligned}$$

where $x = 1^{n-2}$.

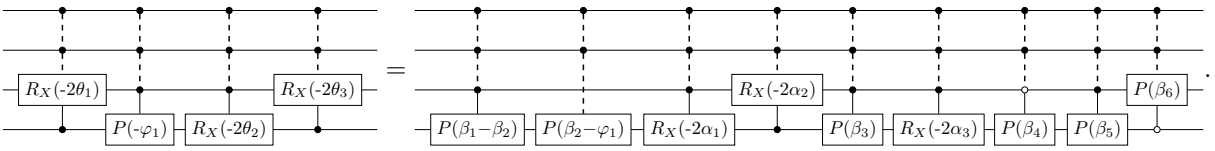
The left-hand side is equal (up to using Proposition 6.18) to



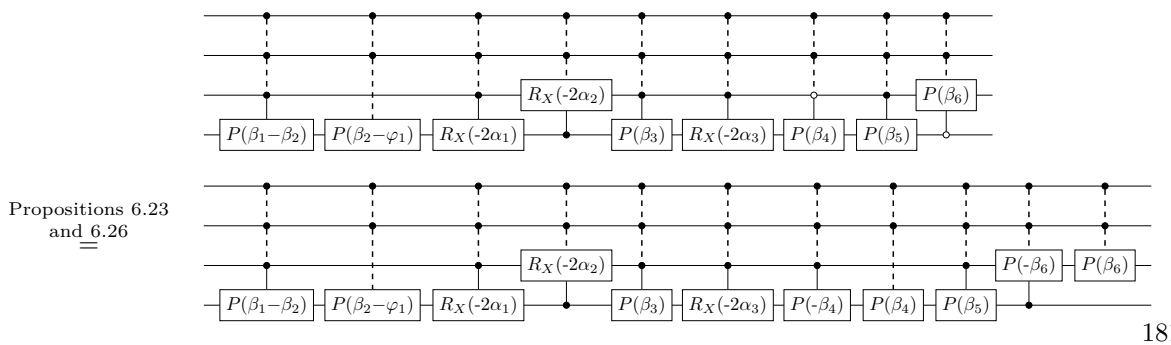
while the right-hand side is equal to



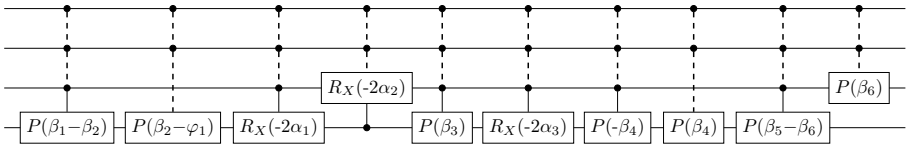
Hence, it suffices to prove that



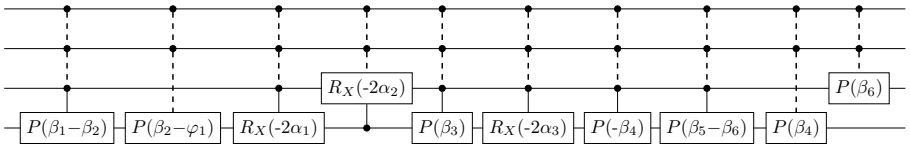
The left-hand side matches the left-hand side of Equation (6.r), hence it suffices to prove that the right-hand side can be put in the form of the right-hand side of Equation (6.r) with the angles satisfying the conditions. One has



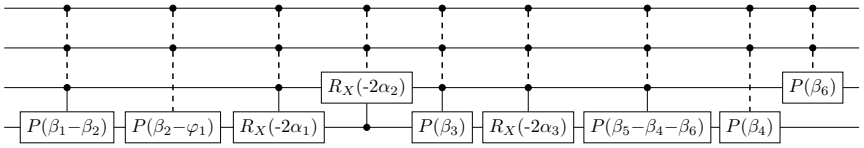
Propositions 6.18 and 6.23 =



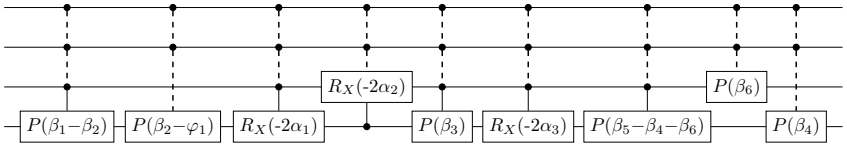
Propositions 6.23, 6.26 and 6.27 =



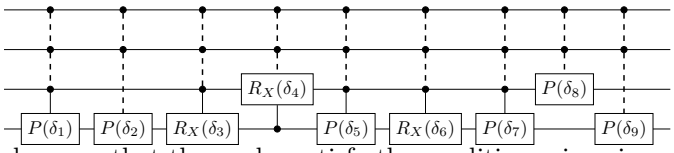
Proposition 6.23 =



Propositions 6.18, 6.23, 6.26 and 6.27 =



It remains to prove that any circuit of the form

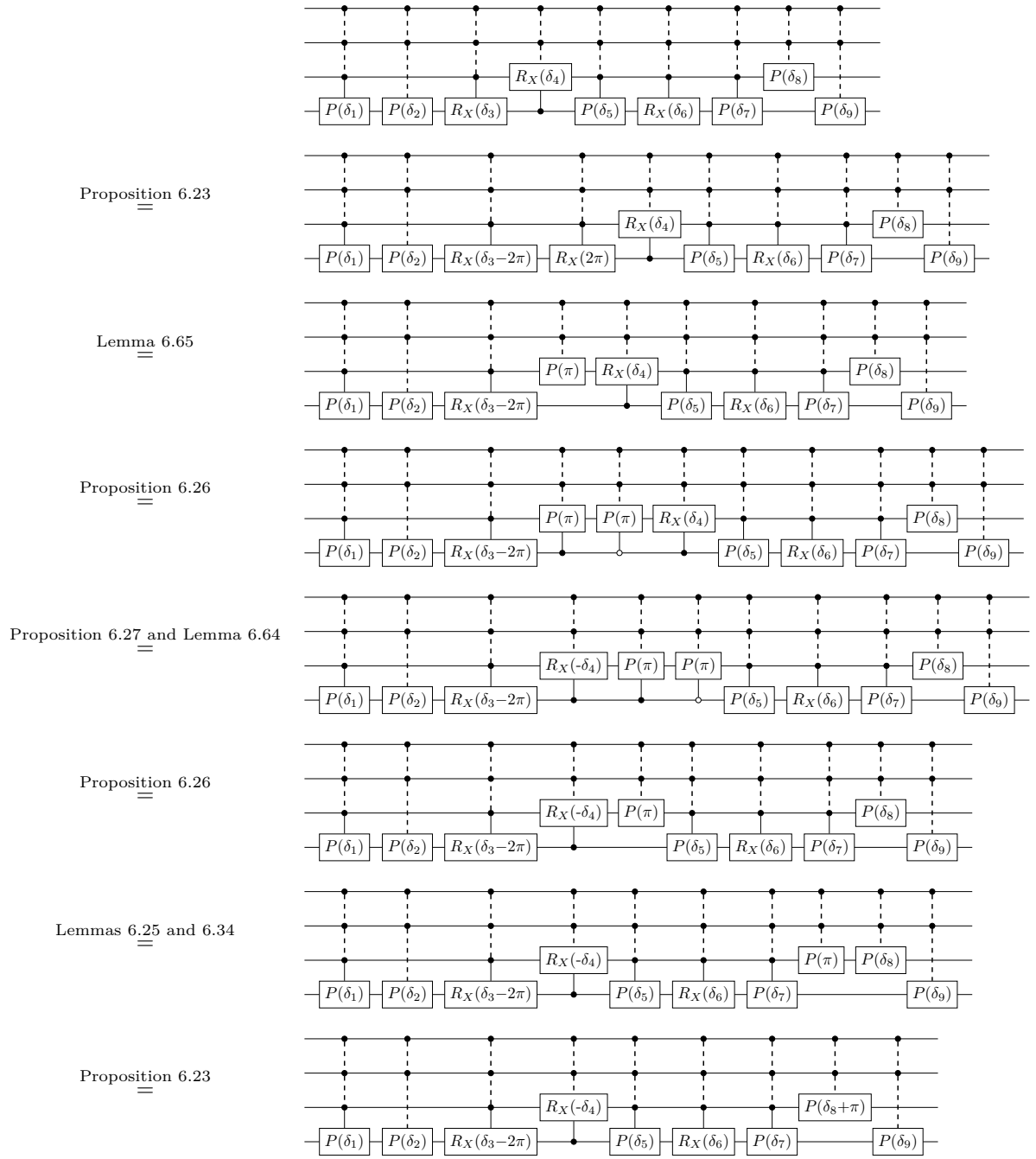


can be transformed using the axioms of QC in such a way that the angles satisfy the conditions given in Figure 6.4. We treat the conditions in the following order (note that some of the conditions of Figure 6.4 have been split into two parts):

- $\delta_3 \in [0, 2\pi)$
- $\delta_4 \in [0, 2\pi)$
- $\delta_6 \in [0, 2\pi)$
- if $\delta_3 = 0$ then $\delta_2 = 0$
- if $\delta_3 \neq 0$ but $\delta_4 = \pi$ then $\delta_2 = 0$
- if $\delta_3 = 0$ and $\delta_4 = \pi$ then $\delta_1 = 0$
- if $\delta_3 = \pi$ then $\delta_1 = 0$
- if $\delta_4 = 0$ then $\delta_1 = \delta_2 = \delta_3 = 0$
- if $\delta_3 \neq 0$ then $\delta_1 \in [0, \pi)$
- if $\delta_3 = 0$ then $\delta_1 \in [0, \pi)$
- if $\delta_6 = 0$ then $\delta_5 = 0$
- if $\delta_6 = \pi$ then $\delta_5 = 0$
- $\delta_2 \in [0, \pi)$
- $\delta_5 \in [0, \pi)$
- $\delta_7, \delta_8, \delta_9 \in [0, 2\pi)$.

For each of them, we prove that given a circuit satisfying the previous conditions, we can transform it into a circuit satisfying also the considered condition, which implies that this condition can be assumed without loss of generality.

If $\delta_3 \notin [0, 2\pi)$, then by Proposition 6.39, we can assume that it is in $[0, 4\pi)$, and then if it is in $[2\pi, 4\pi)$, then:



with $\delta_3 - 2\pi \in [0, 2\pi)$. Hence, we can assume that $\delta_3 \in [0, 2\pi)$.

The other conditions are treated in a similar way in Appendix D.2. □

6.2.4.4 Completeness Proof

We are now ready to prove the main result of this chapter.

Theorem 6.67 (Quantum circuit completeness)**.** QC *is a complete equational theory for quantum circuits: for any quantum circuits* C_1, C_2, *if* $[\![C_1]\!] = [\![C_2]\!]$ *then* $\mathrm{QC} \vdash C_1 = C_2$.

Proof. Given two quantum circuits C_1, C_2 s.t. $[\![C_1]\!] = [\![C_2]\!]$, let C_1' (resp. C_2') be a raw quantum circuit, representative of C_1 (resp. C_2). Thanks to Proposition 6.44 we have $[\![E(C_1')]\!]_{\mathrm{pp}} = [\![E(C_2')]\!]_{\mathrm{pp}}$. The completeness of $\mathrm{LO}_{\mathrm{PP}}$ implies $\mathrm{LO}_{\mathrm{PP}} \vdash E(C_1') = E(C_2')$. By Lemma 6.61, we have $\mathrm{QC} \vdash D(E(C_1')) = D(E(C_2'))$. Moreover Lemma 6.49 implies $\mathrm{QC} \vdash C_1' = C_2'$. From this derivation we obtain a derivation of $\mathrm{QC} \vdash C_1 = C_2$, where the steps corresponding to the equivalence relation $\equiv$ are trivialised. □

Chapter 7

Coherent Control and Distinguishability of Quantum Channels via PBS-Diagrams

General quantum evolutions — a.k.a. quantum channels — are commonly represented as completely positive trace-preserving (CPTP) maps. CPTP maps can naturally be composed in sequence and in parallel. However, it has been realised that the description of quantum channels in terms of CPTP maps is not appropriate for some particular setups involving coherent control [107, 4, 35, 97]. One indeed needs some more information about their practical implementation to unambiguously determine the behaviour of such setups, and it was proposed to complete the description of channels by so-called transformation matrices [4], or vacuum extensions [35, 97].

In this chapter, we come back to the coherent control point of view of PBS-diagrams (that is, to the approach of using diagrams primarily as an abstract tool for representing coherently controlled processes, as opposite to the linear optical point of view adopted in Chapter 5), and study how they can be used to coherently control quantum channels. We build upon the language of Chapter 3, and extend it to allow for the control of more general quantum channels. As the description of channels as CPTP maps is inadequate here, we propose to work with *purified channels* based on a unitary extension of Stinespring's dilation [124].

We address the question of the observational equivalence of purified channels. To do so, we use PBS-diagrams to formalise three kinds of *contexts*: when the context is PBS-free, we recover that two purified channels are indistinguishable if and only if they lead to the same CPTP map. When the context allows for PBS but no negations, we recover the characterisation in terms of superoperators and transformation matrices which was introduced for a particular setup [4]. When we allow for arbitrary contexts, we obtain a characterisation of observational equivalence involving "second-level" superoperators and transformation matrices. We finally open the discussion to more general coherent-control settings, and propose a refined equivalence relation as a candidate for characterising channel (in)distinguishability in such scenarios.

7.1 PBS-Diagrams

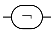
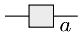
PBS-diagrams were introduced in Chapter 3 as a language for coherent control of "pure" quantum evolutions. They can be seen as describing practical scenarios where a flying particle goes through an experimental setup, and is routed via polarising beam splitters. In addition to its polarisation, the particle carries some "data" register, whose state is described in some Hilbert space $\mathcal{H}$, and on which a number of "pure" linear (typically, unitary) operators are applied.

Here we shall enrich the pure PBS-diagram language so as to incorporate the coherent control of more general quantum channels. To this purpose, we start by defining an abstract version of PBS-diagrams that we call *bare diagrams*, and which we equip with a word path semantics describing the trajectory and

change of polarisation of a particle that enters the diagram through some given input wire: the word path semantics gives its new polarisation and position at the output of the diagram, together with a word over some alphabet describing the sequence of *bare gates* — where the quantum channels we want to control are located — crossed. Subscribing to the idea that any general quantum operation can be seen as a unitary evolution of the system under consideration and its environment, we then define *purified channels*, which can be coherently controlled in a similar way to the PBS-diagrams of Chapter 3. Replacing bare gates with purified channels, we obtain an extension[50] of the graphical language of Chapter 3, which we call *extended* PBS-*diagrams* and which we equip with a quantum semantics obtained after discarding the (inaccessible) environments of all gates.

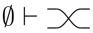
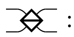
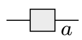
7.1.1 Bare PBS-Diagrams

7.1.1.1 Syntax

The traced PROP of bare PBS-diagrams is generated by polarising beam splitters  , polarisation flips  , and bare gates  . Every bare gate is indexed by a unique label (here, a) used to identify the gate in the diagram. In other word, a bare PBS-diagram is a $\mathcal{G}^*$-diagram (as of Section 4.1) where all wires are black and whose gates bear pairwise distinct, single-letter labels.

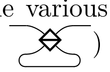
We define bare PBS-diagrams by a typing judgement $\Gamma \vdash D : n$, where Γ is the alphabet containing all gate indices of the diagram,[51] to guarantee that the diagrams are well-formed — in particular, that the gate indices are unique — using a linear typing discipline:

Definition 7.1 (Bare PBS-diagram)**.** *A bare* PBS-*diagram* $\Gamma \vdash D : n$ *(with* $n \in \mathbb{N}$*) is inductively defined as:*

$\emptyset \vdash$  $: 0$ $\quad \emptyset \vdash — : 1$ $\quad \emptyset \vdash$  $: 1$ $\quad \emptyset \vdash$  $: 2$ $\quad \emptyset \vdash$  $: 2$ $\quad \{a\} \vdash$  $: 1$

$$\frac{\Gamma_1 \vdash D_1 : n \quad \Gamma_2 \vdash D_2 : n \quad \Gamma_1 \cap \Gamma_2 = \emptyset}{\Gamma_1 \cup \Gamma_2 \vdash D_2 \circ D_1 : n} \qquad \frac{\Gamma_1 \vdash D_1 : n_1 \quad \Gamma_2 \vdash D_2 : n_2 \quad \Gamma_1 \cap \Gamma_2 = \emptyset}{\Gamma_1 \cup \Gamma_2 \vdash D_1 \oplus D_2 : n_1 + n_2} \qquad \frac{\Gamma \vdash D : n+1}{\Gamma \vdash Tr(D) : n}$$

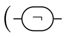
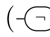
Examples of bare PBS-diagrams are given in Figure 7.1 below.

As original PBS-diagrams, bare PBS-diagrams have a structure of traced PROP[52] and therefore are defined up to deformation. Note in particular that the length of the wires does not matter. Physically, if these diagrams were to be realised in practical setups, this would mean that the experiment should be insensible to the time at which the particle would go through the various elements; if needed one could always add (possibly polarisation-dependent) delay lines (e.g. ) to correct for a possible time mismatch between different paths.

7.1.1.2 Word Path Semantics

The word path semantics of a bare PBS-diagram $\Gamma \vdash D : n$ describes the trajectory of a particle which enters it with a polarisation in the standard basis state $c \in \{\mathbf{V}, \mathbf{H}\}$ (vertical or horizontal) and from a definite position $p \in [n] := \{0, \ldots, n-1\}$. It is identical to its path semantics when seen as a Γ^*-diagram:

Definition 7.2 (Word path semantics)**.** *Given a bare* PBS-*diagram* $\Gamma \vdash D : n$*, a polarisation* $c \in \{\mathbf{V}, \mathbf{H}\}$ *and a position* $p \in [n]$*, let* $(D, c, p) \overset{w}{\Rightarrow} (c', p')$ *with* $w \in \Gamma^*$ *a word over* Γ *(or just* $(D, c, p) \Rightarrow (c', p')$ *for the empty word* $w = \epsilon$*) be inductively defined as follows:*

$(—, c, 0) \Rightarrow (c, 0)$ $\qquad$ ( $, \mathbf{H}, 0) \Rightarrow (\mathbf{V}, 0)$ $\qquad$ ( $, \mathbf{V}, 0) \Rightarrow (\mathbf{H}, 0)$

[50] Strictly speaking, the PBS-diagrams of Chapter 3 did not require the operations inside the gates to be unitary, while here we impose such a restriction *a priori*. One could however also consider non-unitary operations in our framework here, although one would lose our motivation based on the unitary extension of Stinespring's dilation.

[51] We may write simply $D : n$, or even just D, when Γ is not relevant or is clear from the context. Note that we write $D : n$ instead of $D : n \to n$ in order to lighten the notation, since all diagrams considered in this chapter have their input and output types equal.

[52] They do not strictly speaking form a traced PROP, since they cannot be freely composed in sequence or in parallel, but they are contained in a traced PROP.

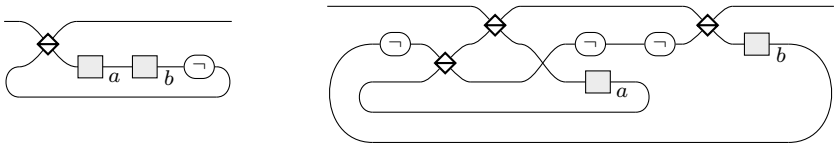


Figure 7.1: Two examples of bare PBS-diagrams, with the same word path semantics: $(D, \mathbf{H}, 0) \overset{abab}{\Longrightarrow} (\mathbf{H}, 0)$ and $(D, \mathbf{V}, 0) \overset{\epsilon}{\Rightarrow} (\mathbf{V}, 0)$.

$$(\times,\ c,\ p) \Rightarrow (c, 1-p) \qquad (\mathbf{V},\ \mathbf{V}, p) \Rightarrow (\mathbf{V}, p) \qquad (\mathbf{H},\ \mathbf{H}, p) \Rightarrow (\mathbf{H}, 1-p)$$

$$(-\boxed{a}-, c, 0) \overset{a}{\Rightarrow} (c, 0) \qquad \frac{(D_1, c, p) \overset{w_1}{\Longrightarrow} (c', p') \qquad (D_2, c', p') \overset{w_2}{\Longrightarrow} (c'', p'')}{(D_2 \circ D_1, c, p) \overset{w_1 w_2}{\Longrightarrow} (c'', p'')} (\circ)$$

$$\frac{D_1 : n_1 \quad p < n_1 \quad (D_1, c, p) \overset{w}{\Rightarrow} (c', p')}{(D_1 \oplus D_2, c, p) \overset{w}{\Rightarrow} (c', p')} (\oplus_1) \qquad \frac{D_1 : n_1 \quad p \geq n_1 \quad (D_2, c, p-n_1) \overset{w}{\Rightarrow} (c', p')}{(D_1 \oplus D_2, c, p) \overset{w}{\Rightarrow} (c', p'+n)} (\oplus_2)$$

$$\frac{D : n+1 \qquad \forall i \in \{0, \ldots, k\}, (D, c_i, p_i) \overset{w_i}{\Longrightarrow} (c_{i+1}, p_{i+1})}{(Tr(D), c_0, p_0) \overset{w_0 \cdots w_k}{\Longrightarrow} (c_{k+1}, p_{k+1})} (\mathsf{T}_k)$$

with $p_0, p_{k+1} < n$, $\forall i \in \{1, ..., k\}, p_i = n$, *and* $k \in \{0, 1, 2\}$.

We denote by $w^D_{c,p} \in \Gamma^*$ *the word,* $c^D_{c,p} \in \{\mathbf{H}, \mathbf{V}\}$ *the polarisation, and* $p^D_{c,p} \in [n]$ *the position s.t.* $(D, c, p) \overset{w^D_{c,p}}{\Longrightarrow} (c^D_{c,p}, p^D_{c,p})$.

As before, the word path semantics is invariant modulo structural congruence (i.e. diagram deformation), and a particle cannot go through a feedback loop (or any other part of the diagram) twice with the same polarisation, which justifies that the word path semantics is well-defined even with k going only up to 2 in Rule (T_k) above. The formal proofs of these facts are similar to those given for the pure PBS-diagram language (see the proof of Propositions 3.6 and 3.7), and the intuition is the same: if a particle goes twice in a feedback loop with the same polarisation then it will loop forever; but because of time symmetry this also means that the particle went though the feedback loop infinitely many times in the past, which contradicts the fact that it entered through an input wire.

For similar reasons, each gate cannot appear more than twice along any path, or even in the family of all the possible paths of a diagram. The formalism of bare PBS-diagrams is particularly well-suited to formally express this property:

Proposition 7.3. *Given a bare* PBS*-diagram* $\Gamma \vdash D : n$, $\forall a \in \Gamma$, *one has* $\sum_{c \in \{\mathbf{V}, \mathbf{H}\}, p \in [n]} |w^D_{c,p}|_a \leq 2$, *where* $|w|_a$ *denotes the number of occurrences of* a *in the word* w. *Moreover, if* D *is* $-\!\!\ominus\!\!-$*-free then for any* c *one has* $\sum_{p \in [n]} |w^D_{c,p}|_a \leq 1$.

Proof. We proceed by stuctural induction on D.

- If $D = \boxdot, -, -\!\!\ominus\!\!-, \times$ or $\mathbf{V}\!\!\mathbf{H}$, then the sums are equal to 0 (they are in particular empty for $D = \boxdot$), so the result is trivially true.
- If $D = -\boxed{a}-$, then one has $w^D_{\mathbf{V},0} = w^D_{\mathbf{H},0} = a$, so the result holds.
- If $D = D_2 \circ D_1$ with $\Gamma_1 \vdash D_1 : n, \Gamma_2 \vdash D_2 : n, \Gamma_1 \cap \Gamma_2 = \emptyset$, then

$$\sum_{\substack{c \in \{\mathbf{V}, \mathbf{H}\} \\ p \in [n]}} |w^D_{c,p}|_a \quad = \quad \sum_{\substack{c \in \{\mathbf{V}, \mathbf{H}\} \\ p \in [n]}} \left| w^{D_1}_{c,p} w^{D_2}_{c^{D_1}_{c,p}, p^{D_1}_{c,p}} \right|_a \quad = \quad \sum_{\substack{c \in \{\mathbf{V}, \mathbf{H}\} \\ p \in [n]}} |w^{D_1}_{c,p}|_a + \sum_{\substack{c \in \{\mathbf{V}, \mathbf{H}\} \\ p \in [n]}} \left| w^{D_2}_{c^{D_1}_{c,p}, p^{D_1}_{c,p}} \right|_a .$$

Since the map $(c,p) \mapsto (c^{D_1}_{c,p}, p^{D_1}_{c,p})$ is a bijection, the sum above is equal to

$$\sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n]}} |w^{D_1}_{c,p}|_a + \sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n]}} |w^{D_2}_{c,p}|_a \,.$$

Since D_1 and D_2 have disjoint alphabets Γ_1 and Γ_2, at least one of the two sums is equal to 0, and by induction hypothesis, the other one is no greater than 2.

Moreover, if D is -⃝¬-free then for any $c \in \{\mathbf{V},\mathbf{H}\}$,

$$\sum_{p\in[n]} |w^{D}_{c,p}|_a = \sum_{p\in[n]} |w^{D_1}_{c,p}|_a + \sum_{p\in[n]} \left| w^{D_2}_{c^{D_1}_{c,p}, p^{D_1}_{c,p}} \right|_a \,.$$

It is easy to see that since D_1 is -⃝¬-free, it cannot change the polarisation so that $c^{D_1}_{c,p} = c$. Moreover, the map $(c,p) \mapsto (c, p^{D_1}_{c,p})$ is again a bijection, so that the sum above is equal to

$$\sum_{p\in[n]} |w^{D_1}_{c,p}|_a + \sum_{p\in[n]} |w^{D_2}_{c,p}|_a \,.$$

Since D_1 and D_2 have disjoint alphabets, at least one of the two sums is equal to 0, and by induction hypothesis, the other one is no greater than 1.

- If $D = D_1 \oplus D_2$ with $\Gamma_1 \vdash D_1 : n_1, \Gamma_2 \vdash D_2 : n_2$ such that $n_1 + n_2 = n, \Gamma_1 \cap \Gamma_2 = \emptyset$, then

$$\sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n]}} |w^{D}_{c,p}|_a \;=\; \sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n_1]}} |w^{D}_{c,p}|_a + \sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ n_1\le p<n}} |w^{D}_{c,p}|_a \;=\; \sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n_1]}} |w^{D_1}_{c,p}|_a + \sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n_2]}} |w^{D_2}_{c,p}|_a \,.$$

Since D_1 and D_2 have disjoint alphabets Γ_1 and Γ_2, at least one of the two sums is equal to 0, and by induction hypothesis, the other one is no greater than 2.

Moreover, if D is -⃝¬-free then similarly, for any $c \in \{\mathbf{V},\mathbf{H}\}$,

$$\sum_{p\in[n]} |w^{D}_{c,p}|_a = \sum_{p\in[n_1]} |w^{D_1}_{c,p}|_a + \sum_{p\in[n_2]} |w^{D_2}_{c,p}|_a \,.$$

Since D_1 and D_2 have disjoint alphabets, at least one of the two sums is equal to 0, and by induction hypothesis, the other one is no greater than 1.

- If $D = Tr(D')$ with $D' : n+1$, then for any $c \in \{\mathbf{V},\mathbf{H}\}$ and any $p \in [n]$,[53] the couple $(c^D_{c,p}, p^D_{c,p})$ is the unique couple such that there exists a sequence of arrows $(D', c, p) \overset{w_0}{\Longrightarrow} (c_1, n)$, $(D', c_1, n) \overset{w_1}{\Longrightarrow} (c_2, n), \ldots, (D', c_{k-1}, n) \overset{w_{k-1}}{\Longrightarrow} (c_k, n)$, $(D', c_k, n) \overset{w_k}{\Longrightarrow} (c^D_{c,p}, p^D_{c,p})$ (we additionally know that $k \le 2$, although this does not change the proof). Given such a sequence, one has $|w^D_{c,p}|_a = |w^{D'}_{c,p}|_a + |w^{D'}_{c_1,n}|_a + \cdots + |w^{D'}_{c_k,n}|_a$.

Since the map $(c',p') \mapsto (c^{D'}_{c',p'}, p^{D'}_{c',p'})$ is a bijection, a given couple (c',p'), now with $p' \in [n+1]$, cannot appear more than once on the left of an arrow (i.e. as a polarisation and position configuration entering the diagram D') among the family of all possible such sequences. In particular for $p' = n$, it follows that the sum of all partial sums $|w^{D'}_{c_1,n}|_a + \cdots + |w^{D'}_{c_k,n}|_a$ above, for all possible sequences (i.e. for all starting configurations c, p), is upper-bounded by $\sum_{c\in\{\mathbf{V},\mathbf{H}\}} |w^{D'}_{c,n}|_a$. Therefore,

$$\sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n]}} |w^{D}_{c,p}|_a \le \sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n]}} |w^{D'}_{c,p}|_a + \sum_{c\in\{\mathbf{V},\mathbf{H}\}} |w^{D'}_{c,n}|_a = \sum_{\substack{c\in\{\mathbf{V},\mathbf{H}\}\\ p\in[n+1]}} |w^{D'}_{c,p}|_a$$

[53] The argument that follows applies to $n \ge 1$; for $n = 0$ the sums are again empty (as in the case of $D =$ ⃞), so that the result trivially holds.

which, by induction hypothesis, is no greater than 2.

Moreover, if D is -⊖-free then since the polarisation cannot change, one can proceed in the same way for each of the two polarisations $\mathbf{V}$ and $\mathbf{H}$ separately. We similarly get that for any $c \in \{\mathbf{V}, \mathbf{H}\}$,

$$\sum_{p\in[n]} |w^D_{c,p}|_a \leq \sum_{p\in[n+1]} |w^{D'}_{c,p}|_a$$

which, by induction hypothesis, is no greater than 1. □

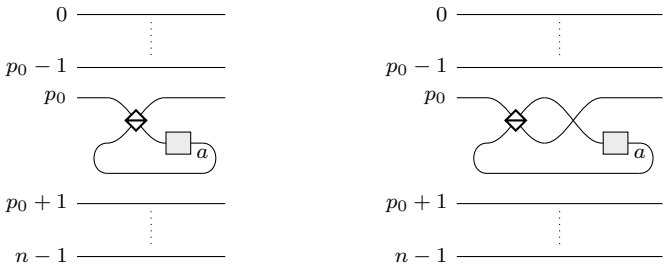
The converse of Proposition 7.3 is also true:

Proposition 7.4. *For any family of words $\{w_{c,p}\}_{(c,p)\in\{\mathbf{V},\mathbf{H}\}\times[n]}$ such that every letter appears at most twice in the whole family, there exists a bare* PBS*-diagram $D : n$ such that $w_{c,p} = w^D_{c,p}$ for all c, p. Furthermore, if for any $c \in \{\mathbf{V}, \mathbf{H}\}$, every letter appears at most once in $\{w_{c,p}\}_{p\in[n]}$, the bare* PBS*-diagram D can be chosen -⊖-free.*

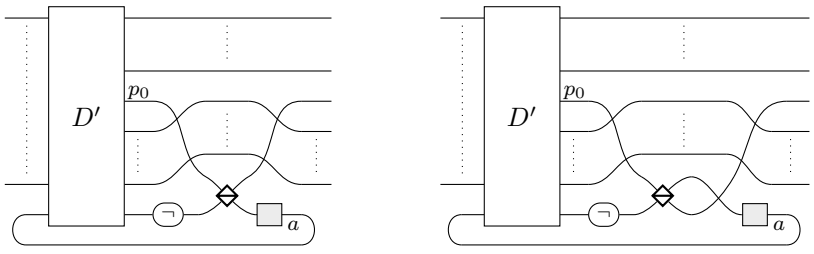
Proof. We prove by induction on $\sum_{c,p} |w_{c,p}|$ (where $|w|$ denotes the length of the word w) that there exists D such that $(D, c, p) \xRightarrow{w_{c,p}} (c, p)$, which ensures the proposition.

We say that such a diagram realises the family $W = \{w_{c,p}\}_{(c,p)\in\{\mathbf{V},\mathbf{H}\}\times[n]}$.

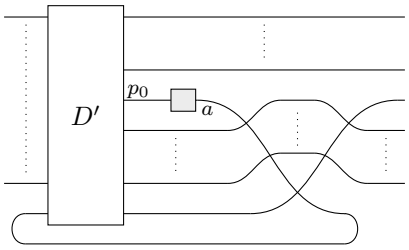
- If $\sum_{c,p} |w_{c,p}| = 0$, the identity diagram $—^{\oplus n}$ gives $(—^{\oplus n}, c, p) \Rightarrow (c, p)$, and therefore realises the family $W = \{w_{c,p} = \epsilon\}_{(c,p)\in\{\mathbf{V},\mathbf{H}\}\times[n]}$ (the only one satisfying $\sum_{c,p} |w_{c,p}| = 0$).
- If $W = \{w_{c,p}\}_{(c,p)\in\{\mathbf{V},\mathbf{H}\}\times[n]}$ is such that $w_{c_0,p_0} = a$ for some (c_0, p_0) and some label a, and $w_{c,p}$ is the empty word otherwise (i.e. if $\sum_{c,p} |w_{c,p}| = 1$), then the following diagrams realise W when $c_0 = \mathbf{H}$ and $c_0 = \mathbf{V}$, respectively:



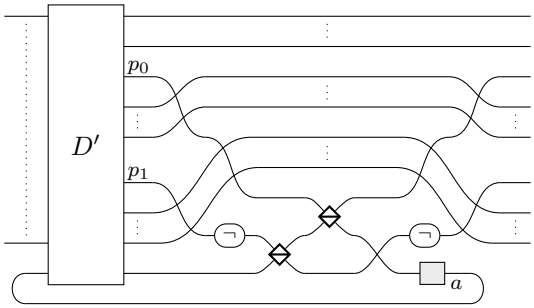
- For any family $W = \{w_{c,p}\}_{(c,p)\in\{\mathbf{V},\mathbf{H}\}\times[n]}$ with at least one nonempty word (i.e. with $\sum_{c,p} |w_{c,p}| \geq 1$) such that every letter appears at most twice in the whole family, consider a nonempty w_{c_0,p_0}. It can be written in the form ua with $|a| = 1$:
  - If $\sum_{c,p} |w_{c,p}|_a = 1$, then composing a diagram D' realising $W' = \{w'_{c,p}\}_{(c,p)\in\{\mathbf{V},\mathbf{H}\}\times[n]}$ where $w'_{c_0,p_0} = u$ and $w'_{c,p} = w_{c,p}$ otherwise (which exists by induction) with a diagram D_a realising (as in the previous case) $W'' = \{w''_{c,p}\}_{(c,p)\in\{\mathbf{V},\mathbf{H}\}\times[n]}$ such that $w''_{c_0,p_0} = a$ and $w''_{c,p}$ is the empty word otherwise, allows one to realise W.
  - Otherwise, there exists a second occurrence of a in some w_{c_1,p_1}, that one can write in the form $w_{c_1,p_1} = vaw$ with $a \notin v$.
    - If $p_1 = p_0$ and $c_0 = c_1$ then $\exists \tilde{w},\ w_{c_0,p_0} = va\tilde{w}a$. Let D' be a diagram on $n + 1$ wires realising $w'_{c_0,p_0} = v$, $w'_{c_0,n} = \tilde{w}$, $w'_{\neg c_0,n} = \epsilon$ (where $\neg(\mathbf{V}) = \mathbf{H}, \neg(\mathbf{H}) = \mathbf{V}$) and $w'_{c,p} = w_{c,p}$ on the first n wires otherwise. The following diagrams realise W when $c_0 = \mathbf{H}$ and $c_0 = \mathbf{V}$, respectively:



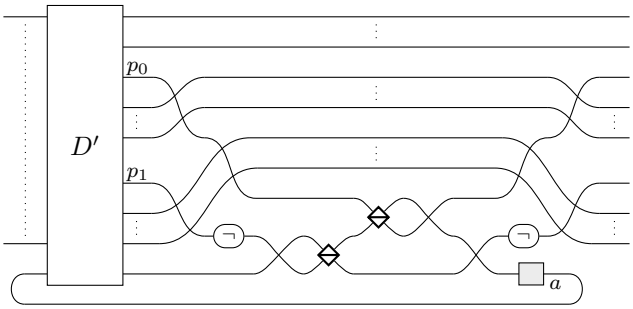
* If $p_1 = p_0$ and $c_0 \neq c_1$ then $w_{c_0,p_0} = ua$ and $w_{c_1,p_0} = vaw$. Let D' be a diagram on $n+1$ wires realising $w'_{c_0,p_0} = u$, $w'_{c_1,p_0} = v$, $w'_{c_0,n} = \epsilon$, $w'_{c_1,n} = w$ and $w'_{c,p} = w_{c,p}$ on the first n wires otherwise. The following diagram realises W:



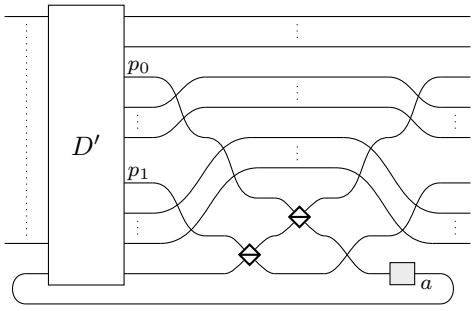
* If $p_1 \neq p_0$ and $c_0 = c_1$ then $w_{c_0,p_0} = ua$ and $w_{c_0,p_1} = vaw$. Let D' be a diagram on $n+1$ wires realising $w'_{c_0,p_0} = u$, $w'_{c_0,n} = \epsilon$, $w'_{c_0,p_1} = v$, $w'_{\neg c_0,n} = w$, and $w'_{c,p} = w_{c,p}$ on the first n wires otherwise. The following diagram realises W when $c_0 = \mathbf{H}$:



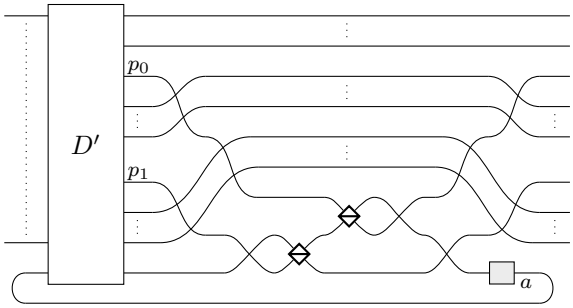
and the following diagram realises W when $c_0 = \mathbf{V}$:



* If $p_1 \neq p_0$ and $c_0 \neq c_1$, let D' be a diagram on $n+1$ wires realising $w'_{c_0,p_0} = u$, $w'_{c_0,n} = \epsilon$, $w'_{c_1,p_1} = v$, $w'_{c_1,n} = w$, and $w'_{c,p} = w_{c,p}$ on the first n wires otherwise. The following diagram realises W with $c_0 = \mathbf{H}$:



and the following diagram realises W with $c_0 = \mathbf{V}$:



Note that for the cases where $p_0 \neq p_1$, although strictly speaking the last four pictures illustrate the case where $p_0 < p_1$, they aim at representing the general case. If $p_1 < p_0$, then one should include a swap between the two corresponding wires in order to connect them to the appropriate ports.

Note that this proof is constructive, although not deterministic. That is, by following the induction steps, one can build a diagram realising a given family W, although, depending on how one follows these steps (i.e. on which word w_{c_0,p_0} one singles out at each step), one may end up with different possible diagrams. Moreover, the only cases where some -(¬)- are added are the cases where the letter a under consideration appears twice for the same polarisation c_0. Therefore, if every letter appears at most once for each polarisation c, then any diagram built by unfolding the induction is -(¬)-free. This proves the second statement. □

Example 7.5. *By unfolding the proof of Proposition 7.4 with the family* $\{w_{\mathbf{H},0} = abab, w_{\mathbf{V},0} = \epsilon\}$ *one can obtain the diagram of Figure 7.1 (right). Note that one does not always get the simplest possible diagram in this way, for instance Figure 7.1 (left) shows a simpler diagram with the same word path semantics.*

7.1.2 Extended PBS-Diagrams

We will now introduce extended PBS-diagrams by filling every bare gate with the description of a quantum channel. As recalled in the introduction of this chapter, however, defining the coherent control of general channels (as we wish to do with PBS-diagrams) in an unambiguous way is not trivial. Here we propose to do so through the notion of purified channels, which are an extension of Stinespring's dilation of quantum channels [124].

7.1.2.1 Purified Channels

A standard paradigm for quantum channels acting on a Hilbert space $\mathcal{H}$ is to describe them as CPTP maps, or superoperators $\mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$,[54] where $\mathcal{L}(\mathcal{H})$ denotes the set of linear operators on $\mathcal{H}$. As exemplified e.g. in [107, 4], this representation is however ambiguous when it comes to describing quantum coherent control: two quantum channels with the same superoperator can behave differently in a coherent-control setting.

A possible way to overcome this issue is to "go to the Church of the larger Hilbert space", according to which any quantum channel can be interpreted as a pure quantum operation acting on both the quantum system and an environment. Mathematically, this corresponds to Stinespring's dilation theorem [124], which states that any CPTP map acting on a Hilbert space $\mathcal{H}$ can be implemented with an isometry $V : \mathcal{H} \to \mathcal{H} \otimes \mathcal{E}$, where $\mathcal{E}$ denotes the Hilbert space attached to the environment, followed by a partial trace of the latter. In this chapter, we will only consider the case where the Hilbert space $\mathcal{H}$ is finite-dimensional. Then the environment $\mathcal{E}$ can also be taken of finite dimension. At least in this case, the isometry V can be understood as encoding both the creation of the environment $\mathcal{E}$ and the evolution of the joint system $\mathcal{H} \otimes \mathcal{E}$. Indeed, when $\mathcal{H}$ is finite-dimensional, V can always be decomposed into an

[54] As this is the case of interest in PBS-diagrams (with $\mathcal{H}$ corresponding to the data register), we consider here channels with the same input and output Hilbert spaces.

environment initialisation $|\varepsilon\rangle \in \mathcal{E}$ and a unitary evolution $U : \mathcal{H} \otimes \mathcal{E} \to \mathcal{H} \otimes \mathcal{E}$ such that $V = U(I_{\mathcal{H}} \otimes |\varepsilon\rangle)$, where $I_{\mathcal{H}}$ denotes the identity operator over $\mathcal{H}$.

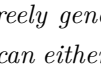
In our approach to defining coherent control for quantum channels, we will precisely abide by this description in terms of unitary purifications, which we formalise as follows:

Definition 7.6 (Purified channel)**.** *Given a finite-dimensional Hilbert space $\mathcal{H}$, a* purified $\mathcal{H}$-channel *(or simply* purified channel*, for short) is a triplet $[U, |\varepsilon\rangle, \mathcal{E}]$, where $\mathcal{E}$ is the local environment (finite-dimensional) Hilbert space, $|\varepsilon\rangle \in \mathcal{E}$ is the environment initial state, and $U : \mathcal{H} \otimes \mathcal{E} \to \mathcal{H} \otimes \mathcal{E}$ is a unitary operator representing the evolution of the joint system. We denote the set of purified $\mathcal{H}$-channels by $\mathfrak{C}(\mathcal{H})$.*

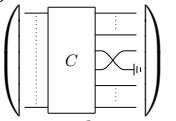
As seen above, it directly follows from Stinespring's dilation theorem that any CPTP map $\mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ can be represented by a purified $\mathcal{H}$-channel, which is however not unique. Reciprocally, with any purified $\mathcal{H}$-channel $[U, |\varepsilon\rangle, \mathcal{E}]$, we naturally associate the CPTP map $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}) :: \rho \mapsto \mathrm{Tr}_{\mathcal{E}}\big(U(\rho \otimes |\varepsilon\rangle\langle\varepsilon|)U^\dagger\big)$, where $\mathrm{Tr}_{\mathcal{E}}$ denotes the partial trace over $\mathcal{E}$, and which we shall represent graphically, using the circuit notations of Section 2.3, as follows: $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} =$ 

.

One may however not trace out the environment straight away. In fact, decomposing Stinespring's dilation into an environment state initialisation and a unitary evolution of the joint system, as we did above, allows one to apply the same channel several times in a coherent manner if a particle goes through a gate several times. In that case we will consider that the same unitary is applied each time, without re-initialising the environment state (which we assume to not evolve between two applications of the channel).

Remark 7.7 (Remarks about the circuit notations)**.** *In this chapter, we actually futher extend the circuits described in Section 2.3 by allowing the wires to represent not just qubits but any quantum systems. Unless clear from the context, we label the wires with the corresponding state space. Note that, following the literature, the definition of a coloured traced PROP given in Definition 1.6 requires that the set of objects is freely generated, that is, that there is no non-trivial relations between them. Since for instance $\mathcal{H}_1 \otimes \mathcal{H}_2$ can either be considered as a single colour* 

or as a composite object

, circuits do no strictly speaking form a coloured traced PROP but a more general structure called a traced monoidal category*. However, this does not change the axioms, they still guarantee that circuits are defined up to deformation, and the straightforward extension of the semantics keeps its properties, namely, it is still compatible with deformation, and ⊣∣ symbols can still be placed anywhere in a circuit without creating ambiguity. In particular, we still have* 

, which allows us to express the semantics of any circuit using only the partial trace $\mathrm{Tr}_{\mathcal{B}} \colon \mathcal{L}(\mathcal{A} \otimes \mathcal{B}, \mathcal{A}' \otimes \mathcal{B}) \to \mathcal{L}(\mathcal{A}, \mathcal{A}')$ *over the last factor of a tensor product.*

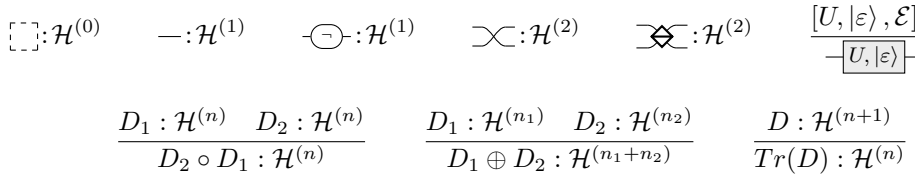
Additionally, in this chapter, since we use this kind of circuits only to graphically represent matrices or linear maps, we will identify them with their semantics. Note that a priori, this could lead to ambiguity with ⊣∣-free circuits since they can be interpreted both as their "pure" semantics, which is a matrix, or as the associated CPTP map (of the form $\rho \mapsto U\rho U^\dagger$). To avoid this ambiguity, we take the convention that unless otherwise specified, a ⊣∣-free circuit represents a matrix. Note however that we will actually never encounter the case where a ⊣∣-free circuit has to be interpreted as a CPTP map.

7.1.2.2 From Bare to Extended PBS-Diagrams

We are now in a position to define extended PBS-diagrams of type $\mathcal{H}^{(n)}$, which are essentially bare PBS-diagrams of type n, where the gate indices are replaced by purified $\mathcal{H}$-channels. Hence, instead of bare gates —□$_a$—, an extended PBS-diagram contains gates of the form —$\boxed{U, |\varepsilon\rangle}$—, parametrised by a purified channel $[U, |\varepsilon\rangle, \mathcal{E}] \in \mathfrak{C}(\mathcal{H})$ (where the Hilbert space $\mathcal{E}$ is not represented explicitly, in order not to overload the diagrams). In other words, an extended PBS-diagram is the interpretation of a bare PBS-diagram in a monoid of purified channels (see Definition 4.7, and Footnote 17 in Section 4.1).

Extended PBS-diagrams are inductively defined as follows:

Definition 7.8 (Extended PBS-diagram)**.** *An extended* PBS*-diagram* $D : \mathcal{H}^{(n)}$ *(with* $n \in \mathbb{N}$*) is inductively defined as:*



Extended PBS-diagrams are defined up to the same structural congruence as for bare PBS-diagrams, that is, they form a traced PROP.[55] It is convenient to explicitly define the map which, given a family of purified channels, transforms a bare diagram into the corresponding extended PBS-diagram:[56]

Definition 7.9. *Given a bare* PBS*-diagram* $\Gamma \vdash D' : n$ *and a family of purified* $\mathcal{H}$*-channels* $\mathcal{G} = ([U_a, |\varepsilon_a\rangle, \mathcal{E}_a])_{a\in\Gamma}$ *indexed by elements of* Γ*, let* $[D']_{\mathcal{G}} : \mathcal{H}^{(n)}$ *be the extended* PBS*-diagram inductively defined as* $[\text{—}\boxed{\ }_a\text{—}]_{([U_a,|\varepsilon_a\rangle,\mathcal{E}_a])} = \text{—}\boxed{U_a, |\varepsilon_a\rangle}\text{—}$*,* $\forall g \in \{$  $\}$*,* $[g]_\emptyset = g$*,* $[D'_2 \circ D'_1]_{\mathcal{G}_1 \uplus \mathcal{G}_2} = [D'_2]_{\mathcal{G}_2} \circ [D'_1]_{\mathcal{G}_1}$*,* $[D'_1 \oplus D'_2]_{\mathcal{G}_1\uplus\mathcal{G}_2} = [D'_1]_{\mathcal{G}_1} \oplus [D'_2]_{\mathcal{G}_2}$ *and* $[Tr(D')]_{\mathcal{G}} = Tr([D']_{\mathcal{G}})$*, where* $\uplus$ *is the disjoint union.*

For any extended PBS-diagram $D : \mathcal{H}^{(n)}$, there exists a bare diagram $\Gamma \vdash D' : n$ and an indexed family of purified $\mathcal{H}$-channels $\mathcal{G}$ s.t. $[D']_{\mathcal{G}} = D$. We call D' an *underlying bare diagram* of D (which is unique, up to relabelling of the gates).

7.1.2.3 Quantum Semantics

We now equip extended PBS-diagrams with a quantum semantics, which is a CPTP map acting on the complete state of the particle that goes through the diagram, i.e. its joint polarisation, position and data state. To describe the quantum semantics of an extended PBS-diagram $D : \mathcal{H}^{(n)}$, it is convenient to rely on an underlying bare diagram $\Gamma \vdash D' : n$ and a family of purified channels $\mathcal{G}$ s.t. $[D']_{\mathcal{G}} = D$ (so as to keep track of the environment spaces and be able to identify them via the bare gate indices).

As we defined them, every purified channel comes with its local environment and a unitary evolution acting on both the data register and its local environment. In order to define the overall evolution of the diagram, we consider the global environment as the tensor product of these local environments, and extend every unitary transformation to a global transformation acting on the data register and the global environment:

Definition 7.10. *Given an indexed family of purified* $\mathcal{H}$*-channels* $\mathcal{G} = ([U_a, |\varepsilon_a\rangle, \mathcal{E}_a])_{a\in\Gamma}$*, let* $\mathcal{E}_{\mathcal{G}} \coloneqq \bigotimes_{a\in\Gamma} \mathcal{E}_a$*,* $|\varepsilon_{\mathcal{G}}\rangle \coloneqq \bigotimes_{a\in\Gamma} |\varepsilon_a\rangle \in \mathcal{E}_{\mathcal{G}}$*, and* $\forall\, a \in \Gamma$*, let* $V_a^{\mathcal{G}} \coloneqq U_a \bigotimes_{x\in\Gamma\setminus\{a\}} I_{\mathcal{E}_x} \in \mathcal{L}(\mathcal{H} \otimes \mathcal{E}_{\mathcal{G}})$*.*

If a particle enters an extended PBS-diagram D with a definite polarisation and position in some basis states $|c\rangle \in \mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}$ and $|p\rangle \in \mathbb{C}^{[n]}$, respectively, the sequence of transformations applied to the particle and the global environment when the particle goes through the diagram can be deduced from the word path semantics of the underlying bare diagram D':

$$|c\rangle \otimes |p\rangle \otimes |\psi\rangle \otimes |\varepsilon_{\mathcal{G}}\rangle \mapsto \left|c_{c,p}^{D'}\right\rangle \otimes \left|p_{c,p}^{D'}\right\rangle \otimes V^{\mathcal{G}}_{w_{c,p}^{D'}}(|\psi\rangle \otimes |\varepsilon_{\mathcal{G}}\rangle)$$

where $w_{c,p}^{D'}$, $c_{c,p}^{D'}$, and $p_{c,p}^{D'}$ are given by the word path semantics, i.e. $(D', c, p) \overset{w_{c,p}^{D'}}{\Longrightarrow} (c_{c,p}^{D'}, p_{c,p}^{D'})$, and $V_w^{\mathcal{G}}$ is inductively defined as $V_\epsilon^{\mathcal{G}} \coloneqq I_{\mathcal{H}\otimes\mathcal{E}}$ and $\forall a \in \Gamma, \forall w \in \Gamma^*$, $V_{aw}^{\mathcal{G}} \coloneqq V_w^{\mathcal{G}} V_a^{\mathcal{G}}$.

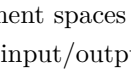
One can actually consider inputting a particle in an arbitrary initial state (i.e. including superpositions of polarisation and position); the transformation applied by the diagram is then obtained from the one above, by linearity. This leads us to define the following:

[55] Without caveat here, as an extended PBS-diagram can contain several identical channels (see Footnote 52).

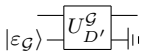
[56] To clarify which kind of diagram we are dealing with, in this subsection we use primed names (e.g. D') when referring to bare PBS-diagrams, and nonprimed names for extended PBS-diagrams.

Definition 7.11. *Given a bare* PBS*-diagram* $\Gamma \vdash D' : n$ *and a family of purified* $\mathcal{H}$*-channels* $\mathcal{G}$ *indexed with* Γ*, let*

$$U^{\mathcal{G}}_{D'} \coloneqq \sum_{c\in\{\mathbf{V},\mathbf{H}\},p\in[n]} \left|c^{D'}_{c,p}\right\rangle\langle c| \otimes \left|p^{D'}_{c,p}\right\rangle\langle p| \otimes V^{\mathcal{G}}_{w^{D'}_{c,p}}$$

The triplet $[U^{\mathcal{G}}_{D'}, |\varepsilon_{\mathcal{G}}\rangle, \mathcal{E}_{\mathcal{G}}]$ is nothing but a purified $(\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}} \otimes \mathbb{C}^{[n]} \otimes \mathcal{H})$-channel, which describes the action of the corresponding extended PBS-diagram on the complete state of the particle. Once the particle exits the diagram, the environments of all purified channels are not accessible anymore. As is well-known, the statistics of any "input/output test", which consists in preparing an arbitrary input state of the particle and measuring the output in an arbitrary basis, then only depends on the CPTP map (the superoperator) induced by $U^{\mathcal{G}}_{D'}$ above, with all environments initially prepared in the global state $|\varepsilon_{\mathcal{G}}\rangle$, and after tracing out all environment spaces — i.e. using circuit-like notations:  . This superoperator thus precisely captures input/output (in)distinguishability: two quantum channels have the same superoperator if and only if they are indistinguishable in any input/output test. This provides the ground for our definition of the following quantum semantics:

Definition 7.12 (Quantum semantics)**.** *Given an extended* PBS*-diagram* $D : \mathcal{H}^{(n)}$*, let* $[\![D]\!] : \mathcal{L}(\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}} \otimes \mathbb{C}^{[n]} \otimes \mathcal{H}) \to \mathcal{L}(\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}} \otimes \mathbb{C}^{[n]} \otimes \mathcal{H})$ *be the superoperator defined as*

$$[\![D]\!] \coloneqq \rho \mapsto \mathrm{Tr}_{\mathcal{E}_{\mathcal{G}}}(U^{\mathcal{G}}_{D'}(\rho \otimes |\varepsilon_{\mathcal{G}}\rangle\langle\varepsilon_{\mathcal{G}}|)U^{\mathcal{G}\dagger}_{D'}) \quad = \quad$$ 

where $\Gamma \vdash D' : n$ *is an underlying bare diagram and* $\mathcal{G}$ *is an indexed family of purified* $\mathcal{H}$*-channels s.t.* $[D']_{\mathcal{G}} = D$*.*

Note that the quantum semantics is preserved by the "only topology matters" structural congruence on diagrams. Indeed, it is defined using only the family $\mathcal{G}$ and the word path semantics of its underlying bare diagram D', which is invariant modulo diagram deformation. It is clear that when deforming D we do not have to change D' and $\mathcal{G}$, since it suffices to deform D' accordingly.

7.2 Observational Equivalence of Purified Channels

In this section we address the problem of deciding whether two purified channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$ can be distinguished in an experiment involving coherent control, within the framework of PBS-diagrams just established. We introduce for that the notion of *contexts*, which are extended PBS-diagrams with a "hole": if for any context, filling its hole with $[U, |\varepsilon\rangle, \mathcal{E}]$ or $[U', |\varepsilon'\rangle, \mathcal{E}']$ leads to diagrams with the same quantum semantics, then the two purified channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$ are indistinguishable within our framework, even with the help of the coherent control provided by extended PBS-diagrams.

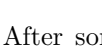
7.2.1 Contexts

A context is an extended PBS-diagram with a *hole*, i.e. a (unique) particular empty gate, without any purified channel specified *a priori*. Equivalently a context can be seen as a bare PBS-diagram partially filled: all but one gates are filled with purified channels. Formally:

Definition 7.13 (Context)**.** *A context* $C[\cdot] : \mathcal{H}^{(n)}$ *(with* $n \in \mathbb{N}$*) is inductively defined as follows:*

- *The hole gate* $-\boxed{\cdot}- : \mathcal{H}^{(1)}$ *is a context;*
- *If* $C[\cdot] : \mathcal{H}^{(n)}$ *is a context and* $D : \mathcal{H}^{(n)}$ *is an extended* PBS*-diagram then* $D \circ C[\cdot] : \mathcal{H}^{(n)}$ *and* $C[\cdot] \circ D : \mathcal{H}^{(n)}$ *are contexts;*
- *If* $C[\cdot] : \mathcal{H}^{(n)}$ *is a context and* $D : \mathcal{H}^{(m)}$ *is an extended* PBS*-diagram then* $D \oplus C[\cdot] : \mathcal{H}^{(m+n)}$ *and* $C[\cdot] \oplus D : \mathcal{H}^{(n+m)}$ *are contexts;*
- *If* $C[\cdot] : \mathcal{H}^{(n+1)}$ *is a context then* $Tr(C[\cdot]) : \mathcal{H}^{(n)}$ *is a context.*

Like bare and extended PBS-diagrams, contexts are defined up to structural congruence.

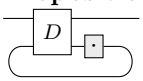
Definition 7.14 (Substitution)**.** *For any context $C[\cdot] : \mathcal{H}^{(n)}$ and any purified $\mathcal{H}$-channel $[U, |\varepsilon\rangle, \mathcal{E}]$, let $C[U, |\varepsilon\rangle, \mathcal{E}] : \mathcal{H}^{(n)}$ be the extended* PBS*-diagram obtained by replacing the single hole*  *in $C[\cdot]$ by the purified channel*  *.*

After some purified channel is plugged in, contexts allow one to compare the quantum semantics $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!]$ and $[\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$ induced by different purified channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$. We consider in the following three subclasses of contexts, depending on the kind of coherent control one may allow to distinguish purified channels: whether we exclude the use of PBS (), of polarisation flips ("negations" ), or whether we allow both. This leads us to define the following equivalence relations:

Definition 7.15 (Observational equivalences)**.** *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, we consider the three following refinements of observational equivalences (for $i \in \{0, 1, 2\}$): $[U, |\varepsilon\rangle, \mathcal{E}] \approx_i [U', |\varepsilon'\rangle, \mathcal{E}']$ if $\forall C[\cdot] \in \mathcal{C}_i$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$, where:*

- *$\mathcal{C}_0$ is the set of*  *-free contexts $C[\cdot] : \mathcal{H}^{(1)}$;*
- *$\mathcal{C}_1$ is the set of*  *-free contexts $C[\cdot] : \mathcal{H}^{(1)}$;*
- *$\mathcal{C}_2$ is the set of all contexts $C[\cdot] : \mathcal{H}^{(1)}$.*

Note that contexts in $\mathcal{C}_0$ do not perform any coherent control; these consist in just a linear sequence of gates and negations, possibly composed in parallel with closed loops (i.e. traces of such sequences), including a hole gate somewhere. It is clear, by deformation of diagrams, that more general contexts can always be described as follows:

Proposition 7.16. *For any context $C[\cdot] \in \mathcal{C}_2$ there exists an extended* PBS*-diagram D such that $C[\cdot] =$*  *. Moreover if $C[\cdot] \in \mathcal{C}_1$ then D can be chosen*  *-free.*

Remark 7.17. *In Definition 7.15 we only consider contexts with a single input/output wire. This is because we intend to use contexts to distinguish purified channels: if one can distinguish two purified channels with a context of type $\mathcal{H}^{(n)}$ but no context of type $\mathcal{H}^{(1)}$, then intuitively this means that the extra power comes from the preparation of the initial state and/or some particular measurement, which are not represented in the context. Actually, except in the $\mathcal{C}_0$ case, allowing multiple input/output wires does not increase the distinguishability power of the contexts (see Propositions 7.22 and 7.27).*

7.2.2 Observational Equivalence Using PBS-Free Contexts

Let us start by characterising which purified channels are indistinguishable by  -free contexts in $\mathcal{C}_0$. Not surprisingly, we recover the usual indistinguishability by input/output tests, which is captured by the fact that the two purified channels lead to the same superoperator:[57]

Definition 7.18 ((First-level) Superoperator)**.** *Given a purified $\mathcal{H}$-channel $[U, |\varepsilon\rangle, \mathcal{E}]$, let $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H}) :: \rho \mapsto \mathrm{Tr}_{\mathcal{E}}\big(U(\rho \otimes |\varepsilon\rangle\langle\varepsilon|)U^\dagger\big)$ be the ("first-level") superoperator of $[U, |\varepsilon\rangle, \mathcal{E}]$. Graphically,*

$$\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \coloneqq$$ 

Theorem 7.19. *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, $[U, |\varepsilon\rangle, \mathcal{E}] \approx_0 [U', |\varepsilon'\rangle, \mathcal{E}']$ iff they have the same (first-level) superoperator. Graphically,*

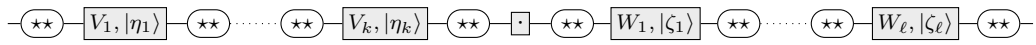
$$[U, |\varepsilon\rangle, \mathcal{E}] \approx_0 [U', |\varepsilon'\rangle, \mathcal{E}'] \qquad \textit{iff} \qquad$$  (S1)

[57] In other words, if two purified channels can be distinguished using a  -free context, then they could already be distinguished with simply an input/output test (or with a trivial context ).

Proof. By considering the trivial context $-\boxed{\cdot}-$, if $[U, |\varepsilon\rangle, \mathcal{E}] \approx_0 [U', |\varepsilon'\rangle, \mathcal{E}']$ then in particular, $[\![-\boxed{U, |\varepsilon\rangle}-]\!] = [\![-\boxed{U', |\varepsilon'\rangle}-]\!]$, hence, $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = \mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$.

Conversely, let us assume that $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = \mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$. Let $C[\cdot] \in \mathcal{C}_0$. By deformation of diagrams one can write it in one of the following two forms:

- $C'[\cdot] \oplus D$, with $D : \mathcal{H}^{(0)}$ and $C'[\cdot]$ of the form

  for some purified channels $[V_i, |\eta_i\rangle, \mathcal{V}_i], [W_j, |\zeta_j\rangle, \mathcal{Z}_j] \in \mathfrak{C}(\mathcal{H})$, and where $-\textcircled{\star\star}-$ denotes any sequence of $-\textcircled{\neg}-$, possibly of length 0;
- $D \oplus C'[\cdot]$, with $D : \mathcal{H}^{(1)}$ and $C'[\cdot] : \mathcal{H}^{(0)}$.

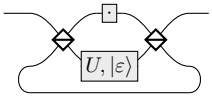
In the latter case, the semantics does not depend on what is plugged in the hole, so that $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$. In the former case,

$$\begin{aligned}
[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] &= \mathcal{X}^* \otimes \mathcal{I}_{\mathbb{C}} \otimes \left(\mathcal{S}^{(1)}_{[W_\ell,|\zeta_\ell\rangle,\mathcal{Z}_\ell]} \circ \cdots \circ \mathcal{S}^{(1)}_{[W_1,|\zeta_1\rangle,\mathcal{Z}_1]} \circ \mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \circ \mathcal{S}^{(1)}_{[V_k,|\eta_k\rangle,\mathcal{V}_k]} \circ \cdots \circ \mathcal{S}^{(1)}_{[V_1,|\eta_1\rangle,\mathcal{V}_1]}\right) \\
&= \mathcal{X}^* \otimes \mathcal{I}_{\mathbb{C}} \otimes \left(\mathcal{S}^{(1)}_{[W_\ell,|\zeta_\ell\rangle,\mathcal{Z}_\ell]} \circ \cdots \circ \mathcal{S}^{(1)}_{[W_1,|\zeta_1\rangle,\mathcal{Z}_1]} \circ \mathcal{S}^{(1)}_{[U',|\varepsilon\rangle',\mathcal{E}']} \circ \mathcal{S}^{(1)}_{[V_k,|\eta_k\rangle,\mathcal{V}_k]} \circ \cdots \circ \mathcal{S}^{(1)}_{[V_1,|\eta_1\rangle,\mathcal{V}_1]}\right) \\
&= [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]
\end{aligned}$$

where $\mathcal{X}^*$ is either the identity map over $\mathcal{L}(\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}})$ if the total number of $-\textcircled{\neg}-$ in $C'[\cdot]$ is even, or the linear map $|c\rangle\langle c'| \mapsto |\neg c\rangle\langle \neg c'|$ if the total number of $-\textcircled{\neg}-$ in $C'[\cdot]$ is odd, and $\mathcal{I}_{\mathbb{C}}$ is the identity map over $\mathbb{C}$. Hence, $[U, |\varepsilon\rangle, \mathcal{E}] \approx_0 [U', |\varepsilon'\rangle, \mathcal{E}']$. □

7.2.3 Observational Equivalence Using Negation-Free Contexts

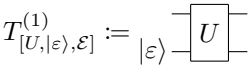
Allowing contexts with PBS significantly increases their power to distinguish purified channels. In [4], a particular kind of coherent control — namely, the *"first half of a quantum switch"* [34, 10, 68] — has been considered, which can be rephrased using contexts of the form:



The authors proved that with these particular contexts, two purified channels leading to the same (first-level) superoperator are indistinguishable if and only if they also have the same *(first-level) transformation matrix*, which is defined as follows:[58]

Definition 7.20 ((First-level) Transformation matrix)**.** *Given a purified $\mathcal{H}$-channel $[U, |\varepsilon\rangle, \mathcal{E}]$, let $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \coloneqq (I_{\mathcal{H}} \otimes \langle\varepsilon|)U(I_{\mathcal{H}} \otimes |\varepsilon\rangle) \in \mathcal{L}(\mathcal{H})$ be the ("first-level") transformation matrix of $[U, |\varepsilon\rangle, \mathcal{E}]$. Graphically,*

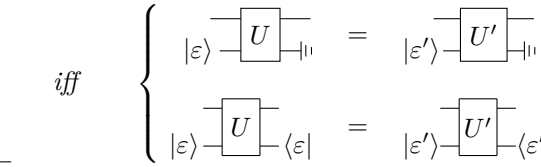
$$T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \coloneqq$$



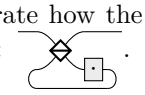
We extend this result to any $-\textcircled{\neg}-$-free context:

Theorem 7.21. *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, $[U, |\varepsilon\rangle, \mathcal{E}] \approx_1 [U', |\varepsilon'\rangle, \mathcal{E}']$ iff they have the same (first-level) superoperator and the same (first-level) transformation matrix. Graphically,*

$$[U, |\varepsilon\rangle, \mathcal{E}] \approx_1 [U', |\varepsilon'\rangle, \mathcal{E}'] \qquad \textit{iff} \qquad$$



[58] Originally, in [4], the transformation matrix was defined for a given unitary purification of a CPTP map $\mathcal{S} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ in the form $U : |\psi\rangle_{\mathcal{H}} \otimes |\varepsilon\rangle \mapsto \sum_i K_i |\psi\rangle_{\mathcal{H}} \otimes |i\rangle_{\mathcal{E}}$ (where the K_i's are Kraus operators of $\mathcal{S}$, and where an environment space $\mathcal{E}$ was introduced, with an orthonormal basis $\{|i\rangle_{\mathcal{E}}\}_i$ and an initial state $|\varepsilon\rangle$), as $T \coloneqq \sum_i \langle\varepsilon|\, i\rangle_{\mathcal{E}}\, K_i$. This is indeed consistent with our Definition 7.20 here, as with these notations $U(I_{\mathcal{H}} \otimes |\varepsilon\rangle) = \sum_i K_i \otimes |i\rangle_{\mathcal{E}}$, so that $(I_{\mathcal{H}} \otimes \langle\varepsilon|)U(I_{\mathcal{H}} \otimes |\varepsilon\rangle) = \sum_i \langle\varepsilon|\, i\rangle_{\mathcal{E}}\, K_i = T$.

One can illustrate how the transformation matrices enter the game by considering for example the following context :  . By plugging in $[U, |\varepsilon\rangle, \mathcal{E}]$, the extended PBS-diagram maps a pure input state $\frac{|\mathbf{V}\rangle+|\mathbf{H}\rangle}{\sqrt{2}} \otimes |\psi\rangle \in \mathbb{C}^{\{\mathbf{V},\mathbf{H}\}} \otimes \mathcal{H}$ (together with the environment initial state $|\varepsilon\rangle \in \mathcal{E}$) to the state $\frac{1}{\sqrt{2}} |\mathbf{V}\rangle \otimes |\psi\rangle \otimes |\varepsilon\rangle + \frac{1}{\sqrt{2}} |\mathbf{H}\rangle \otimes U(|\psi\rangle \otimes |\varepsilon\rangle)$, so that after tracing out the environment a cross term $\frac{1}{2} |\mathbf{H}\rangle\langle\mathbf{V}| \otimes \mathrm{Tr}_{\mathcal{E}}\big[U(|\psi\rangle\langle\psi| \otimes |\varepsilon\rangle\langle\varepsilon|)\big] = \frac{1}{2} |\mathbf{H}\rangle\langle\mathbf{V}| \otimes T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} |\psi\rangle\langle\psi|$ appears.

We note also that the two conditions (S1) and (T1) are nonredundant, i.e. one does not imply the other. Indeed, there exist cases where $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = \mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$ but $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \neq T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$ (e.g. given any $\mathcal{H}$, $\mathcal{E} = \mathcal{E}' = \mathbb{C}$, $U = I_{\mathcal{H}}, U' = -I_{\mathcal{H}}$ and $|\varepsilon\rangle = |\varepsilon'\rangle = 1$), and cases where $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \neq \mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$ but $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$ (e.g. $\mathcal{H} = \mathcal{E} = \mathcal{E}' = \mathbb{C}^2$, $U = I_{\mathcal{H}} \otimes X, U' = X \otimes X$ and $|\varepsilon\rangle = |\varepsilon'\rangle = |0\rangle$).[59]

We are now going to prove at the same time Theorem 7.21 and the fact that allowing multiple input/output wires does not increase the power of -⟨¬⟩-free contexts, stated as the following proposition:

Proposition 7.22. *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, one has $[U, |\varepsilon\rangle, \mathcal{E}] \approx_1 [U', |\varepsilon'\rangle, \mathcal{E}']$ (that is, for any -⟨¬⟩-free context $C[\cdot] : \mathcal{H}^{(1)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$) if and only if for any -⟨¬⟩-free context $C[\cdot] : \mathcal{H}^{(n)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$.*

Namely, what we are going to prove is the following lemma:

Lemma 7.23. *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, the following three statements are equivalent:*

(I) $[U, |\varepsilon\rangle, \mathcal{E}] \approx_1 [U', |\varepsilon'\rangle, \mathcal{E}']$, *that is, for any -⟨¬⟩-free context $C[\cdot] : \mathcal{H}^{(1)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$*

(II) *for any -⟨¬⟩-free context $C[\cdot] : \mathcal{H}^{(n)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$*

(III) $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = \mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$ *and* $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$

It is clear that it implies both Theorem 7.21 and Proposition 7.22. Indeed, Theorem 7.21 is exactly (I) ⇔ (III), while Proposition 7.22 is (I) ⇔ (II).

Proof of Lemma 7.23. It is clear that (II) ⇒ (I). Therefore, what one has to prove is that (III) ⇒ (II) (that is, the conditions given by Theorem 7.21 are sufficient even with contexts with mutiple input/output wires) and that (I) ⇒ (III) (or equivalently ¬(III) ⇒ ¬(I), that is, these conditions are necessary).

Proof of Strong Sufficiency ((III) ⇒ (II)). Let us assume (III). Let $C[\cdot] : \mathcal{H}^{(n)}$ be any -⟨¬⟩-free context. Let $\Gamma \vdash D : n$ be an underlying bare diagram of both $C[U, |\varepsilon\rangle, \mathcal{E}]$ and $C[U', |\varepsilon'\rangle, \mathcal{E}']$. Let $\mathcal{G} = ([U_x, |\varepsilon_x\rangle, \mathcal{E}_x])_{x\in\Gamma}$ and $\mathcal{G}' = ([U'_x, |\varepsilon'_x\rangle, \mathcal{E}'_x])_{x\in\Gamma}$ be such that $[U_a, |\varepsilon_a\rangle, \mathcal{E}_a] = [U, |\varepsilon\rangle, \mathcal{E}]$ and $[U'_a, |\varepsilon'_a\rangle, \mathcal{E}'_a] = [U', |\varepsilon'\rangle, \mathcal{E}']$ for some $a \in \Gamma$, while $[U_x, |\varepsilon_x\rangle, \mathcal{E}_x] = [U'_x, |\varepsilon'_x\rangle, \mathcal{E}'_x]$ for all $x \in \Gamma\backslash\{a\}$; and let $\mathcal{F} = ([U_x, |\varepsilon_x\rangle, \mathcal{E}_x])_{x\in\Gamma\backslash\{a\}}$.

Let $c, c' \in \{\mathbf{V}, \mathbf{H}\}$ and $p, p' \in [n]$. By Proposition 7.3 one has $|w^D_{c,p}|_a \leq 1$ and $|w^D_{c',p'}|_a \leq 1$, so that there are four cases:

- If $|w^D_{c,p}|_a = |w^D_{c',p'}|_a = 1$, then one can write $w^D_{c,p} = uav$ and $w^D_{c',p'} = u'av'$ with $u, v, u', v' \in (\Gamma\backslash\{a\})^*$. Then for any $\rho \in \mathcal{L}(\mathcal{H})$:

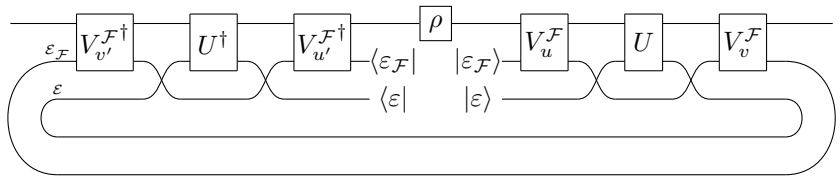
$$[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!]\,(|c, p\rangle\langle c', p'| \otimes \rho) = \big|c^D_{c,p}, p^D_{c,p}\big\rangle\big\langle c^D_{c',p'}, p^D_{c',p'}\big| \otimes \mathrm{Tr}_{\mathcal{E}_{\mathcal{G}}}\big(V^{\mathcal{G}}_{w^D_{c,p}}(\rho \otimes |\varepsilon_{\mathcal{G}}\rangle\langle\varepsilon_{\mathcal{G}}|)V^{\mathcal{G}\,\dagger}_{w^D_{c',p'}}\big)$$

[59] Where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

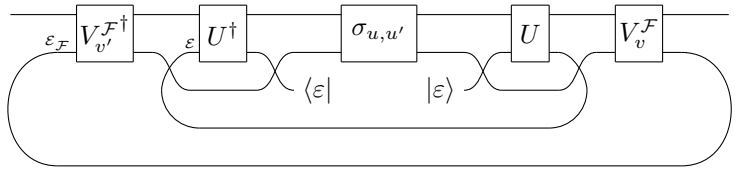
with (using the circuit notations defined in Section 2.3, and noting for instance that $V_u^{\mathcal{G}} = V_u^{\mathcal{F}} \otimes I_{\mathcal{E}}$ and that $V_a^{\mathcal{G}} = U \otimes I_{\mathcal{E}_{\mathcal{F}}}$)

$$\mathrm{Tr}_{\mathcal{E}_{\mathcal{G}}}(V^{\mathcal{G}}_{w^D_{c,p}}(\rho \otimes |\varepsilon_{\mathcal{G}}\rangle\langle\varepsilon_{\mathcal{G}}|)V^{\mathcal{G}\dagger}_{w^D_{c',p'}}) = \mathrm{Tr}_{\mathcal{E}_{\mathcal{F}},\mathcal{E}}\left(V_v^{\mathcal{G}} V_a^{\mathcal{G}} V_u^{\mathcal{G}} (\rho \otimes |\varepsilon_{\mathcal{F}}\rangle\langle\varepsilon_{\mathcal{F}}| \otimes |\varepsilon\rangle\langle\varepsilon|) V_{u'}^{\mathcal{G}\dagger} V_a^{\mathcal{G}\dagger} V_{v'}^{\mathcal{G}\dagger}\right)$$

$=$



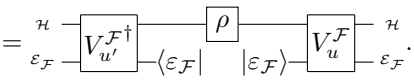
$=$



$$= \mathrm{Tr}_{\mathcal{E}_{\mathcal{F}}}\left(V_v^{\mathcal{F}}\ \mathrm{Tr}_{\mathcal{E}}\left((U \otimes I_{\mathcal{E}_{\mathcal{F}}})(\sigma_{u,u'} \otimes |\varepsilon\rangle\langle\varepsilon|)(U^\dagger \otimes I_{\mathcal{E}_{\mathcal{F}}})\right) V_{v'}^{\mathcal{F}\dagger}\right)$$

$$= \mathrm{Tr}_{\mathcal{E}_{\mathcal{F}}}\left(V_v^{\mathcal{F}}\left(\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \otimes \mathcal{I}_{\mathcal{E}_{\mathcal{F}}}\right)[\sigma_{u,u'}]V_{v'}^{\mathcal{F}\dagger}\right),$$

where $\mathcal{I}_{\mathcal{E}_{\mathcal{F}}}$ is the identity map over $\mathcal{L}(\mathcal{E}_{\mathcal{F}})$ and $\sigma_{u,u'} =$



.

Similarly,

$$[\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!]\left(|c,p\rangle\langle c',p'|\otimes\rho\right) = \left|c^D_{c,p},p^D_{c,p}\right\rangle\left\langle c^D_{c',p'},p^D_{c',p'}\right| \otimes \mathrm{Tr}_{\mathcal{E}_{\mathcal{F}}}\left(V_v^{\mathcal{F}}\left(\mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']} \otimes \mathcal{I}_{\mathcal{E}_{\mathcal{F}}}\right)[\sigma_{u,u'}]V_{v'}^{\mathcal{F}\dagger}\right).$$

Since $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = \mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, this is equal to $[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!]\left(|c,p\rangle\langle c',p'|\otimes\rho\right)$.

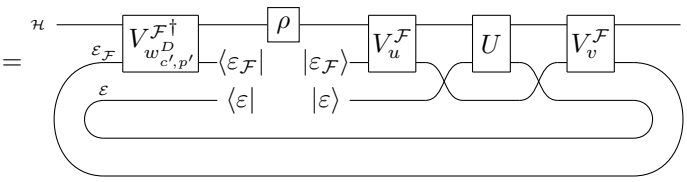
- If $|w^D_{c,p}|_a = 1$ and $|w^D_{c',p'}|_a = 0$, then one can write $w^D_{c,p} = uav$ with $u,v \in (\Gamma\backslash\{a\})^*$. Then for any $\rho \in \mathcal{L}(\mathcal{H})$:

$$[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!]\left(|c,p\rangle\langle c',p'|\otimes\rho\right) = \left|c^D_{c,p},p^D_{c,p}\right\rangle\left\langle c^D_{c',p'},p^D_{c',p'}\right| \otimes \mathrm{Tr}_{\mathcal{E}_{\mathcal{G}}}\left(V^{\mathcal{G}}_{w^D_{c,p}}(\rho \otimes |\varepsilon_{\mathcal{G}}\rangle\langle\varepsilon_{\mathcal{G}}|)V^{\mathcal{G}\dagger}_{w^D_{c',p'}}\right)$$

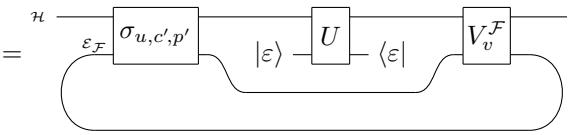
with

$$\mathrm{Tr}_{\mathcal{E}_{\mathcal{G}}}(V^{\mathcal{G}}_{w^D_{c,p}}(\rho \otimes |\varepsilon_{\mathcal{G}}\rangle\langle\varepsilon_{\mathcal{G}}|)V^{\mathcal{G}\dagger}_{w^D_{c',p'}}) = \mathrm{Tr}_{\mathcal{E}_{\mathcal{F}},\mathcal{E}}\left(V_v^{\mathcal{G}} V_a^{\mathcal{G}} V_u^{\mathcal{G}} (\rho \otimes |\varepsilon_{\mathcal{F}}\rangle\langle\varepsilon_{\mathcal{F}}| \otimes |\varepsilon\rangle\langle\varepsilon|) V^{\mathcal{G}\dagger}_{w^D_{c',p'}}\right)$$

$=$

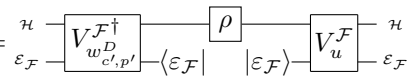


$=$



$$= \mathrm{Tr}_{\mathcal{E}_{\mathcal{F}}}\left(V_v^{\mathcal{F}}\left(T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \otimes I_{\mathcal{E}_{\mathcal{F}}}\right)\sigma_{u,c',p'}\right),$$

where $\sigma_{u,c',p'} =$



.

Again, similarly, one has

$$[\![C[U',|\varepsilon'\rangle,\mathcal{E}']\!](|c,p\rangle\langle c',p'|\otimes\rho) = |c^D_{c,p},p^D_{c,p}\rangle\langle c^D_{c',p'},p^D_{c',p'}| \otimes \mathrm{Tr}_{\mathcal{E}_\mathcal{F}}\left(V^\mathcal{F}_v\left(T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}\otimes I_{\mathcal{E}_\mathcal{F}}\right)\sigma_{u,c',p'}\right).$$

Since $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, this is equal to $[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|c,p\rangle\langle c',p'|\otimes\rho)$.

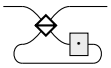
- The case $|w^D_{c,p}|_a = 0$ and $|w^D_{c',p'}|_a = 1$ is similar to the previous case.
- If $|w^D_{c,p}|_a = |w^D_{c',p'}|_a = 0$, then for any $\rho\in\mathcal{L}(\mathcal{H})$:

$$\begin{aligned}
[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|c,p\rangle\langle c',p'|\otimes\rho) &= |c^D_{c,p},p^D_{c,p}\rangle\langle c^D_{c',p'},p^D_{c',p'}| \otimes \mathrm{Tr}_{\mathcal{E}_\mathcal{G}}\left(V^\mathcal{G}_{w^D_{c,p}}(\rho\otimes|\varepsilon_\mathcal{G}\rangle\langle\varepsilon_\mathcal{G}|)V^{\mathcal{G}\dagger}_{w^D_{c',p'}}\right)\\
&= |c^D_{c,p},p^D_{c,p}\rangle\langle c^D_{c',p'},p^D_{c',p'}| \otimes \mathrm{Tr}_{\mathcal{E}_\mathcal{F}}\left(V^\mathcal{F}_{w^D_{c,p}}(\rho\otimes|\varepsilon_\mathcal{F}\rangle\langle\varepsilon_\mathcal{F}|)V^{\mathcal{F}\dagger}_{w^D_{c',p'}}\right)\\
&= |c^D_{c,p},p^D_{c,p}\rangle\langle c^D_{c',p'},p^D_{c',p'}| \otimes \mathrm{Tr}_{\mathcal{E}_{\mathcal{G}'}}\left(V^{\mathcal{G}'}_{w^D_{c,p}}(\rho\otimes|\varepsilon_{\mathcal{G}'}\rangle\langle\varepsilon_{\mathcal{G}'}|)V^{\mathcal{G}'\dagger}_{w^D_{c',p'}}\right)\\
&= [\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!](|c,p\rangle\langle c',p'|\otimes\rho).
\end{aligned}$$

We have thus proved that $[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|c,p\rangle\langle c',p'|\otimes\rho) = [\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!](|c,p\rangle\langle c',p'|\otimes\rho)$ for all c,p,c',p' and ρ, that is, $[U,|\varepsilon\rangle,\mathcal{E}]\approx_1[U',|\varepsilon'\rangle,\mathcal{E}']$.

Proof of Necessity ($\neg$(III) $\Rightarrow$ $\neg$(I)).

- If $\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]}\neq\mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, then already with the trivial context $-\boxed{\cdot}-$ one can distinguish $[U,|\varepsilon\rangle,\mathcal{E}]$ and $[U',|\varepsilon'\rangle,\mathcal{E}']$. Indeed, one has $[\![-\boxed{U,|\varepsilon\rangle}-]\!] = \mathcal{I}_{\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}\otimes\mathbb{C}}\otimes\mathcal{S}^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]}$, whereas $[\![-\boxed{U',|\varepsilon'\rangle}-]\!] = \mathcal{I}_{\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}\otimes\mathbb{C}}\otimes\mathcal{S}^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$ (where $\mathcal{I}_{\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}\otimes\mathbb{C}}$ is the identity map over $\mathcal{L}(\mathbb{C}^{\{\mathbf{V},\mathbf{H}\}}\otimes\mathbb{C})$).
- If $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]}\neq T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, then by considering the following context:

$C[\cdot] =$ 

one gets in particular

$$[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes I_\mathcal{H}) = |\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes\mathrm{Tr}_\mathcal{E}\big(U(I_\mathcal{H}\otimes|\varepsilon\rangle\langle\varepsilon|)\big) = |\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]}$$

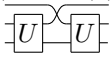
and similarly

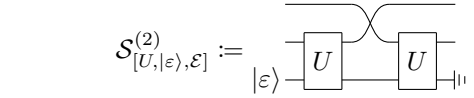
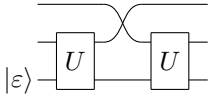
$$[\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!](|\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes I_\mathcal{H}) = |\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}.$$

Since $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]}\neq T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, this implies that $[U,|\varepsilon\rangle,\mathcal{E}]\not\approx_1[U',|\varepsilon'\rangle,\mathcal{E}']$. □

7.2.4 Observational Equivalence Using General Contexts

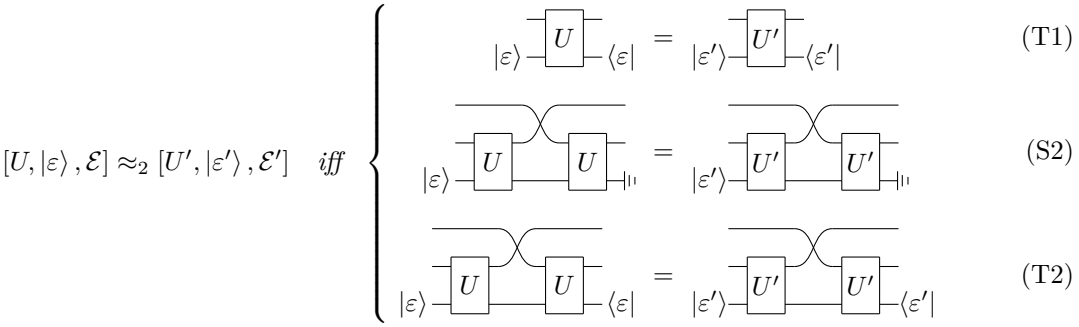
We will now see that allowing negations ($-\boxed{\neg}-$) increases the power of contexts to distinguish purified channels. To characterise the indistinguishability of purified channels with arbitrary contexts, we introduce *second-level* superoperators and *second-level* transformation matrices:

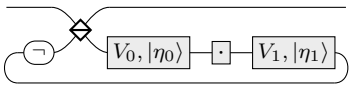
Definition 7.24 (Second-level superoperator and transformation matrix)**.** *Given a purified $\mathcal{H}$-channel $[U,|\varepsilon\rangle,\mathcal{E}]$, let $\mathcal{S}^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} : \mathcal{L}(\mathcal{H}^{\otimes2})\to\mathcal{L}(\mathcal{H}^{\otimes2}) :: \rho\mapsto\mathrm{Tr}_\mathcal{E}\big(U^{(2)}(\rho\otimes|\varepsilon\rangle\langle\varepsilon|)U^{(2)\dagger}\big)$ be the "second-level" superoperator and $T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \coloneqq (I_{\mathcal{H}^{\otimes2}}\otimes\langle\varepsilon|)U^{(2)}(I_{\mathcal{H}^{\otimes2}}\otimes|\varepsilon\rangle)\in\mathcal{L}(\mathcal{H}^{\otimes2})$ be the "second-level" transformation matrix of $[U,|\varepsilon\rangle,\mathcal{E}]$, where $U^{(2)}\coloneqq(I_\mathcal{H}\otimes U)(\mathfrak{S}\otimes I_\mathcal{E})(I_\mathcal{H}\otimes U)$ and $\mathfrak{S}\coloneqq|\psi_1\rangle\otimes|\psi_2\rangle\mapsto|\psi_2\rangle\otimes|\psi_1\rangle$ is the swap operator. Graphically, $U^{(2)} =$*  *,*

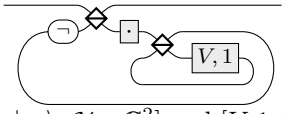
$\mathcal{S}^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \coloneqq$  *and* $T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \coloneqq$ 

Theorem 7.25. *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, $[U, |\varepsilon\rangle, \mathcal{E}] \approx_2 [U', |\varepsilon'\rangle, \mathcal{E}']$ iff they have the same (first-level) transformation matrix, the same second-level superoperator and the same second-level transformation matrix. Graphically,*

$[U, |\varepsilon\rangle, \mathcal{E}] \approx_2 [U', |\varepsilon'\rangle, \mathcal{E}']$ *iff*



The contexts used in the proof to show that the constraints (S2) and (T2) are required are of the form 

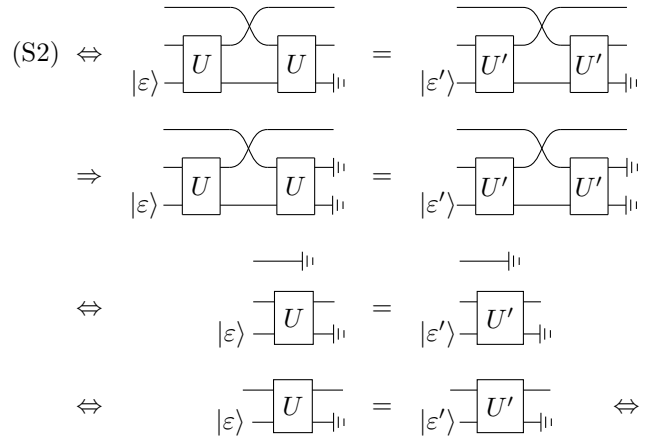
and 

, respectively, for some specific choices of purified channels $[V_0, |\eta_0\rangle, \mathcal{H} \otimes \mathbb{C}^2]$, $[V_1, |\eta_1\rangle, \mathcal{H} \otimes \mathbb{C}^2]$ and $[V, 1, \mathbb{C}]$. Hence, if either the second-level superoperators or the second-level transformation matrices of two purified channels differ, then the channels can be distinguished by using such contexts.

One may have expected the condition (S1) — i.e. that the two channels have the same first-level superoperator — to also appear in Theorem 7.25 (as it did in the previous two cases). This would however have been redundant, as can be seen from the following remark:

Remark 7.26. *Two purified channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$ having the same second-level superoperator also have the same first-level superoperator, i.e. Condition* (S2) *implies* (S1).

Proof.



□

We note, on the other hand, that the three remaining conditions (T1), (S2) and (T2) are nonredundant. I.e. for each of the three there exist cases where only this condition is not satisfied, and where $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon\rangle', \mathcal{E}']$ can be distinguished. E.g. with $\mathcal{E} = \mathcal{E}' = \mathbb{C}$, $U = I_{\mathcal{H}}, U' = -I_{\mathcal{H}}, |\varepsilon\rangle = |\varepsilon'\rangle = 1$, only (T1) fails to hold; with $\mathcal{H} = \mathcal{E} = \mathcal{E}' = \mathbb{C}^2$, $U = \text{CNot}, U' = (\sqrt{Z} \otimes Z)\text{CNot}, |\varepsilon\rangle = |\varepsilon'\rangle = |0\rangle$, only (S2) fails to hold; and with $\mathcal{H} = \mathcal{E} = \mathcal{E}' = \mathbb{C}^2$, $U = I_{\mathcal{H}} \otimes X, U' = I_{\mathcal{H}} \otimes ZX, |\varepsilon\rangle = |\varepsilon'\rangle = |0\rangle$, only (T2) fails to be satisfied.[60]

[60] Where $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}$ and $\text{CNot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

As we did for Theorem 7.21, we are going to prove Theorem 7.25 at the same time as the fact that allowing multiple input/output wires in the contexts does not increase their power, stated as the following proposition:

Proposition 7.27. *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, one has $[U, |\varepsilon\rangle, \mathcal{E}] \approx_2 [U', |\varepsilon'\rangle, \mathcal{E}']$ (that is, for any context $C[\cdot] : \mathcal{H}^{(1)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$) if and only if for any context $C[\cdot] : \mathcal{H}^{(n)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$.*

Namely, what we are going to prove is the following lemma:

Lemma 7.28. *Given two purified $\mathcal{H}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, the following three statements are equivalent:*

(I) $[U, |\varepsilon\rangle, \mathcal{E}] \approx_2 [U', |\varepsilon'\rangle, \mathcal{E}']$, *that is, for any context* $C[\cdot] : \mathcal{H}^{(1)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$

(II) *for any context* $C[\cdot] : \mathcal{H}^{(n)}$, $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] = [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$

(III) $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = T^{(1)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, $\mathcal{S}^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = \mathcal{S}^{(2)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$ *and* $T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = T^{(2)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$

Again, it is clear that this lemma implies both Theorem 7.25 and Proposition 7.27. Indeed, Theorem 7.25 is exactly (I) $\Leftrightarrow$ (III), while Proposition 7.27 is (I) $\Leftrightarrow$ (II).

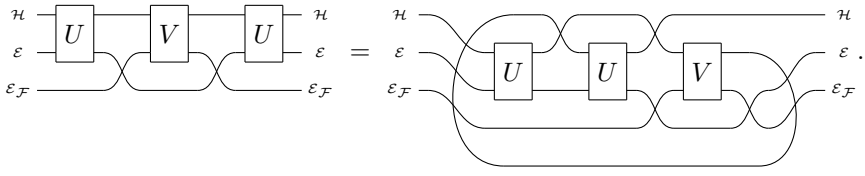
Proof of Lemma 7.28. The structure of the proof is the same as for Theorem 7.21. It is clear that (II) $\Rightarrow$ (I). Therefore, what one has to prove is that (III) $\Rightarrow$ (II) (that is, Conditions (T1), (S2) and (T2) are sufficient even with contexts with mutiple input/output wires) and that (I) $\Rightarrow$ (III) (or equivalently $\neg$(III) $\Rightarrow$ $\neg$(I), that is, the three conditions are necessary).

Proof of Strong Sufficiency ((III) $\Rightarrow$ (II)). Let us assume (III). Let $C[\cdot] : \mathcal{H}^{(n)}$ be any context. Let $\Gamma \vdash D : n$ be an underlying bare diagram of both $C[U, |\varepsilon\rangle, \mathcal{E}]$ and $C[U', |\varepsilon'\rangle, \mathcal{E}']$. Let $\mathcal{G} = ([U_x, |\varepsilon_x\rangle, \mathcal{E}_x])_{x\in\Gamma}$ and $\mathcal{G}' = ([U'_x, |\varepsilon'_x\rangle, \mathcal{E}'_x])_{x\in\Gamma}$ be such that $[U_a, |\varepsilon_a\rangle, \mathcal{E}_a] = [U, |\varepsilon\rangle, \mathcal{E}]$ and $[U'_a, |\varepsilon'_a\rangle, \mathcal{E}'_a] = [U', |\varepsilon'\rangle, \mathcal{E}']$ for some $a \in \Gamma$, while $[U_x, |\varepsilon_x\rangle, \mathcal{E}_x] = [U'_x, |\varepsilon'_x\rangle, \mathcal{E}'_x]$ for all $x \in \Gamma\backslash\{a\}$; and let $\mathcal{F} = ([U_x, |\varepsilon_x\rangle, \mathcal{E}_x])_{x\in\Gamma\backslash\{a\}}$.

Let $c, c' \in \{\mathbf{V}, \mathbf{H}\}$ and $p, p' \in [n]$. By Proposition 7.3, the possible cases are the following:

- $|w^D_{c,p}|_a \leq 1$ and $|w^D_{c',p'}|_a \leq 1$
- $(c,p) \neq (c',p')$, $|w^D_{c,p}|_a = 2$ and $|w^D_{c',p'}|_a = 0$
- $(c,p) \neq (c',p')$, $|w^D_{c,p}|_a = 0$ and $|w^D_{c',p'}|_a = 2$
- $(c,p) = (c',p')$ and $|w^D_{c,p}|_a = 2$.

The first case can be treated exactly in the same way as in the proof of Lemma 7.23. To address the other three cases, one can first note that by deformation, for any $V \in \mathcal{L}(\mathcal{H} \otimes \mathcal{E}_\mathcal{F})$,



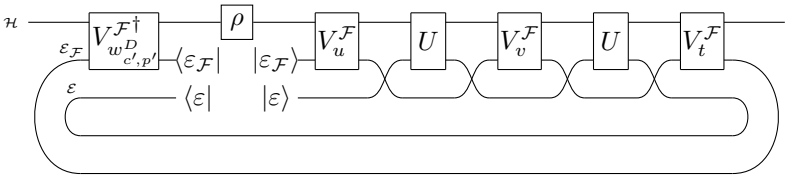
- If $(c,p) \neq (c',p')$, $|w^D_{c,p}|_a = 2$ and $|w^D_{c',p'}|_a = 0$, then one can write $w^D_{c,p} = uavat$ with $u, v, t \in (\Gamma\backslash\{a\})^*$. Then for any $\rho \in \mathcal{L}(\mathcal{H})$:

$$[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!]\left(|c,p\rangle\langle c',p'| \otimes \rho\right) = \left|c^D_{c,p}, p^D_{c,p}\right\rangle\left\langle c^D_{c',p'}, p^D_{c',p'}\right| \otimes \mathrm{Tr}_{\mathcal{E}_\mathcal{G}}\left(V^\mathcal{G}_{w^D_{c,p}}(\rho \otimes |\varepsilon_\mathcal{G}\rangle\langle\varepsilon_\mathcal{G}|)V^{\mathcal{G}\,\dagger}_{w^D_{c',p'}}\right)$$

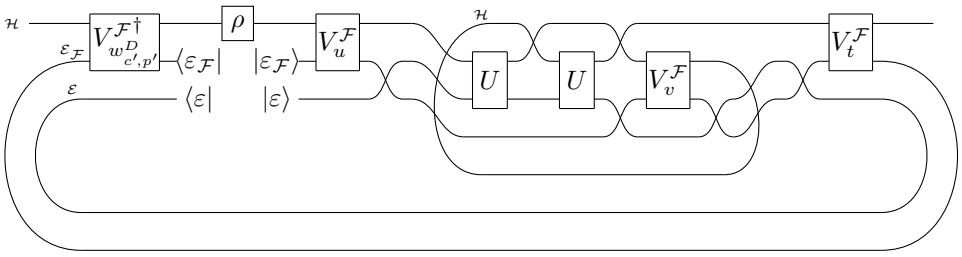
with

$$\mathrm{Tr}_{\mathcal{E}_\mathcal{G}}(V^{\mathcal{G}}_{w^D_{c,p}}(\rho\otimes|\varepsilon_\mathcal{G}\rangle\langle\varepsilon_\mathcal{G}|)V^{\mathcal{G}\dagger}_{w^D_{c',p'}}) = \mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{E}}\left(V^{\mathcal{G}}_t V^{\mathcal{G}}_a V^{\mathcal{G}}_v V^{\mathcal{G}}_a V^{\mathcal{G}}_u(\rho\otimes|\varepsilon_\mathcal{F}\rangle\langle\varepsilon_\mathcal{F}|\otimes|\varepsilon\rangle\langle\varepsilon|)V^{\mathcal{G}\dagger}_{w^D_{c',p'}}\right)$$

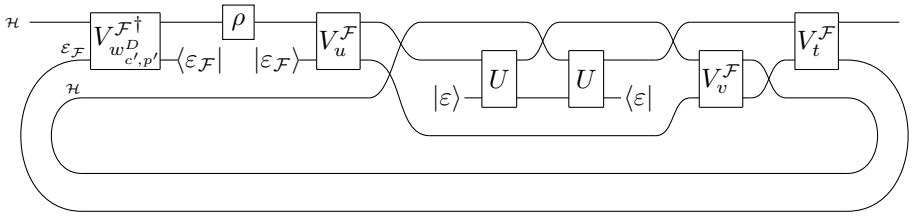
$=$



$=$

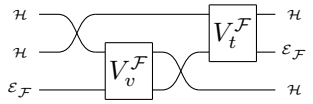


$=$

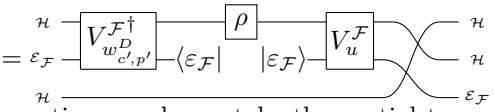


$$= \mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{H}}\left(\sigma_{v,t}\left(T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]}\otimes I_{\mathcal{E}_\mathcal{F}}\right)\sigma_{u,c',p'}\right),$$

where $\sigma_{v,t} =$



and $\sigma_{u,c',p'} =$



(and $\mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{E}} \coloneqq \mathrm{Tr}_{\mathcal{E}_\mathcal{F}}\circ\mathrm{Tr}_{\mathcal{E}}$, $\mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{H}} \coloneqq \mathrm{Tr}_{\mathcal{E}_\mathcal{F}}\circ\mathrm{Tr}_{\mathcal{H}}$; by convention we always take the partial trace over the last factor of the tensor product in both the input and output spaces, so that there is no ambiguity about which copy of $\mathcal{H}$ is traced out in the last formula).

Similarly,

$$[\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!](|c,p\rangle\langle c',p'|\otimes\rho) = \left|c^D_{c,p},p^D_{c,p}\right\rangle\left\langle c^D_{c',p'},p^D_{c',p'}\right|\otimes\mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{H}}\left(\sigma_{v,t}\left(T^{(2)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}\otimes I_{\mathcal{E}_\mathcal{F}}\right)\sigma_{u,c',p'}\right).$$

Since $T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = T^{(2)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, this is equal to $[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|c,p\rangle\langle c',p'|\otimes\rho)$.

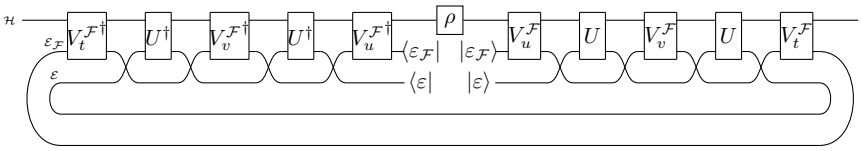
- The case $(c,p)\neq(c',p')$, $|w^D_{c,p}|_a = 0$ and $|w^D_{c',p'}|_a = 2$ is similar to the previous case.
- If $(c,p) = (c',p')$ and $|w^D_{c,p}|_a = 2$, then one can again write $w^D_{c,p}(= w^D_{c',p'}) = uavat$ with $u,v,t\in(\Gamma\backslash\{a\})^*$. Then for any $\rho\in\mathcal{L}(\mathcal{H})$:

$$[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|c,p\rangle\langle c,p|\otimes\rho) = \left|c^D_{c,p},p^D_{c,p}\right\rangle\left\langle c^D_{c,p},p^D_{c,p}\right|\otimes\mathrm{Tr}_{\mathcal{E}_\mathcal{G}}\left(V^{\mathcal{G}}_{w^D_{c,p}}(\rho\otimes|\varepsilon_\mathcal{G}\rangle\langle\varepsilon_\mathcal{G}|)V^{\mathcal{G}\dagger}_{w^D_{c,p}}\right)$$

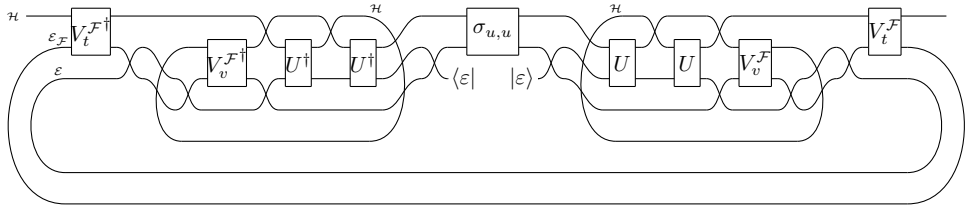
with

$$\mathrm{Tr}_{\mathcal{E}_\mathcal{G}}(V^{\mathcal{G}}_{w^D_{c,p}}(\rho\otimes|\varepsilon_\mathcal{G}\rangle\langle\varepsilon_\mathcal{G}|)V^{\mathcal{G}\dagger}_{w^D_{c,p}}) = \mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{E}}\big(V^\mathcal{G}_t V^\mathcal{G}_a V^\mathcal{G}_v V^\mathcal{G}_a V^\mathcal{G}_u(\rho\otimes|\varepsilon_\mathcal{F}\rangle\langle\varepsilon_\mathcal{F}|\otimes|\varepsilon\rangle\langle\varepsilon|)V^{\mathcal{G}\dagger}_u V^{\mathcal{G}\dagger}_a V^{\mathcal{G}\dagger}_v V^{\mathcal{G}\dagger}_a V^{\mathcal{G}\dagger}_t\big)$$

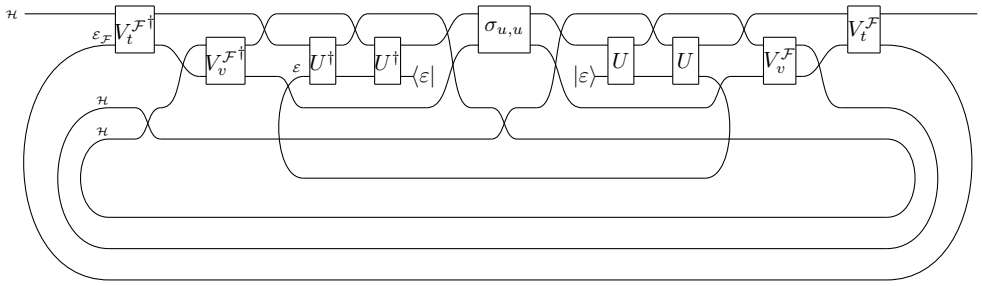
=



=



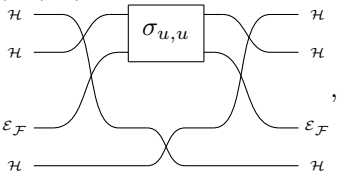
=



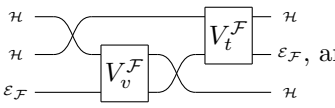
$$= \mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{H},\mathcal{H}}\Big((\sigma_{v,t}\otimes I_\mathcal{H})\mathrm{Tr}_\mathcal{E}\big[(U^{(2)}\otimes I_{\mathcal{E}_\mathcal{F}\otimes\mathcal{H}})(\sigma'_{u,u}\otimes|\varepsilon\rangle\langle\varepsilon|)(U^{(2)}\otimes I_{\mathcal{E}_\mathcal{F}\otimes\mathcal{H}})^\dagger\big](\sigma_{v,t}\otimes I_\mathcal{H})^\dagger(I_{\mathcal{H}\otimes\mathcal{E}_\mathcal{F}}\otimes\mathfrak{S})\Big)$$

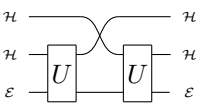
$$= \mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{H},\mathcal{H}}\left((\sigma_{v,t}\otimes I_\mathcal{H})\left(\mathcal{S}^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]}\otimes\mathcal{I}_{\mathcal{E}_\mathcal{F}\otimes\mathcal{H}}\right)[\sigma'_{u,u}](\sigma_{v,t}\otimes I_\mathcal{H})^\dagger(I_{\mathcal{H}\otimes\mathcal{E}_\mathcal{F}}\otimes\mathfrak{S})\right),$$

where $\mathcal{I}_{\mathcal{E}_\mathcal{F}\otimes\mathcal{H}}$ is the identity map over $\mathcal{L}(\mathcal{E}_\mathcal{F}\otimes\mathcal{H})$, $\mathfrak{S} = |\psi_1\rangle\otimes|\psi_2\rangle\mapsto|\psi_2\rangle\otimes|\psi_1\rangle$ is the swap operator (here acting on $\mathcal{H}\otimes\mathcal{H}$), $\sigma_{u,u} =$ 

, $\sigma'_{u,u} =$ 

,

$\sigma_{v,t} =$ 

, and $U^{(2)} =$ 

as in Definition 7.24.

Again, similarly,

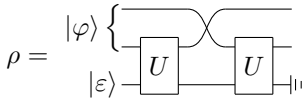
$$[\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!](|c,p\rangle\langle c',p'|\otimes\rho) = \left|c^D_{c,p},p^D_{c,p}\right\rangle\left\langle c^D_{c',p'},p^D_{c',p'}\right|\otimes$$
$$\mathrm{Tr}_{\mathcal{E}_\mathcal{F},\mathcal{H},\mathcal{H}}\left((\sigma_{v,t}\otimes I_\mathcal{H})\left(\mathcal{S}^{(2)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}\otimes\mathcal{I}_{\mathcal{E}_\mathcal{F}\otimes\mathcal{H}}\right)[\sigma'_{u,u}](\sigma_{v,t}\otimes I_\mathcal{H})^\dagger(I_{\mathcal{H}\otimes\mathcal{E}_\mathcal{F}}\otimes\mathfrak{S}_{\mathcal{H},\mathcal{H}})\right).$$

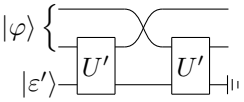
Since $\mathcal{S}^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = \mathcal{S}^{(2)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, this is equal to $[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|c,p\rangle\langle c',p'|\otimes\rho)$.

Proof of Necessity ($\neg$(III) $\Rightarrow$ $\neg$(I)).

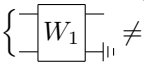
- If $T^{(1)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \neq T^{(1)}_{[U',|\varepsilon\rangle',\mathcal{E}']}$, then by Theorem 7.21, $[U,|\varepsilon\rangle,\mathcal{E}]$ and $[U',|\varepsilon\rangle',\mathcal{E}']$ can be distinguished using a -(¬)--free context $C[\cdot]:\mathcal{H}^{(1)}$, so in particular, $[U,|\varepsilon\rangle,\mathcal{E}] \not\approx_2 [U',|\varepsilon\rangle',\mathcal{E}']$.

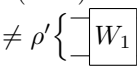
- If $\mathcal{S}^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \neq \mathcal{S}^{(2)}_{[U',|\varepsilon'\rangle,\mathcal{E}']}$, then one can distinguish $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon\rangle', \mathcal{E}']$ as follows.
  By assumption, there exists $|\varphi\rangle \in \mathcal{H} \otimes \mathcal{H}$ s.t. $\rho \neq \rho'$, where $\rho, \rho' \in \mathcal{L}(\mathcal{H} \otimes \mathcal{H})$ are defined as follows:

$\rho =$ 

$\rho' =$ 

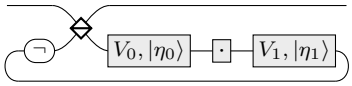
  Let then W_0 be a unitary in $\mathcal{L}(\mathcal{H}^{\otimes 2})$ such that $W_0 |00\rangle = |\varphi\rangle$.

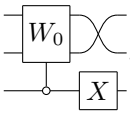
  Note, on the other hand, that matrices of the form $W_1^\dagger(|0\rangle\langle 0| \otimes I_\mathcal{H})W_1$, for all unitaries $W_1 \in \mathcal{L}(\mathcal{H}^{\otimes 2})$, span the whole space $\mathcal{L}(\mathcal{H}^{\otimes 2})$.[61] It follows that for $\rho \neq \rho'$ defined above, there exists a unitary W_1 such that ρ 

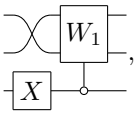
$\neq \rho'$ 

.[62]

  In order to distinguish the two purified channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$, we then consider the following context:

$C[\cdot] =$ 

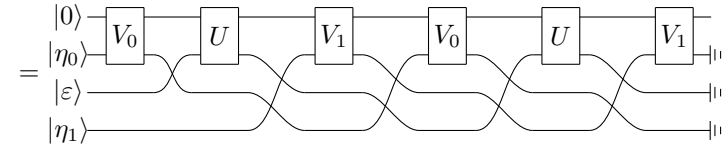
  where $V_0 =$ 

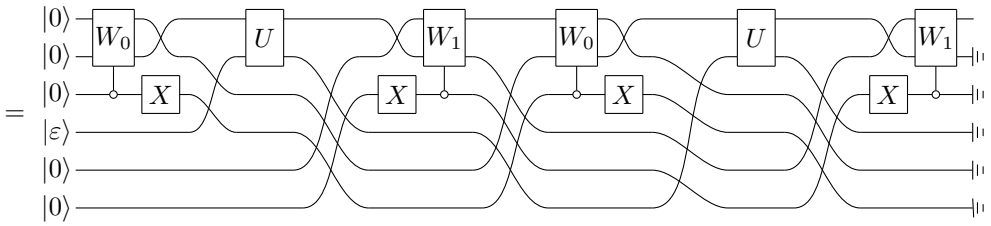
, $V_1 =$ 

, with W_0, W_1 just introduced and $|\eta_0\rangle = |\eta_1\rangle = |0\rangle \otimes |0\rangle \in \mathcal{H} \otimes \mathbb{C}^2$.[63]

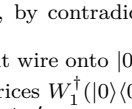
  One then has

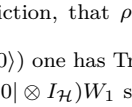
$$(\langle \mathbf{H}, 0| \otimes I_\mathcal{H}) \Big([\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] (|\mathbf{H}, 0\rangle\langle \mathbf{H}, 0| \otimes |0\rangle\langle 0|) \Big) (|\mathbf{H}, 0\rangle \otimes I_\mathcal{H})$$

$=$ 

$=$ 

[61] This can be seen for instance explicitly by noting that any $|\phi\rangle\langle\phi| = V_\phi |00\rangle\langle 00| V_\phi^\dagger$ (which themselves span the whole space, for some unitaries V_ϕ) can be decomposed onto vectors of the form $W_1^\dagger(|0\rangle\langle 0| \otimes I_\mathcal{H})W_1$, as $V_\phi |00\rangle\langle 00| V_\phi^\dagger = V_\phi[(|0\rangle\langle 0| \otimes I_\mathcal{H}) - \frac{1}{d}\sum_{i=0}^{d-1} V_i(|0\rangle\langle 0| \otimes I_\mathcal{H})V_i^\dagger + \frac{1}{d}\mathfrak{S}(|0\rangle\langle 0| \otimes I_\mathcal{H})\mathfrak{S}^\dagger]V_\phi^\dagger$, where d is the dimension of $\mathcal{H}$, with the unitaries $V_i = I_{\mathcal{H}^{\otimes 2}} - (|0\rangle - |i\rangle)(\langle 0| - \langle i|) \otimes |0\rangle\langle 0|$ $\big($such that $V_i(|0\rangle\langle 0| \otimes I_\mathcal{H})V_i^\dagger = |0\rangle\langle 0| \otimes I_\mathcal{H} + (|i\rangle\langle i| - |0\rangle\langle 0|) \otimes |0\rangle\langle 0|\big)$ and the swap operator $\mathfrak{S}$.

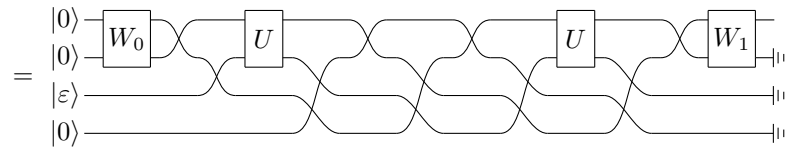
[62] Indeed: assume, by contradiction, that ρ 

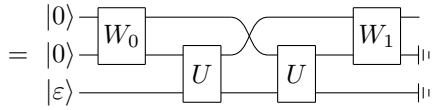
$= \rho'$ 

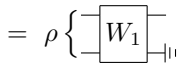
for all unitaries W_1. Then in particular (by projecting the output wire onto $|0\rangle$) one has $\mathrm{Tr}[\rho W_1^\dagger(|0\rangle\langle 0| \otimes I_\mathcal{H})W_1] = \mathrm{Tr}[\rho' W_1^\dagger(|0\rangle\langle 0| \otimes I_\mathcal{H})W_1]$ for all W_1. Given, as just noted, that the matrices $W_1^\dagger(|0\rangle\langle 0| \otimes I_\mathcal{H})W_1$ span the whole space $\mathcal{L}(\mathcal{H}^{\otimes 2})$, one concludes that $\rho = \rho'$ — in contradiction with the fact that $\rho \neq \rho'$.

[63] Where, given $W \in \mathcal{L}(\mathcal{K})$, the controlled linear operation 

is defined as $W \otimes |0\rangle\langle 0| + I_\mathcal{K} \otimes |1\rangle\langle 1|$, and where $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.





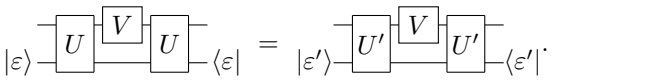


$$\neq \quad \rho'\Big\{ \boxed{W_1} \quad = \quad (\langle \mathbf{H}, 0| \otimes I_{\mathcal{H}}) \Big([\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!] (|\mathbf{H}, 0\rangle\langle \mathbf{H}, 0| \otimes |0\rangle\langle 0|) \Big) (|\mathbf{H}, 0\rangle \otimes I_{\mathcal{H}}).$$

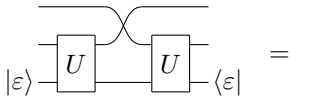
Hence $[\![C[U, |\varepsilon\rangle, \mathcal{E}]]\!] \neq [\![C[U', |\varepsilon'\rangle, \mathcal{E}']]\!]$, and therefore $[U, |\varepsilon\rangle, \mathcal{E}] \not\approx_2 [U', |\varepsilon\rangle', \mathcal{E}']$.

- If $T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \neq T^{(2)}_{[U',|\varepsilon\rangle',\mathcal{E}']}$, then let us first introduce the following lemma:

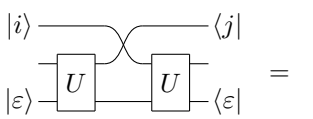
  Lemma 7.29. *Given two purified channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon\rangle', \mathcal{E}']$, $T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} = T^{(2)}_{[U',|\varepsilon\rangle',\mathcal{E}']}$ if and only if for any $V \in \mathcal{L}(\mathcal{H})$,*



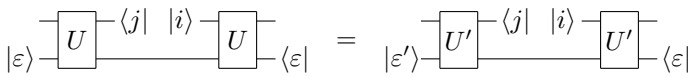
  Proof.



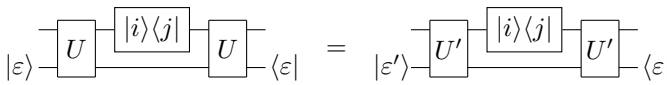
$$\Leftrightarrow \quad \forall i, j,$$



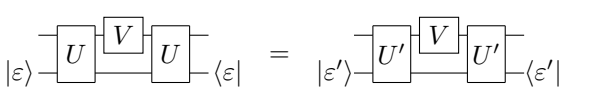
$$\Leftrightarrow \quad \forall i, j,$$



$$\Leftrightarrow \quad \forall i, j,$$

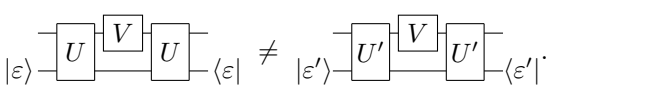


$$\Leftrightarrow \quad \forall V \in \mathcal{L}(\mathcal{H}),$$

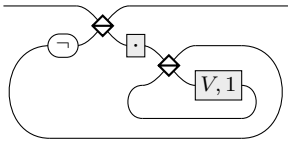


  □

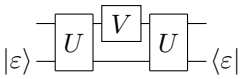
  By this lemma, since unitary operators span the whole space $\mathcal{L}(\mathcal{H})$, if $T^{(2)}_{[U,|\varepsilon\rangle,\mathcal{E}]} \neq T^{(2)}_{[U',|\varepsilon\rangle',\mathcal{E}']}$ then there exists a unitary operator $V \in \mathcal{L}(\mathcal{H})$ such that



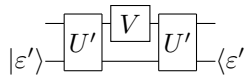
Then by considering the following context:

$C[\cdot] =$ 

one gets

$$[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!](|\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes I_{\mathcal{H}}) = |\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes$$ 

whereas

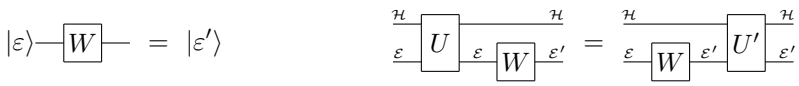
$$[\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!](|\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes I_{\mathcal{H}}) = |\mathbf{H},0\rangle\langle\mathbf{V},0|\otimes$$ 

Hence $[\![C[U,|\varepsilon\rangle,\mathcal{E}]]\!] \neq [\![C[U',|\varepsilon'\rangle,\mathcal{E}']]\!]$, which proves that $[U,|\varepsilon\rangle,\mathcal{E}] \not\approx_2 [U',|\varepsilon\rangle',\mathcal{E}']$. □

7.3 Observational Equivalence Beyond PBS-Diagrams

In this section, we define a new equivalence relation, inspired by the uniqueness (up to an isometry) of Stinespring's dilations, which subsumes the observational equivalences defined so far. For that let us first introduce an isometry-based preorder over purified channels:

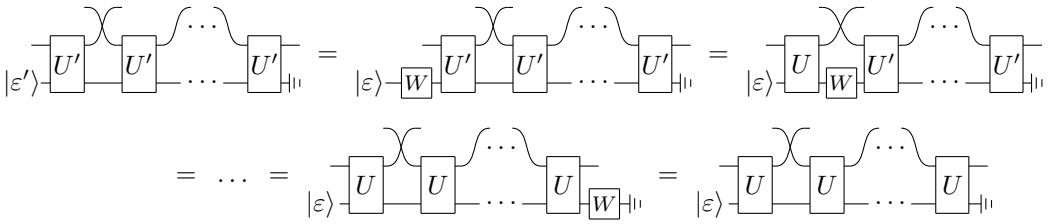
Definition 7.30. *Given two purified $\mathcal{H}$-channels $[U,|\varepsilon\rangle,\mathcal{E}]$ and $[U',|\varepsilon'\rangle,\mathcal{E}']$, one has $[U,|\varepsilon\rangle,\mathcal{E}] \triangleleft_{iso} [U',|\varepsilon'\rangle,\mathcal{E}']$ if there exists an isometry $W:\mathcal{E}\to\mathcal{E}'$ s.t. $W|\varepsilon\rangle = |\varepsilon'\rangle$ and $(I_{\mathcal{H}}\otimes W)U = U'(I_{\mathcal{H}}\otimes W)$. In pictures:*



Note that $\triangleleft_{iso}$ is not an equivalence relation. It is not symmetric; moreover, its symmetric closure is not transitive.[64] This leads us to consider the following:

Definition 7.31 (Iso-equivalence)**.** *The* iso-equivalence *of purified channels is defined as the symmetric and transitive closure of $\triangleleft_{iso}$: $\approx_{iso} \coloneqq \triangleleft_{iso}^{*}$.*

The iso-equivalence is a candidate for characterising indistinguishability of purified channels in more general coherent-control settings. Actually, if $[U,|\varepsilon\rangle,\mathcal{E}]$ and $[U',|\varepsilon'\rangle,\mathcal{E}']$ are two iso-equivalent purified channels, then intuitively, in any coherent-control setting, $[U,|\varepsilon\rangle,\mathcal{E}]$ can be replaced by $[U',|\varepsilon'\rangle,\mathcal{E}']$ without changing the global behaviour. Indeed, the evolution of the environment associated with the purified channel is roughly speaking the same (up to the isometry W): initialised in the state $W|\varepsilon\rangle$(and with the data register in the state $|\phi\rangle$), the application of U' leads to the state $U'(I_{\mathcal{H}}\otimes W)(|\phi\rangle\otimes|\varepsilon\rangle)$, which is equal to $(I_{\mathcal{H}}\otimes W)U(|\phi\rangle\otimes|\varepsilon\rangle)$. So applying U' somehow first cancels the application of W, then applies U, and finally applies W again — which will be cancelled again by the next application of U', and so on. The last application of W is absorbed when the environment is traced out. In pictures:



In the framework of PBS-diagrams, one can actually show that the iso-equivalence subsumes, but does not coincide with the $\approx_2$-equivalence (which in turn subsumes the $\approx_1$- and $\approx_0$-equivalences).

[64] Taking $\mathcal{H}=\mathbb{C}$, one has $[1,1,\mathbb{C}] \triangleleft_{iso} [I_{\mathbb{C}^2},|0\rangle,\mathbb{C}^2]$ (with $W=|0\rangle$) but $\neg([I_{\mathbb{C}^2},|0\rangle,\mathbb{C}^2] \triangleleft_{iso} [1,1,\mathbb{C}])$ (as there is no isometry from $\mathbb{C}^2$ to $\mathbb{C}$). With the Pauli operator $Z=\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$ one also has $[1,1,\mathbb{C}] \triangleleft_{iso} [Z,|0\rangle,\mathbb{C}^2]$ (again with $W=|0\rangle$), but $[I_{\mathbb{C}^2},|0\rangle,\mathbb{C}^2]$ and $[Z,|0\rangle,\mathbb{C}^2]$ are not in relation since there is no unitary W such that $WI_{\mathbb{C}^2} = ZW$ (as $I_{\mathbb{C}^2}$ and Z have distinct eigenvalues).

Proposition 7.32. $\approx_{iso} \subsetneq \approx_2 \subsetneq \approx_1 \subsetneq \approx_0$.

Proof. [$\approx_{iso} \subseteq \approx_2$] Since $\approx_2$ is an equivalence relation it is enough to show that $\lhd_{iso} \subseteq \approx_2$. If $[U, |\varepsilon\rangle, \mathcal{E}] \lhd_{iso} [U', |\varepsilon'\rangle, \mathcal{E}']$, then the three conditions of Theorem 7.25 are satisfied, implying $[U, |\varepsilon\rangle, \mathcal{E}] \approx_2 [U', |\varepsilon'\rangle, \mathcal{E}']$.
[$\approx_2 \neq \approx_{iso}$] We consider the following two purified $\mathbb{C}$-channels: $[X, |0\rangle, \mathbb{C}^3]$ and $[XN, |0\rangle, \mathbb{C}^3]$ where $X = |x\rangle \mapsto |x-1 \bmod 3\rangle$ and $N = |x\rangle \mapsto (-1)^x |x\rangle$ are two (qutrit) unitary transformations. The two purified channels are $\approx_2$-equivalent as they satisfy the conditions of Theorem 7.25. In order to show that they are not iso-equivalent, note that if two purified $\mathbb{C}$-channels $[U, |\varepsilon\rangle, \mathcal{E}]$ and $[U', |\varepsilon'\rangle, \mathcal{E}']$ are iso-equivalent then for any $k \geq 0$ one has $\langle\varepsilon| U^k |\varepsilon\rangle = \langle\varepsilon'| WU^k |\varepsilon\rangle = \langle\varepsilon'| U'^k W |\varepsilon\rangle = \langle\varepsilon'| U'^k |\varepsilon'\rangle$. Since $\langle 0| X^3 |0\rangle = 1 \neq -1 = \langle 0| (XN)^3 |0\rangle$, it follows that $[X, |0\rangle, \mathbb{C}]$ and $[XN, |0\rangle, \mathbb{C}]$ are indeed not iso-equivalent.
[$\approx_2 \subsetneq \approx_1 \subsetneq \approx_0$] The inclusions are clear from the characterisations of Theorems 7.19, 7.21 and 7.25, together with Remark 7.26. The fact that the inclusions are strict follows from the observations that the various conditions appearing in these theorems are non-redundant. □

In unpublished work, that we cannot expose here in details due to time constraints, we have considered a natural extension of the language of extended PBS-diagrams, with a n-dimensional "polarisation" and natural generalisations of negations and PBS. The observational equivalence $\approx_n$ is then characterised by natural generalisations of Conditions (S1), (T1), (S2) and (T2). We have proved that two purified channels are $\approx_n$-equivalent for all n if and only if they are iso-equivalent.

Moreover, we have proved that the natural merge between the language of extended PBS-diagrams and that of $\mathrm{LO_v}$-circuits (that is, the traced PROP generated by the generators of both languages — which can be seen as the language of extended PBS-diagrams enriched with additional optical components, or equivalently as the language of $\mathrm{LO_v}$-circuits enriched with purified channels and a trace operator), equipped with a natural extension of the quantum semantics of extended PBS-diagrams — in which the trace follows the physical intuition of the instant-travel trace described in Section 5.5.1 — provides a coherent-control setting for purified channels in which the observational equivalence is precisely captured by the iso-equivalence. In other words, $\mathrm{LO_v}$-circuits with instant-travel trace have the same distinguishing power as PBS-diagrams with a control system of arbitrary dimension. Intuitively, by considering a context of the same shape as the left-hand side of Equation (5.78), with the hole gate in the loop, the global unitary evolution is an infinite sum whose terms correspond to all possible numbers of iterations of the purified channel, and by varying the parameter of the beam splitter, one can extract enough information about the terms of the series to decide the $\approx_n$-equivalence of two purified channels for any n.

An open question is whether the iso-equivalence still characterises the observational equivalence in other settings, for instance if in the language of $\mathrm{LO_v}$-circuits with purified channels and trace just mentioned, one considers a delayed trace semantics (see Section 5.5.2).

Conclusion

The first goal of this PhD was to develop a formal framework for representing quantum computations involving coherent control, studying their various properties and reasoning about them. Starting from the observation that it is easy with optical schemes to perform coherent control of quantum operations, the initial idea for doing so was to start from those optical implementations, and to abstract them into a graphical language.

Essentially following this idea, a first contribution of this thesis is to start developing such a framework, by introducing the PBS-calculus in Chapter 3, and its variants in Chapters 4 and 7. We have in particular equipped these languages with semantics consistent with their physical interpretation, and provided complete axiomatisations for the PBS-calculus and its coloured refinement.

A second contribution is to start using this framework, with the limited features it already offers, for the study of coherent control. In particular, we have investigated the question of resource optimisation of coherently controlled quantum computations in Chapter 4. We have also studied the distinguishability of quantum channels in the presence of coherent control, by using PBS-diagrams to formalise and precisely describe families of coherent control contexts, in Chapter 7.

The idea of starting from a class of linear optical setups to develop our framework has naturally introduced another point of view on our graphical languages, which consists in seeing the diagrams as primarily representing physical linear optical schemes. Taking this point of view, a third contribution of this thesis is to introduce a graphical language, the LO_{v}-calculus, for representing and reasoning on photon-preserving linear optical circuits. We have equipped both this language and its fragment for polarisation-preserving circuits (the $\mathrm{LO}_{\mathrm{PP}}$-calculus) with complete equational theories. Additionally, we have introduced a normal form for polarisation-preserving circuits, as a refinement of the universal form of Reck *et al.* [114], This normal form makes it possible to represent any unitary transformation in a unique way. We have also defined a strongly normalising and confluent rewriting system which puts any polarisation-preserving circuit in this form.

Finally, as a last contribution, the complete equational theory found for polarisation-preserving linear optical circuits has enabled us to find the first known complete equational theory for quantum circuits, by exploiting a correspondence between their generators and multi-controlled gates of quantum circuits.

An obvious direction for future research is to increase the expressiveness of our languages, in particular those dedicated to coherent control. Indeed, in the PBS-calculus and its variants, the fact that the polarisation is of dimension 2, and that therefore a particle can pass at most twice at the same place, somehow makes the language look like a programming language in which the only available loops are for-loops bounded to 2 iterations, which additionally cannot be nested. Therefore, a natural extension of these languages consists in allowing for a control state of arbitrary dimension. Note that then the diagrams cannot be immediately interpreted as linear optical schemes anymore.

Another possible extension consists in adding generators such as those of the LO_{v}-calculus, able to create superpositions in the polarisation or the position (instead of just exploiting a preexisting superposition in the input state of the particle). We have briefly discussed such an extension at the end of Chapter 7, and we have seen that this makes superpositions of arbitrarily long evolutions possible, and — at least if we do not take time into account — allows for distinguishing purified channels as efficiently as allowing for a control state of arbitrary dimension. A natural question is to what extent this can be compared to recursion or while-loop features.

Developing extensions of our languages that allow for more general coherent control would naturally raise the question of extending the study of resource optimisation made in Chapter 4 to those settings. More generally, it would be interesting to consider resource optimisation in a language for quantum control more expressive than the PBS-calculus, and to develop resource optimisation techniques for quantum computations involving arbitrary quantum control.

Concerning the results of Chapter 7, other open questions raised by our work include equipping extended PBS-diagrams with an equational theory, and lifting the observational equivalence to diagrams themselves (that is, considering contexts with a bigger hole in which diagrams can be plugged).

Additionally, note that in our description of purified channels, the state of the environment does not evolve by itself, but only when the particle goes through the channel and the unitary U is applied to the joint system. In fact, under reasonable modeling hypotheses, as long as each channel is used at most twice (as it was the case in Chapter 7), any free evolution of the environment between two uses could be included in U; however, introducing such an evolution could make a difference when considering extensions of the language, if the channels are used more than twice, and the evolution is different between different uses.

Concerning the LO_{v}-calculus, as mentioned in Remark 5.10, its semantics can be straightforwardly extended to the case of several photons. A direction for future work is to extend its syntax to allow for sources and detectors of a non-zero number of photons. A natural question is then in particular to look for a complete equational theory for the extended language. A more exploratory research direction is to add support for features such as squeezed states or continuous variables.

Note that given a $\mathrm{LO}_{\mathrm{PP}}^{\mathrm{PRO}}$-circuit, it is actually possible to give an upper bound on the maximum number of rewriting steps needed to reach a normal form. An open question is whether we can make this upper bound tight enough to be useful in practice.

Note also that contrary to the PBS-calculus and the CPBS-calculus, we have not proved that the axiomatisation of the LO_{v}-calculus is minimal. Proving such a minimality result, or simplifying the equational theory, is therefore a natural open question. Additionally, one can wonder whether Equation (5.G) can be simplified, for instance by removing the phases. Indeed, the two sides could then directly be interpreted as two Euler decompositions of a rotation in three-dimensional space.

Concerning the complete equational theory for quantum circuits, an open question of interest is to simplify the set of equations. In particular, Equation (6.r) is a family of equations acting on an unbounded number of qubits. Such a family of equations is a natural byproduct of our proof technique: the decoding of each axiom of $\mathrm{LO}_{\mathrm{PP}}$ produces an equation made of multi-controlled gates that has to be derived using QC. In fact, one can even find surprising that Equation (6.r) is the only remaining equation with multi-controlled gates. Nonetheless, it would be of interest to know whether it can be deduced from equations on a bounded number of qubits. Note that the ZX-calculus has a complete axiomatisation with an Euler equation only on one qubit [127].

Apart from Equation (6.r), note that some progress has already been made in simplifying the equational theory [36]. In particular, Equations (6.n) and (6.o) have been proved to be derivable in QC, moreover without using Equation (6.r).

A natural application of the completeness result is to design procedures for quantum circuit optimisation based on this equational theory. Note however that to use Equation (6.r), one has to decompose a gate into multi-controlled gates. Since the number of multi-controlled gates in the decomposition is exponential in the number of controls added, it might be difficult to keep such procedures tractable. This is one of the motivations for simplifying Equation (6.r).

Another question for future work is to prove (upper or lower) bounds on the size of a derivation between two given equivalent circuits, as well as a bound on the size of the intermediate quantum circuits. Proving lower bounds might be useful for providing a verifiable quantum advantage, in particular if there exist polysize quantum circuits requiring exponentially many rewrites [1].

Appendix A

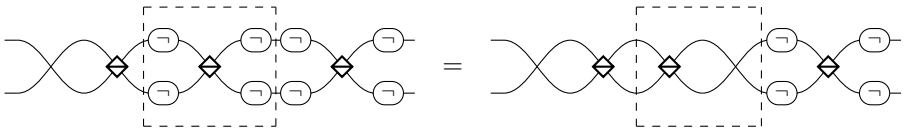
PBS-Diagrams and the PBS-Calculus

A.1 Derivations of Ancillary Equations

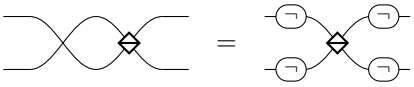
A.1.1 Derivations of the Ancillary Equations of the Proof of Lemma 3.26.

It remains to prove Equations (3.12) to (3.22).

To prove Equation (3.17), we have, by Equation (3.5):

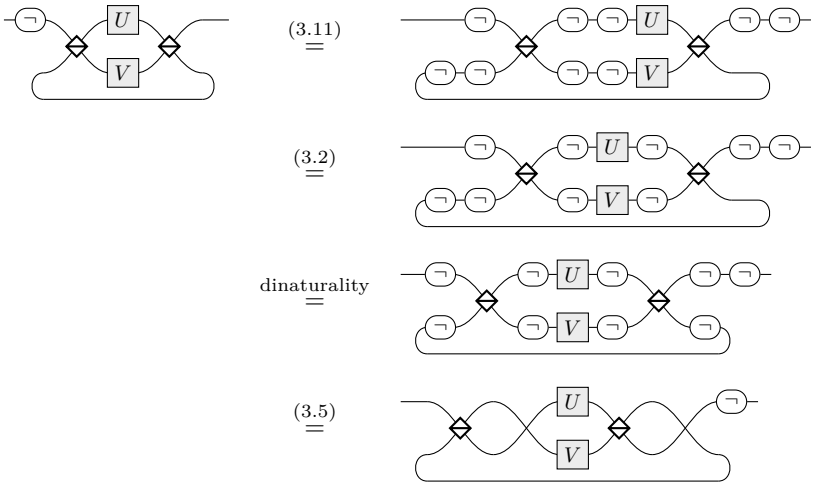


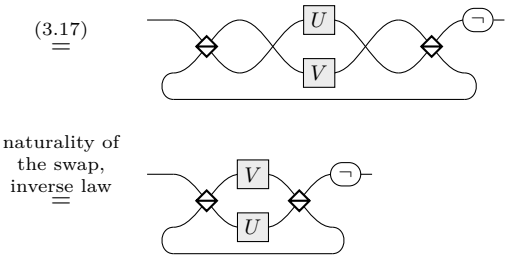
by Equations (3.11) and (3.8), and inverse law, this implies that



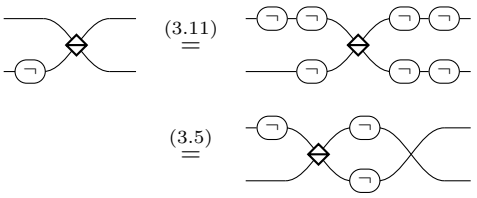
which, together with Equation (3.5), implies Equation (3.17).

To prove Equation (3.12), we have:

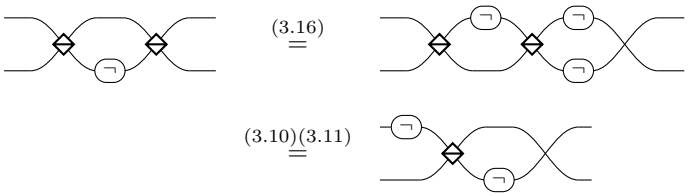




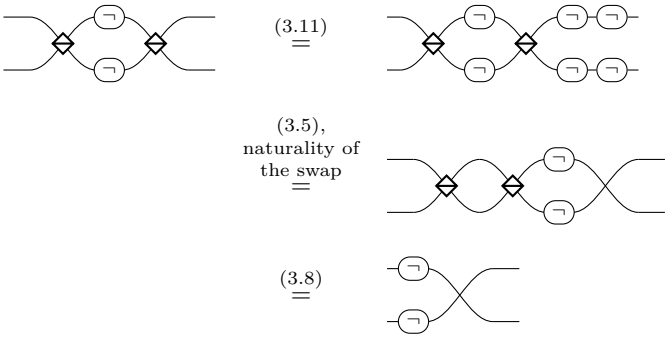
To prove Equation (3.16), we have:



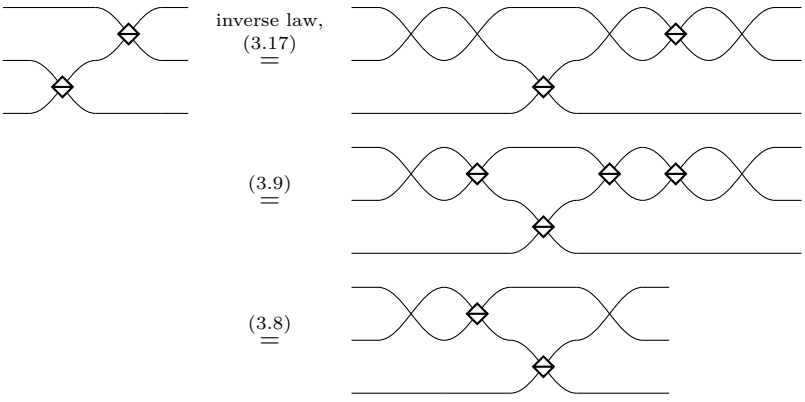
To prove Equation (3.21), we have:



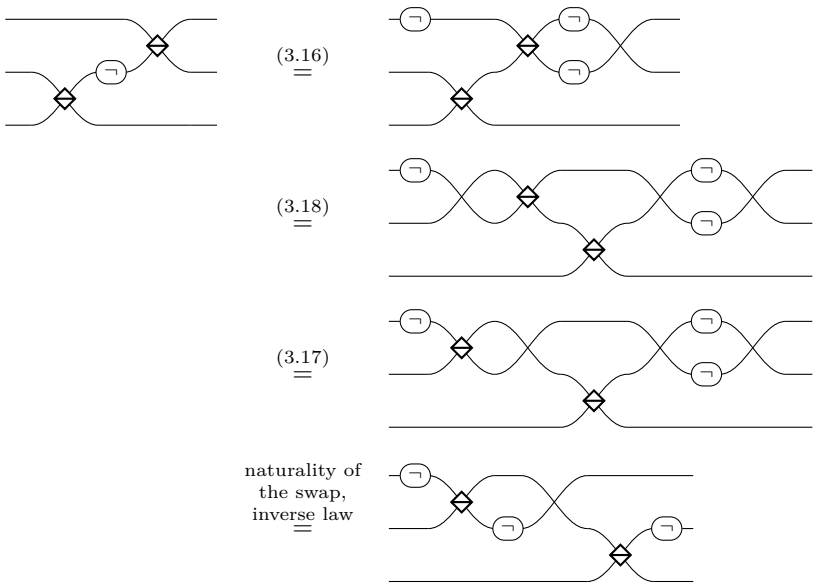
To prove Equation (3.22), we have:



To prove Equation (3.18), we have:

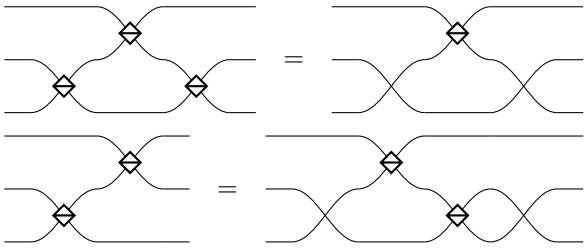


To prove Equation (3.19), we have :



Ancillary Equations. To prove the remaining equations, we need some ancillary equations:

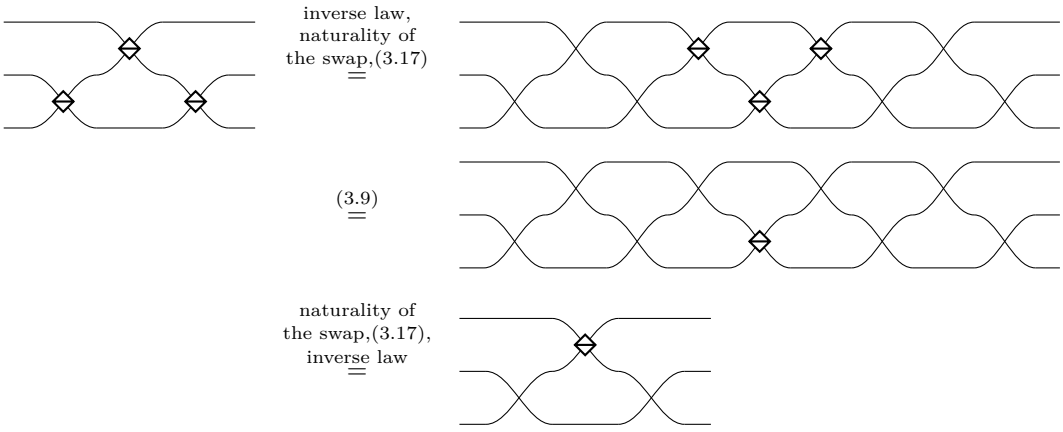
Lemma A.33. *The following equations are consequences of the axioms of the* PBS*-calculus:*



(A.1)

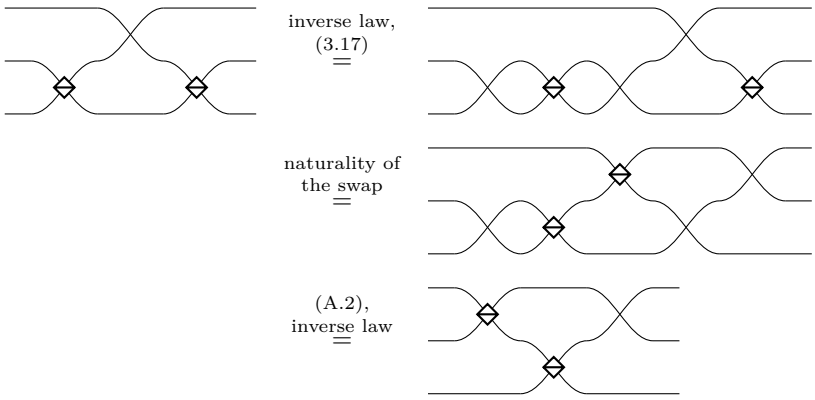
(A.2)

Proof. To prove Equation (A.1), we have:



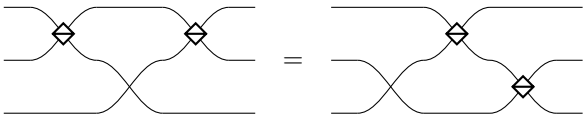
The proof of Equation (A.2) is obtained by rotating the proof of Equation (3.18) by 180° (it uses Equation (A.1) instead of Equation (3.9)). □

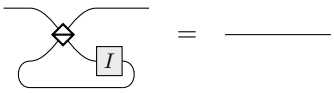
To prove Equation (3.20), we have:



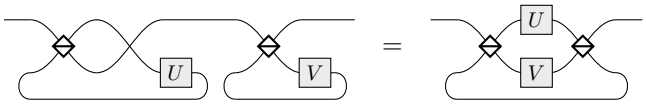
Ancillary Equations. To prove the remaining equations, we need additional ancillary equations:

Lemma A.34. *The following equations are consequences of the axioms of the* PBS*-calculus:*

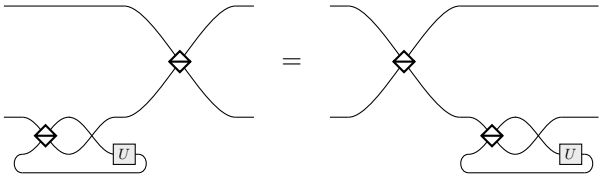

(A.3)



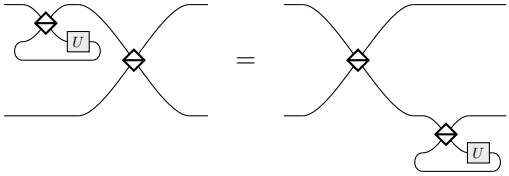
(A.4)



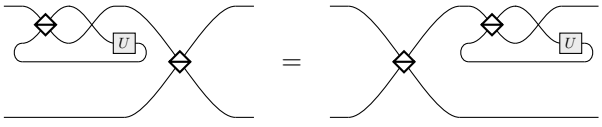
(A.5)



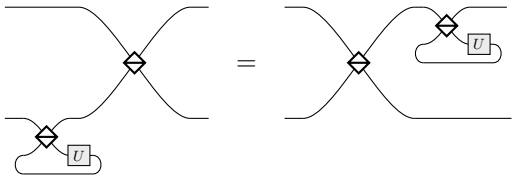
(A.6)



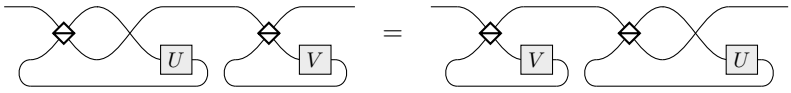
(A.7)



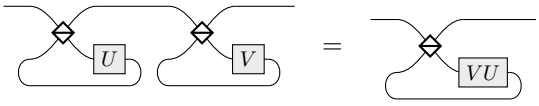
(A.8)



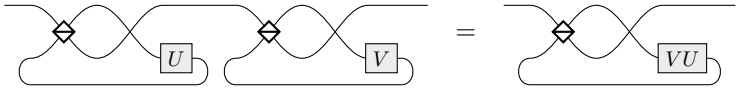
(A.9)



(A.10)



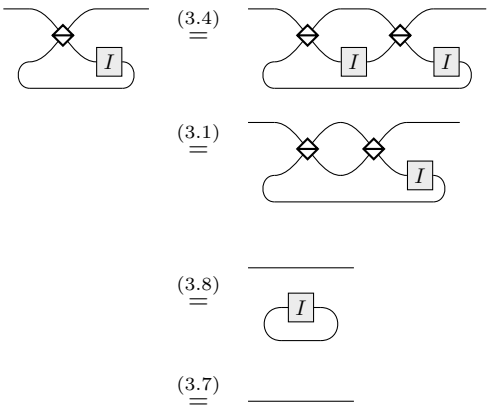
(A.11)



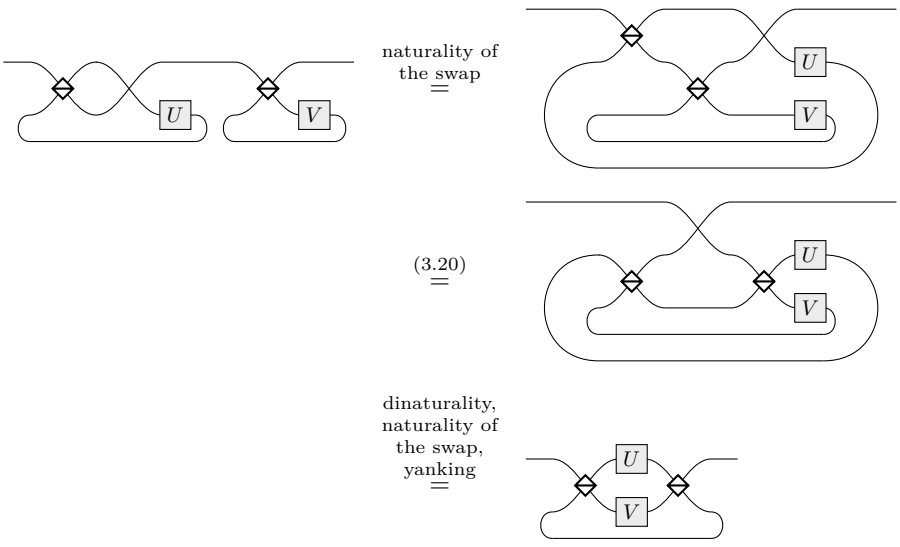
(A.12)

Proof. The proof of Equation (A.3) is obtained by rotating the proof of Equation (3.20) by 180° (it uses Equation (3.18) instead of Equation (A.2)).

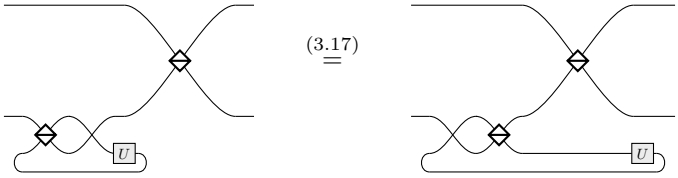
To prove Equation (A.4), we have:

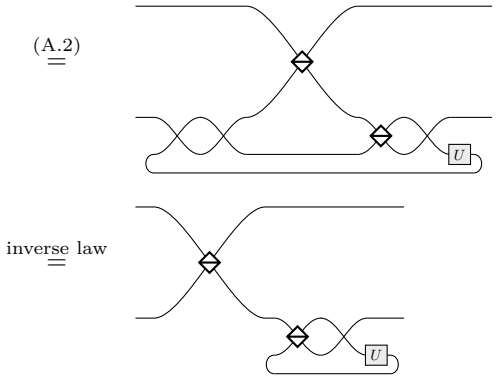


To prove Equation (A.5), we have:

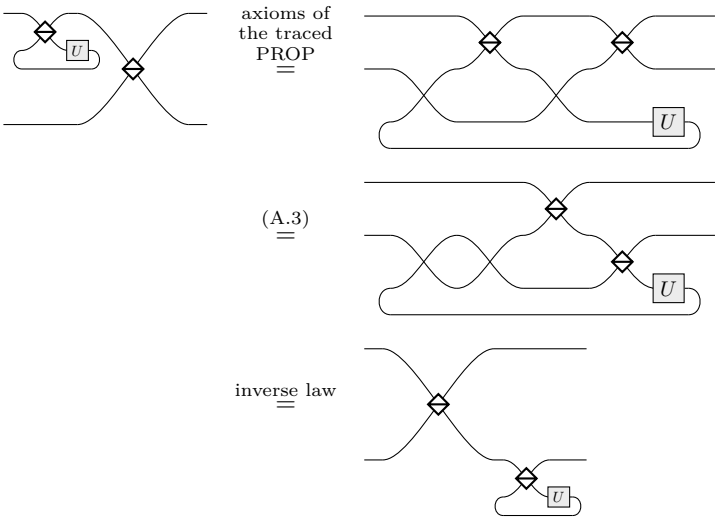


To prove Equation (A.6), we have:

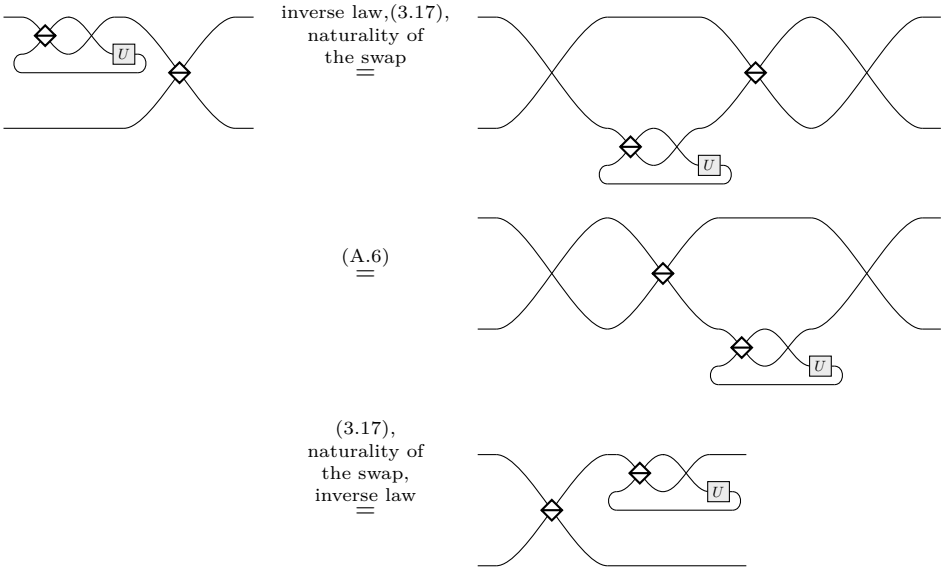




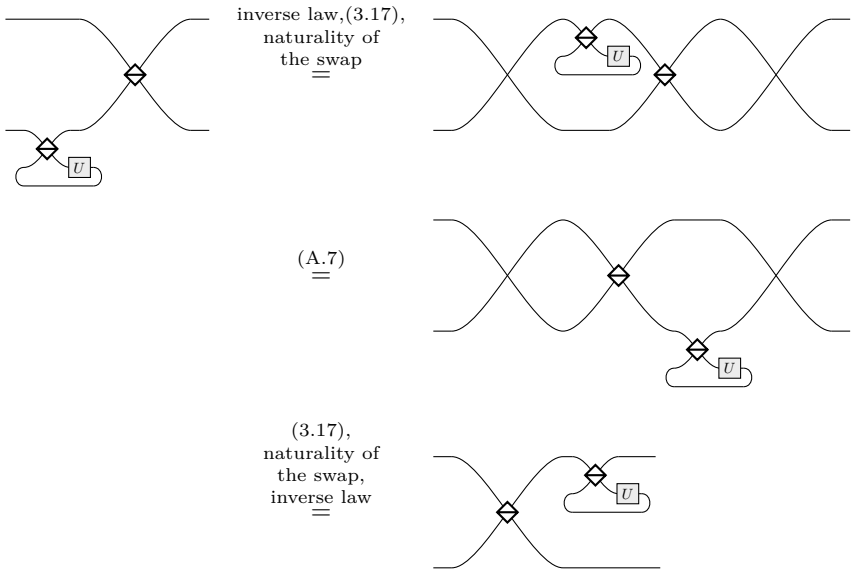
To prove Equation (A.7), we have:



To prove Equation (A.8), we have:

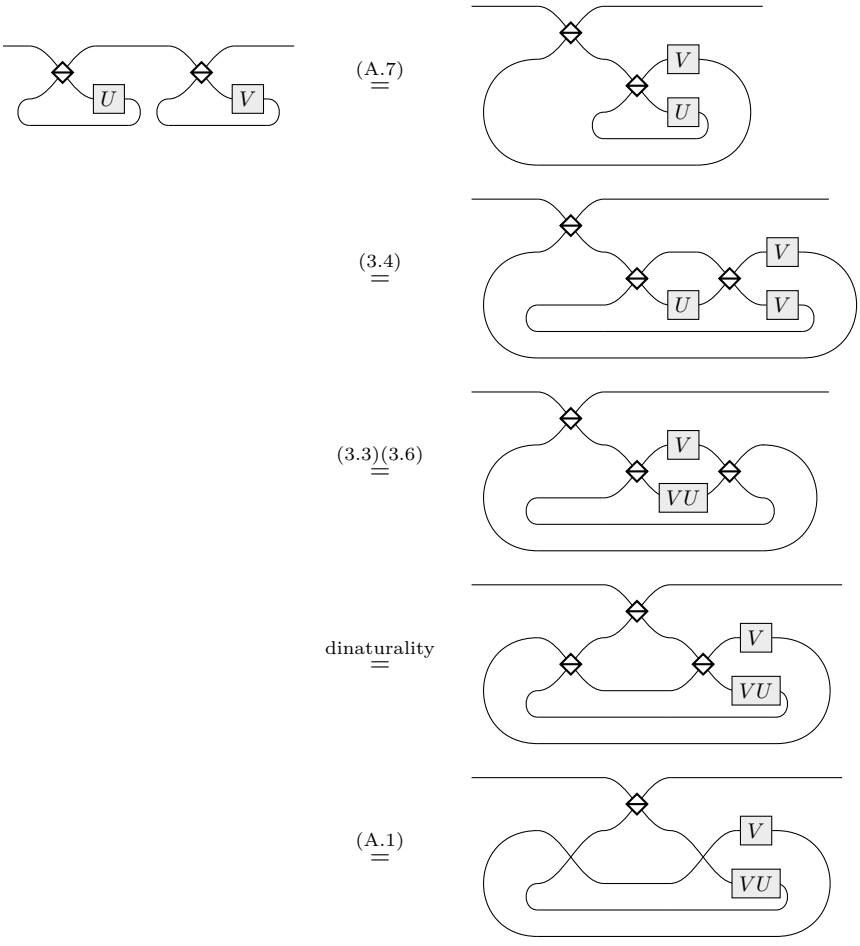


To prove Equation (A.9), we have:

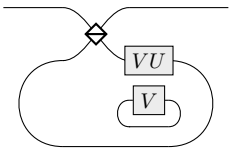


Equation (A.10) is a direct consequence of Equation (A.8).

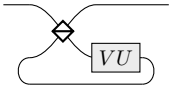
To prove Equation (A.11), we have:



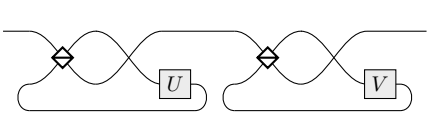
dinaturality, naturality of the swap, inverse law =



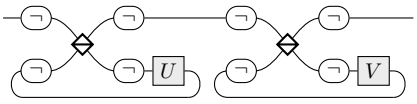
(3.7) =



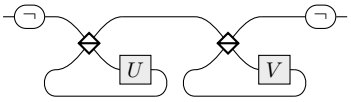
To prove Equation (A.12), we have:



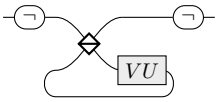
(3.5) =



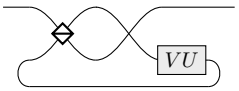
dinaturality, (3.2),(3.11) =



(A.11) =

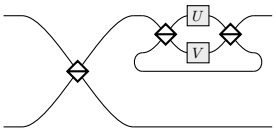


(3.11), dinaturality, (3.2),(3.5) =

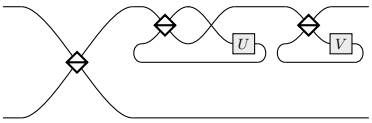


□

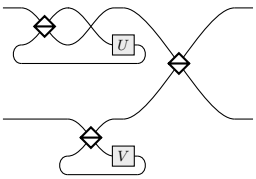
Now we are ready to prove the last three equations:
To prove Equation (3.13), we have:



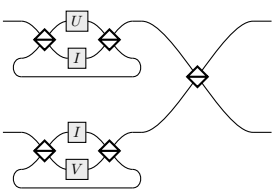
(A.5) =



(A.8)(A.9) =

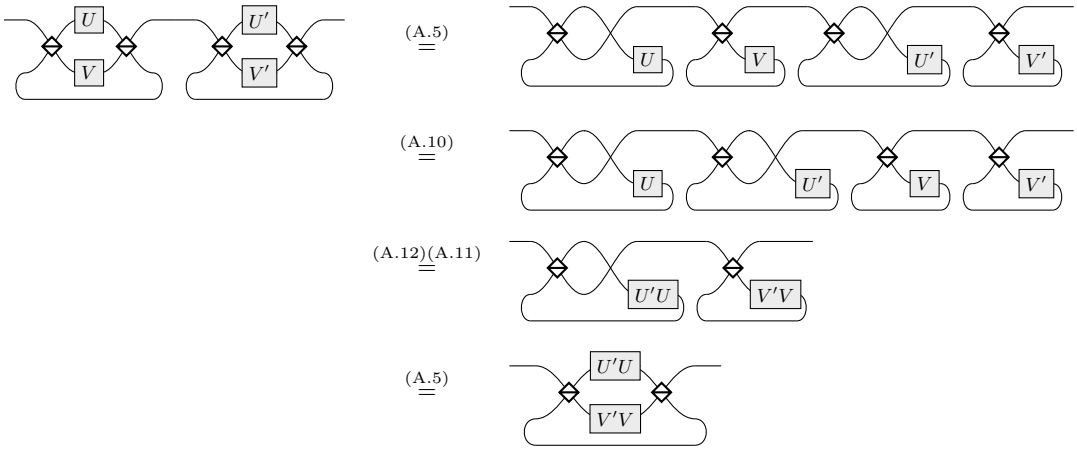


(A.4)(A.5)(3.4)(3.1) =



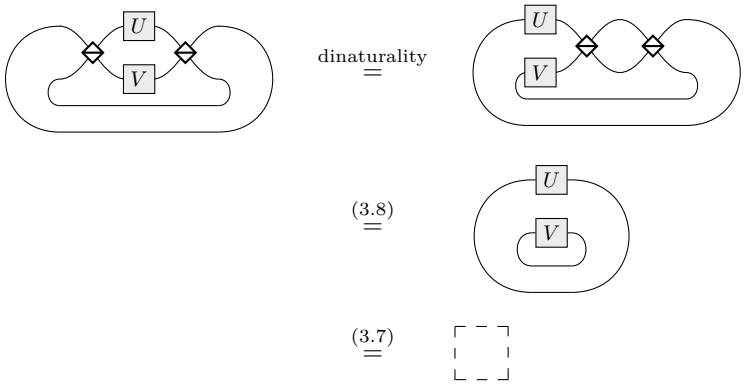
Equation (3.14) is proved in the same way as Equation (3.13), using Equations (A.6) and (A.7) instead of (A.8) and (A.9).

To prove Equation (3.15), we have:

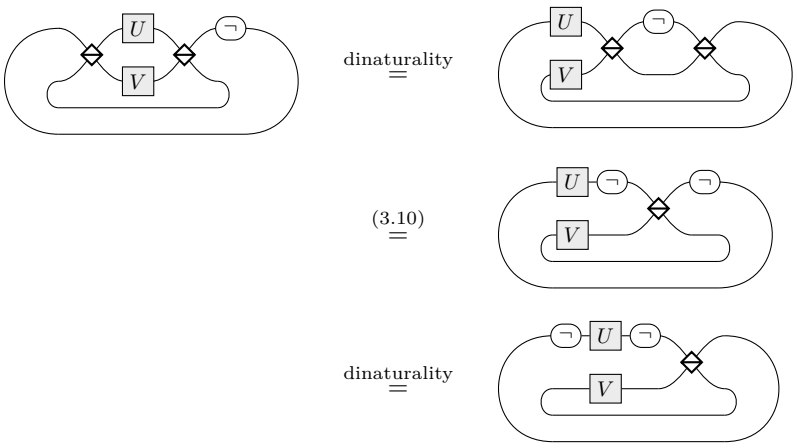


A.1.2 Derivations of the Ancillary Equations of the Proof of Lemma 3.28.

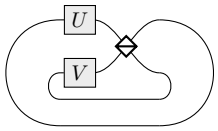
To prove Equation (3.23), we have:



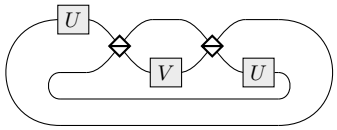
To prove Equation (3.24), we have:



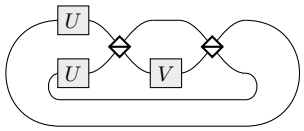
(3.2)(3.11) =



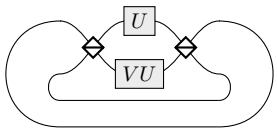
(3.4) =



dinaturality =

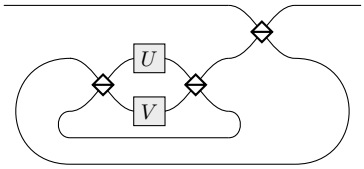


(3.3)(3.6) =

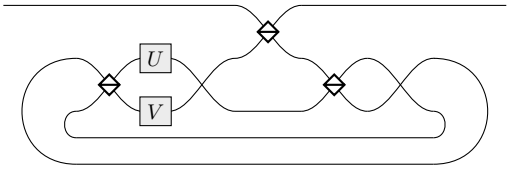


(3.23) =

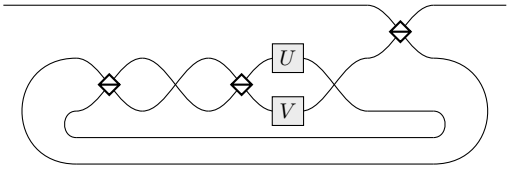
To prove Equation (3.25), we have:



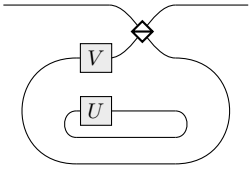
(A.2) =



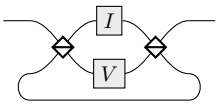
dinaturality =



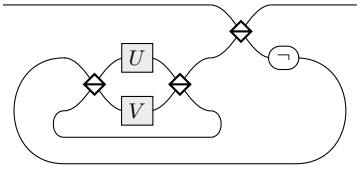
(3.17),(3.8), inverse law =



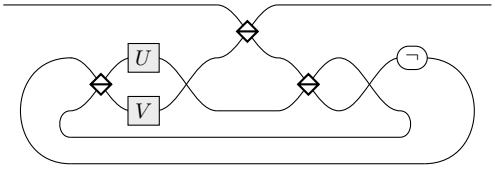
(3.7)(3.4)(3.1) =



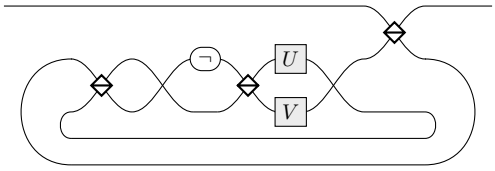
To prove Equation (3.26), we have:



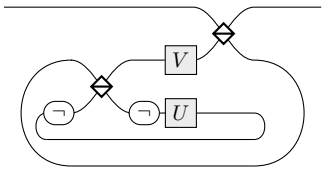
(A.2) =



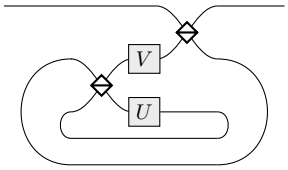
dinaturality
=



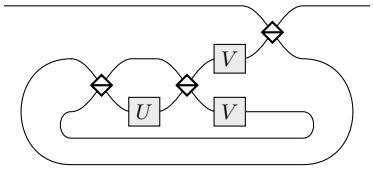
(3.17),(3.10),
naturality of
the swap,(3.17),
inverse law
=



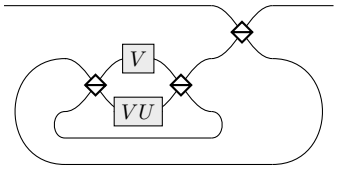
dinaturality,
(3.2),(3.11)
=



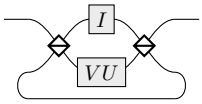
(3.4)
=



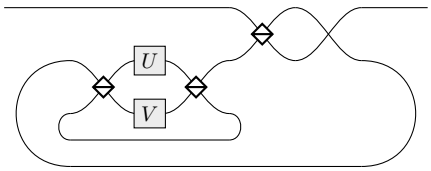
(3.3)(3.6)
=



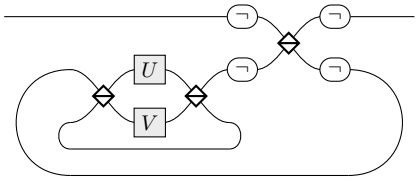
(3.25)
=



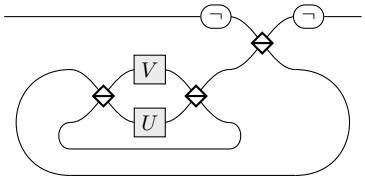
To prove Equation (3.27), we have:



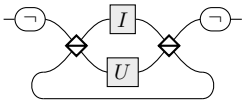
(3.5)
=

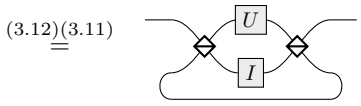


dinaturality,
(3.12),(3.11)
=

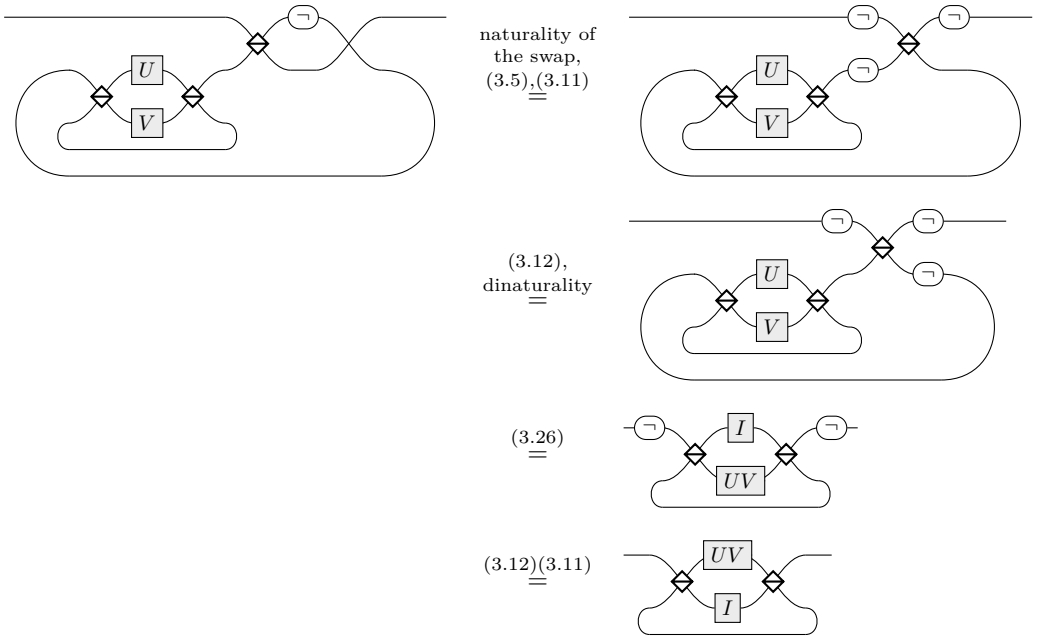


(3.25)
=





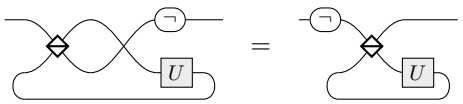
To prove Equation (3.28), we have:



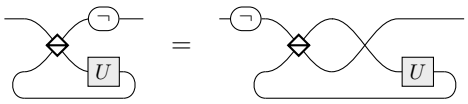
A.2 Proof of Equivalence Between the Two Diagrams of Figure 3.2 Using the PBS-Calculus

We need the following two ancillary equations:

Lemma A.35. *The following equations are consequences of the axioms of the* PBS*-calculus:*

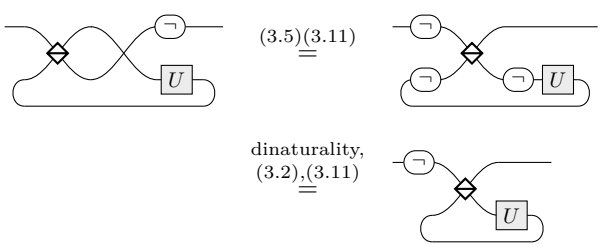


(A.47)

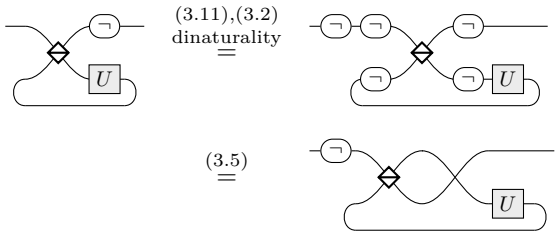


(A.48)

Proof. To prove Equation (A.47), we have:

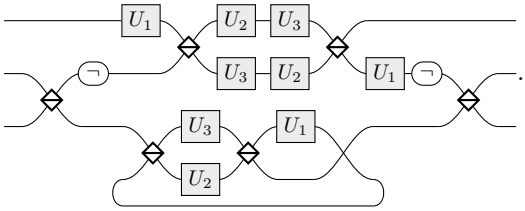


To prove Equation (A.48), we have:

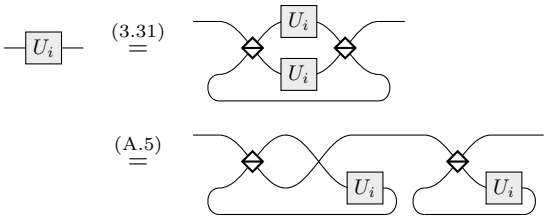


□

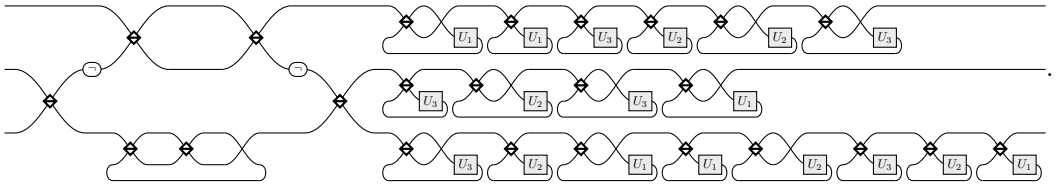
We have to transform the following diagram into the other one of Figure 3.2:



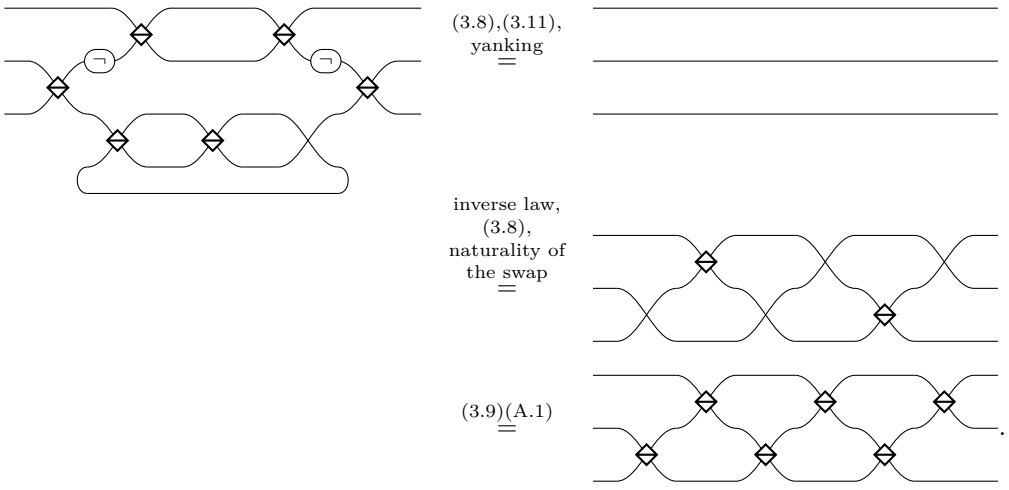
First, we transform each gate into two loops using Equations (3.31) and (A.5):



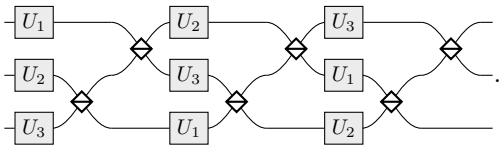
then we slide all loops to the right using Equations (A.6), (A.7), (A.8), (A.9), (A.47) and (A.48). We get:



Next, we transform the left part:



Finally, using again Equations (A.6) to (A.9), (A.47) and (A.48), then (A.5) and (3.31), we slide the loops into the diagram and merge them two by two to get the desired diagram:

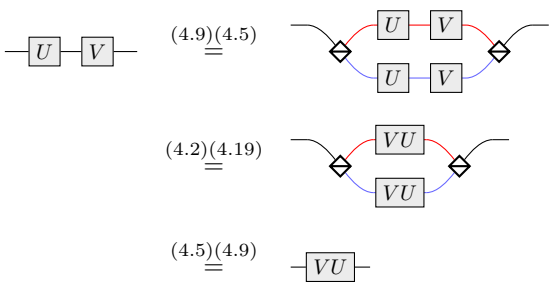


Appendix B

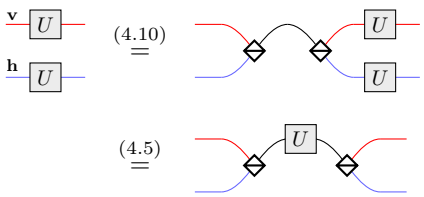
Coloured PBS-Diagrams and Resource Optimisation

B.1 Derivations of Equations (4.21) to (4.27)

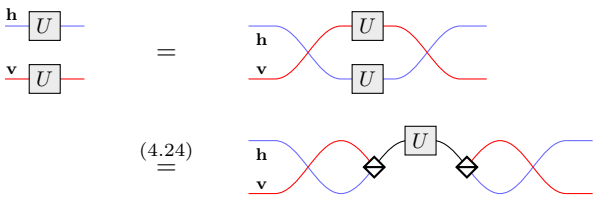
Note that Equation (4.21) is a particular case of Equation (4.2) and that Equation (4.22) is a particular case of Equation (4.19). To prove Equation (4.23), we derive a more general version, analogous to Equations (4.2) and (4.19): for any monoid M and any $U, V \in \mathsf{M}$,

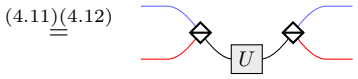


To prove Equation (4.24), we have:

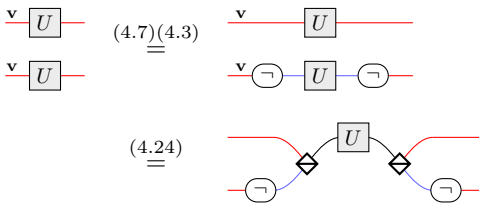


To prove Equation (4.25), we have:

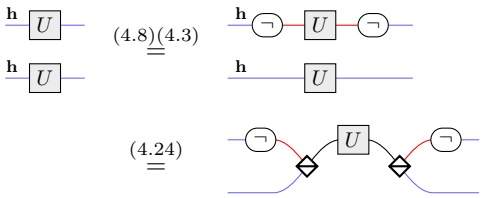




To prove Equation (4.26), we have:



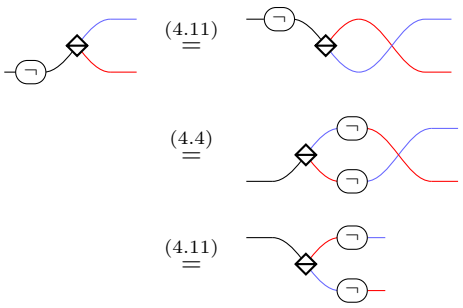
To prove Equation (4.27), we have:



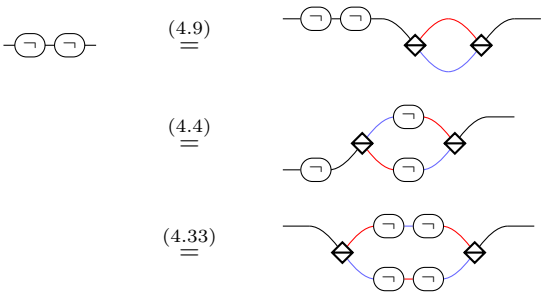
B.2 Derivations of the Ancillary Equations Used in the PGT procedure

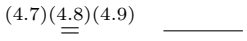
We have to derive Equations (4.28) to (4.41) from the equations of Figure 4.4. In order to benefit from some dependencies between the derivations, we treat the equations in the following order: (4.33), (4.28), (4.29), (4.30), (4.31), (4.41), (4.32), (4.34), (4.35), (4.36), (4.37), (4.38), (4.39), (4.40).

For Equation (4.33), the derivation is the following:

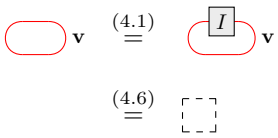


For Equation (4.28):

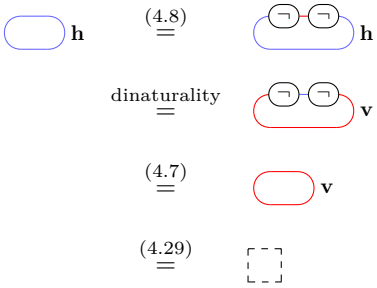




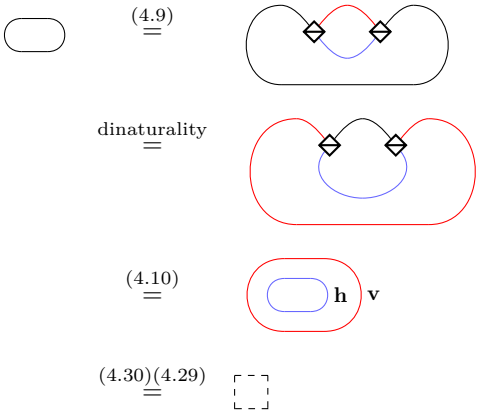
For Equation (4.29):



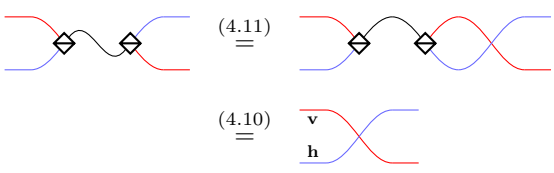
For Equation (4.30):



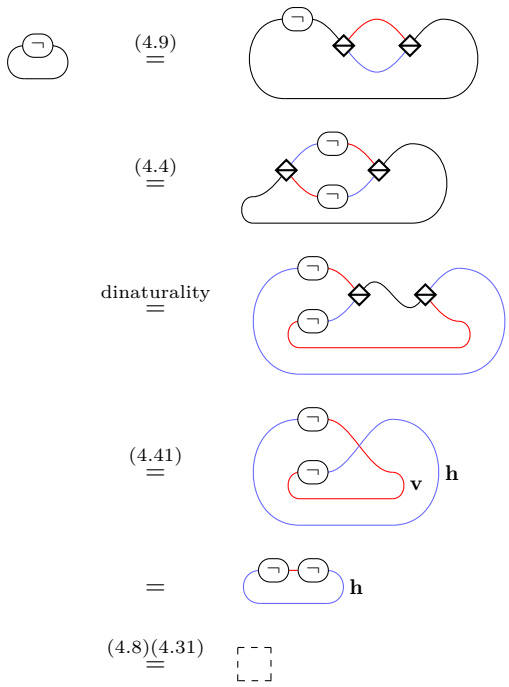
For Equation (4.31):



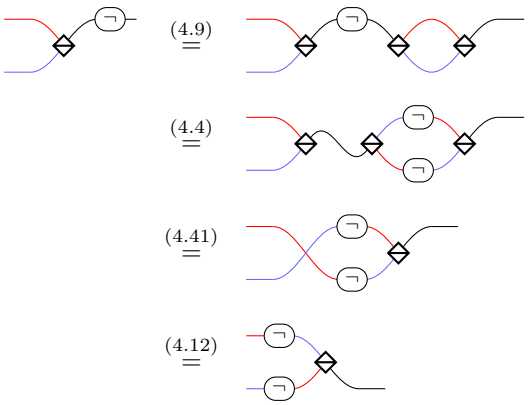
For Equation (4.41):



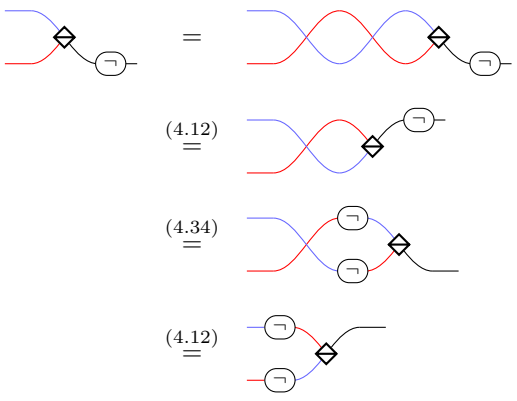
For Equation (4.32):



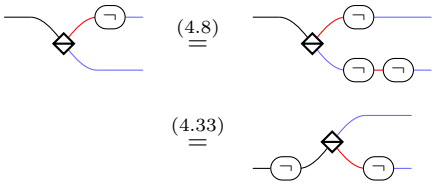
For Equation (4.34):



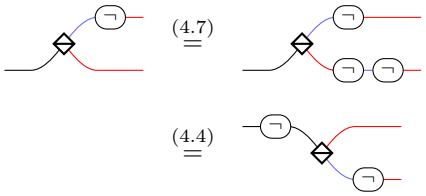
For Equation (4.35):



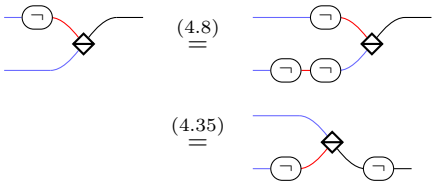
For Equation (4.36):



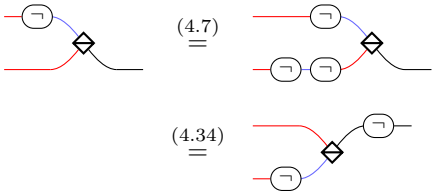
For Equation (4.37):



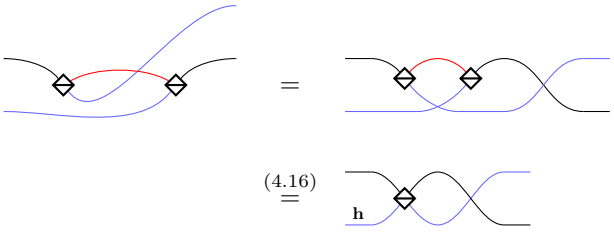
For Equation (4.38):



For Equation (4.39):



For Equation (4.40):

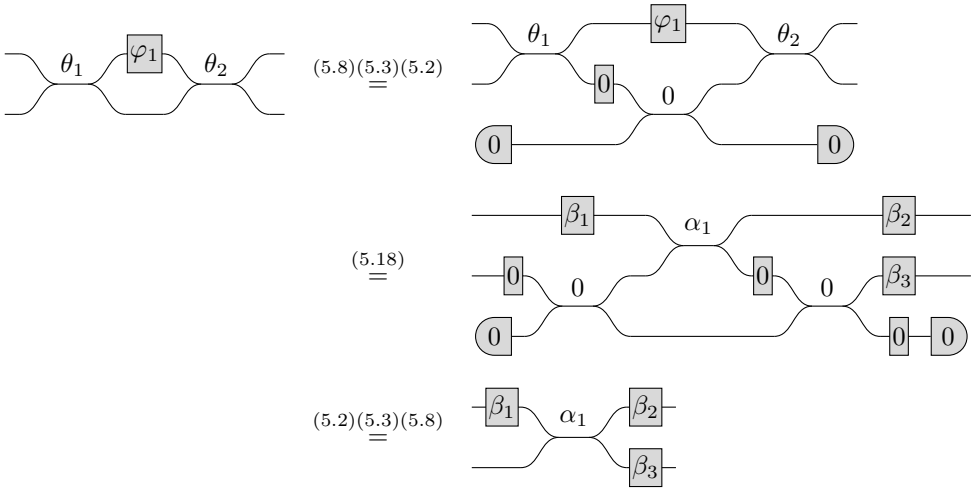


Appendix C

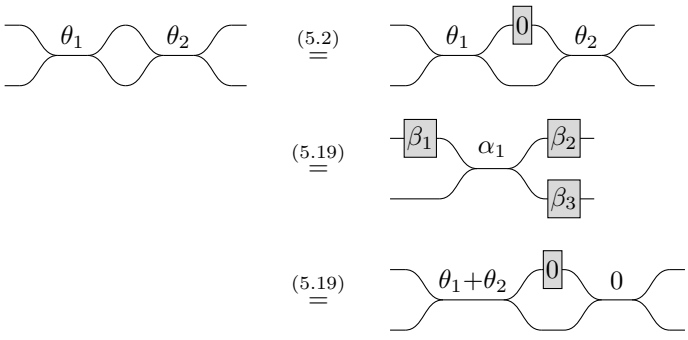
$\mathbf{LO_V}$-Calculus : A Graphical Language for Photon-Preserving Linear Optical Circuits

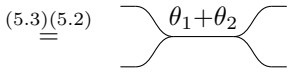
C.1 Useful Consequences of the Axioms

To prove Equation (5.19), we have:

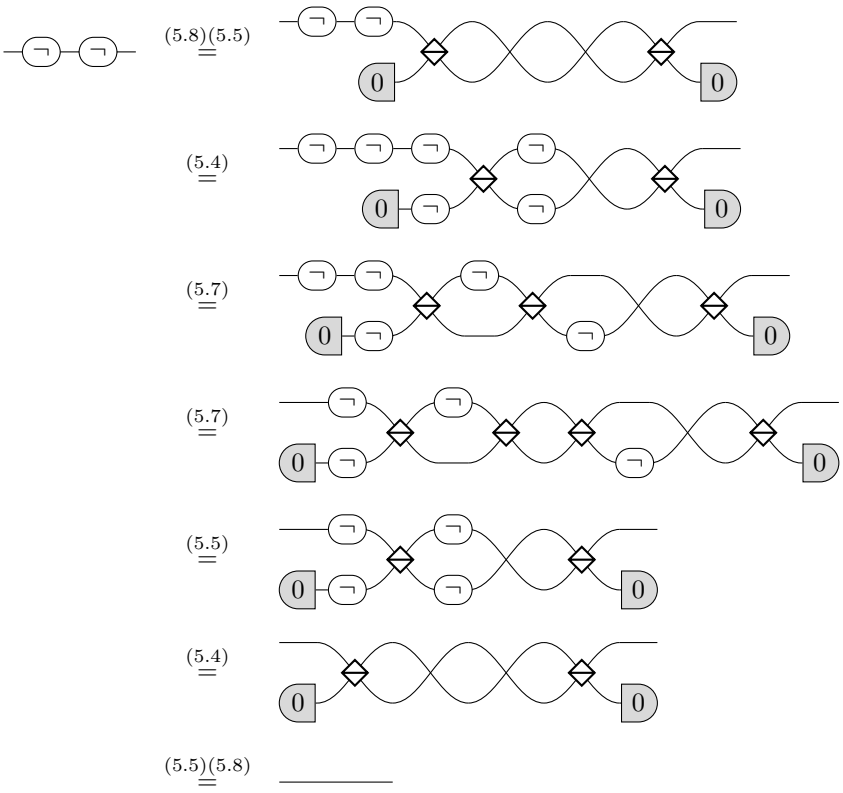


To prove Equation (5.20), we have:

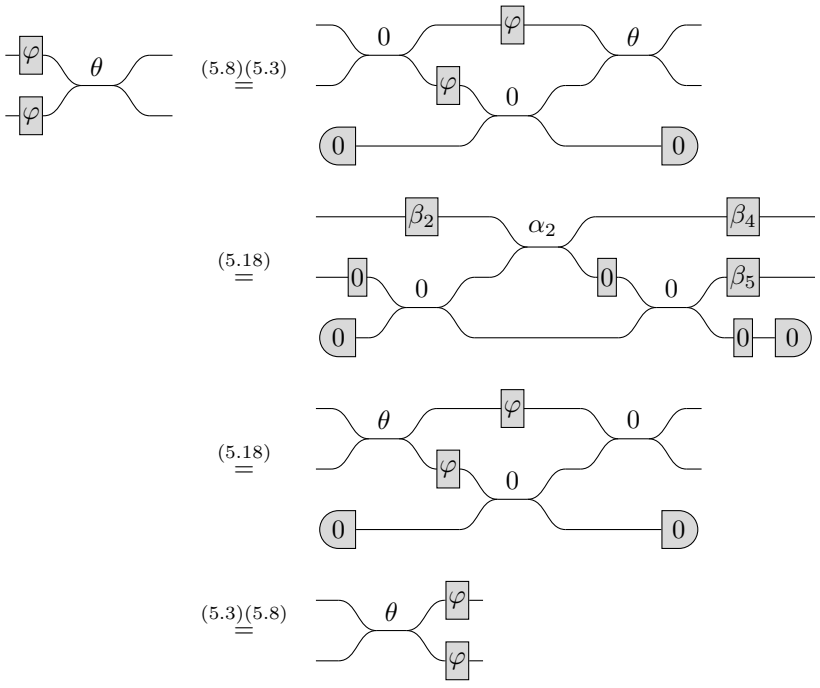




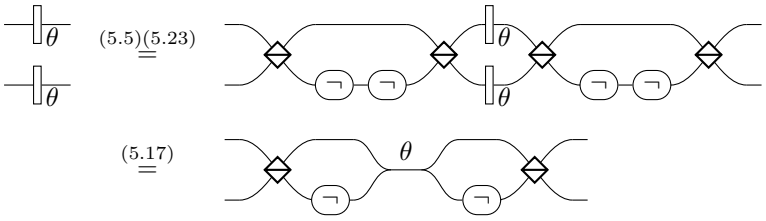
To prove Equation (5.23), we have (cf. Proposition 3.21):



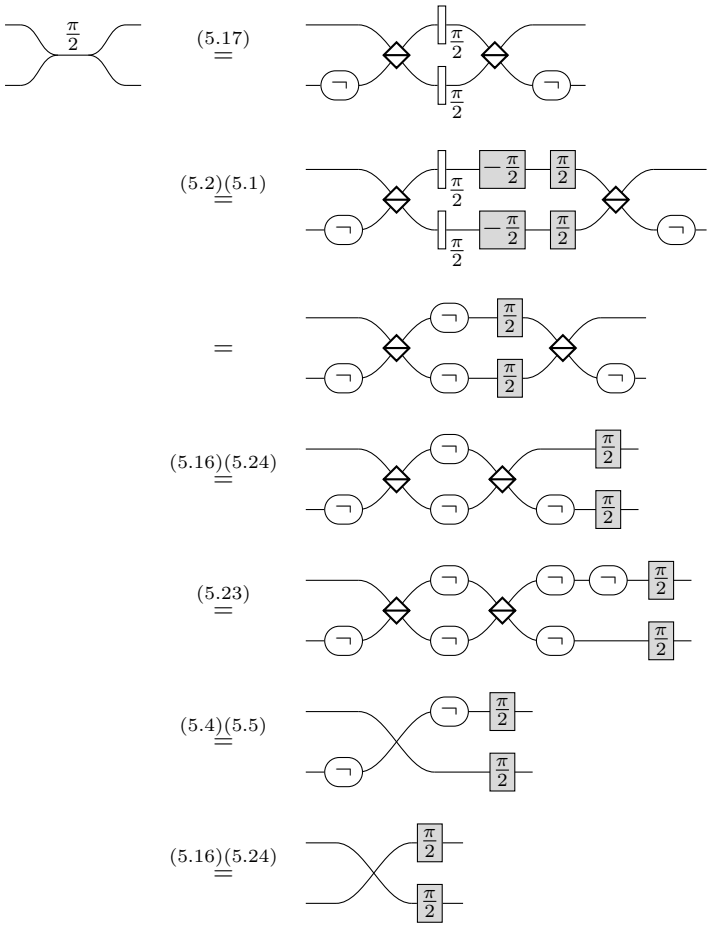
Equation (5.24) is a direct consequence of Equations (5.1) and (5.15).
To prove Equation (5.21), we have:



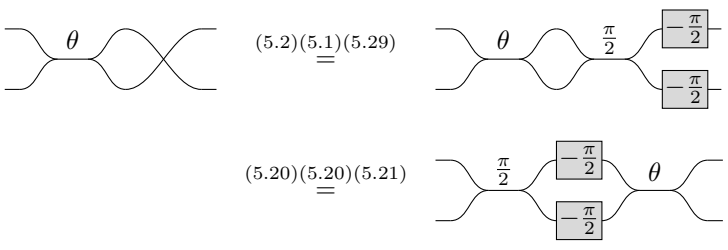
To prove Equation (5.22), we have:



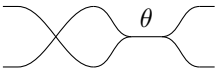
Equation (5.25) is a direct consequence of Equations (5.9) and (5.10).
Equation (5.26) is a direct consequence of Equations (5.12) and (5.13).
Equation (5.27) is a direct consequence of Equations (5.10), (5.11), (5.17) and (5.25).
Equation (5.28) is a direct consequence of Equations (5.13), (5.14), (5.17) and (5.26).
To prove Equation (5.29), we have:



To prove Equation (5.30), we have:



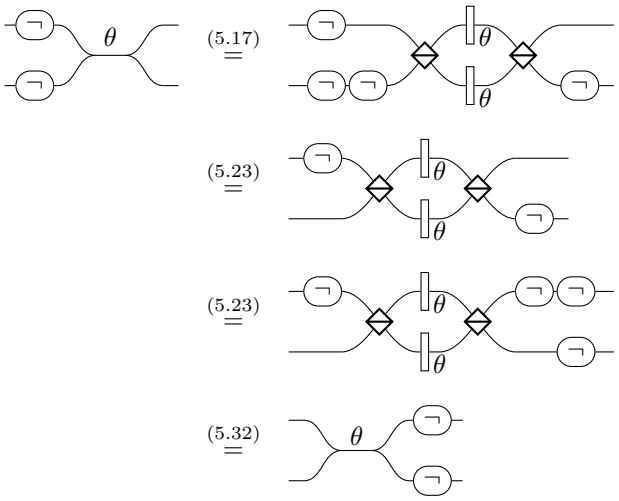
(5.29)(5.1)(5.2) =



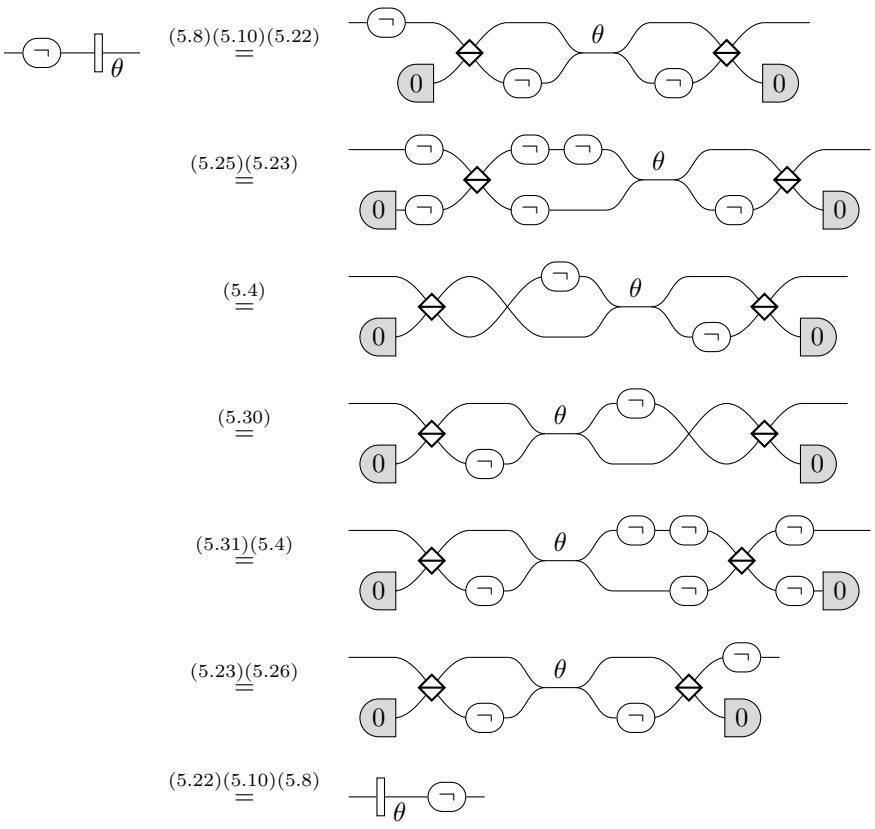
Equation (5.31) is proved at the beginning of Appendix A.1.1 as Equation (3.17). The derivation only uses Equations (3.5), (3.8) and (3.11), which correspond respectively to Equations (5.4), (5.5) and (5.23).

Equation (5.32) is a direct consequence of Equations (5.17), (5.30) and (5.31).

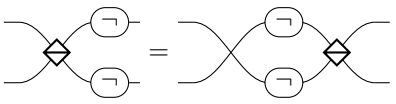
To prove Equation (5.33), we have:

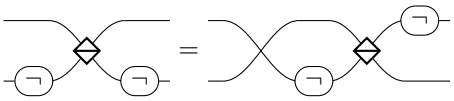


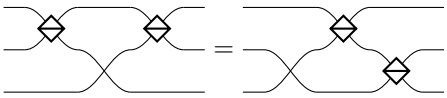
To prove Equation (5.34), we have:

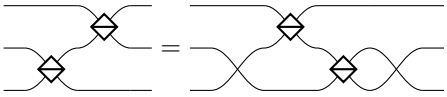


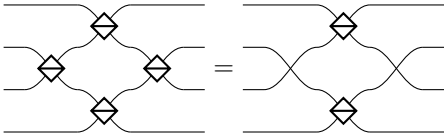
Proof of Equation (5.35). To prove Equation (5.35), we need the following auxiliary equations, which are consequences of Equations (5.4), (5.5), (5.6) and (5.7):

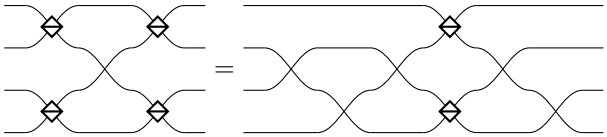

(C.1)

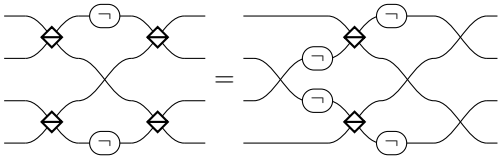

(C.2)

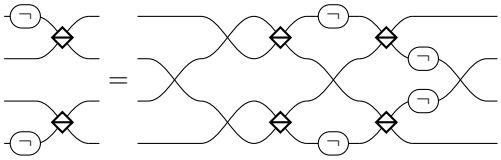

(C.3)


(C.4)


(C.5)

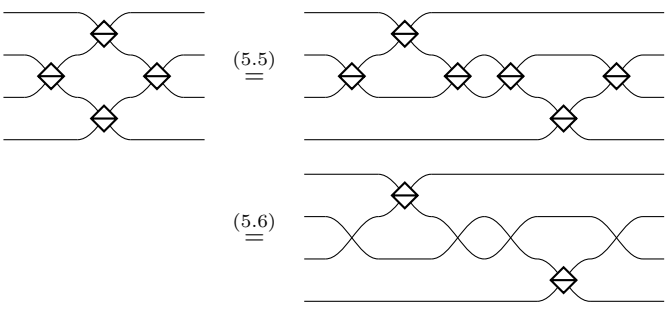

(C.6)

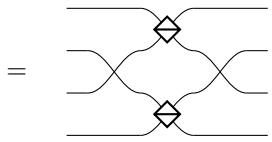

(C.7)


(C.8)

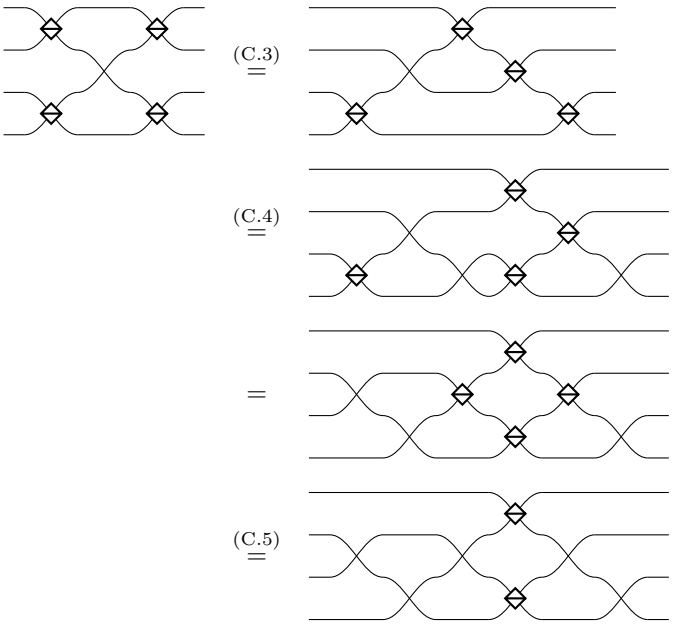
Equations (C.3) and (C.4) have already been proved as Equations (A.3) and (A.2) respectively (note that Equations (5.4), (5.5), (5.6), (5.7) and (5.23) correspond to Equations (3.5), (3.8), (3.9), (3.10) and (3.11) of the PBS-calculus). Equations (C.1) and (C.2) are direct consequences of Equations (5.4) and (5.23).

To prove Equation (C.5), we have:

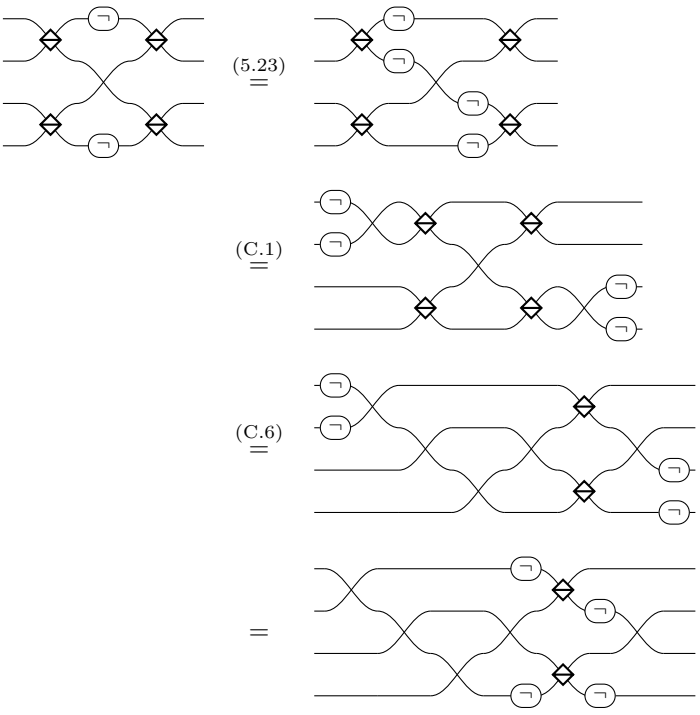


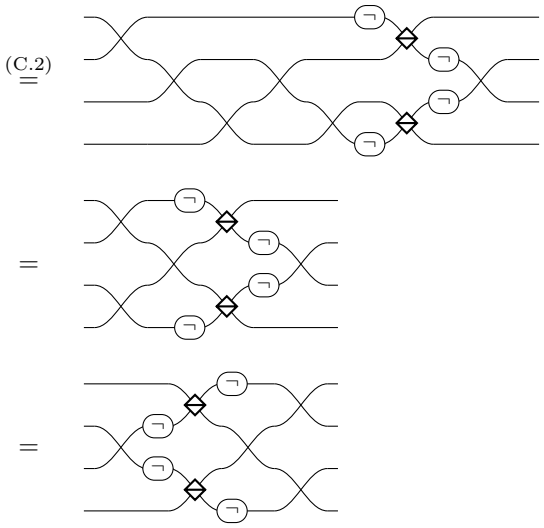


to prove Equation (C.6), we have:

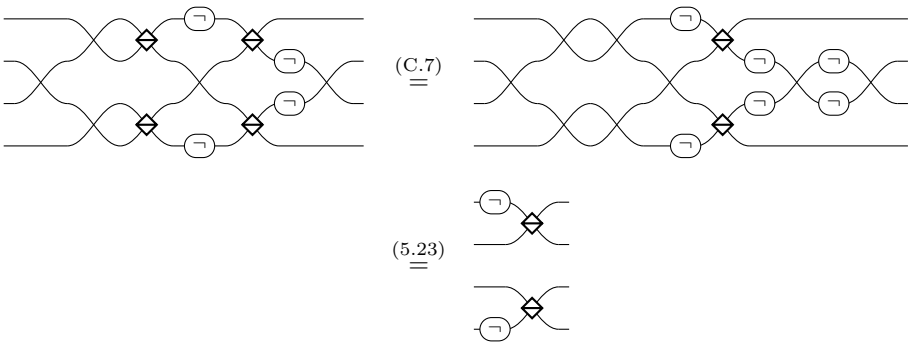


and to prove Equation (C.7), we have

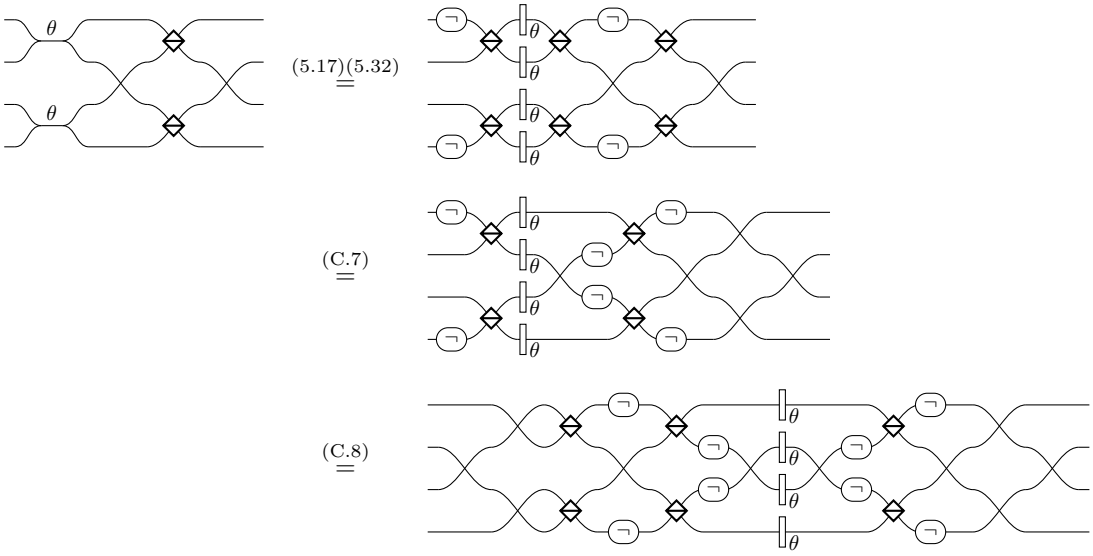


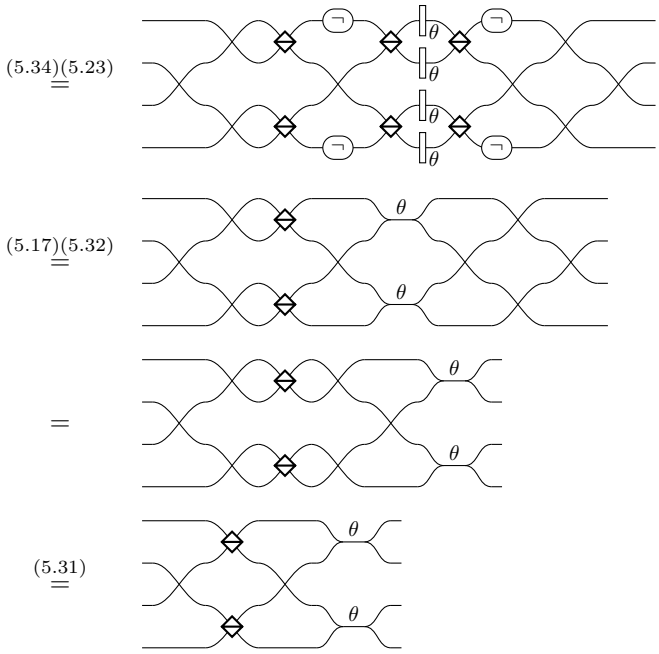


The last step is by mere deformation of the circuit, by exchanging the two PBS. To prove Equation (C.8), we have:



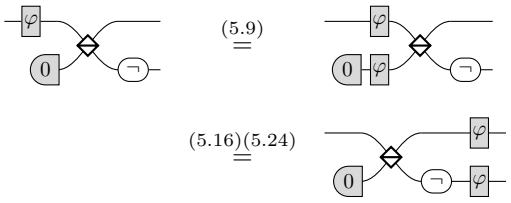
Now we can prove Equation (5.35):



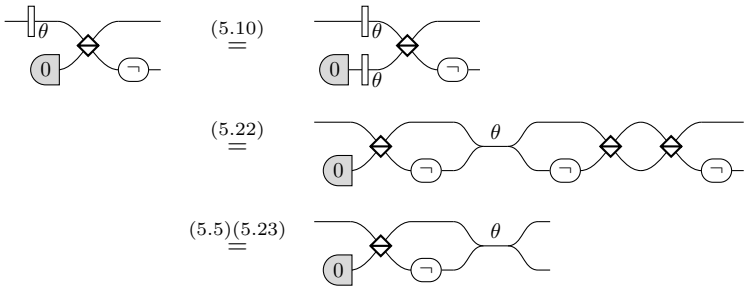


C.2 Derivations of the Ancillary Equations of the Proof of Lemma 5.40

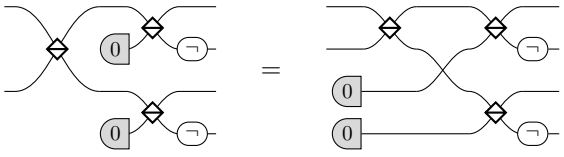
To prove Equation (5.67), we have:

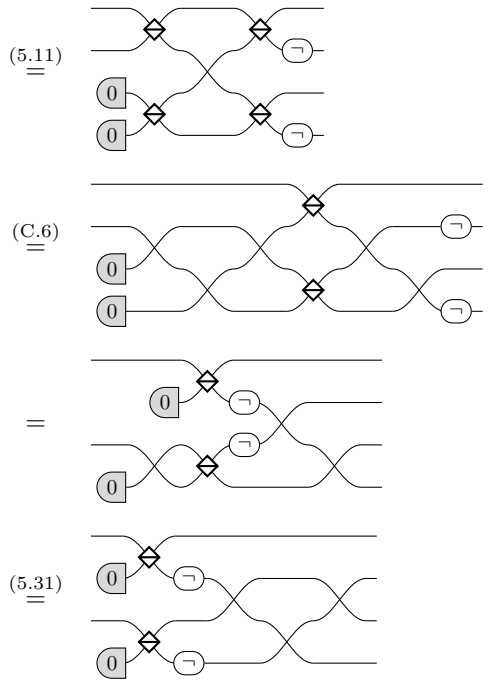


To prove Equation (5.68), we have:

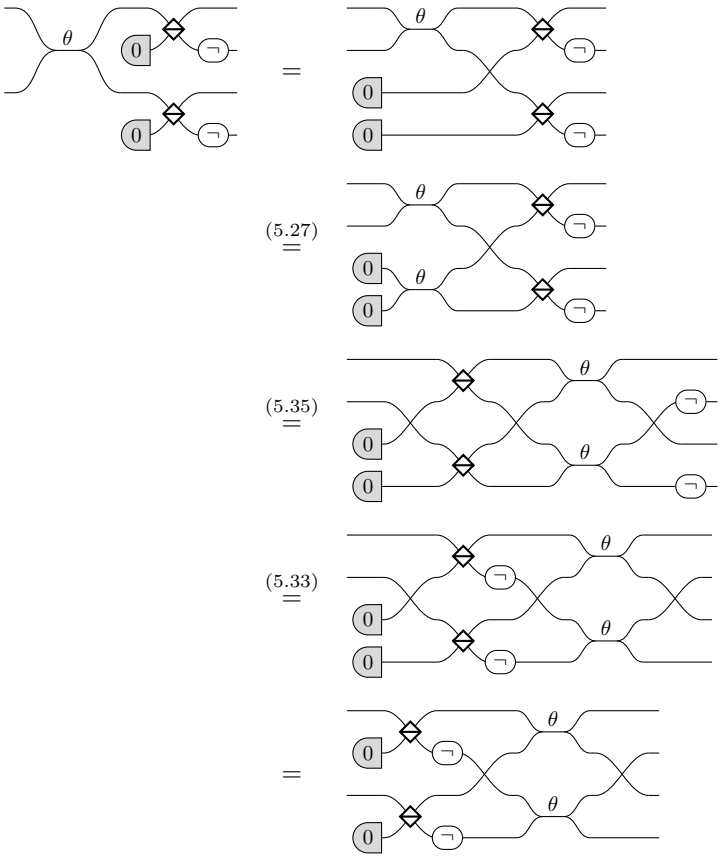


To prove Equation (5.69), we have:





To prove Equation (5.70), we have:



Equation (5.71) is by mere deformation.

C.3 Equality of Unitary Transformations on a Subspace

In this section we show that if two unitary maps coincide on some subspaces then they are equal up to unitaries on the orthogonal subspaces:

Lemma C.36. *Let $\mathcal{H}$ be a Hilbert space, $U, U' \colon \mathcal{H} \to \mathcal{H}$ be two unitary maps, and let $\mathcal{H} = \mathcal{H}_0^{\mathrm{in}} \oplus \mathcal{H}_1^{\mathrm{in}}$ and $\mathcal{H} = \mathcal{H}_0^{\mathrm{out}} \oplus \mathcal{H}_1^{\mathrm{out}}$ be two decompositions of $\mathcal{H}$ into orthogonal subspaces. Given any subspace $\mathcal{H}'$ of $\mathcal{H}$, we denote by $\pi_{\mathcal{H}'} \colon \mathcal{H} \to \mathcal{H}'$ the orthogonal projector on $\mathcal{H}'$ and by $\iota_{\mathcal{H}'} \colon \mathcal{H}' \to \mathcal{H}$ the canonical injection. If $\pi_{\mathcal{H}_0^{\mathrm{out}}} \circ U \circ \iota_{\mathcal{H}_0^{\mathrm{in}}} = \pi_{\mathcal{H}_0^{\mathrm{out}}} \circ U' \circ \iota_{\mathcal{H}_0^{\mathrm{in}}}$, then there exists two unitary maps $Q_{\mathrm{in}} \colon \mathcal{H}_1^{\mathrm{in}} \to \mathcal{H}_1^{\mathrm{in}}$ and $Q_{\mathrm{out}} \colon \mathcal{H}_1^{\mathrm{out}} \to \mathcal{H}_1^{\mathrm{out}}$ such that $U' = (I \oplus Q_{\mathrm{out}}) \circ U \circ (I \oplus Q_{\mathrm{in}})$.*

Proof. We denote $U_0 \coloneqq U \circ \iota_{\mathcal{H}_0^{\mathrm{in}}}$, $U_{00} \coloneqq \pi_{\mathcal{H}_0^{\mathrm{out}}} \circ U \circ \iota_{\mathcal{H}_0^{\mathrm{in}}}$ and $U_{01} \coloneqq \pi_{\mathcal{H}_1^{\mathrm{out}}} \circ U \circ \iota_{\mathcal{H}_0^{\mathrm{in}}}$. We also define analogous notations for U'. Note that U_0 and U_0' are isometries. For any $v, v' \in \mathcal{H}_0^{\mathrm{in}}$, one has $\langle v|v'\rangle = \langle U_0(v)|U_0(v')\rangle = \langle U_{00}(v)|U_{00}(v')\rangle + \langle U_{01}(v)|U_{01}(v')\rangle$. Similarly, $\langle v|v'\rangle = \langle U'_{00}(v)|U'_{00}(v')\rangle + \langle U'_{01}(v)|U'_{01}(v')\rangle$. Since $U_{00} = U'_{00}$, this implies that

$$\forall v, v' \in \mathcal{H}_0^{\mathrm{in}}, \quad \langle U_{01}(v)|U_{01}(v')\rangle = \langle U'_{01}(v)|U'_{01}(v')\rangle \,. \tag{C.9}$$

Let $v_1, ..., v_d \in \mathcal{H}_0^{\mathrm{in}}$ such that $U_{01}(v_1), ..., U_{01}(v_d)$ is an orthonormal basis of the image $U_{01}(\mathcal{H}_0^{\mathrm{in}})$ of U_{01}. By (C.9), $U'_{01}(v_1), ..., U'_{01}(v_d)$ is an orthonormal basis of $U'_{01}(\mathcal{H}_0^{\mathrm{in}})$. Let $Q_{\mathrm{out}} \colon \mathcal{H}_1^{\mathrm{out}} \to \mathcal{H}_1^{\mathrm{out}}$ be any unitary map such that $\forall i \in \{1, ..., d\}, Q_{\mathrm{out}}(U_{01}(v_i)) = U'_{01}(v_1)$. For any $v \in \mathcal{H}_0^{\mathrm{in}}$, there exist $\lambda_1, ..., \lambda_d \in \mathbb{C}$ such that $U_{01}(v) = \sum_{i=1}^d \lambda_i U_{01}(v_i)$. Then by (C.9), $\|U'_{01}(v) - \sum_{i=1}^d \lambda_i U'_{01}(v_i)\| = \|U_{01}(v) - \sum_{i=1}^d \lambda_i U_{01}(v_i)\| = 0$, so that $U'_{01}(v) = \sum_{i=1}^d \lambda_i U'_{01}(v_i)$. Hence, $Q_{\mathrm{out}}(U_{01}(v)) = U'_{01}(v)$. Thus, $U'_{01} = Q_{\mathrm{out}} \circ U_{01}$. Since $U_0 = U_{00} + U_{01}$ and $U'_0 = U'_{00} + U'_{01}$, this implies that $U'_0 = (I \oplus Q_{\mathrm{out}}) \circ U_0$.

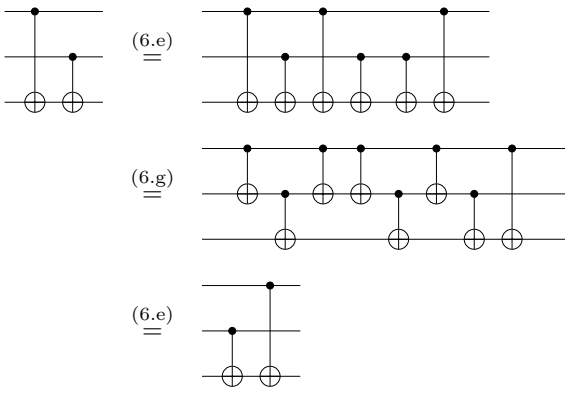
In other words $\forall v \in \mathcal{H}_0^{\mathrm{in}}, U'(v) = (I \oplus Q_{\mathrm{out}}) \circ U(v)$. Hence, $U'(\mathcal{H}_0^{\mathrm{in}}) = (I \oplus Q_{\mathrm{out}}) \circ U(\mathcal{H}_0^{\mathrm{in}})$, so that since $\mathcal{H}_0^{\mathrm{in}}$ and $\mathcal{H}_1^{\mathrm{in}}$ are the orthogonal complement of each other and U, U' are unitary, we also have $U'(\mathcal{H}_1^{\mathrm{in}}) = (I \oplus Q_{\mathrm{out}}) \circ U(\mathcal{H}_1^{\mathrm{in}})$ (which is the orthogonal complement of $U'(\mathcal{H}_0^{\mathrm{in}})$). Let $w_1, ..., w_k$ be an orthonormal basis of $\mathcal{H}_1^{\mathrm{in}}$, and for every $i \in \{1, ..., k\}$, let $w'_i \coloneqq {U'}^{\dagger} \circ (I \oplus Q_{\mathrm{out}}) \circ U(w_i)$. The fact that $U'(\mathcal{H}_1^{\mathrm{in}}) = (I \oplus Q_{\mathrm{out}}) \circ U(\mathcal{H}_1^{\mathrm{in}})$ implies that $w'_1, ..., w'_k$ is also an orthonormal basis of $\mathcal{H}_1^{\mathrm{in}}$. Let $Q_{\mathrm{in}} \colon \mathcal{H}_1^{\mathrm{in}} \to \mathcal{H}_1^{\mathrm{in}}$ be the unique unitary map such that for all $i \in \{1, ..., k\}$, $Q_{\mathrm{in}}(w'_i) = w_i$. Then $U' = (I \oplus Q_{\mathrm{out}}) \circ U \circ (I \oplus Q_{\mathrm{in}})$, as desired. □

Appendix D

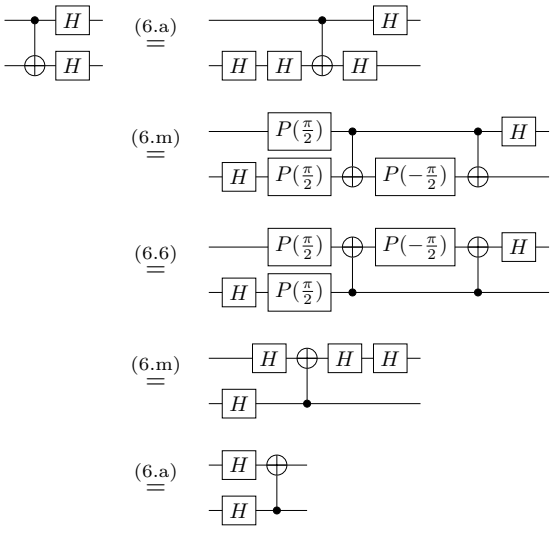
A Complete Equational Theory for Quantum Circuits

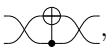
D.1 Proofs of Equations (6.8) to (6.19)

Proof of Equation (6.8):

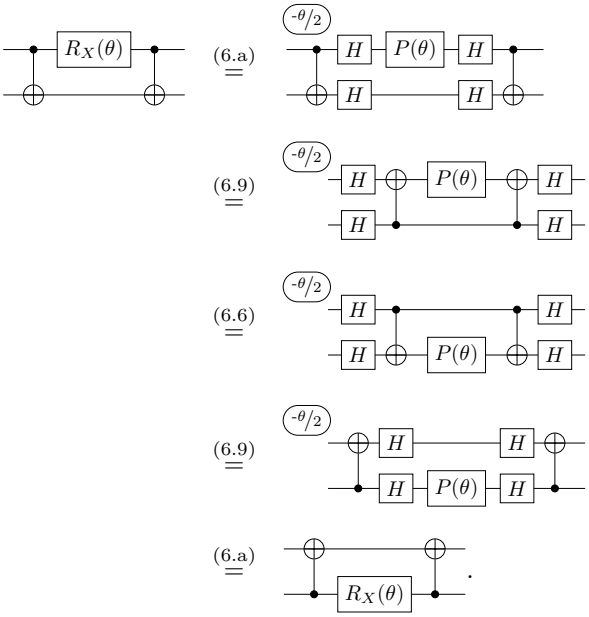


Proof of Equation (6.9):

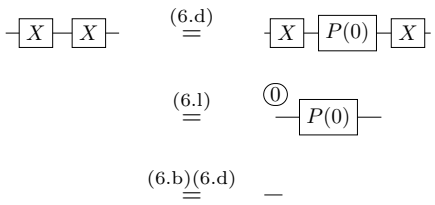


Note that the second use of Equation (6.m) relies on the fact that  is defined as  , and uses a few topological rules.

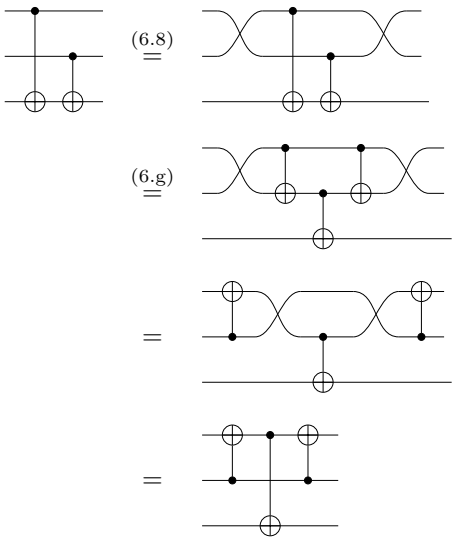
Proof of Equation (6.7):



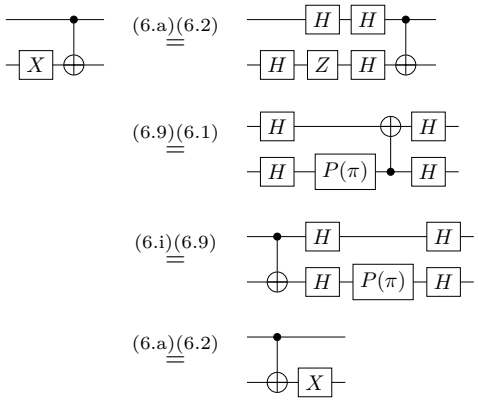
Proof of Equation (6.10):



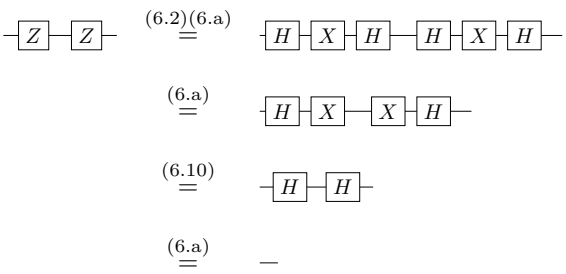
Proof of Equation (6.11):



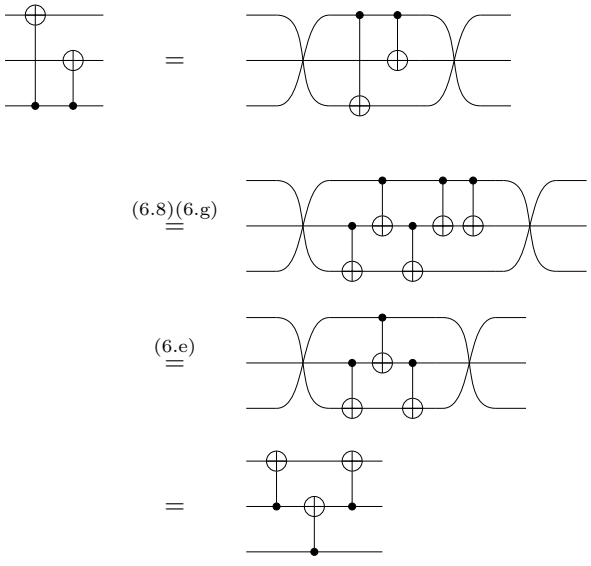
Proof of Equation (6.12):



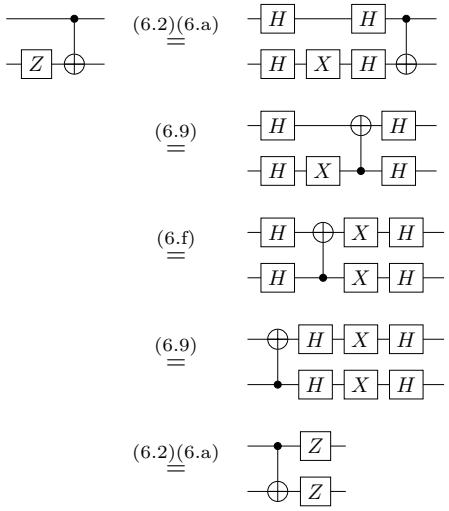
Proof of Equation (6.13):



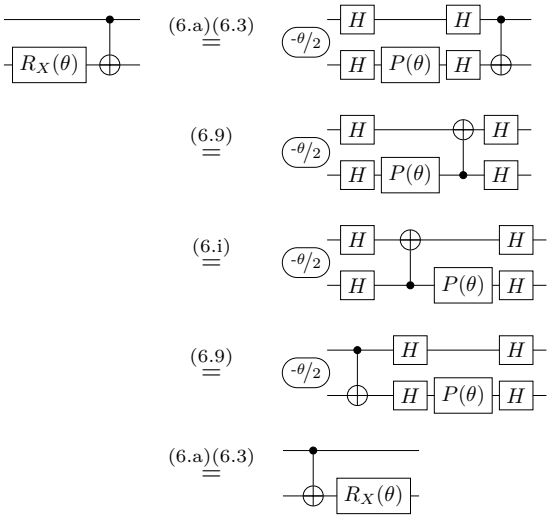
Proof of Equation (6.14):



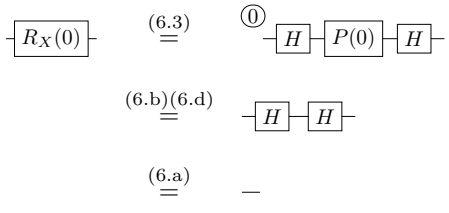
Proof of Equation (6.15):



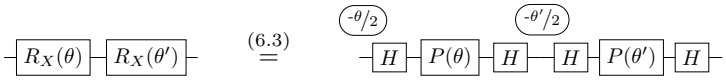
Proof of Equation (6.16):

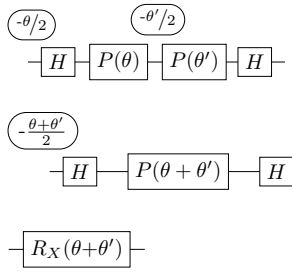


Proof of Equation (6.17):

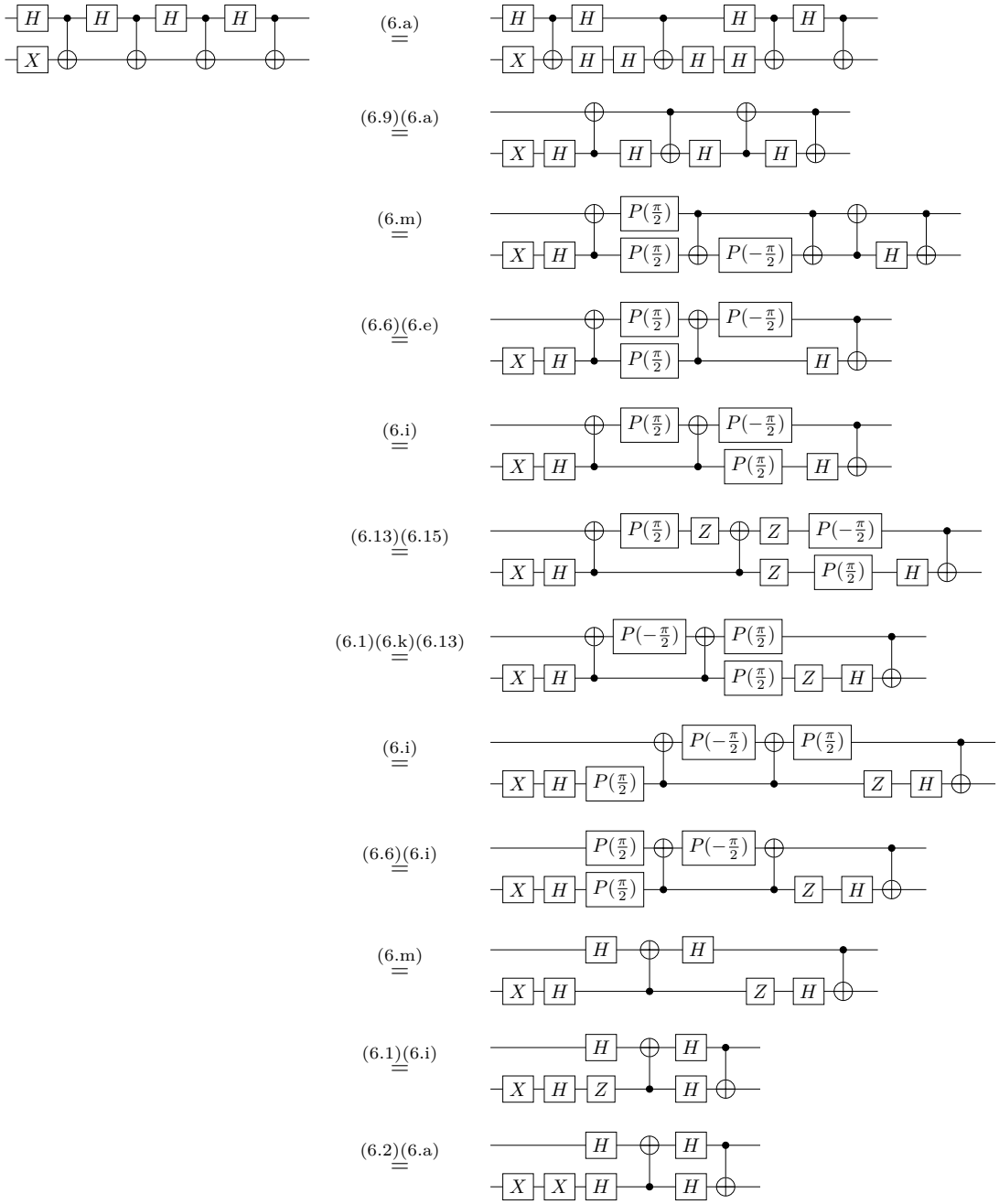


Proof of Equation (6.18):

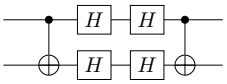




Proof of Equation (6.19):

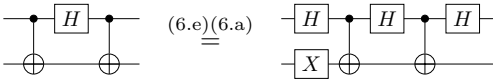


(6.10)(6.9) =



(6.a)(6.e) =

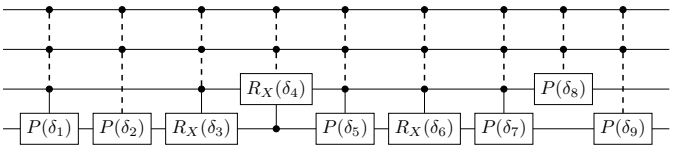
It follows that



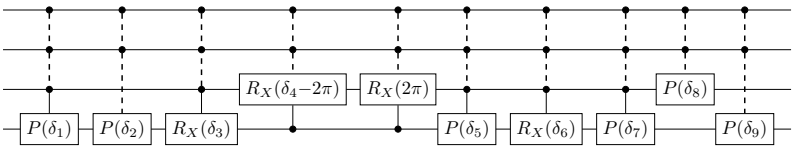
D.2 End of the Proof of Lemma 6.61: Satisfying the Conditions on the Angles

We have prove that we can assume without loss of generality that $\delta_3 \in [0, 2\pi)$.

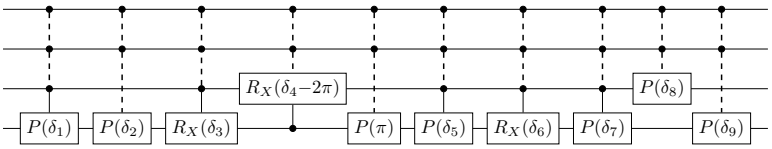
If $\delta_4 \notin [0, 2\pi)$, then by Proposition 6.39, we can ensure that it is in $[0, 4\pi)$, and then if it is in $[2\pi, 4\pi)$, then:



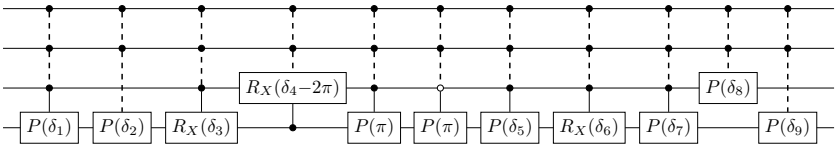
Proposition 6.23 =



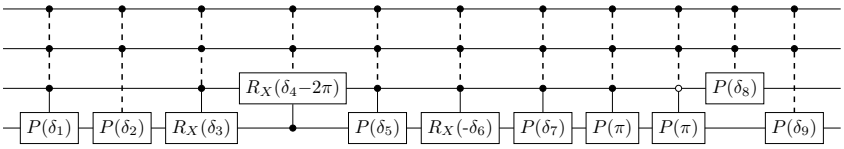
Lemma 6.65 =



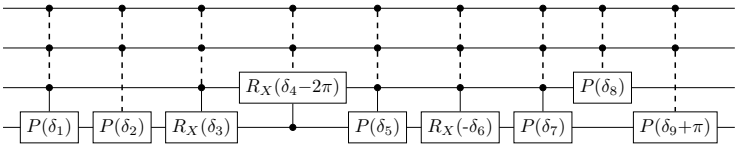
Proposition 6.26 =



Propositions 6.27 and 6.23 and Lemma 6.64 =

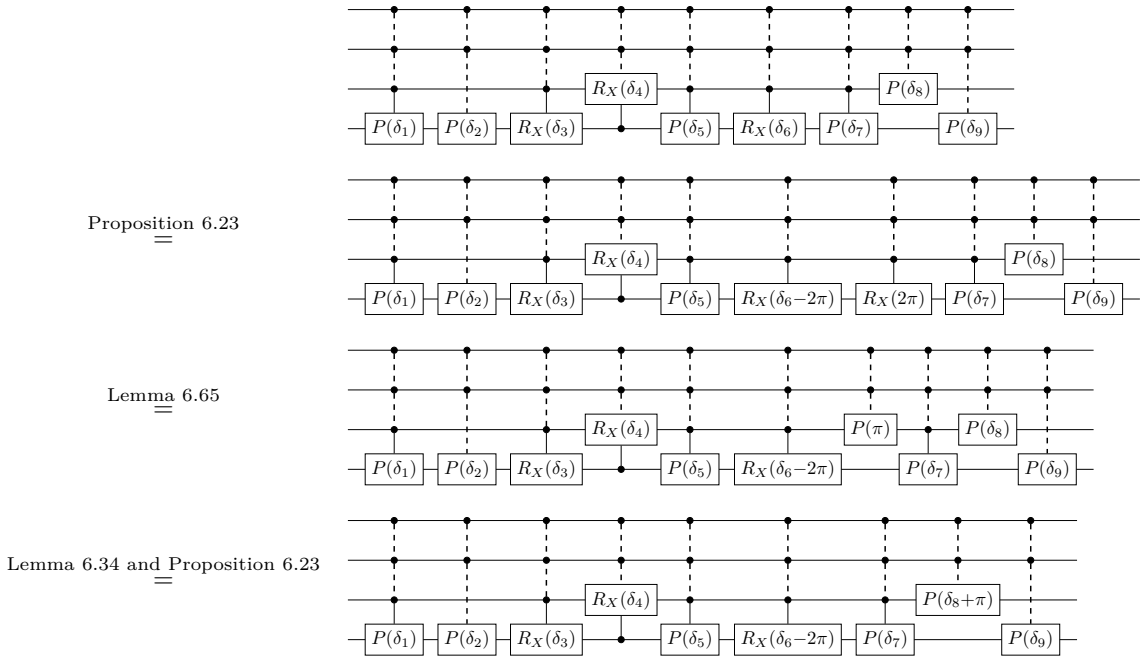


Lemma 6.34, Propositions 6.23 and 6.26 =



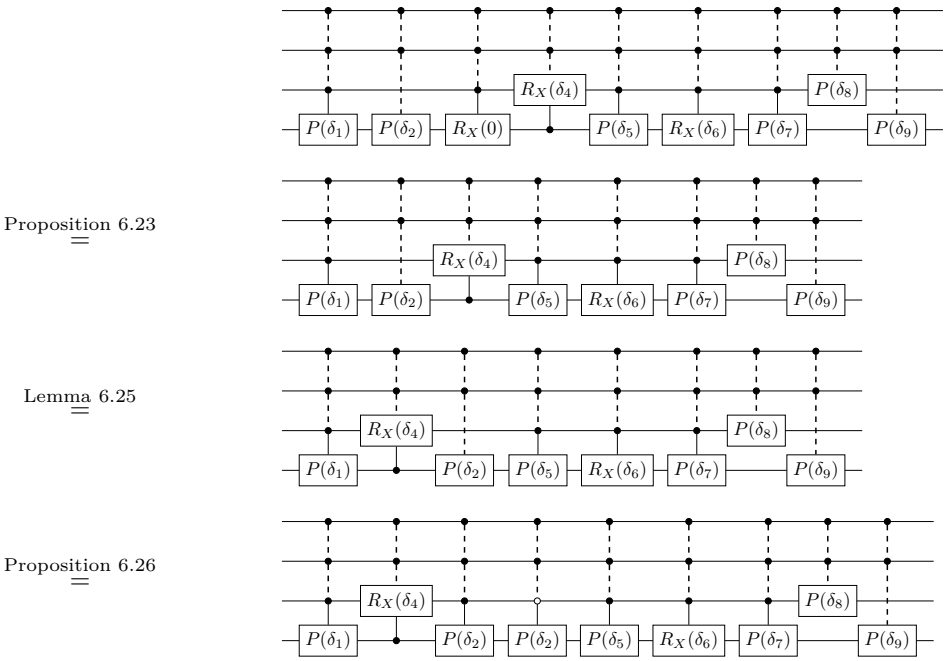
with $\delta_4 - 2\pi \in [0, 2\pi)$. Hence, we can assume additionally that $\delta_4 \in [0, 2\pi)$.

If $\delta_6 \notin [0, 2\pi)$, then by Proposition 6.39, we can ensure that it is in $[0, 4\pi)$, and then if it is in $[2\pi, 4\pi)$, then:

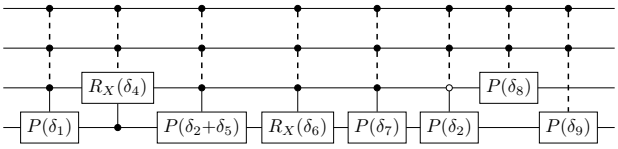


with $\delta_6 - 2\pi \in [0, 2\pi)$. Hence, we can assume additionally that $\delta_6 \in [0, 2\pi)$.

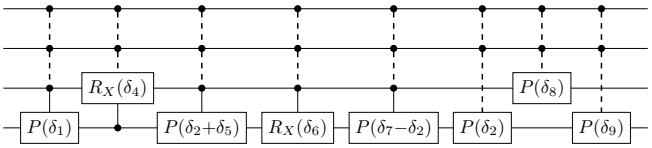
If $\delta_3 = 0$ but $\delta_2 \neq 0$, then:



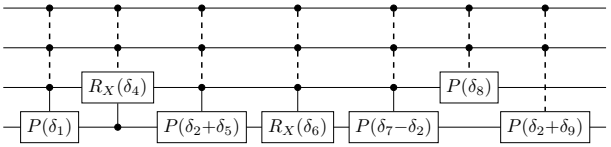
Propositions 6.27 and 6.23 =



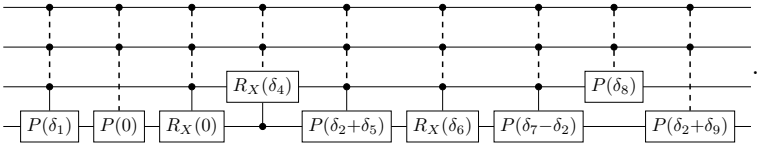
Propositions 6.23 and 6.26 =



Propositions 6.18, 6.23, 6.26 and 6.27 =



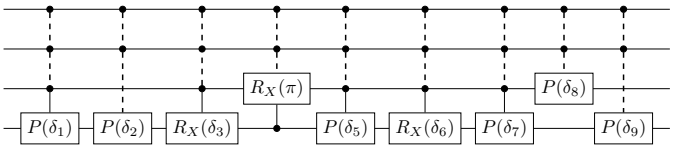
Proposition 6.23 =



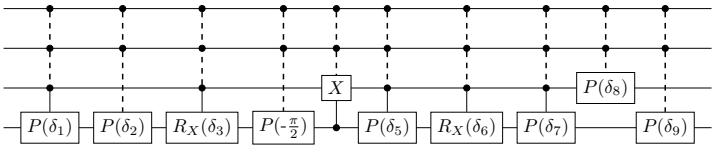
.

Hence, we can assume additionally that if $\delta_3 = 0$ then $\delta_2 = 0$.

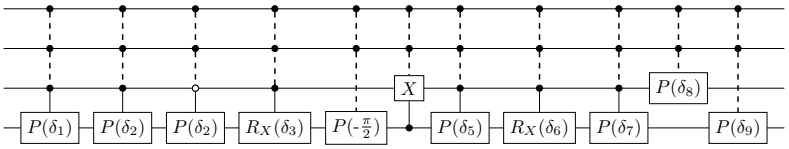
If $\delta_3 \neq 0$, and $\delta_4 = \pi$ but $\delta_2 \neq 0$, then:



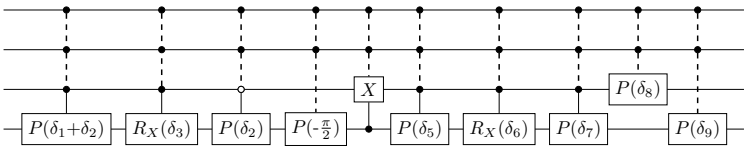
Proposition 6.23 and Equation (6.28) =



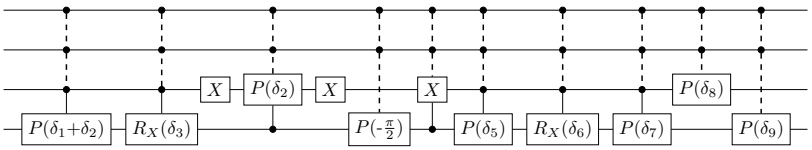
Proposition 6.26 =



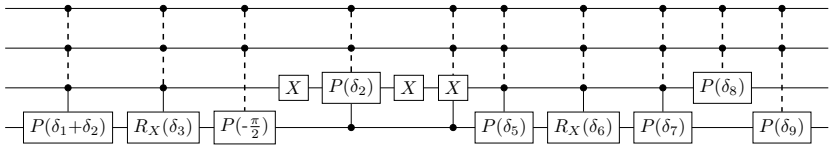
Propositions 6.23 and 6.27 =



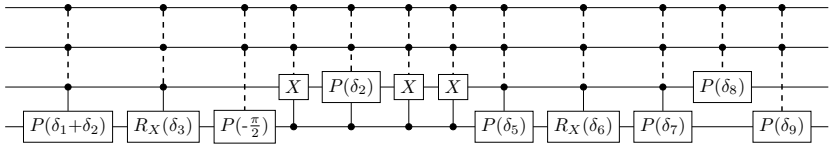
Proposition 6.18 =



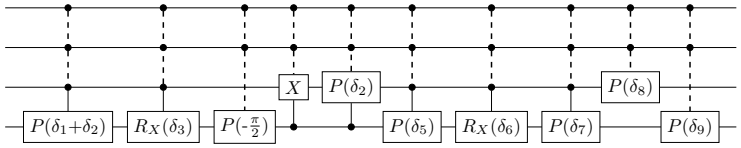
Lemma 6.34
=



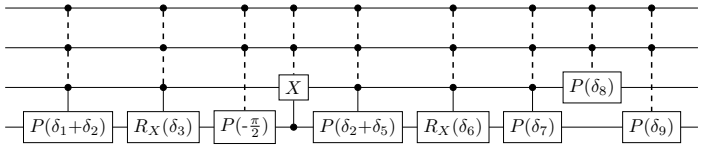
Lemmas 6.33 and 6.63
=



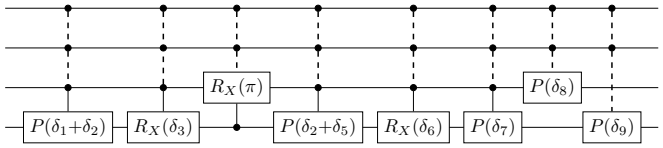
Proposition 6.38
=



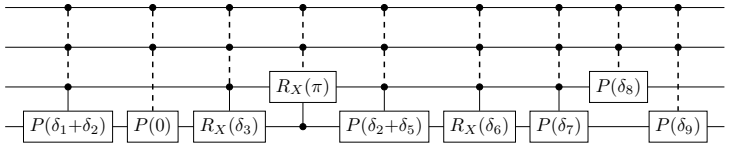
Propositions 6.18 and 6.23
=



Equation (6.28) and Proposition 6.23
=

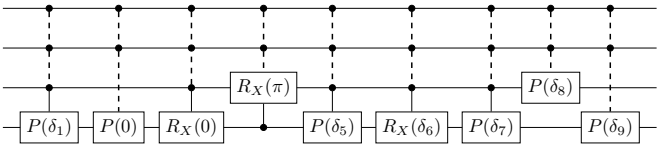


Proposition 6.23
=

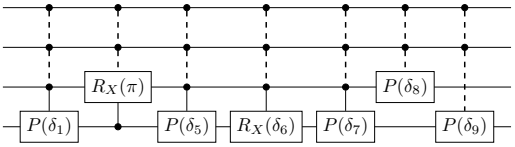


Hence, we can assume additionally that if $\delta_4 = \pi$ then $\delta_2 = 0$ (note that by the previous assumption we already had $\delta_2 = 0$ when $\delta_3 = 0$).

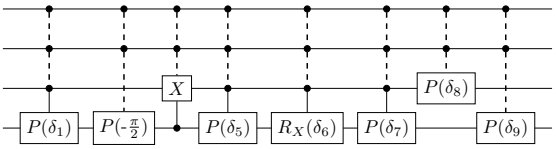
If $\delta_3 = 0$ and $\delta_4 = \pi$, then by assumption, $\delta_2 = 0$. If we do not have additionally that $\delta_1 = 0$, then:



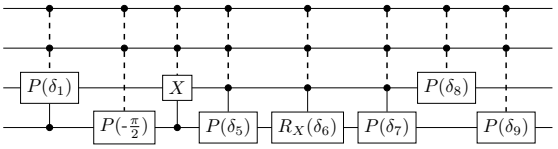
Proposition 6.23
=



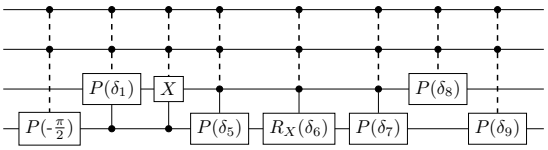
Proposition 6.23 and Equation (6.28)
=



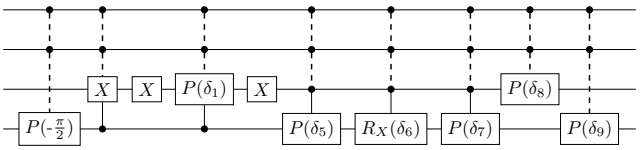
Proposition 6.18
=



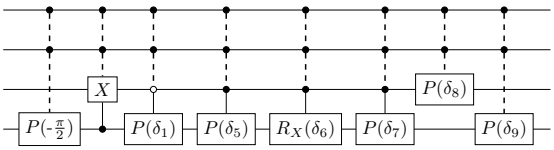
Lemma 6.34
=



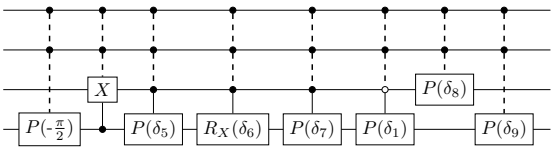
Proposition 6.38 and Lemmas 6.63 and 6.33
=



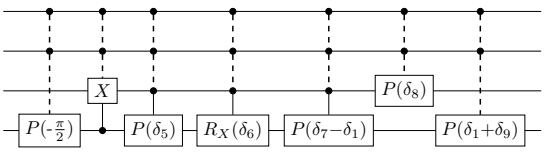
Proposition 6.18
=



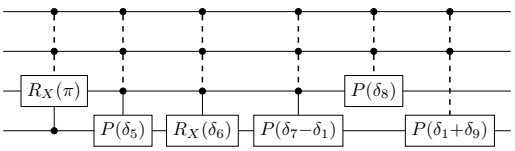
Proposition 6.27
=



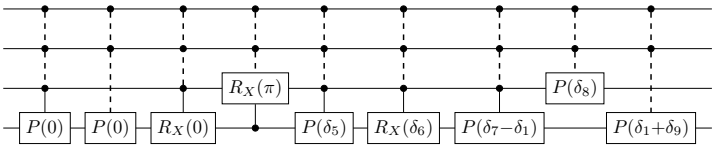
Propositions 6.23 and 6.26 and Lemma 6.34
=



Equation (6.28) and Proposition 6.23
=

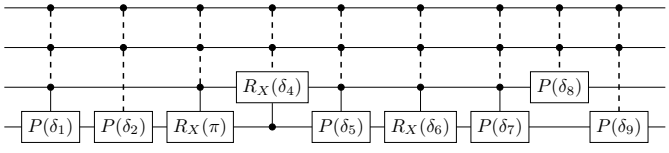


Proposition 6.23
=

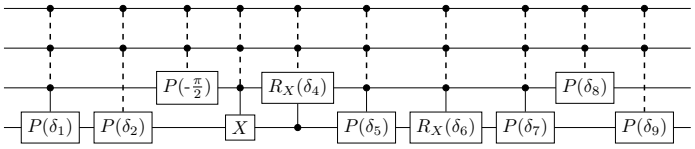


Hence, we can assume additionally that if $\delta_3 = 0$ and $\delta_4 = \pi$ then $\delta_1 = 0$.

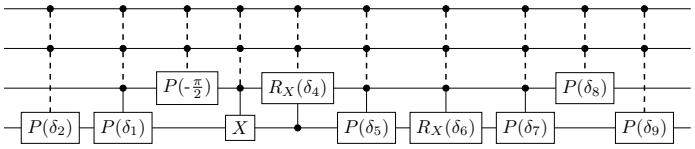
If $\delta_3 = \pi$ but $\delta_1 \neq 0$, then:



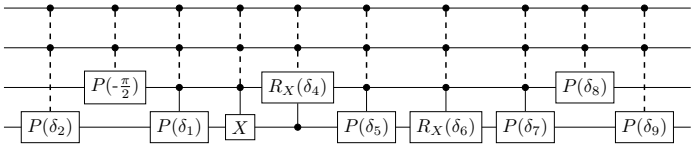
Proposition 6.23 and Equation (6.28)
=



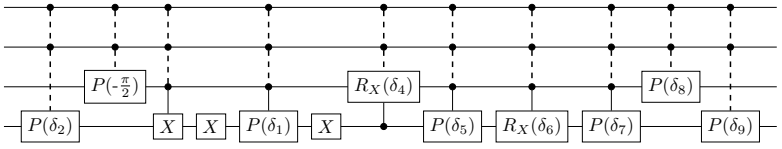
Propositions 6.23, 6.26 and 6.27
=



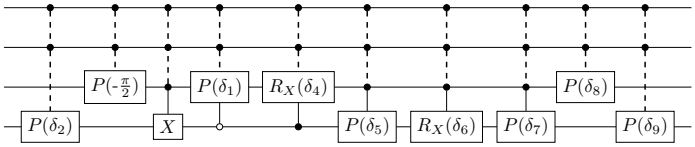
Lemma 6.34
=



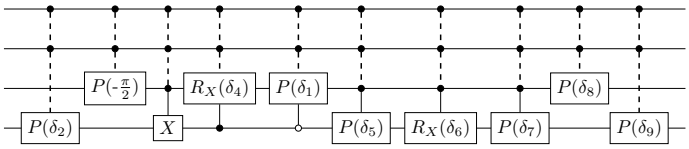
Proposition 6.38,
Lemmas 6.63 and 6.33
=



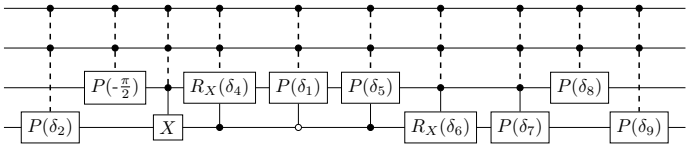
Proposition 6.18
=



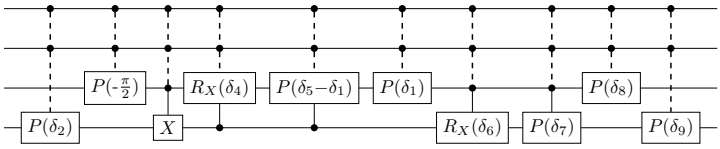
Proposition 6.27
=



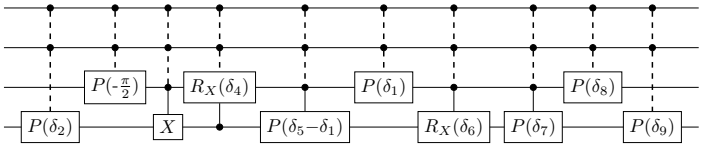
Proposition 6.18
=



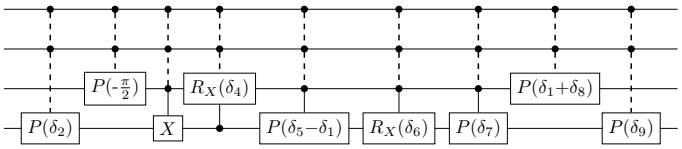
Propositions 6.23, 6.26 and 6.27
=



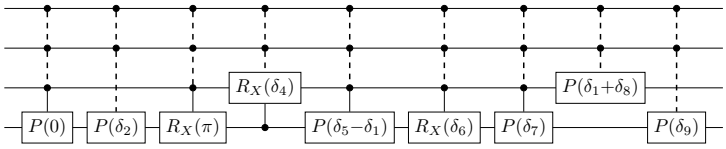
Proposition 6.18
=



Lemmas 6.25 and 6.34
and Proposition 6.23
=

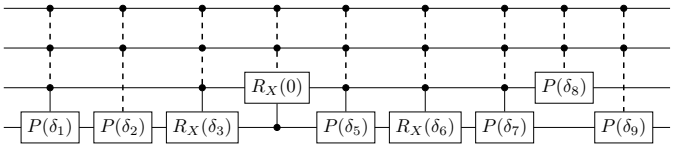


Equation (6.28) and Proposition 6.23 =

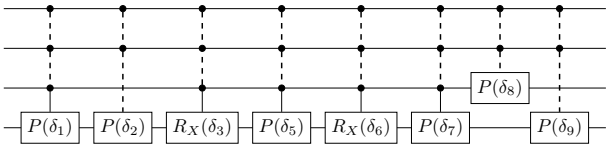


Hence, we can assume additionally that if $\delta_3 = \pi$ then $\delta_1 = 0$.

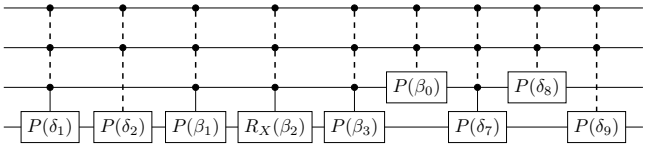
If $\delta_4 = 0$ but $(\delta_1, \delta_2, \delta_3) \neq (0, 0, 0)$, then:



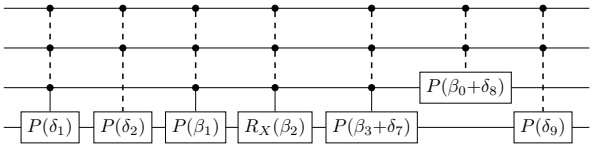
Proposition 6.23 =



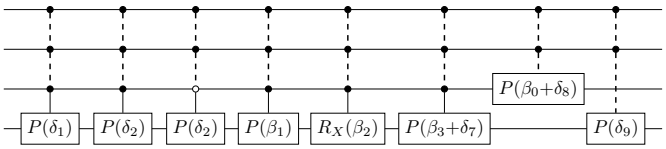
(6.34) =



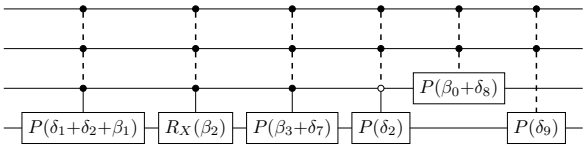
Lemma 6.34 and Proposition 6.23 =



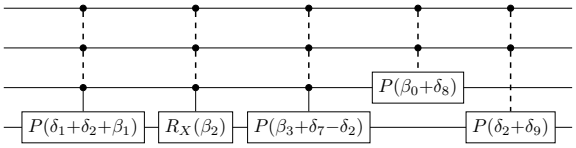
Proposition 6.26 =



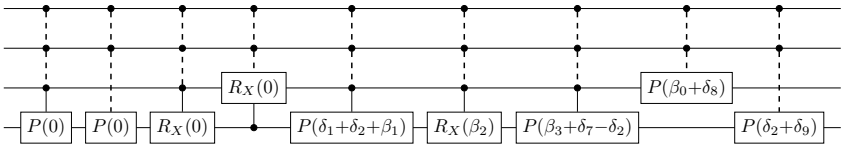
Propositions 6.27 and 6.23 =



Propositions 6.23 and 6.26 and Lemma 6.34 =

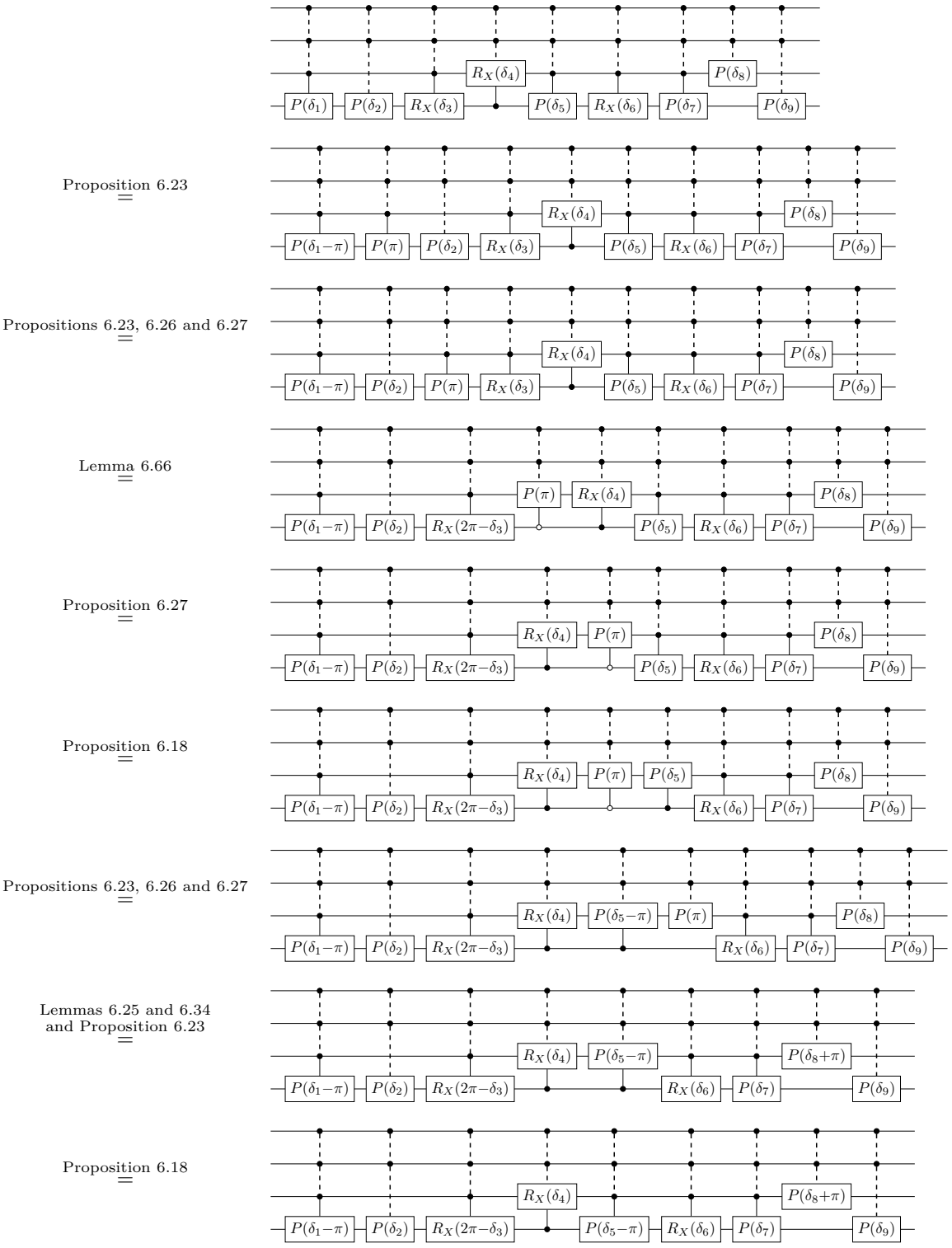


Proposition 6.23 =



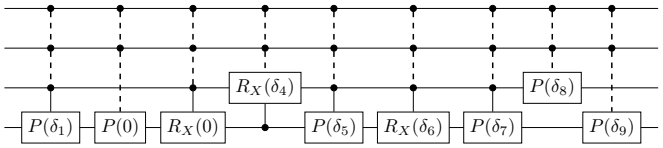
where $\beta_0, \beta_1, \beta_2$ and β_3 satisfy the conditions given in Figure 6.4. In particular, $\beta_2 \in [0, 2\pi)$, so that the previous assumptions are preserved. This implies that we can assume additionally that if $\delta_4 = 0$ then $\delta_1 = \delta_2 = \delta_3 = 0$.

If $\delta_1 \notin [0, \pi)$, then by Proposition 6.39, we can ensure that it is in $[0, 2\pi)$, and then if it is in $[\pi, 2\pi)$, then, if $\delta_3 \neq 0$:

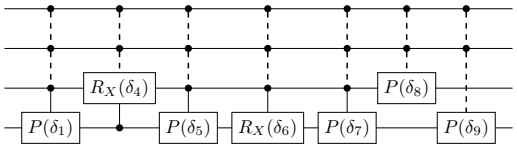


with $\delta_1 - \pi \in [0, \pi)$. Moreover, since $\delta_3 \neq 0$, one has $2\pi - \delta_3 \in [0, 2\pi)$, so that the previous assumptions are preserved.

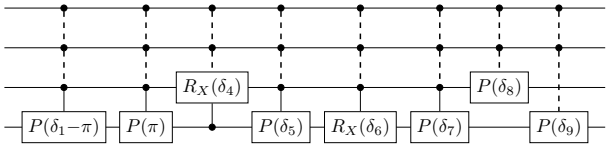
And, still in the case where $\delta_1 \in [\pi, 2\pi)$, if $\delta_3 = 0$, then by assumption, $\delta_2 = 0$, and one has:



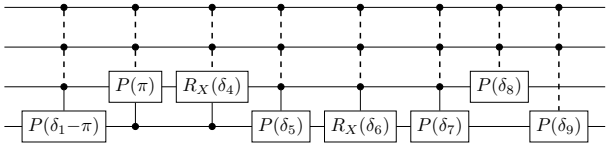
Proposition 6.23
=



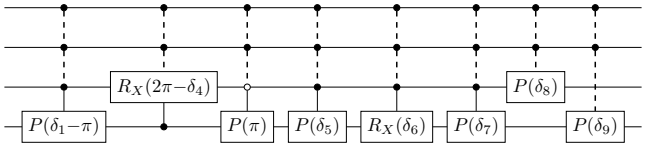
Proposition 6.23
=



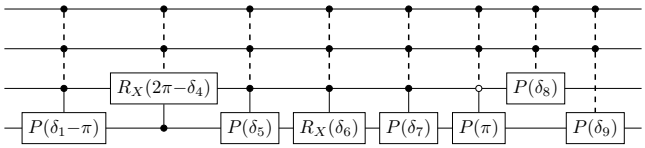
Proposition 6.18
=



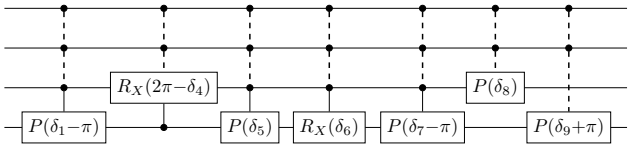
Lemma 6.66
=



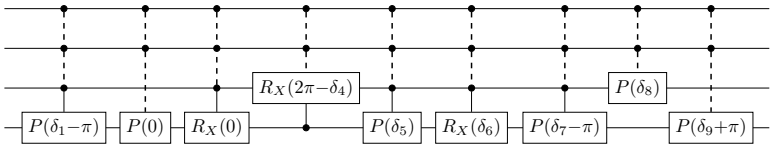
Proposition 6.27
=



Propositions 6.23 and 6.26
and Lemma 6.34
=

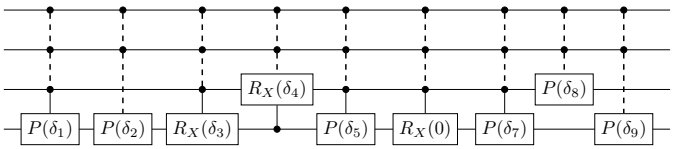


Proposition 6.23
=

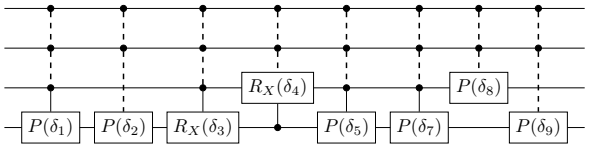


with $\delta_1 - \pi \in [0, \pi)$.

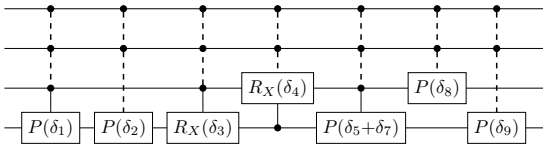
If $\delta_6 = 0$ but $\delta_5 \neq 0$, then:



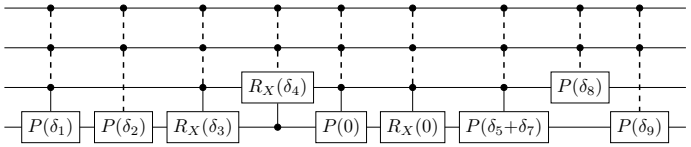
Proposition 6.23 =



Proposition 6.23 =

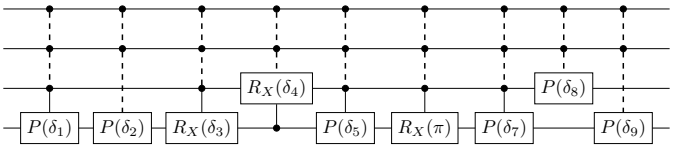


Proposition 6.23 =

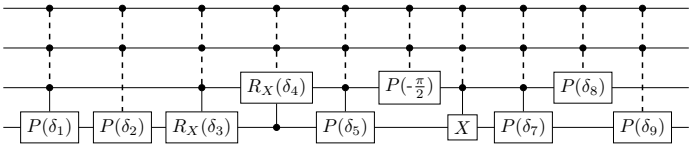


Hence, we can assume additionally that if $\delta_6 = 0$ then $\delta_5 = 0$.

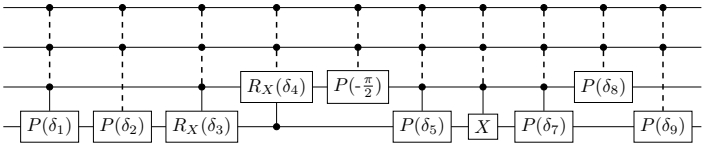
If $\delta_6 = \pi$ but $\delta_5 \neq 0$, then:



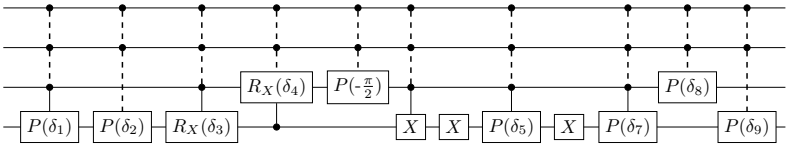
Proposition 6.23 and Equation (6.28) =



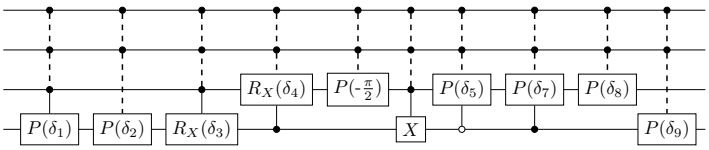
Lemma 6.34 =



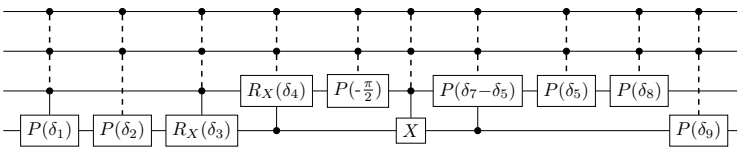
Proposition 6.38, Lemmas 6.63 and 6.33 =



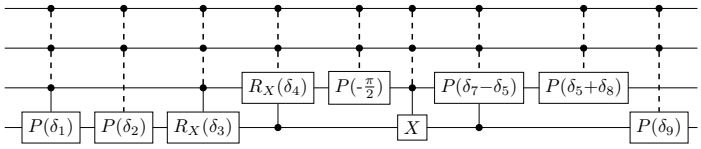
Proposition 6.18 =



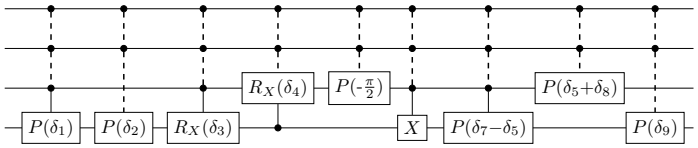
Propositions 6.27, 6.23 and 6.26 =



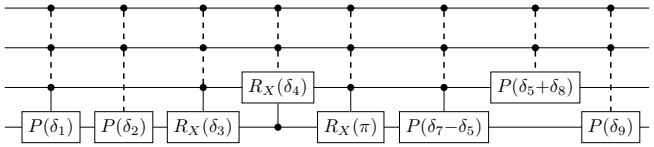
Proposition 6.23 =



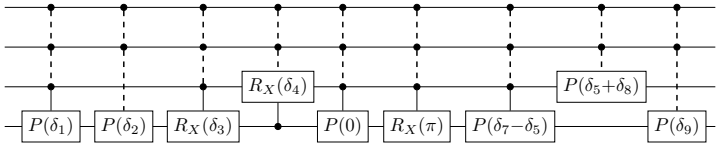
Proposition 6.18 =



Equation (6.28) and Proposition 6.23 =

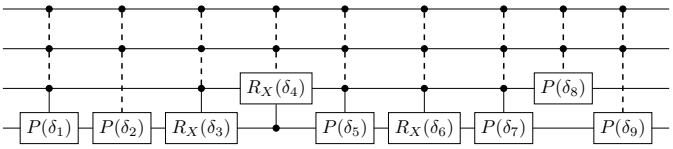


Proposition 6.23 =

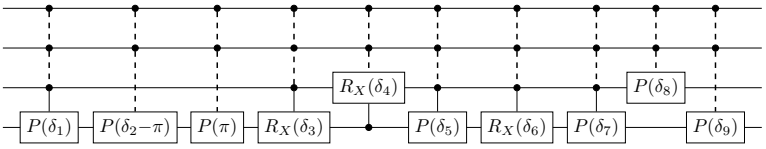


Hence, we can assume additionally that if $\delta_6 = \pi$ then $\delta_5 = 0$.

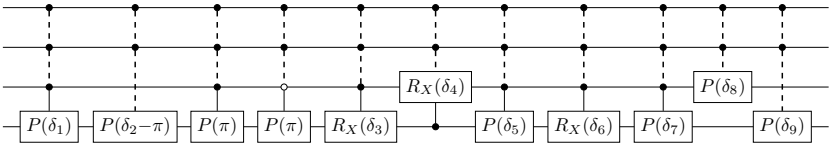
If $\delta_2 \notin [0, \pi)$, then by Proposition 6.39, we can ensure that it is in $[0, 2\pi)$, and then if it is in $[\pi, 2\pi)$, then:



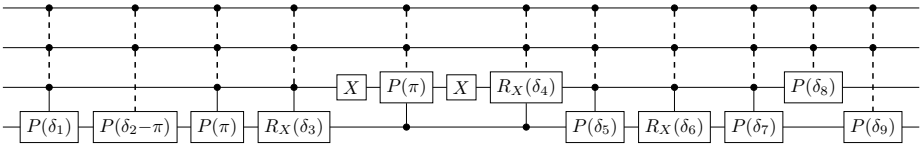
Proposition 6.23 =



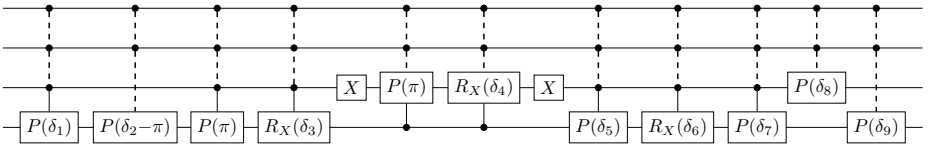
Proposition 6.26 =



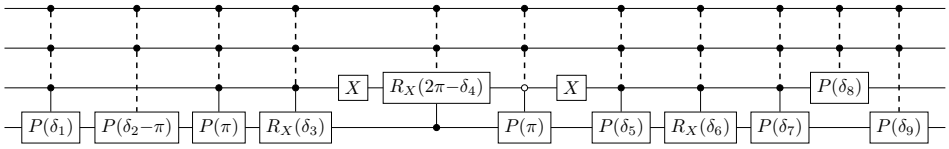
Propositions 6.27 and 6.18 =



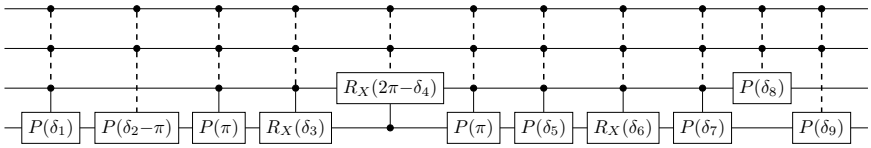
Lemma 6.32 =



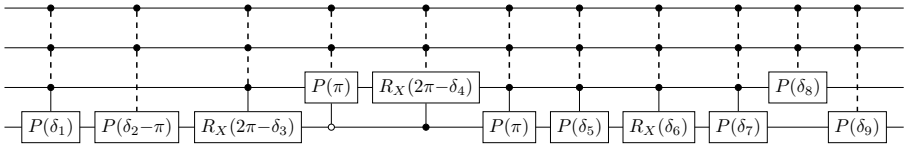
Lemma 6.66 =



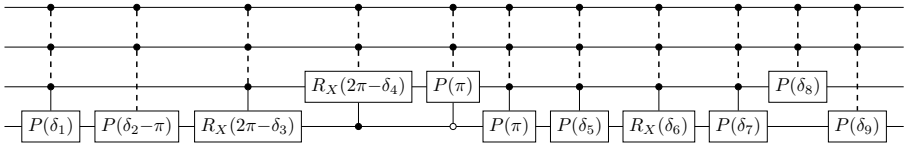
Lemma 6.32 and Equation (6.10) =



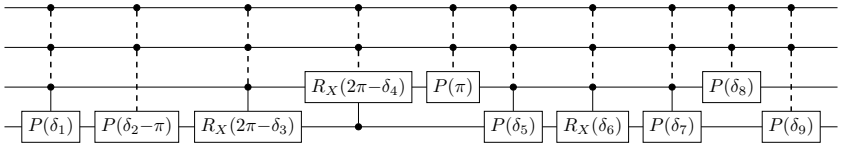
Lemma 6.66 =



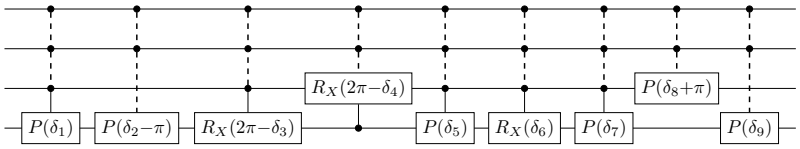
Proposition 6.27 =



Propositions 6.18, 6.27 and 6.26 =

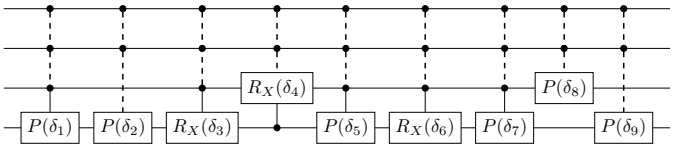


Lemmas 6.25 and 6.34 and Proposition 6.23 =

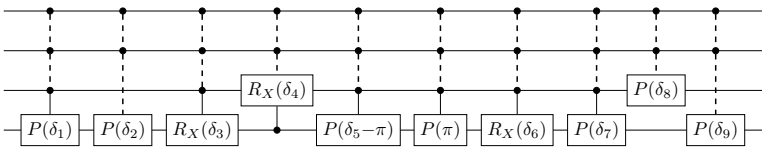


with $\delta_2 - \pi \in [0, \pi)$. Moreover, since $\delta_2 \neq 0$, by assumption $\delta_3 \neq 0$ and $\delta_4 \neq 0$, so that $2\pi - \delta_3$ and $2\pi - \delta_4$ are still in $[0, 2\pi)$ and the previous assumptions are preserved.

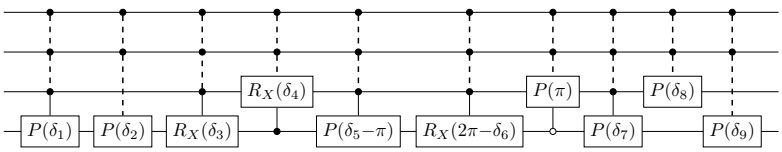
If $\delta_5 \notin [0, \pi)$, then by Proposition 6.39, we can ensure that it is in $[0, 2\pi)$, and then if it is in $[\pi, 2\pi)$, then:



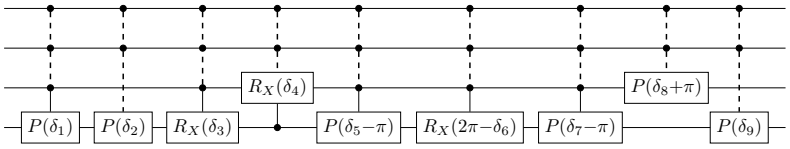
Proposition 6.23 =



Lemma 6.66 =



Propositions 6.18, 6.23, 6.26 and 6.27
=



with $\delta_5 - \pi \in [0, \pi)$. Moreover, since $\delta_5 \neq 0$, by assumption $\delta_6 \neq 0$, so that $2\pi - \delta_6 \in [0, 2\pi)$ and the previous assumptions are preserved.

Finally, by Proposition 6.39 we can put δ_7, δ_8 and δ_9 in $[0, 2\pi)$ without modifying the other angles.

Bibliography

[1] Scott Aaronson. Verifiable quantum advantage: What I hope will be done. Set of slides, presented at *Quantum Advantage Workshop*, Chicago, IL, August 1, 2022. Slide 10. Online at https://www.scottaaronson.com/talks/whatihope.ppt.

[2] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 9(4):143–252, 2013. URL: `http://www.theoryofcomputing.org/articles/v009a004`, `doi:10.4086/toc.2013.v009a004`.

[3] Scott Aaronson and Lijie Chen. Complexity-theoretic foundations of quantum supremacy experiments. *arXiv preprint*, December 2016. `arXiv:1612.05903`.

[4] Alastair A. Abbott, Julian Wechs, Dominic Horsman, Mehdi Mhalla, and Cyril Branciard. Communication through coherent control of quantum channels. *Quantum*, 4:333, September 2020. `arXiv:1810.09826`, `doi:10.22331/q-2020-09-24-333`.

[5] Nabila Abdessaied, Mathias Soeken, and Rolf Drechsler. Quantum circuit optimization by hadamard gate reduction. In *International Conference on Reversible Computation*, pages 149–162. Springer, 2014.

[6] Thorsten Altenkirch and Jonathan Grattage. A functional quantum programming language. In *20th Annual IEEE Symposium on Logic in Computer Science (LICS'05)*, pages 249–258. IEEE, 2005. `arXiv:quant-ph/0409065`, `doi:10.1109/LICS.2005.1`.

[7] Amihood Amir, Tzvika Hartman, Oren Kapah, Avivit Levy, and Ely Porat. On the cost of interchange rearrangement in strings. *SIAM Journal on Computing*, 39(4):1444–1461, 2010. Also available from `https://www.researchgate.net/publication/220616739_On_the_Cost_of_Interchange_Rearrangement_in_Strings`. `doi:10.1137/080712969`.

[8] Matthew Amy, Jianxin Chen, and Neil J. Ross. A finite presentation of CNOT-dihedral operators. *Electronic Proceedings in Theoretical Computer Science*, 266:84–97, February 2018. `doi:10.4204/eptcs.266.5`.

[9] Matthew Amy, Dmitri Maslov, and Michele Mosca. Polynomial-time T-depth optimization of Clifford+T circuits via matroid partitioning. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(10):1476–1489, 2014.

[10] Mateus Araújo, Fabio Costa, and Časlav Brukner. Computational advantage from quantum-controlled ordering of gates. *Physical Review Letters*, 113(25):250402, December 2014. `arXiv:1401.8127`, `doi:10.1103/PhysRevLett.113.250402`.

[11] Mateus Araújo, Adrien Feix, Fabio Costa, and Časlav Brukner. Quantum circuits cannot control unknown operations. *New Journal of Physics*, 16(9):093026, 2014.

[12] Pablo Arrighi, Christopher Cedzich, Marin Costes, Ulysse Rémond, and Benoît Valiron. Addressable quantum gates. *arXiv preprint*, 2021. `arXiv:2109.08050`.

[13] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G.S.L. Brandão, David A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[14] Miriam Backens and Aleks Kissinger. ZH: A complete graphical calculus for quantum computations involving classical non-linearity. *Electronic Proceedings in Theoretical Computer Science*, 287:23–42, January 2019. doi:10.4204/eptcs.287.2.

[15] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52(5):3457–3467, November 1995. doi:10.1103/physreva.52.3457.

[16] Miklós Bartha. Quantum turing automata. *Electronic Proceedings in Theoretical Computer Science*, 143:17–31, March 2014. URL: https://doi.org/10.4204%2Feptcs.143.2, doi:10.4204/eptcs.143.2.

[17] Sara Bartolucci, Patrick Birchall, Hector Bombin, Hugo Cable, Chris Dawson, Mercedes Gimeno-Segovia, Eric Johnston, Konrad Kieling, Naomi Nickerson, Mihir Pant, Fernando Pastawski, Terry Rudolph, and Chris Sparro. Fusion-based quantum computation, 2021. arXiv:2101.09310.

[18] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. URL: https://www.sciencedirect.com/science/article/pii/S0304397514004241, doi:10.1016/j.tcs.2014.05.025.

[19] Xiaoning Bian and Peter Selinger. Generators and relations for 2-qubit Clifford+T operators. *arXiv preprint*, 2022. arXiv:2204.02217.

[20] Filippo Bonchi, Joshua Holland, Robin Piedeleu, Paweł Sobociński, and Fabio Zanasi. Diagrammatic algebra: from linear to concurrent systems. *Proceedings of the ACM on Programming Languages*, 3(POPL):1–28, 2019. doi:10.1145/3290338.

[21] Filippo Bonchi, Robin Piedeleu, Pawel Sobociński, and Fabio Zanasi. Graphical affine algebra. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12. IEEE, 2019. URL: https://discovery.ucl.ac.uk/id/eprint/10081075/, doi:10.1109/LICS.2019.8785877.

[22] Filippo Bonchi, Paweł Sobociński, and Fabio Zanasi. Interacting hopf algebras. *Journal of Pure and Applied Algebra*, 221(1):144–184, 2017. Preprint available from https://eprints.soton.ac.uk/406232. doi:10.1016/j.jpaa.2016.06.002.

[23] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. On the complexity and verification of quantum random circuit sampling. *Nature Physics*, 15(2):159–163, 2019. doi:10.1038/s41567-018-0318-2.

[24] Cyril Branciard, Alexandre Clément, Mehdi Mhalla, and Simon Perdrix. Coherent control and distinguishability of quantum channels via PBS-diagrams. In Filippo Bonchi and Simon J. Puglisi, editors, *46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)*, volume 202 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 22:1–22:20, Dagstuhl, Germany, August 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL: https://hal.science/hal-03325456, arXiv:2103.02073, doi:10.4230/LIPIcs.MFCS.2021.22.

[25] Alberto Caprara. Sorting permutations by reversals and Eulerian cycle decompositions. *SIAM Journal on Discrete Mathematics*, 12(1):91–110, 1999. doi:10.1137/S089548019731994X.

[26] Titouan Carette, Marc de Visme, and Simon Perdrix. Graphical Language with Delayed Trace: Picturing Quantum Computing with Finite Memory. In *LICS 2022 - 36th Annual ACM/IEEE Symposium on Logic in Computer Science*, Rome, Italy, June 2021. URL: https://hal.science/hal-03153305.

[27] Titouan Carette and Emmanuel Jeandel. A recipe for quantum graphical languages. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 118:1–118:17, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. URL: https://drops.dagstuhl.de/opus/volltexte/2020/12525, doi:10.4230/LIPIcs.ICALP.2020.118.

[28] Titouan Carette, Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Completeness of graphical languages for mixed states quantum mechanics. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, volume 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 108:1–108:15, Dagstuhl, Germany, 2019. Schloss Dagstuhl - Leibniz-Zentrum für Informatik. URL: https://hal.science/hal-02025720, arXiv:1902.07143, doi:10.4230/LIPIcs.ICALP.2019.108.

[29] Kostia Chardonnet, Marc de Visme, Benoît Valiron, and Renaud Vilmart. The many-worlds calculus. *arXiv preprint*, 2022. arXiv:2206.10234.

[30] Kostia Chardonnet, Benoît Valiron, and Renaud Vilmart. Geometry of interaction for ZX-diagrams. In *MFCS 2021 - 46th International Symposium on Mathematical Foundations of Computer Science*, volume 202 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 30:1–30:16, Tallinn, Estonia, August 2021. URL: https://hal.science/hal-03154573, arXiv:2206.10916, doi:10.4230/LIPIcs.MFCS.2021.30.

[31] Giulio Chiribella. Perfect discrimination of no-signalling channels via quantum superposition of causal structures. *Physical Review A*, 86(4):040301, 2012. arXiv:1109.5154, doi:10.1103/PhysRevA.86.040301.

[32] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Transforming quantum operations: Quantum supermaps. *EPL*, 83(3):30004, July 2008. arXiv:0804.0180, doi:10.1209/0295-5075/83/30004.

[33] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. Theoretical framework for quantum networks. *Physical Review A*, 80(2):022339, August 2009. arXiv:0904.4483, doi:10.1103/PhysRevA.80.022339.

[34] Giulio Chiribella, Giacomo Mauro D'Ariano, Paolo Perinotti, and Benoît Valiron. Quantum computations without definite causal structure. *Physical Review A*, 88:022318, August 2013. arXiv:0912.0195, doi:10.1103/PhysRevA.88.022318.

[35] Giulio Chiribella and Hlér Kristjánsson. Quantum shannon theory with superpositions of trajectories. *Proceedings of the Royal Society A*, 475:20180903, May 2019. arXiv:1812.05292, doi:10.1098/rspa.2018.0903.

[36] Alexandre Clément, Noé Delorme, Simon Perdrix, and Renaud Vilmart. Simple Complete Equational Theories for Quantum Circuits with Ancillae or Partial Trace. Preprint, March 2023. URL: https://hal.science/hal-04016498, arXiv:2303.03117.

[37] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. A complete equational theory for quantum circuits. *arXiv preprint*, 2022. arXiv:2206.10577.

[38] Alexandre Clément, Nicolas Heurtel, Shane Mansfield, Simon Perdrix, and Benoît Valiron. LO_{v}-calculus: A graphical language for linear optical quantum circuits. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 35:1–35:16, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. arXiv:2204.11787, doi:10.4230/LIPIcs.MFCS.2022.35.

[39] Alexandre Clément and Simon Perdrix. PBS-calculus: A graphical language for coherent control of quantum computations. In Javier Esparza and Daniel Kráľ, editors, *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, volume 170 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:14, Dagstuhl, Germany, August 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. URL: https://hal.science/hal-02929291, arXiv:2002.09387, doi:10.4230/LIPIcs.MFCS.2020.24.

[40] Alexandre Clément and Simon Perdrix. Resource optimisation of coherently controlled quantum computations with the PBS-calculus. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:15, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. arXiv:2202.05260, doi:10.4230/LIPIcs.MFCS.2022.36.

[41] William R. Clements, Peter C. Humphreys, Benjamin J. Metcalf, W. Steven Kolthammer, and Ian A. Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, December 2016. URL: http://www.osapublishing.org/optica/abstract.cfm?URI=optica-3-12-1460, doi:10.1364/OPTICA.3.001460.

[42] Robin Cockett and Cole Comfort. The category TOF. In Peter Selinger and Giulio Chiribella, editors, *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018*, volume 287 of *EPTCS*, pages 67–84, 2019.

[43] Robin Cockett, Cole Comfort, and Priyaa Srinivasan. The category CNOT. In Peter Selinger and Giulio Chiribella, editors, *Proceedings 15th International Conference on Quantum Physics and Logic, QPL 2018*, volume 287 of *EPTCS*, pages 258–293, 2019. doi:10.4204/EPTCS.266.18.

[44] Bob Coecke and Ross Duncan. Interacting quantum observables. In *International Colloquium on Automata, Languages, and Programming*, pages 298–310. Springer, 2008.

[45] Bob Coecke and Ross Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, 2011. doi:10.1088/1367-2630/13/4/043016.

[46] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, 2017. doi:10.1017/9781316219317.

[47] Bob Coecke and Simon Perdrix. Environment and classical channels in categorical quantum mechanics. *Logical Methods in Computer Science*, Volume 8, Issue 4, November 2012. arXiv:1004.1598, doi:10.2168/LMCS-8(4:14)2012.

[48] Bob Coecke and Quanlong Wang. ZX-rules for 2-qubit Clifford+T quantum circuits. In *International Conference on Reversible Computation*, pages 144–161. Springer, 2018.

[49] Donald J. Collins. A simple presentation of a group with unsolvable word problem. *Illinois Journal of Mathematics*, 30(2):230 – 234, 1986. doi:10.1215/ijm/1256044631.

[50] Timoteo Colnaghi, Giacomo Mauro D'Ariano, Stefano Facchini, and Paolo Perinotti. Quantum computation with programmable connections between gates. *Physics Letters A*, 376(45):2940–2943, 2012. arXiv:1109.5987, doi:10.1016/j.physleta.2012.08.028.

[51] Alexander Cowtan, Silas Dilkes, Ross Duncan, Will Simmons, and Seyon Sivarajah. Phase gadget synthesis for shallow circuits. *Electronic Proceedings in Theoretical Computer Science*, 318:213–228, May 2020. URL: https://doi.org/10.4204%2Feptcs.318.13, doi:10.4204/eptcs.318.13.

[52] Niel de Beaudrap, Aleks Kissinger, and John van de Wetering. Circuit extraction for ZX-diagrams can be #P-hard. *arXiv preprint*, 2022. arXiv:2202.09194.

[53] Giovanni de Felice and Bob Coecke. Quantum linear optics via string diagrams. *arXiv preprint*, 2022. arXiv:2204.12985.

[54] Giovanni de Felice, Amar Hadzihasanovic, and Kang Feng Ng. A diagrammatic calculus of fermionic quantum circuits. *Logical Methods in Computer Science*, 15(3), 2019. doi:10.23638/LMCS-15(3:26)2019.

[55] D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 425(1868):73–90, 1989.

[56] Gilles Dowek and Pablo Arrighi. Lineal: A linear-algebraic lambda-calculus. *Logical Methods in Computer Science*, 13(1), 2017. doi:10.23638/LMCS-13(1:8)2017.

[57] Ross Duncan, Aleks Kissinger, Simon Perdrix, and John Van De Wetering. Graph-theoretic simplification of quantum circuits with the ZX-calculus. *Quantum*, 4:279, 2020.

[58] Daniel Ebler, Sina Salek, and Giulio Chiribella. Enhanced communication with the assistance of indefinite causal order. *Physical Review Letters*, 120(12):120502, March 2018. arXiv:1711.10165, doi:10.1103/PhysRevLett.120.120502.

[59] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, August 1991. URL: https://link.aps.org/doi/10.1103/PhysRevLett.67.661, doi:10.1103/PhysRevLett.67.661.

[60] Stefano Facchini and Simon Perdrix. Quantum circuits for the unitary permutation problem. In *International Conference on Theory and Applications of Models of Computation*, pages 324–331. Springer, 2015. arXiv:1405.5205, doi:10.1007/978-3-319-17142-5_28.

[61] Adrien Feix, Mateus Araújo, and Časlav Brukner. Quantum superposition of the order of parties as a communication resource. *Physical Review A*, 92(5):052326, 2015. arXiv:1508.07840, doi:10.1103/PhysRevA.92.052326.

[62] Zbigniew Fiedorowicz, Manfred Stelzer, and Rainer Vogt. Homotopy colimits of algebras over cat-operads and iterated loop spaces. *Advances in Mathematics*, 248, November 2013. doi:10.1016/j.aim.2013.07.016.

[63] Herbert Fleischner. *Eulerian Graphs and Related Topics*, volume 50 of *Annals of Discrete Mathematics*. Elsevier, 1991. URL: https://www.elsevier.com/books/eulerian-graphs-and-related-topics/fleischner/978-0-444-89110-5.

[64] Zuzana Gavorová, Matan Seidel, and Yonathan Touati. Topological obstructions to implementing controlled unknown unitaries. *arXiv preprint*, 2020. Presented as a talk at QIP 2021. arXiv:2011.10031.

[65] Brett Giles and Peter Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Physical Review A*, 87:032332 (7 pages), 2013. Also available from arXiv:1212.0506. doi:10.1103/PhysRevA.87.032332.

[66] Brett Giles and Peter Selinger. Remarks on Matsumoto and Amano's normal form for single-qubit Clifford+T operators. *arXiv preprint*, 2019. arXiv:1312.6584.

[67] Kaumudibikash Goswami, Y. Cao, Gerardo A. Paz-Silva, Jacquiline Romero, and Andrew G. White. Increasing communication capacity via superposition of order. *Phys. Rev. Research*, 2:033292, August 2020. arXiv:1807.07383, doi:10.1103/PhysRevResearch.2.033292.

[68] Kaumudibikash Goswami, Christina Giarmatzi, Michael Kewming, Fabio Costa, Cyril Branciard, Jacquiline Romero, and Andrew G. White. Indefinite causal order in a quantum switch. *Physical Review Letters*, 121:090503, August 2018. arXiv:1803.04302, doi:10.1103/PhysRevLett.121.090503.

[69] Alexander S. Green, Peter LeFanu Lumsdaine, Neil J. Ross, Peter Selinger, and Benoît Valiron. Quipper: A scalable quantum programming language. In Hans-Juergen Boehm and Cormac Flanagan, editors, *Proceedings of the ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI'13*, pages 333–342. ACM, 2013. arXiv:1304.3390, doi:10.1145/2491956.2462177.

[70] Seth Eveson Murray Greylyn. *Generators and relations for the group* $U_4(\mathbb{Z}[\frac{1}{\sqrt{2}}, i])$. MSc thesis, Dalhousie University, 2014. Available from arXiv:1408.6204.

[71] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. Association for Computing Machinery. doi:10.1145/237814.237866.

[72] Philippe Allard Guérin, Adrien Feix, Mateus Araújo, and Časlav Brukner. Exponential communication complexity advantage from quantum superposition of the direction of communication. *Physical Review Letters*, 117(10):100502, 2016. arXiv:1605.07372, doi:10.1103/PhysRevLett.117.100502.

[73] Yu Guo, Xiao-Min Hu, Zhi-Bo Hou, Huan Cao, Jin-Ming Cui, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, and Giulio Chiribella. Experimental transmission of quantum information using a superposition of causal orders. *Physical Review Letters*, 124:030502, January 2020. URL: https://link.aps.org/doi/10.1103/PhysRevLett.124.030502, arXiv:1811.07526, doi:10.1103/PhysRevLett.124.030502.

[74] Philip Hackney and Marcy Robertson. On the category of props. *Applied Categorical Structures*, 23(4):543–573, March 2014. arXiv:1207.2773, doi:10.1007/s10485-014-9369-4.

[75] Amar Hadzihasanovic. *The algebra of entanglement and the geometry of composition*. PhD thesis, University of Oxford, 2017. URL: https://ora.ox.ac.uk/objects/uuid:711fc159-cd6a-42c3-a4b6-7ed7f594f781, arXiv:1709.08086.

[76] Amar Hadzihasanovic, Kang Feng Ng, and Quanlong Wang. Two complete axiomatisations of pure-state qubit quantum computing. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 502–511. ACM, 2018. doi:10.1145/3209108.3209128.

[77] Lucien Hardy. Probability theories with dynamic causal structure: A new framework for quantum gravity. *arXiv preprint*, 2005. arXiv:gr-qc/0509120.

[78] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103(15), October 2009. arXiv:0811.3171, doi:10.1103/physrevlett.103.150502.

[79] Masahito Hasegawa, Martin Hofmann, and Gordon Plotkin. Finite dimensional vector spaces are complete for traced symmetric monoidal categories. In *Pillars of computer science*, pages 367–385. Springer, 2008.

[80] Nicolas Heurtel, Andreas Fyrillas, Grégoire de Gliniasty, Raphaël Le Bihan, Sébastien Malherbe, Marceau Pailhas, Boris Bourdoncle, Pierre-Emmanuel Emeriau, Rawad Mezher, Luka Music, Nadia Belabas, Benoît Valiron, Pascale Senellart, Shane Mansfield, and Jean Senellart. Perceval: A software platform for discrete variable photonic quantum computing. *arXiv preprint*, 2022. arXiv:2204.00602.

[81] Ian Holyer. The NP-completeness of some edge-partition problems. *SIAM Journal on Computing*, 10(4):713–717, 1981. doi:10.1137/0210054.

[82] Kazuo Iwama, Yahiko Kambayashi, and Shigeru Yamashita. Transformation rules for designing CNOT-based quantum circuits. In *Proceedings of the 39th annual Design Automation Conference*, pages 419–424, 2002.

[83] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 559–568, 2018. URL: https://hal.science/hal-01529623, doi:10.1145/3209108.3209131.

[84] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 569–578, 2018.

[85] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Completeness of the ZX-Calculus. *Logical Methods in Computer Science*, Volume 16, Issue 2, June 2020. URL: https://lmcs.episciences.org/6532, doi:10.23638/LMCS-16(2:11)2020.

[86] Michio Jimbo. Introduction to the Yang-Baxter equation. *International Journal of Modern Physics A*, 4(15):3759–3777, 1989.

[87] André Joyal and Ross Street. Planar diagrams and tensor algebra. Unpublished manuscript, available from Ross Street's website, 1988. URL: http://web.science.mq.edu.au/~street/PlanarDiags.pdf.

[88] André Joyal and Ross Street. The geometry of tensor calculus, I. *Advances in Mathematics*, 88(1):55–112, 1991. URL: https://www.sciencedirect.com/science/article/pii/000187089190003P, doi:https://doi.org/10.1016/0001-8708(91)90003-P.

[89] André Joyal, Ross Street, and Dominic Verity. Traced monoidal categories. *Mathematical Proceedings of the Cambridge Philosophical Society*, 119(3):447–468, 1996. URL: https://www.researchgate.net/publication/231966472_Traced_monoidal_categories, doi:10.1017/S0305004100074338.

[90] Gregory M. Kelly and Miguel L. Laplaza. Coherence for compact closed categories. *Journal of Pure and Applied Algebra*, 19:193–213, 1980. doi:10.1016/0022-4049(80)90101-2.

[91] Aleks Kissinger and Arianne Meijer-van de Griend. CNOT circuit extraction for topologically-constrained quantum memories. *arXiv preprint*, 2019. arXiv:1904.00633.

[92] Aleks Kissinger and John van de Wetering. Reducing the number of non-Clifford gates in quantum circuits. *Phys. Rev. A*, 102:022406, August 2020. URL: https://link.aps.org/doi/10.1103/PhysRevA.102.022406, doi:10.1103/PhysRevA.102.022406.

[93] Vadym Kliuchnikov and Dmitri Maslov. Optimization of Clifford circuits. *Physical Review A*, 88(5):052307, 2013.

[94] Emanuel Knill, Raymond Laflamme, and Gerald J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001. doi:10.1038/35051009.

[95] Pieter Kok and Brendon W. Lovett. *Introduction to Optical Quantum Information Processing*. Cambridge University Press, 2010.

[96] Pieter Kok, William J. Munro, Kae Nemoto, Timothy C. Ralph, Jonathan P. Dowling, and Gerald J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79:135–174, January 2007. arXiv:quant-ph/0512071, doi:10.1103/RevModPhys.79.135.

[97] Hlér Kristjánsson, Giulio Chiribella, Sina Salek, Daniel Ebler, and Matthew Wilson. Resource theories of communication. *New Journal of Physics*, 22(7):073014, July 2020. arXiv:1910.08197, doi:10.1088/1367-2630/ab8ef7.

[98] Saunders MacLane. Categorical algebra. *Bulletin of the American Mathematical Society*, 71(1):40–106, 1965. doi:10.1090/S0002-9904-1965-11234-4.

[99] Justin Makary, Neil J. Ross, and Peter Selinger. Generators and relations for real stabilizer operators. In Chris Heunen and Miriam Backens, editors, *Proceedings of the 18th International Conference on Quantum Physics and Logic, QPL 2021*, volume 343 of *EPTCS*, pages 14–36, 2021. doi:10.4204/EPTCS.343.2.

[100] Dmitri Maslov, Gerhard W. Dueck, D. Michael Miller, and Camille Negrevergne. Quantum circuit simplification and level compaction. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 27(3):436–444, 2008.

[101] Dmitri Maslov, Christina Young, D. Michael Miller, and Gerhard W. Dueck. Quantum circuit simplification using templates. In *Design, Automation and Test in Europe*, pages 1208–1213. IEEE, 2005.

[102] Ken Matsumoto and Kazuyuki Amano. Representation of quantum circuits with Clifford and $\pi/8$ gates. *arXiv preprint*, 2008. arXiv:0806.3834.

[103] Yunseong Nam, Neil J. Ross, Yuan Su, Andrew M. Childs, and Dmitri Maslov. Automated optimization of large quantum circuits with continuous parameters. *npj Quantum Information*, 4(1):1–12, 2018.

[104] Beatrice Nash, Vlad Gheorghiu, and Michele Mosca. Quantum circuit optimizations for NISQ architectures. *Quantum Science and Technology*, 5(2):025010, 2020.

[105] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, NY, USA, 2011. doi:10.1017/CBO9780511976667.

[106] Pyotr S. Novikov. Über die algorithmische Unentscheidbarkeit des Wortproblems in der Gruppentheorie. Tr. Mat. Inst. Steklova 44, 140 S., 1955.

[107] Daniel K. L. Oi. Interference of quantum channels. *Physical Review Letters*, 91:067902, August 2003. arXiv:quant-ph/0303178, doi:10.1103/PhysRevLett.91.067902.

[108] Ognyan Oreshkov, Fabio Costa, and Časlav Brukner. Quantum correlations with no causal order. *Nature communications*, 3(1):1–8, 2012.

[109] João Paixão and Paweł Sobociński. Calculational proofs in relational graphical linear algebra. In Gustavo Carvalho and Volker Stolz, editors, *Formal Methods: Foundations and Applications*, pages 83–100. Springer, 2020.

[110] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, and Jeremy L. O'brien. A variational eigenvalue solver on a photonic quantum processor. *Nature communications*, 5(1):1–7, 2014.

[111] Christopher Portmann, Christian Matt, Ueli Maurer, Renato Renner, and Björn Tackmann. Causal boxes: Quantum information-processing systems closed under composition. *IEEE Transactions on Information Theory*, 63(5):3277–3305, 2017. arXiv:1512.02240, doi:10.1109/TIT.2017.2676805.

[112] Lorenzo M. Procopio, Amir Moqanaki, Mateus Araújo, Fabio Costa, Irati Alonso Calafell, Emma G. Dowd, Deny R. Hamel, Lee A. Rozema, Časlav Brukner, and Philip Walther. Experimental superposition of orders of quantum gates. *Nature communications*, 6:7913, 2015. doi:10.1038/ncomms8913.

[113] André Ranchin and Bob Coecke. Complete set of circuit equations for stabilizer quantum mechanics. *Physical Review A*, 90(1):012109, 2014. arXiv:1310.7932.

[114] Michael Reck, Anton Zeilinger, Herbert J. Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73:58–61, July 1994. URL: https://link.aps.org/doi/10.1103/PhysRevLett.73.58, doi:10.1103/PhysRevLett.73.58.

[115] Martin J. Renner and Časlav Brukner. Reassessing the computational advantage of quantum-controlled ordering of gates. *Physical Review Research*, 3(4):043012, 2021.

[116] Giulia Rubino, Lee A. Rozema, Adrien Feix, Mateus Araújo, Jonas M. Zeuner, Lorenzo M. Procopio, Časlav Brukner, and Philip Walther. Experimental verification of an indefinite causal order. *Science Advances*, 3(3):e1602589, 2017. doi:10.1126/sciadv.1602589.

[117] Giulia Rubino, Lee A. Rozema, Francesco Massa, Mateus Araújo, Magdalena Zych, Časlav Brukner, and Philip Walther. Experimental entanglement of temporal order. *Quantum*, 6:621, January 2022. doi:10.22331/q-2022-01-11-621.

[118] Amr Sabry, Benoît Valiron, and Juliana Kaizer Vizzotto. From symmetric pattern-matching to quantum control. In *International Conference on Foundations of Software Science and Computation Structures*, pages 348–364. Springer, 2018. doi:10.1007/978-3-319-89366-2_19.

[119] Peter Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004. doi:10.1017/S0960129504004256.

[120] Peter Selinger. A survey of graphical languages for monoidal categories. In Bob Coecke, editor, *New Structures for Physics*, volume 813 of *Lecture Notes in Physics*, pages 289–355. Springer, 2011. Also available from arXiv:0908.3347. doi:10.1007/978-3-642-12821-9_4.

[121] Peter Selinger. Finite dimensional Hilbert spaces are complete for dagger compact closed categories. *Logical Methods in Computer Science*, Volume 8, Issue 3, August 2012. doi:10.2168/LMCS-8(3:6)2012.

[122] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. arXiv:quant-ph/9508027, doi:10.1137/S0097539795293172.

[123] Mirjam Solberg. Weak braided monoidal categories and their homotopy colimits. *Theory and Applications of Categories*, 30(3):40–48, 2015. URL: http://www.tac.mta.ca/tac/volumes/30/3/30-03.pdf.

[124] W. Forrest Stinespring. Positive functions on C^*-algebras. *Proceedings of the American Mathematical Society*, 6:211–216, 1955. doi:10.1090/S0002-9939-1955-0069403-4.

[125] Terese. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 2003.

[126] Augustin Vanrietvelde, Hlér Kristjánsson, and Jonathan Barrett. Routed quantum circuits. *Quantum*, 5:503, 2021.

[127] Renaud Vilmart. A near-minimal axiomatisation of ZX-calculus for pure qubit quantum mechanics. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–10. IEEE, 2019.

[128] Julian Wechs, Hippolyte Dourdent, Alastair A. Abbott, and Cyril Branciard. Quantum circuits with classical versus quantum control of causal order. *PRX Quantum*, 2:030335, August 2021. doi:10.1103/PRXQuantum.2.030335.

[129] Kejin Wei, Nora Tischler, Si-Ran Zhao, Yu-Huai Li, Juan Miguel Arrazola, Yang Liu, Weijun Zhang, Hao Li, Lixing You, Zhen Wang, Yu-Ao Chen, Barry C. Sanders, Qiang Zhang, Geoff J. Pryde, Feihu Xu, and Jian-Wei Pan. Experimental quantum switching for exponentially superior quantum communication complexity. *Physical Review Letters*, 122:120504, March 2019. arXiv:1810.10238, doi:10.1103/PhysRevLett.122.120504.

[130] Matt Wilson and Giulio Chiribella. A diagrammatic approach to information transmission in generalised switches. *Electronic Proceedings in Theoretical Computer Science*, 340:333–348, September 2021. URL: https://doi.org/10.4204%2Feptcs.340.17, doi:10.4204/eptcs.340.17.

[131] Yulin Wu, Wan-Su Bao, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, et al. Strong quantum computational advantage using a superconducting quantum processor. *Physical Review Letters*, 127(18):180501, 2021.

[132] Mingsheng Ying, Nengkun Yu, and Yuan Feng. Alternation in quantum programming: from superposition of data to superposition of programs. *arXiv preprint*, 2014. arXiv:1402.5172.

[133] Fabio Zanasi. *Interacting Hopf Algebras- the Theory of Linear Systems*. PhD thesis, Ecole normale supérieure de lyon - ENS LYON, October 2015. URL: https://tel.archives-ouvertes.fr/tel-01218015, arXiv:1805.03032.

[134] Han-Sen Zhong, Yu-Hao Deng, Jian Qin, Hui Wang, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Dian Wu, Si-Qiu Gong, Hao Su, et al. Phase-programmable Gaussian boson sampling using stimulated squeezed light. *Physical Review Letters*, 127(18):180502, 2021.

[135] Han-Sen Zhong, Hui Wang, Yu-Hao Deng, Ming-Cheng Chen, Li-Chao Peng, Yi-Han Luo, Jian Qin, Dian Wu, Xing Ding, Yi Hu, et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

[136] Magdalena Zych, Fabio Costa, Igor Pikovski, and Časlav Brukner. Bell's theorem for temporal order. *Nature Communications*, 10(1):1–10, 2019.

Résumé

Dans le modèle usuel de calcul quantique, des opérations sur des données quantiques sont contrôlées de manière essentiellement classique. Un contrôle lui aussi quantique est cependant possible, mais a été peu étudié en comparaison. En particulier, il manque au contrôle quantique un formalisme permettant de l'exprimer de manière simple afin de raisonner efficacement sur des processus l'impliquant.

La première contribution de cette thèse est de poser les fondations d'un cadre formel dédié au contrôle quantique, sous la forme d'un langage graphique. Notre principal résultat concernant ce langage est l'introduction d'une théorie équationnelle complète, c'est à dire d'un ensemble d'équations permettant de transformer un diagramme, par réécriture locale successive, en n'importe quel autre diagramme représentant le même programme ou processus physique.

Une deuxième contribution est l'application de ce formalisme d'une part au problème de l'optimisation des ressources dans les processus impliquant un contrôle quantique, et d'autre part à la caractérisation de l'équivalence observationnelle des canaux de communication quantiques.

La troisième contribution de cette thèse est l'introduction d'un langage pour les circuits optiques linéaires. Nous l'équipons d'une théorie équationnelle complète, ainsi que d'une forme normale simple, accessible par un système de réécriture fortement normalisant et confluent.

La dernière contribution de cette thèse, peut-être la plus importante, est l'introduction d'une théorie équationnelle complète pour le langage des circuits quantiques. Nous nous appuyons pour cela sur une correspondance entre les circuits quantiques et les circuits optiques, qui nous permet de transférer la théorie équationnelle déjà obtenue pour les circuits optiques.

Mots-clés: Informatique quantique, Langages graphiques, Contrôle quantique, Optique linéaire, Théories équationnelles complètes.

Abstract

In the models of quantum computing usually considered, some quantum data is manipulated by means of operations which are controlled in an essentially classical way. Controlling these operations in a quantum way is actually possible, but has been much less studied. In particular, quantum control misses a formalism in which one could represent it in a simple way in order to efficiently reason on processes involving it.

The first contribution of this thesis is to lay the foundations of a formal framework dedicated to quantum control, in the form of a graphical language. Our main result about this language is the introduction of a complete equational theory, that is, a set of equations that makes it possible, by successive local rewriting, to transform a given diagram into any other diagram representing the same program or physical process.

A second contribution is to apply this formalism, on the one hand, to the problem of resource optimisation of processes involving quantum control, and on the other hand, to the characterisation of the observational equivalence of quantum communication channels.

A third contribution of this thesis is to introduce a language for linear optical circuits. We equip this language with a complete equational theory, together with a simple normal form, reachable via a strongly normalising and confluent rewriting system.

The last contribution of this thesis, maybe the most significant one, is to introduce a complete equational theory for the language of quantum circuits. We obtain this result by exploiting a correspondence between quantum circuits and optical circuits, which allows us to transfer the equational theory already obtained for optical circuits.

Keywords: Quantum computing, Graphical languages, Quantum control, Linear optics, Complete equational theories.