Aspects algébriques des circuits quantiques de portes de Clifford. Application à l'optimisation des circuits et à l'intrication

Marc Bataille

Normandie Université

UNIVERSITÉ DE ROUEN NORMANDIE

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité INFORMATIQUE

Préparée au sein de l'Université de Rouen Normandie

Aspects algébriques des circuits quantiques de portes de Clifford. Application à l'optimisation des circuits et à l'intrication

Présentée et soutenue par
MARC BATAILLE

Thèse soutenue le 13/06/2023 devant le jury composé de		
M. OMAR FAWZI	DIRECTEUR DE RECHERCHE, INRIA	Rapporteur du jury
M. ALAIN GIORGETTI	MAITRE DE CONFERENCES HDR, UNIVERSITE BESANCON FRANCHE COMTE	Rapporteur du jury
M. BENJAMIN AUDOUX	MAITRE DE CONFERENCES HDR, Aix-Marseille Université	Membre du jury
MME GIOVANNA GUAIANA	MAITRE DE CONFERENCES, Université de Rouen Normandie	Membre du jury
M. FREDERIC HOLWECK	MAITRE DE CONFERENCES HDR, UNIV TECHN BELFORT MONTBELIARD UTBM SEVENANS	Membre du jury
M. THIERRY JOLICOEUR	DIRECTEUR DE RECHERCHE, CENTRE NAT RECH SCIENTIFIQUE	Membre du jury
M. SIMON PERDRIX	DIRECTEUR DE RECHERCHE, Centre régional de l'INRIA Nancy	Président du jury
M. JEAN-GABRIEL LUQUE	PROFESSEUR DES UNIVERSITES, Université de Rouen Normandie	Directeur de thèse

Thèse dirigée par JEAN-GABRIEL LUQUE (Laboratoire d'Informatique, du Traitement de l'Information et des Systèmes)

MIIS

litis

Remerciements

En premier lieu, je veux remercier Jean-Gabriel Luque, mon directeur de thèse, pour au moins trois raisons. D'abord pour m'avoir initié à l'informatique quantique quand j'étais étudiant en master et avoir éveillé ma curiosité sur l'univers quantique et ses manifestations surprenantes, un monde fascinant dont j'ignorais alors presque totalement l'existence. Ensuite pour m'avoir accordé sa confiance en m'acceptant comme doctorant et en me laissant une grande autonomie dans mes recherches. Enfin, pour ses conseils et son esprit critique, son indépendance et sa curiosité intellectuelle qui m'ont donné le goût de la recherche et l'envie de progresser dans la compréhension des concepts. Sous sa supervision, ces quelques années de recherche ont été un enrichissement intellectuel et un véritable plaisir.

Sans être une spécialiste du domaine, Giovanna Guaiana, ma co-encadrante, m'a aidé à mettre au point mon travail par ses conseils avisés et son regard critique de chercheuse expérimentée. Qu'elle en soit remerciée.

Un an avant le début de cette thèse, j'ai eu la chance de faire la connaissance de Frédéric Holweck pendant mon stage de master. Nous sommes restés en contact et je souhaite lui exprimer ma gratitude pour les discussions scientifiques que nous avons pu avoir, pour son accueil chaleureux lors de mes séjours à Belfort, ainsi que pour ses encouragements et sa disponibilité.

Je suis très reconnaissant à Omar Fawzi et à Alain Giorgetti de m'avoir fait l'honneur d'être les rapporteurs de cette thèse. Je remercie également Benjamin Audoux, Thierry Jolicoeur et Simon Perdrix d'avoir accepté de faire partie de mon jury.

La recherche est une activité chronophage, ce qui n'est pas sans impact sur la vie familiale. Ce mémoire n'aurait tout simplement pas pu voir le jour sans le soutien de toujours de ma compagne Maviane. Quant à mes deux petits diables Théo et Marie, ils ont su rendre mes journées plus lumineuses et me ramener les deux pieds sur terre quand j'avais la tête un peu perdue dans les nuages. Merci à eux trois pour tout le bonheur qu'ils m'apportent.

Table des matières

Table des figures

Liste des tableaux

Liste des algorithmes

Notations

Chaque nouvelle notation est décrite de façon détaillée au moment où elle est introduite. Nous récapitulons ici les principales notations utilisées en en donnant une brève description.

Espace de Hilbert

$\mathcal{H}$	Espace de Hilbert complexe
$\mathbb{P}(\mathcal{H})$	Espace projectif de $\mathcal{H}$
$\|\psi\rangle$	Vecteur de l'espace $\mathcal{H}$
$\|\psi\rangle \simeq \|\psi'\rangle$	Vecteurs égaux à une phase près
$A \simeq B$	Opérateurs égaux à une phase près
$\langle\psi\|$	Forme linéaire associée à $\|\psi\rangle$
$\langle\psi\|\psi'\rangle$	Notation de Dirac pour le produit scalaire hermitien
$\|\|\,\|\psi\rangle\,\|\|$	Norme de $\|\psi\rangle$
$\otimes$	Produit tensoriel ou produit de Kronecker
z^*	Conjugué du nombre complexe z
M^*	Matrice conjuguée
M^t	Matrice transposée
$M^\dagger$	Opérateur adjoint ou matrice adjointe

Registre de qubits

n	Nombre de qubits d'un registre quantique
q_i	qubit i d'un système quantique de n qubits $q_0, \ldots, q_{n-1}$
$\mathbb{F}_2$	Corps à deux éléments
$\oplus$	Addition dans $\mathbb{F}_2$, XOR (ou exclusif) ou différence symétrique entre deux ensembles
$\mathcal{H}^{\otimes n}$	Espace de Hilbert d'un système de n qubits avec $\mathcal{H} \simeq \mathbb{C}^2$
$(\|0\rangle, \|1\rangle)$	Base standard de $\mathcal{H} \simeq \mathbb{C}^2$
$\|b_0 b_1 \ldots b_{n-1}\rangle$	Vecteur de la base standard de l'espace $\mathcal{H}^{\otimes n}$ des qubits, avec $b_i \in \mathbb{F}_2$
$\mathbb{F}_2^n$	Espace vectoriel de dimension n sur $\mathbb{F}_2$
$(e_i)_{i=0\ldots n-1}$	Base canonique de $\mathbb{F}_2^n$
$v \cdot w$	Produit scalaire usuel de deux vecteurs de $\mathbb{F}_2^n$

Matrices particulières

I ou I_n	Matrice identité $n \times n$
0 ou 0_n	Matrice $n \times n$ dont toutes les entrées sont nulles
E_{ij}	Matrice à coefficients dans $\mathbb{F}_2$ ayant l'entrée (i, j) égale à 1 et les autres entrées nulles
$E_{\{i,j\}}$	Matrice symétrique à coefficients dans $\mathbb{F}_2$ égale à $E_{ij} + E_{ji}$
$[i : j]$	Matrice de transvection, égale à $I + E_{ij}$
$\mathcal{B}_n$	Ensemble des matrices symétriques $n \times n$ à entrées dans $\mathbb{F}_2$
$\mathcal{B}_n^0$	Ensemble des matrices symétriques $n \times n$ de diagonale nulle à entrées dans $\mathbb{F}_2$

Groupes classiques

U_m	Groupe unitaire en dimension m
SU_m	Groupe spécial unitaire en dimension m
$\mathrm{PSU_m}$	Groupe projectif spécial unitaire en dimension m
$\mathrm{SO}_m(\mathbb{R})$	Groupe spécial orthogonal en dimension m
$\mathrm{GL}_m(\mathbb{F}_2)$	Groupe linéaire sur $\mathbb{F}_2$ en dimension m
$\mathrm{Sp}_{2m}(\mathbb{F}_2)$	Groupe symplectique sur $\mathbb{F}_2$ en dimension $2m$

Groupes engendrés par des portes quantiques

$\langle CNOT \rangle_n$	Groupe engendré par les portes $CNOT$ agissant sur un système de n qubits
$\langle SWAP \rangle_n$	Groupe engendré par les portes $SWAP$ agissant sur un système de n qubits
$\langle CZ \rangle_n$	Groupe engendré par les portes CZ agissant sur n qubits
$\langle CZ, SWAP \rangle_n$	Groupe engendré par les portes CZ et $SWAP$ agissant sur n qubits
$\langle CZ, CNOT \rangle_n$	Groupe engendré par les portes CZ et $CNOT$ agissant sur n qubits
$\mathcal{E}_n$	Groupe de Pauli pour n qubits
$\mathcal{C}_n$	Groupe de Clifford pour n qubits
Stab_n	Groupe des circuits stabilisateurs pour n qubits

Portes et circuits quantiques

X, Y, Z	Les trois portes de Pauli
H	Porte de Hadamard
P	Porte de changement de phase
T	Porte $\frac{\pi}{8}$
U_i	Porte quantique unaire agissant sur le qubit i d'un registre quantique
U_v	Produit de portes U_i défini par le vecteur $v \in \mathbb{F}_2^n$
$X_{[i:j]}$	Porte NOT sur le qubit i contrôlée par le qubit j
$Z_{\{i,j\}}$	Porte contrôle Pauli-Z entre les qubits i et j
$(i\ \ j)$	Transposition qui échange i et j
$S_{(i\ \ j)}$	Porte $SWAP$ entre les qubits i et j d'un système de n qubits
S_σ	Opérateur unitaire du groupe $\langle SWAP \rangle_n$ associé à la permutation σ
X_A	Opérateur unitaire du groupe $\langle CNOT \rangle_n$ associé à la matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$
Z_G	Opérateur unitaire du groupe $\langle CZ \rangle_n$ défini par $G \in \mathcal{G}_n$
Z_B	Opérateur unitaire du groupe $\langle CZ \rangle_n$ défini par la matrice $B \in \mathcal{B}_n^0$
Cliff_n	Ensemble des portes de Clifford

Symboles divers

$\lfloor x \rfloor$	Partie entière du réel x
δ_{ij}	Symbole de Kronecker
$\lvert E \rvert$	Cardinal d'un ensemble E
$\mathfrak{S}_n$	Groupe symétrique
$\mathcal{G}_n$	Parties de l'ensemble des paires $\{i, j\}$ pour $0 \leqslant i, j \leqslant n-1$
Δ_n	Hyperdéterminant au format 2^n

Introduction

Sans même que nous en soyons toujours conscients, la physique quantique est omniprésente dans notre quotidien. Née au début du XX^{e} siècle, cette théorie permet d'expliquer les propriétés de la matière à l'échelle atomique et subatomique. Elle est à la base du développement de nombreuses technologies modernes comme les horloges atomiques utilisées par le GPS, l'IRM en médecine, les lasers, les centrales nucléaires ou encore les semi-conducteurs présents dans les transistors des ordinateurs.

La théorie de la calculabilité élaborée par Church et Turing dans les années 1930, puis la théorie de l'information de Shannon à la fin des années 1940, ont permis à l'informatique de se développer sur des fondations solides et les ordinateurs ont progressivement gagné en miniaturisation, en rapidité et en mémoire. Malgré cet essor technologique continu et impressionnant, certains problèmes algorithmiques réputés difficiles, comme la factorisation des grands nombres ou le logarithme discret, sont actuellement impossibles à résoudre avec les ordinateurs les plus performants. Quant à la simulation d'un système quantique sur un ordinateur classique, elle reste cantonnée à des systèmes ayant peu de paramètres alors que des applications pratiques vraiment utiles, par exemple en chimie ou en pharmacologie, nécessiteraient une mémoire et un temps de calcul hors de portée des supercalculateurs actuels.

Afin de franchir ces limites, une piste prometteuse est de développer une théorie de l'information et des ordinateurs basés sur d'autres lois physiques que les lois classiques. En effet, les ordinateurs actuels sont basés sur une vision mécaniste classique des calculs qui sont implantés dans des machines sous la forme d'opérations logiques sur des registres de bits. L'utilisation des propriétés du monde quantique comme l'intrication ou la superposition dans un nouveau type d'ordinateur devrait augmenter les performances et permettre des percées significatives. Cette idée remonte au début des années 1980 [22, 136, 78] et par la suite la théorie de l'information quantique s'est considérablement développée (voir par exemple [148]). Sans attendre l'arrivée d'un ordinateur quantique fonctionnel, des algorithmes spectaculaires ont déjà été inventés, citons par exemple ceux de Deutsch-Josza [68], de Grover [93] ou de Shor [166].

Construire un ordinateur quantique fonctionnel est un des grands défis technologiques de la physique moderne et de nombreuses solutions ont été explorées (voir chapitre 1). Une des principales difficultés est de réussir à garder la superposition quantique pendant toute la durée du calcul. L'autre grand problème concerne les portes quantiques qui sont les composants élémentaires des circuits quantiques des ordinateurs. Ces portes quantiques implantent dans la machine les différentes opérations à effectuer mais dans l'ère actuelle du développement de l'informatique quantique, elles ne peuvent être appliquées sans erreurs, ce qui fausse les résultats.

Pour tenter de surmonter ces difficultés, on peut jouer sur plusieurs leviers. Nous résumons les principales stratégies envisagées de la façon suivante. La première stratégie

consiste à construire des machines plus stables avec des taux d'erreurs plus faibles. La seconde consiste à gérer les erreurs en utilisant des codes quantiques correcteurs d'erreurs (voir chapitre 1, section 1.4). Enfin, la troisième option consiste à optimiser les circuits quantiques en essayant de minimiser le nombre de portes quantiques dans un circuit donné.

Une partie des résultats de cette thèse est liée à l'optimisation des circuits quantiques. Cependant, la découverte de nouvelles méthodes d'optimisation n'est pas notre objectif principal mais plutôt une conséquence pratique de certains résultats. Notre premier objectif est d'étudier du point de vue algébrique certains circuits quantiques très simples qui sont des cas particuliers de circuits bien connus appelés circuits de Clifford. Ces circuits sont composés exclusivement de portes $CNOT$ (portes contrôle-NOT), de portes CZ (portes contrôle-Z), de portes H (portes de Hadamard) et de portes P (portes de changement de phase). Parfois, la structure de groupe sous-jacente aux circuits étudiés fournit des méthodes assez naturelles pour réduire ou optimiser le nombre de portes quantiques utilisées. Ainsi, dans cette thèse, il ne s'agit pas de fournir une méthode générale d'optimisation des circuits améliorant une des nombreuses propositions déjà existantes dans la littérature (voir chapitre 1, section 1.4) mais plus simplement de signaler quelques cas particuliers qui nous semblent utiles, comme par exemple les circuits produisant les états de graphe (*graph states* en anglais).

L'autre thématique abordée dans ce mémoire est celle de l'intrication quantique. Dans un système quantique intriqué, des corrélations apparaissent instantanément entre des mesures effectuées sur deux parties de ce système même si ces parties sont très éloignées dans l'espace. Ce phénomène non classique surprenant est décrit en détail dans le chapitre 1. Cependant, afin d'en donner déjà une première idée au lecteur ne connaissant pas le sujet, nous présentons dès maintenant une analogie souvent utilisée entre un système quantique intriqué et deux pièces de monnaie. Comme toute image, elle est approximative, mais elle présente l'avantage de donner immédiatement une première idée de ce qu'est l'intrication et des difficultés conceptuelles liées à ce phénomène.

Imaginons deux personnages, Alice et Bob, ayant chacun en leur possession une pièce de monnaie. À un moment du passé, ces deux pièces ont été confectionnées ensemble et leur fabriquant leur a donné une propriété particulière qui se manifeste lors de l'expérience suivante. Alice et Bob lancent ensemble leur pièce, à l'aide d'un appareillage permettant à la pièce de tourner dans les airs indéfiniment (par exemple une soufflerie) et de la faire retomber en appuyant sur un bouton. Alice appuie sur son bouton et obtient *face*. Ensuite Bob fait de même et obtient *face* également. Ils recommencent l'expérience, et cette fois-ci ils obtiennent tous les deux *pile*. En continuant, ils s'aperçoivent qu'ils obtiennent toujours, soit deux faces, soit deux piles, à peu près dans les mêmes proportions. Tout se passe comme si le premier résultat obtenu déterminait le second. Est-il possible que les pièces comportent un système caché ultra sophistiqué qui leur permettent de s'influencer à distance en s'envoyant un signal ? Alice et Bob connaissent la théorie de la relativité restreinte d'Einstein qui énonce qu'aucun signal ne peut se propager plus vite que la lumière. Ils décident donc de s'éloigner suffisamment l'un de l'autre de telle sorte qu'aucune information n'ait le temps de se propager entre eux pendant le déroulement de l'expérience. Pourtant, après avoir comparé leurs résultats, ils font encore le même constat : les deux tirages sont toujours identiques avec à peu près autant de double pile que de double face. A l'heure actuelle, Alice et Bob n'ont toujours pas percé le secret de fabrication des pièces.

Dans cette analogie, les pièces représentent un système quantique de deux qubits dans un état *intriqué* particulier, l'état EPR, que nous décrirons en détail dans le

premier chapitre de ce mémoire. Dans la théorie de l'information quantique, les états intriqués sont considérés comme une ressource fondamentale car ils interviennent dans de nombreux protocoles de communication qui utilisent d'une façon judicieuse les corrélations que nous venons de décrire. Nous étudions dans cette thèse les types d'états intriqués pouvant être atteints par l'action de certaines portes quantiques très courantes, essentiellement les portes contrôle-Z et les portes contrôle-NOT. Nous proposons quelques constructions originales d'états intriqués utiles au calcul quantique. Les états construits sont principalement des états génériquement intriqués et des états maximalement intriqués, au sens de la mesure de l'intrication basée sur l'hyperdéterminant de Cayley (voir chapitre 5). Là encore, l'aspect algébrique apparaît naturellement car les classes d'intrication sont décrites par des orbites obtenues par l'action du groupe SLOCC sur l'ensemble des états d'un système quantique (voir chapitre 1, section 1.2.2) et par des variétés algébriques correspondantes à la fermeture de ces orbites.

Organisation du manuscrit

Le chapitre 1 est une introduction détaillée aux circuits quantiques. Il s'agit d'une tentative de synthèse des notions de physique quantique et de théorie de l'information quantique nécessaires à la compréhension du formalisme de ces circuits d'une part et à la notion d'intrication quantique d'autre part. Il ne s'agit pas d'un état de l'art sur les thématiques abordées dans cette thèse mais plutôt d'un chapitre destiné à un lecteur débutant en informatique quantique. Ce chapitre expose les notions de base et donne de nombreuses références vers des approfondissements. Concernant l'état de l'art proprement dit, et afin d'améliorer la lisibilité de ce mémoire, nous avons préféré répartir dans chacun des quatre autres chapitres les résultats déjà connus sur lesquels sont basés nos développements.

Les chapitres 2, 3 et 4 portent globalement sur les différentes structures algébriques présentes dans les circuits de Clifford avec des applications à l'optimisation et à l'implantation de ces circuits dans des ordinateurs quantiques. Nous proposons également différentes formes normales. Dans ces trois chapitres, les portes quantiques composant l'ensemble de Clifford sont introduites progressivement. Le chapitre 2 s'intéresse uniquement aux circuits de portes $CNOT$. Dans le chapitre 3, nous enrichissons les constructions en incorporant à ces circuits des portes CZ. Finalement dans le chapitre 4 nous considérons le cas général des circuits de Clifford en réutilisant les résultats des deux chapitres précédents.

Dans le chapitre 5, nous étudions les circuits de portes $CNOT$ et les circuits de portes CZ sous l'angle de l'intrication. Nous cherchons à déterminer les types d'intrications pouvant apparaître dans ces circuits pour des petits systèmes quantiques. Ce chapitre est relativement indépendant des trois chapitres précédents.

Enfin, la conclusion dresse un bilan de notre recherche en la replaçant dans le contexte actuel du développement de l'informatique quantique et de ses problématiques. Nous esquissons également quelques pistes de recherches qui pourraient prolonger nos travaux.

Notez également la présence en fin de manuscrit de 5 annexes (annexes A, B, C, D et E). L'annexe A rassemble les différentes notions de théorie des groupes utilisées dans ce mémoire. Dès qu'un résultat fait appel à cette théorie, nous renvoyons le lecteur souhaitant rafraîchir ses connaissances vers la partie correspondante de cette annexe.

Les quatre autres annexes contiennent des démonstrations ou des listes de résultats reportées en fin de manuscrit dans le but de rendre la lecture plus fluide. En particulier, l'annexe B contient deux démonstrations assez longues et techniques de théorèmes du chapitre 3 concernant les présentations de groupes.

Liste des travaux et publications

Articles publiés

Pour chaque article, nous avons indiqué l'URL de la prépublication correspondante déposée sur arXiv, ainsi que les chapitres de la thèse qui reprennent les résultats de l'article.

- Marc Bataille and Jean-Gabriel Luque, Quantum circuits of CZ and $SWAP$: optimization and entanglement, Journal of Physics A 52 (2019), No. 32, 325302

  `https://arxiv.org/abs/1810.01769`

  → Chapitres 3 et 5

- Marc Bataille, Quantum circuits of CNOT gates : optimization and entanglement, Quantum Information Processing 21 (2022), No. 7, 269

  `https://arxiv.org/abs/2009.13247`

  → Chapitres 2 et 5

- Marc Bataille, Quantum circuits generating four-qubit maximally entangled states, Mathematical Structures in Computer Science 32 (2022), No. 3, 257–270

  `https://arxiv.org/abs/2110.06362`

  → Chapitre 5

Travaux en cours

Un article basé sur les résultats du chapitre 4 de la thèse et sur la prépublication ci-dessous est en cours de préparation.

- Marc Bataille, Reduced quantum circuits for stabilizer states and graph states, 2021

  `https://arxiv.org/abs/2107.00885`

Chapitre 1

De la physique quantique à l'ordinateur quantique

Dans ce chapitre introductif nous présentons les notions permettant à un lecteur informaticien non spécialiste de lire ce mémoire sans avoir l'obligation de se référer constamment à différents ouvrages. Tous les concepts et résultats abordés ici ne sont pas indispensables à la seule lecture de ce mémoire car notre objectif est plus général : fournir sous un format réduit une synthèse des bases de physique quantique et de théorie de l'information quantique qui nous semblent utiles à la compréhension du formalisme des circuits quantiques, qui est le modèle de calcul dans lequel sont généralement décrits les algorithmes quantiques. Nous avons également souhaité évoquer les débats historiques autour de la notion d'intrication, les inégalités de Bell et la non-localité afin de replacer notre recherche sur l'intrication dans un contexte plus large.

Pour approfondir les notions introduites ici nous conseillons la lecture de deux ouvrages classiques : celui de Cohen-Tannoudji *et al.* [59] pour l'aspect mécanique quantique et celui de Nielsen et Chuang [148] pour l'aspect théorie de l'information quantique et calcul quantique. Nous renvoyons d'ailleurs fréquemment vers ces deux références en mentionnant de façon précise où y trouver approfondissements et compléments d'information.

L'informatique quantique est en plein développement, tant au niveau de la recherche que de l'enseignement supérieur ou de l'intérêt croissant du public et des médias pour cette discipline. Ainsi, on trouve sur la toile de nombreux cours, tutoriels et vidéos sur le sujet et des livres sont régulièrement publiés.

Parmi les publications récentes (2021), nous nous permettons de conseiller au lecteur débutant en informatique quantique deux livres faciles d'accès au contenu très didactique : [28] qui reprend les bases mathématiques nécessaires et donne une description détaillée des principaux algorithmes quantiques, ainsi que [58] pour une introduction à la programmation d'algorithmes quantiques avec le langage *Qiskit*.

Concernant les nombreuses vidéos sur la mécanique quantique présentes sur la toile, les conférences d'Alain Aspect [1] relatant sa démarche d'expérimentateur nous semblent un modèle de clarté et de pédagogie. On y mentionne souvent des applications à la théorie de l'information quantique. Nous conseillons aussi les nombreuses vidéos de David Louapre sur différent thèmes relatifs à la physique quantique ou à la théorie de

1. Alain Aspect, physicien français né en 1947, prix Nobel de physique 2022 pour ses expériences sur les inégalités de Bell et la non-localité.

l'information quantique [130], sans oublier son interview d'Alain Aspect [129]. Enfin, nous avons particulièrement apprécié les vidéos de David Deutsch [2], tant pour aborder les fondements de l'informatique quantique que pour aller plus loin sur l'interprétation de la mécanique quantique [67].

1.1 Quelques bases de physique quantique

Cette section rassemble quelques aspects du formalisme mathématique de la mécanique quantique. Les postulats de la mécanique quantique que nous mentionnons sont énoncés dans [59, chapitre III, section B]. Nous commençons par donner un aperçu de quelques idées importantes de la théorie quantique en les plaçant dans leur contexte historique et en citant les principales expériences qui ont mené à l'émergence de nouveaux concepts.

1.1.1 Naissance de la physique quantique au travers de quelques expériences fondatrices

Les expériences et les découvertes mentionnées ici sont largement documentées sur la toile et dans la littérature, aussi nous serons assez concis, en renvoyant le lecteur curieux d'en savoir plus vers les conférences d'Etienne Klein pour l'aspect historique et épistémologique [115], les vidéos de David Louapre [130] pour une première approche un peu plus technique (mais néanmoins vulgarisée) et vers l'ouvrage classique de Cohen-Tannoudji *et al.* [59] pour une description formelle.

Existence du photon et dualité onde-corpuscule

La mécanique quantique est la théorie utilisée actuellement pour décrire le comportement de systèmes physiques de petite taille, typiquement à l'échelle atomique et subatomique. Cette théorie s'est construite progressivement dans les trois premières décennies du XX^{e} siècle autour de l'impossibilité d'expliquer certains phénomènes expérimentaux de façon classique (voir par exemple [115]). Ainsi la théorie classique de l'électromagnétisme de Maxwell, ne parvenait pas à expliquer de façon satisfaisante le rayonnement du corps noir. Le problème fut résolu en 1900 par Planck [3] qui proposa d'associer à chaque onde électromagnétique de fréquence ν, une énergie égale à un multiple entier d'un *quantum d'énergie* $E = h\nu$, où h est une constante qui sera appelée plus tard *constante de Planck*. Ainsi l'énergie d'une onde électromagnétique ne peut pas prendre des valeurs continues comme dans la description classique car elle est quantifiée en petits paquets d'énergie $h\nu$.

Cette idée de quantification de l'énergie ouvrit la voie à l'explication d'un autre phénomène jusqu'alors incompris ; l'effet photoélectrique, qu'on peut définir de façon sommaire comme l'apparition d'un courant électrique, donc d'une circulation d'électrons, quand un matériau métallique reçoit une onde électromagnétique. En considérant que la lumière était juste une onde, on ne parvenait pas à expliquer pourquoi la circulation des électrons se produisait seulement au dessus d'une certaine fréquence (dépendante du matériau) et cela quelque soit l'intensité de l'onde envoyée. Einstein proposa en 1905 une explication basée sur une description corpusculaire de la lumière : le quanta d'énergie $E = h\nu$ est en fait l'énergie d'une particule, qu'on nommera par la suite *photon*. Ces

2. David Deutsch, né en 1953, physicien israélo-britannique, un des grands spécialistes contemporains de l'informatique quantique.

3. Max Planck (1858-1947), physicien allemand, prix Nobel de physique 1918.

photons sont absorbés par les atomes du matériau uniquement s'ils ont une énergie minimale, énergie qui est proportionnelle à la fréquence ν de l'onde.

En utilisant cette quantification de l'énergie sous forme de photons, Bohr mit au point en 1913 un modèle de l'atome permettant d'expliquer les raies spectrales obtenues lors de l'émission ou de l'absorption d'une onde électromagnétique : un atome va émettre ou absorber des photons ayant une fréquence et donc une énergie bien précise (voir par exemple [59, chapitre I, section B-1]). Si on admet qu'un atome possède un ensemble discret de niveaux d'énergie $E_1, \ldots, E_n$ alors le passage d'un niveau E_i à un niveau E_j se fait par l'absorption ou l'émission d'un photon de fréquence ν_{ij} telle que $h\nu_{ij} = |E_i - E_j|$.

La confirmation expérimentale de l'existence du photon aura lieu en 1922 dans une expérience inventée par Compton [4] : un photon entre en collision avec un électron faiblement lié d'un atome et voit ainsi sa longueur d'onde augmenter, puisque la collision diminue son énergie donc sa fréquence. C'est le fameux *effet Compton*. Ainsi la lumière, dont la nature ondulatoire avait été mise en évidence par la physique classique plus d'un siècle auparavant (expérience des fentes de Young [5] en 1801), ne pouvait plus être considérée uniquement comme une onde.

En 1923, le français De Broglie [6] va plus loin en postulant l'existence d'une onde qui serait associée à toute particule et en donnant une formule permettant d'en calculer la longueur d'onde. Cette hypothèse est confirmée la même année dans l'expérience de Davisson et Germer où des électrons se comportent comme une onde dont la longueur d'onde est bien celle prévue par De Broglie.

Expérience de Young et superposition quantique

Dans l'expérience de Young, une source lumineuse passe au travers de deux petites fentes A et B, entraînant un phénomène de diffraction et l'apparition de franges d'interférences sur un écran, c'est à dire d'une alternance de franges sombres et claires. On peut reprendre cette expérience avec des moyens modernes en baissant suffisamment l'intensité de la source lumineuse pour ne laisser passer qu'un seul photon à la fois (cette expérience et son analyse sont décrites en détail dans [59, chapitre I, section A-2]). Avec quelques photons, on observe sur l'écran des points clairs correspondant à des impacts, ce qui prouve que la lumière n'est pas seulement une onde puisqu'on devrait observer dans ce cas des franges d'interférences de très faible intensité. Si on augmente le temps d'exposition de manière à laisser passer (toujours un par un) une grande quantité de photons, les différents impacts forment progressivement des franges d'interférences alors que dans une interprétation purement corpusculaire on devrait obtenir deux taches séparées, chaque tache correspondant à l'ensemble des photons qui sont passés par une même fente. La conclusion est qu'un photon n'est ni une onde, ni un corpuscule mais une entité dont il est difficile d'avoir une représentation mentale précise et qui va se comporter, aux yeux de l'expérimentateur, parfois comme une onde, parfois comme un corpuscule. On parle alors de *dualité onde-corpuscule*.

Un autre constat fondamental obtenu lors de cette expérience est le suivant : si l'on mesure à l'aide d'un appareil par quelle fente A ou B le photon est passé, alors les franges d'interférences disparaissent et on observe deux taches comme attendu dans l'interprétation corpusculaire. Ainsi l'observation change de façon radicale le comportement du photon. On dit en mécanique quantique que la mesure entraîne *l'effondrement de la fonction d'onde* (on dit aussi *la réduction du paquet d'onde*).

4. Arthur Compton (1892-1962), physicien américain, prix Nobel de physique 1927.
5. Thomas Young (1773-1829), physicien et médecin anglais.
6. Louis de Broglie (1892-1987), physicien français, prix Nobel de physique 1929.

Cette expérience a été répétée assez récemment en 2013 avec des électrons à la place de photons [13] mais elle avait déjà été imaginée par Feynman [7] au début des années 60 comme une expérience de pensée [127].

On observe alors exactement les mêmes phénomènes que pour les photons : diffraction des électrons et interférences, réduction du paquet d'onde en cas de mesure. Ainsi la dualité onde-corpuscule est un concept général applicable à tout objet quantique.

Le modèle proposé par la mécanique quantique associe à chaque particule une *fonction d'onde*, notée généralement $\psi(\mathbf{r}, t)$ dont le carré de l'amplitude à un instant donné t et à un endroit donné de l'espace défini par le vecteur $\mathbf{r}$, est proportionnel à la probabilité que cette particule soit détectée sous forme corpusculaire à cet endroit quand on mesure sa position. On parle alors d'onde de probabilité pour la distinguer d'une onde au sens de la mécanique classique. Ainsi les parties les plus claires des franges d'interférences (là où les impacts des corpuscules sont les plus nombreux) correspondent aux points de l'écran où l'amplitude est la plus forte à l'instant de la mesure. En l'absence d'appareil de mesure au niveau des fentes, cette onde est la somme de deux fonctions d'ondes issues de la diffraction qui se produit au niveau de chaque fente, d'où le phénomène d'interférences. On dit alors que le système est dans un état de superposition de l'onde issue de la fente A et de l'onde issue de la fente B. En cas de mesure au niveau des fentes, il y a réduction du paquet d'onde et à cet instant la particule est parfaitement localisée dans l'espace, du côté de la fente A ou de la fente B mais pas des deux côtés en même temps.

Existence du spin

Pour terminer, mentionnons une dernière expérience fondatrice : celle de Stern et Gerlach en 1922, célèbre pour avoir permis de détecter l'existence du spin (voir par exemple [128] et [59, chapitre IV, section A]). Dans cette expérience, un atome d'argent est projeté selon l'axe $\hat{y}$ dans un champ magnétique non uniforme orienté selon l'axe $\hat{z}$, puis vient impacter une plaque perpendiculaire à l'axe $\hat{y}$. Si un moment magnétique atomique existe, alors, selon les prévisions de la théorie classique, l'atome devrait être dévié de façon aléatoire dans la direction de l'axe $\hat{z}$ et on devrait voir apparaître sur la plaque des impacts répartis uniformément entre un point haut et un point bas. Or, on observe seulement deux petites zones d'impact : l'une autour du point haut, l'autre autour du point bas, et rien entre les deux. On en déduit l'existence, pour cet atome, d'un moment magnétique atomique quantifié dont la projection dans une direction arbitraire prend seulement deux valeurs.

Cette déviation sera attribuée, par Pauli [8] en 1924, à une grandeur physique appelée *spin* absente de la théorie classique. Il s'agit d'une grandeur interne des particules, au même titre que la masse ou la charge électrique. De plus, le spin est la seule grandeur physique décrite par la mécanique quantique qui n'a pas d'équivalent dans la physique classique. Toute particule possède un spin (éventuellement nul comme pour le photon) et cette grandeur est quantifiée, tout comme l'énergie des atomes ou celle d'une onde électromagnétique. Dans le cas d'une particule de spin 1/2 comme l'électron, cette grandeur prend deux valeurs possibles. En notant $\hbar = \frac{h}{2\pi}$ la constante de Planck réduite, ces deux valeurs sont $\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$. On mesure la valeur $\frac{\hbar}{2}$ quand la particule est déviée vers le haut dans un champ magnétique orientée selon l'axe $\hat{z}$ (état de spin *up* noté $\uparrow$) et on mesure $-\frac{\hbar}{2}$ quand elle est déviée vers le bas (état de spin *down* noté $\downarrow$). Avant d'entrer

7. Richard Feynman (1918-1988), physicien américain, prix Nobel de physique 1965.
8. Wolfgang Pauli (1900-1958), physicien autrichien, prix Nobel de physique 1945.

dans le champ magnétique, l'atome d'argent est dans un état de superposition des états de spin up et de spin down. En entrant dans le champ magnétique, par interaction du moment magnétique associé au spin avec celui-ci, il y a réduction du paquet d'onde et l'atome est soit dans un état de spin up, soit dans un état de spin down. La superposition a donc disparu.

Cette binarité des valeurs du spin s'avèrera particulièrement intéressante dans le cadre de la théorie de l'information quantique pour donner une existence physique au concept de qubit (voir plus loin section 1.2).

1.1.2 Espace des états d'un système quantique

Espace des états d'une particule

En mécanique quantique, l'état d'un système à un instant t est entièrement décrit par un vecteur *normalisé* (*i.e.* unitaire) d'un espace de Hilbert [9] complexe $\mathcal{H}$. C'est le *premier postulat* de la mécanique quantique. Cet espace $\mathcal{H}$ est un espace vectoriel de dimension finie ou infinie (la dimension dépend du système étudié), muni d'un produit scalaire dit *hermitien* [10] qui est de plus un espace vectoriel normé *complet* (*i.e. un espace de Banach* [11]) pour la norme définie par ce produit scalaire.

La notation adoptée en mécanique quantique (et donc en informatique quantique) pour les vecteurs de $\mathcal{H}$ est celle introduite par Dirac [12] : un vecteur est noté par un *ket*, c'est à dire une étiquette écrite à l'intérieur du symbole $|\ \rangle$. On trouvera par exemple les notations : $|\psi\rangle$ ou $|\varphi\rangle$ (ψ désigne généralement la fonction d'onde du système), $|\uparrow\rangle$ et $|\downarrow\rangle$ (pour les spins *up* et *down*), $|0\rangle$ et $|1\rangle$ ou encore $|+\rangle$ et $|-\rangle$ pour les deux états de base d'un système formé d'un seul qubit, $|e_0\rangle \dots |e_{m-1}\rangle$ ou bien $|0\rangle, |1\rangle, |2\rangle, \dots, |m-1\rangle$ pour les m vecteurs d'une base, etc. On utilise également parfois la notation $|\lambda\varphi\rangle$ pour le produit $\lambda\,|\varphi\rangle$ ($\lambda \in \mathbb{C}$) et la notation $|\varphi + \psi\rangle$ pour la somme $|\varphi\rangle + |\psi\rangle$.

Deux vecteurs normalisés $|v\rangle$ et $e^{i\varphi}\,|v\rangle$ de l'espace $\mathcal{H}$ ne peuvent pas être distingués par des mesures (voir [148, section 2.2.7]). C'est pourquoi on convient que deux vecteurs égaux *à une phase près* représentent le même état physique. Dans ce mémoire, nous écrirons alors $e^{i\varphi}\,|v\rangle \simeq |v\rangle$.

$$|v\rangle \simeq |w\rangle \iff \exists \varphi \in \mathbb{R}, |v\rangle = e^{i\varphi}\,|w\rangle \tag{1.1}$$

On voit donc que les états possibles du système correspondent aux points de l'espace projectif de $\mathcal{H}$ [13], noté $\mathbb{P}(\mathcal{H})$. Ainsi, dans le chapitre 5, certains états présentant des propriétés similaires seront considérés comme faisant partie de variétés algébriques dans l'espace projectif $\mathbb{P}(\mathcal{H})$.

On rappelle qu'un *produit scalaire hermitien* sur $\mathcal{H}$ est une application de $\mathcal{H}^2$ dans

9. David Hilbert (1862-1943), mathématicien allemand, un des plus grands mathématiciens du 20e siècle.

10. Charles Hermite (1822-1901), mathématicien français.

11. Stefan Banach (1892-1945), mathématicien polonais.

12. Paul Dirac, physicien théoricien anglais (1902-1984), un des fondateurs de la mécanique quantique, prix Nobel 1933.

13. On rappelle que l'espace projectif d'un espace vectoriel est le quotient de cet espace, privé du vecteur nul, par la relation d'équivalence de colinéarité entre les vecteurs. Les droites vectorielles sont donc les points de l'espace projectif.

$\mathbb{C}$, notée $(\cdot,\cdot)$ [14], vérifiant pour tout ket $|v\rangle, |w\rangle$ et tout scalaire $\lambda_i \in \mathbb{C}$ [15] :

$$\textit{linéarité à droite} : (|v\rangle, \sum_i \lambda_i |w_i\rangle) = \sum_i \lambda_i (|v\rangle, |w_i\rangle) \tag{1.2}$$

$$\textit{symétrie hermitienne} : (|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^* \tag{1.3}$$

$$(\cdot,\cdot) \text{ est } \textit{positive} : (|v\rangle, |v\rangle) \geqslant 0 \tag{1.4}$$

$$(\cdot,\cdot) \text{ est } \textit{définie} : (|v\rangle, |v\rangle) = 0 \implies |v\rangle = 0 \tag{1.5}$$

En conséquence de cette définition, on a $(|v\rangle + |v'\rangle, |w\rangle) = (|v\rangle, |w\rangle) + (|v'\rangle, |w\rangle)$ mais $(\lambda |v\rangle, |w\rangle) = \lambda^* (|v\rangle, |w\rangle)$ (semi-linéarité à gauche). Ainsi le produit scalaire hermitien n'est pas une forme bilinéaire comme l'est le produit scalaire euclidien. On le qualifie de forme *sesquilinéaire* [16]. A tout ket $|v\rangle$, on associe une forme linéaire sur $\mathcal{H}$, notée $\langle v|$ et définie par :

$$\forall |w\rangle \in \mathcal{H}, \langle v| (|w\rangle) = (|v\rangle, |w\rangle). \tag{1.6}$$

On dit que $\langle v|$ est le *bra* [17] associé au *ket* $|v\rangle$. On notera que le bra associé au ket $\lambda |v\rangle = |\lambda v\rangle$, noté $\langle \lambda v|$, n'est pas $\lambda \langle v|$ mais $\lambda^* \langle v|$ (semi-linéarité). En général on utilise la notation de Dirac pour le produit scalaire :

$$\langle v|w\rangle = (|v\rangle, |w\rangle) \tag{1.7}$$

Avec cette notation, on a par exemple $\langle v|w\rangle = \langle w|v\rangle^*$, $\langle v|\lambda w\rangle = \lambda \langle v|w\rangle$ et $\langle \lambda v|w\rangle = \lambda^* \langle v|w\rangle$. On définit la notion d'orthogonalité et la norme à partir du produit scalaire :

$$|v\rangle \perp |w\rangle \iff \langle v|w\rangle = 0, \tag{1.8}$$

$$|| |v\rangle || = \sqrt{\langle v|v\rangle}. \tag{1.9}$$

En dimension finie m, une base orthonormale de $\mathcal{H}$ est un ensemble de vecteurs unitaires $(|e_i\rangle)_{i=0\ldots m-1}$ qui sont orthogonaux deux à deux ($i.e$ $\langle e_i|e_j\rangle = \delta_{ij}$) et les coordonnées d'un vecteur $|v\rangle$ dans cette base sont égales aux $\langle e_i|v\rangle$:

$$|v\rangle = \sum_i \langle e_i|v\rangle |e_i\rangle . \tag{1.10}$$

Dans le cas général, la description de l'état d'une particule prend en compte la fonction d'onde $\psi(\mathbf{r}, t)$ de la particule. La dimension de l'espace $\mathcal{H}$ est alors infinie et une base possible de l'espace $\mathcal{H}$ est constituée par un ensemble infini d'états $|\mathbf{r}\rangle$ indexés par toutes les positions possibles $\mathbf{r}$ de l'espace physique E. L'état $|\psi\rangle$ du système à l'instant t est donné par une combinaison linéaire de ces états qui s'exprime sous la forme d'une intégrale (pour plus de détails sur le cas de la dimension infinie voir [59, chapitre II, section E]) :

$$|\psi\rangle = \int_E \langle \mathbf{r}|\psi\rangle |\mathbf{r}\rangle \, \mathrm{d}^3 r. \tag{1.11}$$

Dans le cadre de la théorie de l'information quantique, le qubit sera implanté sous la forme d'un système quantique ayant deux niveaux, comme par exemple le spin d'un électron, la polarisation d'un photon ou l'état d'énergie d'un atome (état de base ou

14. Notation adoptée dans [148].

15. Dans cette thèse, λ^* désigne le conjugué du nombre complexe λ (notation courante chez les physiciens).

16. Le préfixe *sesqui* signifie "dans un rapport de un et demi".

17. Il s'agit bien sûr d'un jeu de mot sur le terme *bracket* (crochet ou parenthèse en anglais).

état excité). Dans ce cas, on peut parfois se dispenser de traiter de façon quantique les variables dites *externes* (comme par exemple la position $\mathbf{r}$) et on modélise la situation dans un espace $\mathcal{H}$ ayant seulement deux dimensions ce qui simplifie grandement l'aspect mathématique (voir [59, chapitre IV]). Ainsi on peut considérer que l'état $|\psi\rangle$ de l'atome d'argent au début de l'expérience de Stern et Gerlach est un état de *superposition* des deux états de base $|\uparrow\rangle$ et $|\downarrow\rangle$ unitaires et orthogonaux :

$$|\psi\rangle = \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\downarrow\rangle . \tag{1.12}$$

Plus généralement, tout état $|\psi\rangle$ d'un système quantique à deux niveaux s'exprimera comme une superposition de deux états *de base* $|e_0\rangle$ et $|e_1\rangle$, c'est à dire comme une combinaison linéaire de deux états formant une base orthonormale $(|e_0\rangle , |e_1\rangle)$ de l'espace $\mathcal{H}$:

$$|\psi\rangle = \alpha |e_0\rangle + \beta |e_1\rangle , \tag{1.13}$$

avec $\alpha, \beta \in \mathbb{C}$ et la condition de normalisation $|\alpha|^2 + |\beta|^2 = 1$. Pour cette raison le premier postulat de la mécanique quantique s'appelle également le *principe de superposition*. Les coefficients α et β sont appelés *amplitudes de probabilité*.

Cette description d'une système physique par un seul vecteur d'état ne permet pourtant pas de décrire toutes les situations pouvant se présenter dans la pratique. Dans certains cas, l'état du système est décrit par un mélange statistique d'états, c'est à dire un ensemble fini d'états $\{|\psi_i\rangle \mid i = 1 \dots q\}$, chacun ayant une probabilité $p_i \neq 0$ d'être l'état du système étudié. Pour décrire l'état du système, on utilise alors un opérateur appelé *opérateur densité*, noté ρ tel que

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| , \tag{1.14}$$

où $|\psi_i\rangle \langle\psi_i|$ est l'opérateur de projection orthogonale sur le vecteur unitaire $|\psi_i\rangle$. Il apparaît que la mécanique quantique peut être entièrement décrite à l'aide de l'opérateur ρ (voir [148, section 2.4]). Le cas où l'état $|\psi\rangle$ du système est connu avec certitude est le cas dit *pur*, dans lequel l'ensemble des états possibles est réduit à un seul élément. Dans ce cas, l'opérateur densité est $|\psi\rangle \langle\psi|$. Dans la suite de ce mémoire, nous considérons uniquement des états purs et nous n'utiliserons pas l'opérateur densité. On supposera aussi que l'espace $\mathcal{H}$ est de dimension finie m.

Espace des états de plusieurs particules

Considérons deux systèmes quantiques (a) et (b) isolés l'un de l'autre. L'état du système (a) évolue au cours du temps dans l'espace de Hilbert $\mathcal{H}_a$ de dimension m et celui du système (b) dans l'espace $\mathcal{H}_b$ de dimension p. Quand ces deux systèmes commencent à interagir, il devient indispensable de considérer un seul système S formé des particules constituant (a) et (b). Ce système va évoluer dans un nouvel espace $\mathcal{H}$ qui est défini comme étant le *produit tensoriel* des deux espaces $\mathcal{H}_a$ et $\mathcal{H}_b$, ce qui se note

$$\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b. \tag{1.15}$$

L'espace $\mathcal{H}$ contient, pour chaque paire de vecteurs $|\psi_a\rangle \in \mathcal{H}_a$ et $|\psi_b\rangle \in \mathcal{H}_b$, un vecteur noté $|\psi_a\rangle \otimes |\psi_b\rangle$ appelé également produit tensoriel de $|\psi_a\rangle$ et $|\psi_b\rangle$. Ce produit est une application bilinéaire de $\mathcal{H}_a \times \mathcal{H}_b$ dans $\mathcal{H}_a \otimes \mathcal{H}_b$. De plus, si $(|e_i\rangle)_{i=0,\dots,m-1}$ est une base de $\mathcal{H}_a$ et $(|f_j\rangle)_{j=0,\dots,p-1})$ est une base de $\mathcal{H}_b$, alors une base de $\mathcal{H}$ est constituée par

l'ensemble des vecteurs $|e_i\rangle \otimes |f_j\rangle$. La dimension de $\mathcal{H}$ est donc $m \times p$. En mécanique quantique, on omet souvent le symbole $\otimes$ dans les produits tensoriels de vecteurs afin d'alléger l'écriture. On écrit ainsi $|\psi_a\rangle |\psi_b\rangle$ au lieu de $|\psi_a\rangle \otimes |\psi_b\rangle$.

Le produit scalaire hermitien sur $\mathcal{H}$ est défini naturellement à partir des produits scalaires sur $\mathcal{H}_a$ et $\mathcal{H}_b$:

$$(|\psi_a\rangle |\psi_b\rangle , |\psi'_a\rangle |\psi'_b\rangle) = \langle\psi_a|\psi'_a\rangle \langle\psi_b|\psi'_b\rangle . \tag{1.16}$$

On remarque que la base constituée des produits $|e_i\rangle |f_j\rangle$ est orthonormale si et seulement si les bases $(|e_i\rangle)$ de $\mathcal{H}_a$ et $(|f_j\rangle)$ de $\mathcal{H}_b$ sont des bases orthonormales.

Certains états de $\mathcal{H}$ peuvent s'écrire comme produit d'un état de $\mathcal{H}_a$ et d'un état de $\mathcal{H}_b$. Par exemple, l'état $|\psi_{ijk\ell}\rangle = \frac{1}{2}(|e_i\rangle |f_k\rangle + |e_i\rangle |f_\ell\rangle + |e_j\rangle |f_k\rangle + |e_j\rangle |f_\ell\rangle)$ est le produit des états $\frac{1}{\sqrt{2}}(|e_i\rangle + |e_j\rangle)$ et $\frac{1}{\sqrt{2}}(|f_k\rangle + |f_l\rangle)$. Dans ce cas, le système formé par l'ensemble des particules constituant (a) et (b) est la juxtaposition d'un état des particules de (a) et d'un état des particules de (b) : on dit que l'état $|\psi_{ijk\ell}\rangle$ est *factorisé* ou *séparable*. Mais $\mathcal{H}$ contient également des états qu'on ne peut factoriser, par exemple l'état $|\varphi_{ijk\ell}\rangle = \frac{1}{\sqrt{2}}(|e_i\rangle |f_k\rangle + |e_j\rangle |f_\ell\rangle)$. Dans ce cas, l'état du système global ne peut plus être considéré comme la simple juxtaposition d'un état de (a) et d'un état de (b) et on dit que l'état $|\varphi_{ijk\ell}\rangle$ est *intriqué*. Les états intriqués jouent un rôle fondamental dans la théorie de l'information quantique (voir plus loin section 1.2.2).

À partir de deux opérateurs linéaires A et B agissant respectivement sur les espaces H_a et H_b, on obtient un nouvel opérateur linéaire $A \otimes B$, agissant sur l'espace $H_a \otimes H_b$ et défini par :

$$(A \otimes B)(|e_i\rangle \otimes |f_j\rangle) = (A |e_i\rangle) \otimes (A |f_j\rangle). \tag{1.17}$$

La matrice de $A \otimes B$ dans la base $(|e_i\rangle \otimes |f_j\rangle)$ est le *produit de Kronecker*, noté également $\otimes$, des matrices représentant A et B dans les bases respectives (e_i) et (f_j). De façon générale, pour toute matrice A de dimensions $m \times n$ et B de dimensions $p \times q$, ce produit est défini par :

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix}. \tag{1.18}$$

On peut généraliser le produit tensoriel à n systèmes quantiques $(a_0), \dots, (a_{n-1})$ évoluant respectivement dans des espaces de Hilbert $\mathcal{H}_0, \dots \mathcal{H}_{n-1}$ de dimensions respectives $m_0, \dots, m_{n-1}$. L'état du système global $\{(a_0), \dots, (a_{n-1})\}$ est alors représenté par un vecteur unitaire $|\psi\rangle$ de l'espace $\mathcal{H}_0 \otimes \dots \otimes \mathcal{H}_{n-1}$ tel que

$$|\psi\rangle = \sum_{i_0,\dots,i_{n-1}} \alpha_{i_0 \dots i_{n-1}} |e_{i_0}^{(0)}\rangle \dots |e_{i_{n-1}}^{(n-1)}\rangle \tag{1.19}$$

où $\left(|e_{i_k}^{(k)}\rangle\right)_{i_k=0,\dots,m_{k-1}}$ constitue une base orthonormale de $\mathcal{H}_k$ pour $k = 0, \dots, n-1$.

1.1.3 Mesures et observables

Étant donné un opérateur A de $\mathcal{H}$, on définit son opérateur adjoint $A^\dagger$ comme étant l'unique opérateur de $\mathcal{H}$ vérifiant pour tout $|v\rangle , |w\rangle$ de $\mathcal{H}$:

$$(|v\rangle , A |w\rangle) = (A^\dagger |v\rangle , |w\rangle). \tag{1.20}$$

On démontre que la matrice de l'opérateur $A^\dagger$ dans une base orthonormale est la *transconjuguée* (la transposée de la conjuguée) de la matrice de A.

En mécanique quantique, toute quantité physique mesurable est décrite par un opérateur *hermitien*, c'est à dire un opérateur autoadjoint (*i.e* $A = A^\dagger$) appelé *une observable*. C'est le *second postulat* de la mécanique quantique. D'après le théorème de décomposition spectrale (voir par exemple [148, p. 72]), les opérateurs hermitiens admettent une base orthonormale de vecteur propres et sont donc diagonalisables. La relation $A = A^\dagger$ implique que les valeurs propres de A sont des nombres réels et le *troisième postulat* de la mécanique quantique énonce que ces valeurs propres sont les différentes mesures possibles de la grandeur physique modélisée par A. Soit $\{\lambda_1, \ldots, \lambda_q\}$ le *spectre* de A (ensemble des valeurs propres) et, pour $i = 1, \ldots, q$, soit E_i le sous-espace propre associé à la valeur λ_i. On démontre que deux vecteurs propres associés à deux valeurs propres distinctes sont orthogonaux (voir par exemple [59, chapitre II, section D-2]). Ainsi les sous-espaces E_i sont orthogonaux deux à deux et l'espace $\mathcal{H}$ est la somme directe orthogonale des E_i. On a donc :

$$I = \sum_{i=1}^{q} P_i, \tag{1.21}$$

où P_i est la projection orthogonale sur l'espace E_i. Le *quatrième postulat* énonce que la probabilité d'obtenir la valeur λ_i lors de la mesure de l'observable A du système dans l'état $|\psi\rangle$ est égale au carré de la norme de $P_i |\psi\rangle$ qui vaut $\langle\psi|P_i|\psi\rangle$. Immédiatement après la mesure, l'état du système quantique est la projection normalisée de $|\psi\rangle$ sur le sous-espace propre E_i, c'est à dire $\frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$: c'est le *cinquième postulat* de la mécanique quantique.

Illustrons la théorie en modélisant l'expérience de Stern et Gerlach (voir section 1.1.1). L'état (de spin) de l'atome d'argent au moment où il interagit avec le champ magnétique orienté selon l'axe $\hat{z}$ est : $|\psi\rangle = \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\downarrow\rangle$. Les vecteurs $|\uparrow\rangle$ et $|\downarrow\rangle$ forment une base orthonormale de l'espace de Hilbert associé à l'état de l'atome, considéré ici par son seul spin. Ils modélisent respectivement un état de spin-up et un état de spin-down selon l'axe $\hat{z}$. L'observable de spin est l'opérateur hermitien dont la matrice dans la base $(|\uparrow\rangle, |\downarrow\rangle)$ est $\frac{\hbar}{2}\sigma_z$ où σ_z est la matrice de Pauli-Z, notée aussi Z :

$$\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.22}$$

Les valeurs propres de $\frac{\hbar}{2}\sigma_z$ sont $\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$, les deux mesures possibles du spin. Chacune de ces valeurs à la probabilité $\left(\frac{1}{\sqrt{2}}\right)^2 = 0,5$ d'être mesurée et après la mesure (qui équivaut au passage dans le champ magnétique), l'état $|\psi\rangle$ est projeté sur l'état $|\uparrow\rangle$ ou sur l'état $|\downarrow\rangle$.

Concernant la mesure des grandeurs physiques, signalons pour finir une différence fondamentale entres les théories classiques et quantiques. En mécanique classique, on peut connaître en théorie toutes les grandeurs physiques d'un système donné. Le degré de précision des mesures provient essentiellement de la qualité des appareils utilisés. En mécanique quantique ce n'est pas toujours vrai car il existe des cas où cette imprécision est intrinsèque : si deux observables ne commutent pas alors il est impossible (même en imaginant des instruments de mesure parfaitement précis) de connaître *simultanément* avec précision les valeurs des grandeurs modélisées par ces

observables. C'est le *principe d'indétermination* formulé par Heisenberg en 1927 [18]. Dans le cas des observables associées à la position x et la quantité de mouvement p, ce principe se traduit mathématiquement par une inégalité sur le produit des écart-types des mesures de ces grandeurs appelée l'*inégalité d'Heisenberg* :

$$\sigma_x \sigma_p \geqslant \frac{\hbar}{2}. \tag{1.23}$$

Plus généralement, on a une inégalité similaire dans le cas de deux observables quelconques A et B qui ne commutent pas.

1.1.4 Évolution d'un système quantique

Soit $|\psi(t_0)\rangle$ l'état d'un système quantique à l'instant t_0. Ce système va évoluer au cours du temps et, à l'instant $t > t_0$, son état sera décrit par un vecteur $|\psi(t)\rangle$ du même espace de Hilbert. Le *sixième postulat* de la mécanique quantique énonce que l'évolution d'un système isolé est gouvernée par l'équation de Schrödinger :

$$\mathrm{i}\hbar \frac{\partial |\psi\rangle}{\partial t} = \hat{H}(t) |\psi\rangle , \tag{1.24}$$

où $\hat{H}(t)$ est un opérateur hermitien appelé *Hamiltonien* du système. Cet opérateur est une observable dont les valeurs propres sont les différentes valeurs que peut prendre l'énergie totale du système. En général $\hat{H}$ dépend du temps (par exemple si un champ électromagnétique est appliqué au système).

On peut démontrer (voir [59, Complément $\mathrm{F_{III}}$]) qu'il existe un opérateur linéaire U_{t,t_0} tel que

$$|\psi(t)\rangle = U_{t,t_0} |\psi(t_0)\rangle \tag{1.25}$$

et que cet opérateur est unitaire, c'est à dire qu'il vérifie la condition

$$U^\dagger = U^{-1}. \tag{1.26}$$

En dimension finie m, la matrice d'un opérateur unitaire dans une base orthonormale est une *matrice unitaire*, c'est à dire une matrice dont l'inverse est égale à la transconjuguée. Ces matrices forment un groupe appelé le *groupe unitaire* en dimension m, noté U_m.

Un opérateur unitaire conserve le produit scalaire et donc la norme. En effet, d'après (1.20), on a pour tout ket $|u\rangle$, $|v\rangle$ de $\mathcal{H}$: $(U|v\rangle , U|w\rangle) = (U^\dagger U|v\rangle , |w\rangle) = (|v\rangle , |w\rangle)$. Ainsi un vecteur unitaire représentant un état évolue au cours du temps vers un (autre) vecteur unitaire.

Déterminer l'Hamiltonien d'un système quantique peut être un problème complexe pour les physiciens (voir [148, p.83]). De plus, même quand on connaît celui-ci, la résolution de l'équation (1.24) n'est pas toujours possible de façon exacte. Cependant, dans le cas où l'Hamiltonien ne dépend pas du temps, on sait résoudre l'équation de Schrödinger et on obtient :

$$|\psi(t)\rangle = \exp\left(-\frac{\mathrm{i}}{\hbar}(t-t_0)\hat{H}\right) |\psi(t_0)\rangle . \tag{1.27}$$

Posons $M_{t,t_0} = -\frac{\mathrm{i}}{\hbar}(t-t_0)\hat{H}$. Puisque la matrice $\hat{H}$ est hermitienne, la matrice $\mathrm{i}\hat{H}$ est *antihermitienne* (égale à l'opposée de sa transconjuguée) et il en est de même de la

18. Werner Heisenberg (1901-1916), physicien allemand, un des fondateurs de la mécanique quantique, prix Nobel de physique 1932.

matrice M. On a donc $\exp(M)^\dagger = \exp(M^\dagger) = \exp(-M) = \exp(M)^{-1}$, ce qui prouve que l'opérateur $\exp(M)$ est bien unitaire. Ainsi la solution (1.27) de l'équation de Schrödinger s'écrit bien sous la forme (1.25).

On remarque que la solution (1.25) est complètement déterminée par la donnée de l'opérateur $\hat{H}$ et de l'état initial. On comprend donc qu'on peut piloter l'état du système en modifiant l'Hamiltonien de façon appropriée : c'est de cette manière que sont appliquées les différentes transformations unitaires implantées sous la forme de portes quantiques dans les ordinateurs quantiques (voir section 1.3).

1.2 Théorie de l'information quantique

1.2.1 Stockage, évolution et lecture de l'information

Le qubit

Dans la théorie de l'information quantique, un *qubit* (de l'anglais *quantum bit*) est un système quantique qui représente l'unité de base de stockage de l'information. Le qubit est donc à la théorie de l'information quantique ce que le bit est à la théorie de l'information classique. Plus précisément, un qubit est un système quantique pour lequel on considère une propriété (une grandeur physique mesurable) pouvant prendre deux valeurs. Cette propriété peut être par exemple le spin d'un électron (spin up ou spin down), la polarisation d'un photon (verticale ou horizontale) ou encore l'énergie d'un atome (état fondamental ou état excité). On a vu dans la section 1.1.2 qu'un tel système pouvait être modélisé par un vecteur unitaire d'un espace de Hilbert $\mathcal{H}$ à deux dimensions. Cet espace est muni d'une base orthonormale $(|0\rangle, |1\rangle)$, chacun des deux vecteurs de cette base correspondant à un des deux états que peut prendre le système immédiatement après la mesure de l'observable modélisant la propriété considérée [19]. D'après le principe de superposition, l'état du système à un instant donné est modélisé par un ket $|\psi\rangle$ de $\mathcal{H}$ tel que

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad (\alpha, \beta) \in \mathbb{C}^2 \text{ et } |\alpha|^2 + |\beta|^2 = 1. \tag{1.28}$$

On dira que $|\psi\rangle$ est l'état du qubit à cet instant. Ainsi, à la différence du bit d'information de la théorie classique qui ne prend qu'une des valeurs 0 ou 1 à un instant donné, le qubit de la théorie de l'information quantique est dans un état de superposition de deux états particuliers $|0\rangle$ et $|1\rangle$ et ce n'est qu'au moment de la mesure qu'un des deux états est déterminé : on obtient soit l'état $|0\rangle$ (avec la probabilité $|\alpha|^2$), soit l'état $|1\rangle$ (avec la probabilité $|\beta|^2$).

On définit les trois matrices de Pauli X, Y, Z, notées également σ_x [20], σ_y, σ_z ou encore $\sigma_1, \sigma_2, \sigma_3$ par :

$$X = \sigma_x = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \sigma_y = \sigma_2 = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad Z = \sigma_z = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.29}$$

Ces matrices peuvent être vues comme les matrices dans la base $(|0\rangle, |1\rangle)$ de trois opérateurs hermitiens et unitaires, notés également X, Y, Z. Ces trois observables ont

19. Un système quantique à deux niveaux peut être décrit par un spin 1/2 fictif associé à ce système et les états propres du système sont alors identifiés aux deux états propres $|0\rangle$ et $|1\rangle$ de l'observable de spin σ_z (1.22) (voir [59, compléments $\mathrm{C_{IV}}$]).

20. Notez bien que la matrice de Pauli σ_x n'a rien à voir avec l'écart-type σ_x utilisé dans l'inégalité d'Heisenberg 1.23

été introduites par Pauli afin de décrire de façon théorique l'interaction d'une particule de spin $\frac{1}{2}$ avec un champ magnétique comme dans l'expérience de Stern et Gerlach. Ce sont, au facteur $\hbar/2$ près, les observables du spin selon les trois axes de l'espace, chacun des axes donnant l'orientation du champ magnétique selon lequel on mesure. Les matrices de Pauli jouent un rôle fondamental dans la théorie de l'information quantique et dans les circuits quantiques, que ce soit comme opérateur unitaire agissant sur un qubit ou comme observable. Le spectre de chacun des opérateurs de Pauli est $\{1, -1\}$ donc

$$X^2 = Y^2 = Z^2 = I. \tag{1.30}$$

On démontre également que les matrices de Pauli anticommutent, c'est à dire que

$$XY = -YX, \qquad XZ = -ZX, \quad YZ = -ZY \tag{1.31}$$

et vérifient de plus les relations suivantes :

$$XY = \mathrm{i}Z, \qquad ZX = \mathrm{i}Y, \qquad YZ = \mathrm{i}X. \tag{1.32}$$

La base $(|0\rangle, |1\rangle)$ de l'espace dans lequel évolue un qubit est donc une base de vecteurs propres de Z, $|0\rangle$ étant associé à la valeur propre 1 et $|1\rangle$ à la valeur propre -1. Cette base est qualifiée de *base standard* de calcul de l'espace $\mathcal{H}$. Mais on peut choisir une autre base pour représenter ce qubit, par exemple la base des vecteurs propres de X, notée $(|+\rangle, |-\rangle)$, où $|+\rangle$ est associé à la valeur propre 1 et $|-\rangle$ à la valeur propre -1. On a donc :

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{et} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{1.33}$$

La matrice de passage de la base $(|0\rangle, |1\rangle)$ vers la base $(|+\rangle, |-\rangle)$ est la matrice de Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{1.34}$$

qui vérifie les relations

$$H^2 = I, \qquad HZH = X, \qquad HXH = Z, \qquad HYH = -Y. \tag{1.35}$$

Enfin, signalons qu'il est possible de représenter l'information quantique en utilisant des systèmes quantiques ayant plus de deux niveaux. Ainsi dans le cas d'une propriété d'un système quantique ayant trois valeurs, l'unité de base de l'information sera le *qutrit* [41, 80, 38]. L'état d'un qutrit s'écrit sous la forme $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$, avec $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$ et $|0\rangle$, $|1\rangle$, $|2\rangle$ trois états propres associés aux trois valeurs propres de l'observable modélisant cette propriété. Il peut s'agir par exemple de 3 niveaux d'énergie d'un système ou des 3 états de spin (-1, 0 ou 1) d'un boson de spin 1.

Dans le cas d'un système ayant plus de trois niveaux, on utilise le terme *qudit* pour désigner l'unité de base de stockage de l'information.

Représentation d'un qubit sur la sphère de Bloch

La sphère de Bloch [21] est un moyen commode de visualiser les états possibles d'une particule de spin 1/2 et plus généralement d'un système quantique à deux niveaux. En information quantique, on l'utilise donc pour représenter le qubit. On considère pour cela la sphère $\mathbb{S}^2$ qui est la sphère de rayon 1 dans l'espace euclidien à trois dimensions

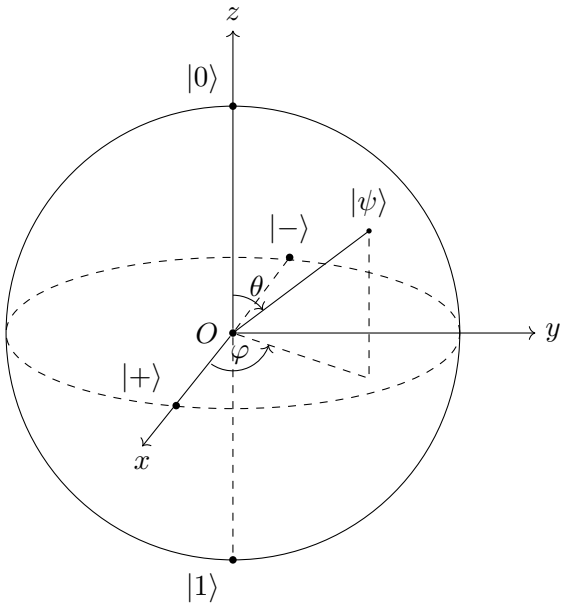
21. Félix Bloch (1905-1983), physicien suisse, prix Nobel de physique 1952.

et on établit une correspondance bijective entre les points de cette sphère et l'espace projectif $\mathbb{P}^1(\mathbb{C})$ associé à l'ensemble des états possibles d'un qubit. On procède de la façon suivante. Soit un qubit dans l'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ avec $\alpha, \beta \neq 0$. On pose $\alpha = r_1 e^{i\varphi_1}$ et $\beta = r_2 e^{i\varphi_2}$. On a donc $|\psi\rangle = e^{i\varphi_1}(r_1\,|0\rangle + r_2 e^{i(\varphi_2-\varphi_1)}\,|1\rangle)$ avec $r_1^2 + r_2^2 = 1$. En posant $\varphi = \varphi_2 - \varphi_1$, $r_1 = \cos\frac{\theta}{2}$, $r_2 = \sin\frac{\theta}{2}$ (avec $\theta \in [0\,;\pi]$), on obtient alors (les facteurs de phase ne changeant pas l'état physique du système) :

$$|\psi\rangle \simeq \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\,. \tag{1.36}$$

Dans un repère orthonormé (O, x, y, z) dont l'origine est le centre de la sphère, on représente l'état $|0\rangle$ par le point de coordonnées $(0, 0, 1)$, l'état $|1\rangle$ par le point $(0, 0, -1)$. Un état différent de $|0\rangle$ et de $|1\rangle$ est représenté par le point de colatitude θ et de longitude φ (voir figure 1.1). On remarque que deux états sont orthogonaux si et seulement si les points correspondant sur la sphère sont diamétralement opposés. Ainsi en est-il des états $(|0\rangle, |1\rangle)$ et des états $(|+\rangle, |-\rangle)$ sur la figure 1.1.

Figure 1.1 La sphère de Bloch et les états propres associés aux observables Z et X.



Soit $M_{|\psi\rangle}$ le point de la sphère de Bloch associé à un état $|\psi\rangle$ et soient (m_x, m_y, m_z) ses coordonnées cartésiennes. Soit $\vec{\sigma}$ un vecteur dont les trois composantes sont les opérateurs de Pauli, on montre que $|\psi\rangle$ est un vecteur propre associé à la valeur propre $+1$ de l'observable

$$\overrightarrow{OM} \cdot \vec{\sigma} = m_x X + m_y Y + m_z Z \tag{1.37}$$

et que le point diamétralement opposé à M représente un vecteur propre associé à la valeur propre -1 de cette observable.

Le grand avantage de la sphère de Bloch est qu'elle permet de visualiser non seulement les états d'un qubit, mais aussi les opérateurs unitaires qui décrivent l'évolution temporelle d'un état à un autre, en faisant correspondre à chacun de ces opérateurs une rotation de l'espace euclidien $\mathbb{R}^3$ agissant sur les points de la sphère. Nous donnons dans ce qui suit quelques explications sur cette correspondance et quelques exemples, sans pour autant fournir de démonstration complète. Le lecteur souhaitant en savoir

plus pourra consulter le cours de Frédéric Paulin [155] à propos de l'isomorphisme entre PSU_2 et $\mathrm{SO}_3(\mathbb{R})$ et des groupes de Lie matriciels. En ce qui concerne les opérateurs de rotation des états d'un système, on pourra se référer à [59, compléments $\mathrm{B_{VI}}$].

Les opérateurs unitaires décrivant l'évolution d'un qubit dans son espace $\mathcal{H}$ constituent un groupe [22]. Une base orthonormale étant fixée, ce groupe est isomorphe [23] au groupe des matrices unitaires 2×2, noté U_2, qui est l'ensemble des matrices complexes dont l'inverse est égale à la transconjuguée. Pour toute matrice $U \in \mathrm{U}_2$, la relation $U^{-1} = U^\dagger$ implique que $|\det(M)| = 1$ donc U s'écrit sous la forme $\mathrm{e}^{\mathrm{i}\varphi}U'$ avec U' appartenant à SU_2, le groupe spécial unitaire, qui est le sous-groupe [24] de U_2 constitué des matrices de déterminant égal à 1. Or, il existe un lien entre le groupe SU_2 et le groupe $\mathrm{SO}_3(\mathbb{R})$, le groupe spécial orthogonal en dimension 3 (groupe des matrices réelles dont l'inverse est égale à la transposée) : ces deux groupes sont des groupes de Lie dont les algèbres de Lie respectives, $\mathfrak{su}_2$ et $\mathfrak{so}_3$, sont isomorphes. On peut montrer que les matrices $\mathrm{i}X$, $\mathrm{i}Y$ et $\mathrm{i}Z$ forment une base de $\mathfrak{su}_2$. Ainsi, toute matrice de $\mathfrak{su}_2$ peut s'écrire sous la forme $-\mathrm{i}\theta\vec{u}\cdot\vec{\sigma}/2$, avec $\vec{u}$ un vecteur unitaire de $\mathbb{R}^3$. De plus, toute matrice de SU_2 peut s'écrire sous la forme d'une exponentielle de matrice de $\mathfrak{su}_2$ (il s'agit d'un lien général entre les groupes de Lie matriciels et leurs algèbres de Lie). On voit donc que toute matrice de SU_2 (et donc toute matrice de U_2 à une phase près) peut s'écrire sous la forme

$$R_{\vec{u}}(\theta) = \mathrm{e}^{-\mathrm{i}\theta\vec{u}\cdot\vec{\sigma}/2}. \tag{1.38}$$

En utilisant le fait que $(\vec{u}\cdot\sigma)^2 = I$, on obtient :

$$R_{\vec{u}}(\theta) = \cos\frac{\theta}{2}I - \mathrm{i}\sin\frac{\theta}{2}(u_xX + u_yY + u_zZ), \tag{1.39}$$

avec u_x, u_y, u_z les composantes de $\vec{u}$. Par exemple, pour la matrice de Hadamard, on a $H = \mathrm{i}R_{\vec{u}_H}(\pi)$ avec $\vec{u}_H = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\end{bmatrix}$.

Comme la notation le laisse supposer, on fait correspondre à la matrice $R_{\vec{u}}(\theta)$ de SU_2, la matrice $\mathcal{R}_{\vec{u}}(\theta)$ de SO_3 qui représente la rotation d'angle θ d'axe dirigé par $\vec{u}$. Il s'agit d'un morphisme qui n'est pas bijectif car d'après (1.39) on a : $R_{\vec{u}}(\theta) = -R_{\vec{u}}(\theta + 2\pi)$. Il n'y a donc pas d'isomorphisme entre les groupes SU_2 et $\mathrm{SO}_3(\mathbb{R})$ comme pourrait le laisser croire l'isomorphisme entre $\mathfrak{su}_2$ et $\mathfrak{so}_3$. En fait, c'est le groupe quotient [25] $\mathrm{SU}_2/\{I, -I\}$, appelé groupe projectif spécial unitaire (noté PSU_2) qui est isomorphe au groupe $\mathrm{SO}_3(\mathbb{R})$.

En information quantique, on utilise fréquemment les trois matrices de rotations autour des axes $\hat{x}, \hat{y}$ et $\hat{z}$ (voir table 1.1) Par exemple, on a : $X = \mathrm{i}R_x(\pi)$, $Y = \mathrm{i}R_y(\pi)$, $Z = \mathrm{i}R_z(\pi)$. On peut démontrer (voir [148, théorème 4.1]) que toute matrice unitaire U peut s'écrire sous la *forme Z-Y*, c'est à dire qu'il existe quatre réels $\alpha, \beta, \gamma, \delta$ tels que

$$U = \mathrm{e}^{\mathrm{i}\alpha}R_z(\beta)R_y(\gamma)R_z(\delta), \qquad \text{(décomposition Z-Y de } U\text{)} \tag{1.40}$$

Nous utiliserons ce résultat dans le dernier chapitre de ce mémoire (chapitre 5, section 5.3).

22. Voir annexe A, section A.1.1
23. Voir annexe A, section A.1.3
24. Voir annexe A, section A.1.2
25. Voir annexe A, section A.2

Table 1.1 Rotations autour des trois axes $\hat{x}, \hat{y}$ et $\hat{z}$

Nom	Symbole	Matrice
Rotation autour de l'axe $\hat{x}$	$R_x(\theta)$	$\mathrm{e}^{-\mathrm{i}\theta X/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -\mathrm{i}\sin\frac{\theta}{2} \\ -\mathrm{i}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$
Rotation autour de l'axe $\hat{y}$	$R_y(\theta)$	$\mathrm{e}^{-\mathrm{i}\theta Y/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$
Rotation autour de l'axe $\hat{z}$	$R_z(\theta)$	$\mathrm{e}^{-\mathrm{i}\theta Z/2} = \begin{bmatrix} \mathrm{e}^{-\mathrm{i}\theta/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta/2} \end{bmatrix}$

On peut établir le résultat suivant par le calcul, par exemple en utilisant la décomposition Z-Y : soit $M_{|\psi\rangle}$ le point de la sphère de Bloch associé à un état $|\psi\rangle$ et soit $|\psi'\rangle = R_{\vec{u}}(\theta)\,|\psi\rangle$ alors $\overrightarrow{OM}_{|\psi'\rangle} = \mathcal{R}_{\vec{u}}(\theta)\overrightarrow{OM}_{|\psi\rangle}$. Prenons à tire d'exemple le cas des points $M_{|0\rangle}$ et $M_{|+\rangle}$ (figure 1.1). On a : $|+\rangle = H\,|0\rangle = \mathrm{i}R_{\vec{u}_H}(\pi)\,|0\rangle$ et le point $M_{|+\rangle}$ est l'image du point $M_{|0\rangle}$ par une rotation d'angle π autour de l'axe orienté par $\vec{u}_H$ (bissectrice de l'angle $\widehat{xOz}$).

Du point de vue de la mécanique quantique, l'état du qubit qui a subi une rotation $R_{\vec{u}}(\theta)$ dans l'espace des états $\mathcal{H}$ est celui d'un qubit qui aurait subi la rotation correspondante $\mathcal{R}_{\vec{u}}(\theta)$ dans l'espace du laboratoire. Quand on fait subir cette même rotation à l'appareil de mesure (assimilé à l'axe du champ magnétique dans le cas d'un spin 1/2) alors on démontre que la nouvelle observable résultant de cette rotation est $RAR^\dagger$, avec A l'observable mesurée par l'appareil avant la rotation. L'espace étant supposé isotrope (sans direction privilégiée), si le qubit avant rotation était dans un état propre de A, alors l'état du qubit après cette rotation est un état propre de la nouvelle observable $RAR^\dagger$ avec la même valeur propre (la même mesure) qu'avant rotation. Ainsi en est-il sur la sphère de Bloch : par exemple $X = HZH = HZH^\dagger$ et les vecteur propres $|0\rangle$ et $|1\rangle$ de Z deviennent, après la rotation $R_{\vec{u}_H}(\pi)$, les vecteurs propres $|+\rangle$ et $|-\rangle$ de la nouvelle observable X définie par l'axe $\hat{x}$ qui est l'image de l'axe $\hat{z}$ par la rotation de l'espace euclidien associée à H.

Registre de qubits

Un registre quantique de n qubits est un système quantique composé de n qubits numérotés de 0 à $n-1$. Son état évolue au cours du temps dans l'espace $\mathcal{H}^{\otimes n}$ égal au produit tensoriel de n copies d'un espace de Hilbert $\mathcal{H}$ de dimension 2 isomorphe à $\mathbb{C}^2$. La dimension de $\mathcal{H}^{\otimes n}$ est donc $m = 2^n$. La *base standard* de $\mathcal{H}^{\otimes n}$ est la base orthonormale $(|e_0\rangle, \ldots, |e_{2^n-1}\rangle)$ telle que, pour tout entier $k = 0, \ldots, 2^n - 1$, on a $|e_k\rangle = |b_0\rangle\,|b_1\rangle \ldots |b_{n-1}\rangle$, avec $b_0 b_1 \ldots b_{n-1}$ l'écriture binaire de k, et $|b_k\rangle$ un vecteur propre associé à la valeur propre $(-1)^{b_k}$ de l'observable Z dans l'espace du qubit k. En général, on simplifie l'écriture du produit tensoriel $|b_0\rangle\,|b_1\rangle \ldots |b_{n-1}\rangle$ en $|b_0 b_1 \ldots b_{n-1}\rangle$. Dans le cas d'un registre de n qubits, l'équation (1.19) qui donne l'état du système à l'instant t s'écrit donc

$$|\psi\rangle = \sum_{b_0,\ldots,b_{n-1}\in\{0,1\}} \alpha_{b_0\ldots b_{n-1}}\,|b_0 \ldots b_{n-1}\rangle\,, \tag{1.41}$$

avec la condition de normalisation $\sum_{b_0,\ldots,b_{n-1}\in\{0,1\}} |\alpha_{b_0\ldots b_{n-1}}|^2 = 1$. On peut d'ailleurs indexer de façon naturelle les 2^n vecteurs de la base standard par les vecteurs de l'espace

$\mathbb{F}_2^n$ et désigner la base standard par $(|b\rangle)_{b\in\mathbb{F}_2^n}$. Cette notation est utilisée dès 1997 par Calderbank dans différents travaux [46, section 2] [43, section 2]. On écrit donc (1.41) sous la forme

$$|\psi\rangle = \sum_{b\in\mathbb{F}_2^n} \alpha_b |b\rangle . \tag{1.42}$$

Certains états sont *complètement factorisés*. Ainsi, pour $n = 3$, on a par exemple :

$$\frac{1}{\sqrt{8}} \sum_{i,j,k\in\{0,1\}} |ijk\rangle = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes 3} .$$

D'autres états sont *partiellement factorisés* comme par exemple

$$\frac{1}{2}(|000\rangle + |011\rangle + |100\rangle + |111\rangle) = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right).$$

Enfin, certains états ne sont pas factorisables comme l'état

$$|GHZ_3\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{1.43}$$

ou l'état

$$|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.44}$$

que nous avons mentionné dans l'introduction de cette thèse.

Soient $\mathcal{H}_a$ et $\mathcal{H}_b$ deux espaces de Hilbert, dans lesquels évoluent respectivement les états de deux registres (a) et (b). On considère l'espace $\mathcal{H}_a \otimes \mathcal{H}_b$ dans lesquels évolue le registre de qubits (c) formé de la concaténation des registres (a) et (b). Soient deux opérateurs unitaires A et B agissant respectivement sur $\mathcal{H}_a$ et $\mathcal{H}_b$. Quand on fait agir l'opérateur factorisé $A \otimes B$ sur un état quelconque (factorisé ou non) $|\psi_c\rangle$ de $\mathcal{H}_a \otimes \mathcal{H}_b$, on dit qu'on a agi *localement* sur les registres (a) et (b). Dans le cas particulier ou $|\psi_c\rangle$ est factorisé, on pose $|\psi_c\rangle = |\psi_a\rangle |\psi_b\rangle$ et l'état résultant de l'action de $A \otimes B$ sur $|\psi_c\rangle$ est $(A|\psi_a\rangle) \otimes (B|\psi_b\rangle)$ qui est encore un état factorisé. Physiquement, cela signifie que lorsqu'on agit localement sur un système constitué de deux sous-systèmes séparés n'ayant jamais interagi ensemble, alors le système global peut toujours être considéré comme la réunion de deux sous-systèmes séparés, ce qui est conforme à l'intuition. Cette idée sera développée dans la section 1.2.2 pour classifier les états intriqués.

Mesure d'un registre de qubits

En informatique quantique on a coutume de dire qu'on mesure un registre de qubits ou un système de qubits *dans une base donnée* et que le résultat de cette mesure est un registre de bits classiques. Donnons quelques exemples concrets.

(i) On mesure un qubit dans l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ dans la base $(|0\rangle, |1\rangle)$. On obtiendra 0 avec la probabilité $|\alpha|^2$ ou 1 avec la probabilité $|\beta|^2$.

(ii) On mesure dans la base $(|+\rangle, |-\rangle)$ un qubit dans l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Pour calculer les probabilités du 0 et du 1, on doit commencer par effectuer un changement de base à l'aide de la matrice de passage H. On a $|\psi\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|+\rangle + (\alpha-\beta)|-\rangle)$. On associe le bit 0 à l'état $|+\rangle$ et le bit 1 à l'état $|-\rangle$. On obtiendra donc 0 avec la probabilité $\frac{1}{2}|\alpha+\beta|^2$ et 1 avec la probabilité $\frac{1}{2}|\alpha-\beta|^2$.

(iii) On mesure dans la base $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ un système de 2 qubits dans l'état $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. On obtient le résultat 00 avec la probabilité $\frac{1}{2}$, 11 avec la probabilité $\frac{1}{2}$ et on a une probabilité nulle d'obtenir 01 ou 10.

(iv) On mesure l'état $|EPR\rangle$ dans la base $(|0\rangle|+\rangle, |0\rangle|-\rangle, |1\rangle|+\rangle, |1\rangle|-\rangle$. Un changement de base permet d'écrire $|EPR\rangle = \frac{1}{2}((|0\rangle|+\rangle + |0\rangle|-\rangle + |1\rangle|+\rangle + |1\rangle|-\rangle)$. Ainsi chacun des résultats $00, 01, 10$ et 11 peut être obtenu avec la probabilité $\frac{1}{4}$.

On notera dans ces exemples qu'on ne parle plus d'observables alors que toute la théorie de la mesure en mécanique quantique est basée sur cette notion (cinquième postulat), ce qui peut surprendre au premier abord. Bien entendu les observables sont toujours là mais ils sont implicites : une base orthonormale $(|e_0\rangle, \ldots, |e_{2^n-1}\rangle)$ de l'espace $\mathcal{H}^{\otimes n}$ étant fixée, l'*observable qu'on mesure* (mécanique quantique) quand on *mesure dans cette base* (informatique quantique) est en fait $M = \sum_{k=0}^{2^n-1} k\,|e_k\rangle\langle e_k|$: quand on mesure la valeur propre k, le qubit est projeté sur l'état propre $|e_k\rangle$ associé à cette valeur et le résultat est la série de bits correspondant à l'entier k en écriture binaire.

Plus généralement, au lieu de définir directement une observable, on peut donner une liste de projecteurs orthogonaux (P_k) tels que $I = \sum_k P_k$ et $P_k P_{k'} = \delta_{kk'} P_k$ (voir [148, section 2.2.5]). L'observable sous-jacente est $M = \sum_k kP_k$, avec P_k le projecteur orthogonal sur le sous-espace propre associé à la valeur propre k. Cela permet aussi de définir des mesures *partielles* du registre de qubits. Par exemple une mesure dans la base $(|0\rangle, |1\rangle)$ du premier qubit d'un registre de deux qubits correspondra au couple de projecteur (P_0, P_1) tel que $P_0 = |00\rangle\langle 00| + |01\rangle\langle 01|$ et $P_1 = |10\rangle\langle 10| + |11\rangle\langle 11|$.

Contrairement aux opérations unitaires, les mesures ne sont pas réversibles. On peut remarquer qu'une mesure change l'état du qubit, à moins que celui-ci ne soit déjà dans un état propre pour l'observable considérée. Cette propriété, associée au théorème de non-clonage qui stipule qu'on ne peut dupliquer un état quantique inconnu (voir par exemple [148, p. 532]), est à la base du protocole BB84, inventé par Bennett et Brassard en 1984 [23], qui permet la création d'une clé cryptographique commune de façon sûre (voir par exemple [28, p. 255-258]).

1.2.2 Intrication quantique

Paradoxe EPR et non localité

Dans les années 1930, deux interprétations de la mécanique quantique opposent Bohr et Einstein. Pour Bohr, le caractère probabiliste des mesures est fondamental et les valeurs d'une observable ne sont pas fixées avant la mesure. Einstein est un partisan du *réalisme local* : dans cette vision du monde, les lois physiques suivent le principe de *localité* (assertion (iii) ci-dessous) et le principe du *réalisme* qui affirme que les différentes propriétés physiques existent en dehors du fait qu'on les mesure ou non, et que leurs valeurs sont déterminées avant la mesure. Selon Einstein, l'aspect aléatoire des valeurs mesurées n'est que le reflet d'une connaissance partielle des propriétés du système et il existe des éléments de la réalité physique que la mécanique quantique ne prend pas en compte ; c'est donc une théorie incomplète. Pour Bohr, la mécanique quantique est complète et l'aléa des mesures est intrinsèque.

En 1935, Einstein et deux autres physiciens, Podolsky et Rosen, publient un article retentissant [26] dans lequel ils entendent démontrer que la mécanique quantique est une théorie incomplète [76]. On se réfère généralement à cet article sous le nom *EPR* ou

26. Sa publication fera la une du New York Times sous le titre « Einstein attacks quantum theory ».

encore *paradoxe EPR*. Cet article décrit une expérience de pensée concernant un système formé de deux particules (a) et (b). Les auteurs supposent que :

(i) aucune information ne peut se propager plus vite que la lumière (*principe de causalité relativiste*),

(ii) aucune influence à distance instantanée n'est possible entre deux systèmes séparés dans l'espace (*principe de localité*),

(iii) la mécanique quantique est *complète* : tout élément de réalité trouve un correspondant dans la théorie.

Ils montrent alors que deux grandeurs physiques associées à des observables qui ne commutent pas, par exemple la position et la quantité de mouvement d'une des particules, peuvent avoir une *réalité*[27] simultanée ce qui est en contradiction avec la mécanique quantique (1.23). Ils en déduisent que, sous les hypothèses (i) et (ii), la mécanique quantique est incomplète. Notez qu'on aurait pu proposer de rejeter (ii) et garder (i) et (iii), mais cela va à l'encontre de la conception d'Einstein. La réponse de Bohr [30] est que EPR ne permet pas de rejeter l'hypothèse (iii) car la définition d'un élément de réalité physique donnée dans l'article est ambiguë. Pour lui, on ne peut considérer de réalité physique indépendante de l'appareil de mesure. Malgré cette réponse, le débat n'est pas tranché et la communauté des physiciens reste partagée.

Version de Bohm du paradoxe EPR

En 1951 David Bohm propose une version du paradoxe EPR basée sur un système de deux particules (a) et (b) de spin 1/2 [29]. L'expérience de pensée proposée est différente mais illustre les mêmes concepts. En notant $|0\rangle$ et $|1\rangle$ les deux états de spin selon l'axe $\hat{z}$, l'état du système considéré par Bohm est :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a |1\rangle_b - |1\rangle_a |0\rangle_b) \qquad \text{(état singulet)} \tag{1.45}$$

On suppose vrai le principe de localité et on suppose que les particules (a) et (b) sont suffisamment éloignées pour ne pas pouvoir interagir pendant l'expérience. Quand on mesure l'observable Z pour (a) et qu'on trouve $+1$ alors le système $(a)+(b)$ est projeté sur l'état $|0\rangle_a |1\rangle_b$ et dans ce cas la mesure de Z pour b donnera -1 avec certitude. Si on trouve -1 pour (a) alors le système est projeté dans l'état $|1\rangle_a |0\rangle_b$ et on trouvera $+1$ pour (b) avec certitude. Selon la conception d'Einstein de la réalité, cela signifie qu'il existe un élément de réalité associé à la mesure de Z pour (b).

Mais on peut également écrire cet état dans la base $(|+\rangle, |-\rangle)$ des états propres de X et on obtient $|\psi\rangle = \frac{1}{\sqrt{2}}(|-\rangle_a |+\rangle_b - |+\rangle_a |-\rangle_b)$. Quand on mesure X pour (a) et qu'on obtient $x \in \{+1, -1\}$ alors on est sûr d'obtenir $-x$ pour la particule (b). Cela signifie donc qu'il existe un élément de réalité associé à la mesure de X pour (b). Ainsi on voit que deux quantités physiques correspondantes à deux observables qui ne commutent pas peuvent avoir une réalité simultanée pour B, ce qui est en contradiction avec la mécanique quantique.

Sans parler d'observables qui ne commutent pas et en se limitant à mesurer Z pour les deux particules, on peut remarquer qu'avant de mesurer Z pour (a), on peut obtenir

27. Le critère de réalité utilisé dans [76] est le suivant : « *If, without in any way disturbing a system, we can predict with certainty (i.e. with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* »

chacune des valeurs $+1$ et -1 avec la probabilité $1/2$ pour (b). Cependant, dès qu'on a mesuré Z pour (a) alors on ne peut obtenir que la valeur opposée pour (b). On a donc une corrélation parfaite des résultats, et cela sans que (a) et (b) n'aient pu interagir si on suppose que la nature respecte le principe de localité. Tout se passe comme ci le résultat obtenu pour (a) déterminait celui de (b) et l'on retrouve donc la situation physique correspondante à l'analogie des pièces de monnaie intriquées développée dans l'introduction de cette thèse. Des états tels que l'état $|\psi\rangle$ ou l'état mentionné dans EPR sont qualifiés par les physiciens d'états *intriqués* parce qu'il existe des corrélations entre les propriétés mesurées de ces états et cela quelle que soit la distance qui les sépare (voir section 1.2.2 pour une définition plus précise de l'intrication).

Bohr *vs* Einstein

Pour les physiciens partisans de l'interprétation d'Einstein, il existe un élément de réalité (autrement dit une propriété physique) que les deux particules se sont échangées dans le passé quand elles ont interagi. La valeur de cette propriété détermine avant la mesure les valeurs des spin, si bien qu'on ne peut obtenir que $(+1_a, -1_b)$ ou $(-1_a, +1_b)$. Cela explique les corrélations entre les mesures tout en respectant le principe de localité. On parle alors de *théorie à variables cachées locales* même si Einstein n'a jamais mentionné ces termes (voir [11, p. 6]), ou encore de théorie *réaliste locale*. Einstein pensait qu'on pouvait compléter la mécanique quantique par une théorie de ce type comme l'indique la dernière phrase d'EPR [76] : « We believe, however, that such a theory is possible. »

Pour les partisans de Bohr (interprétation de l'école de Copenhague qualifiée d'orthodoxe), il n'y a pas de variables cachées et la mécanique quantique est complète. Selon eux, il faut accepter que les deux systèmes (a) et (b), même séparés dans l'espace, forment un tout indissociable et que mesurer le système (a) peut influencer la mesure de (b) instantanément. Cela ne va pas sans difficultés conceptuelles car il s'agit d'une remise en question au moins partielle du principe de localité (iii). Einstein raillait une telle interprétation en parlant *d'actions fantomatiques à distance*[28].

Cependant, dans ce débat, personne ne conteste le fait que la mécanique quantique soit une théorie physique *correcte*, c'est à dire en parfaite adéquation avec les résultats expérimentaux obtenus jusqu'à présent. Ainsi le choix de l'une ou l'autre de ces interprétations reste pendant plusieurs décennies une question d'ordre philosophique sur l'interprétation du monde. Jusqu'à l'arrivée de John Bell sur la scène en 1964[29].

Inégalités de Bell

Dans son article de 1964, Bell [21] démontre que les deux visions du monde de Bohr et Einstein ne sont pas compatibles. A cette fin, il établit des inégalités mathématiques appelées par la suite *inégalités de Bell*. Dans un monde où les lois de la physique obéissent au réalisme local, une certaine inégalité est respectée, mais selon la mécanique quantique, il peut y avoir violation de cette inégalité dans certaines situations expérimentales. Avec Bell, la question épistémologique sur l'interprétation de la mécanique devient une question expérimentale (voir l'interview d'Alain Aspect [129]).

Nous donnons dans ce qui suit la version dite *CHSH* des inégalités de Bell, publiée

28. *spukhafte Fernwirkungen* dans une lettre à Max Born datant de 1947, traduit en anglais par *spooky action at a distance*.

29. John Stewart Bell (1928-1990), physicien nord-irlandais.

en 1969 par Clauser [30], Horne, Shimony et Holt [53] : on considère un système de deux particules (a) et (b) de spin 1/2 dans l'état

$$|EPR\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a |0\rangle_b + |1\rangle_a |1\rangle_b). \tag{1.46}$$

et deux appareils de mesure du spin, l'un pour (a) et l'autre pour (b). Après avoir interagi au moment de leur création, les deux particules se déplacent en ligne droite dans des directions opposées selon un axe $\hat{y}$ et leurs spins sont ensuite mesurés en même temps. Pour la particule (a), on peut mesurer deux observables du spin, A_1 ou A_2, selon des axes d'orientation différente dans le plan défini par $\hat{x}$ et $\hat{z}$. De même pour (b), on considère deux observables B_1 et B_2 dans un plan parallèle. Soit $E(A, B)$ la moyenne des produits des valeurs obtenue en mesurant simultanément deux observables A et B et soit S la somme :

$$S = E(A_1, B_1) - E(A_1, B_2) + E(A_2, B_1) + E(A_2, B_2). \tag{1.47}$$

Dans une vision locale réaliste du monde (existence de variables locales cachées), on a

$$|S| \leqslant 2 \qquad \text{(inégalité CHSH)} \tag{1.48}$$

mais d'après les prédictions de la mécanique quantique on peut choisir les angles entre les différents axes de mesure de façon à avoir $|S| = 2\sqrt{2}$.

Si l'on réussit à monter une expérience permettant de mesurer avec précision la quantité S, alors on obtiendra quelle que soit la valeur obtenue un résultat très important : soit on obtient une violation de l'inégalité (1.48) et cela signifie qu'il faut abandonner le réalisme local cher à Einstein, soit on ne réussit pas à dépasser la valeur 2 pour S et on prend en défaut la théorie quantique pour la première fois, en laissant entrevoir la possibilité d'une nouvelle théorie réaliste locale.

La première expérience ayant permis une violation de l'inégalité CHSH est celle réalisée par Alain Aspect et son équipe en 1981, basée sur un papier de 1976 [10] et relatée dans [11]. C'est *l'expérience d'Orsay* pour laquelle Aspect obtiendra le prix Nobel de physique 2022. Depuis lors, plusieurs expériences ont confirmé les résultats d'Aspect, citons par exemple *l'expérience de Genève* en 1998 [178]. De nos jours, il est possible de constater la violation de l'inégalité de Bell sur les machines quantiques d'IBM accessibles en cloud computing [3] (voir par exemple [182]).

L'intrication, une ressource fondamentale

La violation expérimentale des inégalités de Bell supprime une possibilité d'explication de l'intrication. Pourtant, même si la nature de ce phénomène reste mal comprise, cela n'a pas empêché la communauté des physiciens et des informaticiens d'utiliser les états intriqués dans de nombreux protocoles de communication et d'échange de secret. Ainsi l'intrication et les états intriqués sont devenus une véritable ressource dans le cadre de la théorie de l'information quantique (voir par exemple l'article de revue [103] ainsi que [148, section 12.5]). Nous donnons dans ce qui suit quelques utilisations parmi les plus connues de l'état $|EPR\rangle$. Nous les décrivons sommairement en utilisant les personnages habituels (Alice, Bob et Eve) de la théorie de l'information (classique ou quantique) : Alice veut envoyer de l'information à Bob et Eve est l'oreille indiscrète qui cherche à connaître cette information.

30. John Clauser est un physicien américain, co-récipiendaire du prix Nobel de physique 2022.

- Le *codage superdense*, inventé en 1992 par Bennett et Wiesner [26], consiste à envoyer deux bits d'information classique en utilisant un seul qubit envoyé par un canal quantique. Au départ Alice et Bob possèdent chacun un des qubits d'un système dans l'état intriqué $|EPR\rangle$ (ressource initiale). En envoyant son qubit à Bob, Alice va pouvoir lui communiquer deux bits classiques (voir [148, section 2.3] pour plus de détails).

- La *téléportation quantique*, découverte en 1993 par Bennett *et al.* [24], est un protocole de communication quantique permettant de téléporter un qubit (dont l'état n'est pas connu) à condition d'avoir échangé sur un canal classique deux bits d'information. Au départ, Alice et Bob possèdent chacun un des qubits (a) et (b) d'un système dans l'état intriqué $|EPR\rangle$ (ressource initiale) et Alice veut transmettre à Bob un troisième qubit dans l'état $|\psi\rangle$. En envoyant deux bits classiques à Bob, Alice va lui permettre de mettre son qubit (b) dans l'état $|\psi\rangle$ (voir [148, section 1.3.7] pour plus de détails). La téléportation quantique a été réalisée expérimentalement en 1997 [34, 33] et a fait l'objet de nombreux travaux, notamment une généralisation à des états d'un système avec des variables continues [173].

- *Le protocole EPR* d'Ekert [77] est, tout comme BB84, un protocole de distribution de clé cryptographique. À la différence de BB84, le protocole EPR est basé sur les inégalités de Bell. Une source émet des paires de qubits intriqués dans l'état $|EPR\rangle$ comme dans la version *CHSH* des inégalités de Bell. Le qubit (a) va vers Alice et le qubit (b) va vers Bob. Pour chaque paire émise, Alice mesure le qubit (a) selon un axe choisi au hasard parmi plusieurs orientations possibles, de même pour Bob. S'ils mesurent selon des axes parallèles alors ils obtiennent la même valeur 1 ou 0 qui constitue un bit de la clé commune. En se basant sur les mesures obtenues dans les cas où ils ne choisissent pas le même axe, on calcule la valeur S. Les angles entre les différents axes sont choisis de telle sorte que $|S| = 2\sqrt{2}$ si Eve n'a pas mesuré les qubits avant Alice et Bob. Dans le cas contraire, on démontre que $|S| < 2$, ce qui permet de détecter l'intervention d'Eve.

D'autres états intriqués jouent un rôle important dans la théorie de l'information quantique, notamment l'état $|GHZ\rangle$ [92]) (Greenberger-Horne-Zeilinger) et l'état $|W\rangle$. Ils sont utiles dans différents protocoles de communication et de partage de secret (voir par exemple [69], [98], [87]). À l'origine ces états sont définis pour un système de 3 qubits mais on peut les généraliser à n qubits. Ils sont définis par

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}}\left(|\overbrace{0\cdots0}^{\times n}\rangle + |\overbrace{1\cdots1}^{\times n}\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right) \qquad (n \geqslant 3) \qquad (1.49)$$

et

$$|W_n\rangle = \frac{1}{\sqrt{n}}\left(|10\cdots0\rangle + |010\cdots0\rangle + \cdots + |0\cdots01\rangle\right) \qquad (n \geqslant 3). \qquad (1.50)$$

Dans le chapitre 5 de ce mémoire, nous utiliserons ces états pour des systèmes de 3 ou 4 qubits dans le cadre de la classification des états intriqués.

Classifications et mesures de l'intrication

Les physiciens ont défini plusieurs ensembles d'opérations pour caractériser les actions locales qu'on peut appliquer à un système quantique. Pour rester dans le cadre

de la théorie de l'information quantique, nous supposons sans perte de généralité que le système considéré est un registre de n qubits $q_0, \ldots, q_{n-1}$ partagé entre n parties, chaque partie P_i pouvant agir sur le qubit q_i en sa possession.

Le premier ensemble d'opérations est désigné par l'acronyme LOCC (Local Operations and Classical Communication) : il s'agit d'opérations appliquées localement au système par chaque partie, en donnant de plus la possibilité aux différentes parties de coordonner leurs actions en utilisant des moyens de communication classique. Une définition mathématique précise de ces opérations est donnée dans [25, p. 2] ; elle est plus large que l'exemple que nous avons donné en fin de section 1.2.1 et inclut notamment les mesures des qubits et l'utilisation de qubits auxiliaires (voir aussi [148, proposition 12.14]). On dit que deux états $|\psi\rangle$ et $|\psi'\rangle$ d'un système sont *LOCC-équivalents* et on note

$$|\psi\rangle \underset{LOCC}{\sim} |\psi'\rangle\,, \tag{1.51}$$

s'il existe des opérations locales transformant $|\psi\rangle$ en $|\psi'\rangle$ et des opérations locales transformant $|\psi'\rangle$ en $|\psi\rangle$. L'équivalence LOCC exprime donc l'*interconvertibilité* de deux états par des opérations locales.

On définit un deuxième ensemble constitué des opérations locales unitaires, désigné par l'acronyme LU (Local Unitary), qu'on assimile au groupe produit U_2^n :

$$\mathrm{LU} = \mathrm{U}_2 \times \cdots \times \mathrm{U}_2 = \mathrm{U}_2^n. \tag{1.52}$$

Ce groupe agit [31] sur l'espace $\mathcal{H}^{\otimes n}$ par $(U_0, \ldots, U_{n-1}) \cdot |\psi\rangle = (U_0 \otimes \cdots \otimes U_{n-1})\,|\psi\rangle$, pour tout $(U_0, \ldots, U_{n-1}) \in \mathrm{LU}$ et tout $|\psi\rangle \in \mathcal{H}^{\otimes n}$. On définit *l'équivalence LU* de deux états $|\psi\rangle$ et $|\psi'\rangle$ de $\mathcal{H}^{\otimes n}$ par :

$$|\psi\rangle \underset{LU}{\sim} |\psi'\rangle \iff \exists\, U_0, \ldots, U_{n-1} \in \mathrm{U}_2, \quad (U_0 \otimes \cdots \otimes U_{n-1})\,|\psi\rangle = |\psi'\rangle\,. \tag{1.53}$$

Par exemple, l'état $|GHZ_3\rangle$ est LU-équivalent à l'état $|GHZ_3'\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$ car $|GHZ_3'\rangle = H^{\otimes 3}\,|GHZ_3\rangle$. On démontre que deux états purs sont LOCC-équivalents si et seulement si ils sont LU-équivalents (voir [25, corollaire 1]) :

$$|\psi\rangle \underset{LOCC}{\sim} |\psi'\rangle \iff |\psi\rangle \underset{LU}{\sim} |\psi'\rangle\,. \tag{1.54}$$

Enfin, le troisième ensemble d'opérations locales est nommé SLOCC (Stochastic LOCC) et contient les opérations de LOCC. La convertibilité d'un état $|\psi\rangle$ en un état $|\psi'\rangle$ par SLOCC signifie qu'il existe des opérations de LOCC permettant d'obtenir $|\psi'\rangle$ à partir de $|\psi\rangle$ avec une probabilité non nulle (voir [25, p. 3]). L'équivalence SLOCC entre deux états exprime l'interconvertibilité par SLOCC entre ces deux états. Ainsi l'équivalence LOCC entre deux états est un cas particulier de l'équivalence SLOCC :

$$|\psi\rangle \underset{LOCC}{\sim} |\psi'\rangle \implies |\psi\rangle \underset{SLOCC}{\sim} |\psi'\rangle\,. \tag{1.55}$$

On considère le groupe

$$\mathrm{G_{SLOCC}} = \mathrm{GL}_2(\mathbb{C}) \times \cdots \times \mathrm{GL}_2(\mathbb{C}) \tag{1.56}$$

formé par le produit cartésien de n copies du groupe des opérateurs inversibles agissant sur un qubit. Le groupe $\mathrm{G_{SLOCC}}$ agit sur l'espace $\mathcal{H}^{\otimes n}$ de façon naturelle par $(A_0, \ldots, A_{n-1}) \cdot |\psi\rangle = (A_0 \otimes \cdots \otimes A_{n-1})\,|\psi\rangle$, pour tout $(A_0, \ldots, A_{n-1}) \in \mathrm{G_{SLOCC}}$ et tout

31. Voir annexe A, section A.1.4

$|\psi\rangle \in \mathcal{H}^{\otimes n}$. On démontre dans [74, section II.A] que deux états sont SLOCC-équivalents s'il existe un élément de $\mathrm{G}_{\mathrm{SLOCC}}$ dont l'action sur un état permet d'obtenir l'autre :

$$|\psi\rangle \underset{SLOCC}{\sim} |\psi'\rangle \iff \exists (A_0, \ldots, A_{n-1}) \in \mathrm{G}_{\mathrm{SLOCC}}, \quad |\psi'\rangle = (A_0 \otimes \cdots \otimes A_{n-1}) |\psi\rangle . \quad (1.57)$$

On utilise également le groupe

$$\mathrm{G}'_{\mathrm{SLOCC}} = \mathrm{SL}_2(\mathbb{C}) \times \cdots \times \mathrm{SL}_2(\mathbb{C}) \quad (1.58)$$

où $\mathrm{SL}_2(\mathbb{C})$ désigne le groupe des opérateurs inversibles de déterminant égal à 1 agissant sur un qubit. En effet la SLOCC-équivalence dans l'espace $\mathcal{H}^{\otimes n}$ entre deux états $|\psi\rangle$ et $|\psi'\rangle$ se traduit par l'existence d'un opérateur de $A \in \mathrm{G}'_{\mathrm{SLOCC}}$ et d'un nombre complexe k tel que $A \cdot |\psi\rangle = k\,|\psi'\rangle$. Ainsi quand on considère les états dans l'espace projectif $\mathbb{P}(\mathcal{H}^{\otimes n})$, la SLOCC-équivalence se traduit à l'aide d'un opérateur de $\mathrm{G}'_{\mathrm{SLOCC}}$.

Une première approche pour classifier l'intrication est de créer une partition de l'espace $\mathcal{H}^{\otimes n}$ en classes d'équivalence sous l'action du groupe LU. En effet, l'intrication résulte d'une interaction entre les différentes parties d'un système donc l'action d'un opérateur de LU sur un état ne peut créer de l'intrication ou la détruire. Il semble alors naturel de considérer que des états d'une même classe (donc LOCC-équivalents) représentent le même type d'intrication. Cette classification a été utilisée dans de nombreux travaux, par exemple [125],[131] et [119].

On peut aussi élargir les classes obtenues par l'action de LU en considérant l'action de $\mathrm{G}_{\mathrm{SLOCC}}$ sur l'espace $\mathcal{H}^{\otimes n}$ [142, section 1]. On obtient ainsi une classification moins fine mais qui permet de tenir compte de l'aspect probabiliste des opérations de SLOCC. Le groupe $\mathrm{G}_{\mathrm{SLOCC}}$ contenant le groupe LU, les classes d'équivalence sont plus grandes donc moins nombreuses et plus faciles à décrire que les classes obtenues par l'action de LU. De plus, deux états SLOCC-équivalents sont supposés pouvoir accomplir les mêmes tâches, mais avec des probabilités de succès différentes, lorsqu'ils sont utilisés comme ressources dans le cadre de la théorie de l'information quantique [74, 141]. Ainsi la répartition des états en différentes orbites sous l'action du groupe $\mathrm{G}_{\mathrm{SLOCC}}$ peut être considérée comme une classification qualitative de l'intrication.

On peut également chercher à quantifier l'intrication d'un système et on utilise pour cela différentes mesures. La définition précise d'une mesure de l'intrication (*entanglement monotone*) est donnée dans [175] et rappelée dans [25, p. 2]. Notamment, une mesure de l'intrication doit être invariante sous l'action du groupe LU. Il existe plusieurs mesures de l'intrication (voir [175]) et la thèse de Jaffali [106] propose une synthèse sur ce sujet. Dans ce mémoire, nous n'utiliserons qu'une seule mesure de l'intrication que nous détaillerons dans le chapitre 5 : la valeur absolue de l'hyperdéterminant.

1.3 Circuits quantiques

Différents modèles de calcul quantique ont été développés depuis le modèle des machines de Turing quantiques introduit par Deutsch en 1985 [66]. Parmi les principaux modèles, on peut citer le calcul quantique basé sur la mesure [177], les automates cellulaires quantiques [9], le calcul quantique topologique de Kitaev [79] et enfin les circuits quantiques [14]. Sur les différents modèles de calcul quantique, on pourra par exemple consulter la thèse de Perdrix [156].

Dans ce mémoire, nous nous basons uniquement sur le modèle des circuits quantiques. Nous avons regroupé dans cette section les notions sur les circuits quantiques permettant à un lecteur non spécialiste de lire cette thèse. On y introduit également une bonne partie

du vocabulaire et des notations qui seront constamment utilisées dans les chapitres qui suivent. Pour une introduction complète sur les circuits quantiques, le lecteur pourra se référer à [148, chapitre 4].

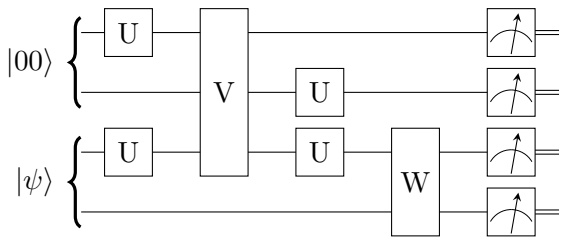
1.3.1 Qu'est-ce qu'un circuit quantique ?

Généralités : circuits quantiques et portes quantiques

D'un point de vue informel, un circuit quantique est une représentation schématique des opérations unitaires et des mesures qui peuvent être appliquées à un registre de qubits au cours du temps. Dans ce schéma, on attribue à chaque qubit une ligne horizontale, la ligne attribuée au qubit i étant située juste au dessus de la ligne du qubit $i+1$. Les différentes opérations effectuées sur le système se lisent de la gauche vers la droite (sens de la flèche du temps). Dans un circuit quantique, chaque opération unitaire est représentée par un motif appelé *porte quantique*, souvent un rectangle étiqueté par le nom de l'opérateur, placé au niveau des lignes des qubits impliqués dans l'opération. Ainsi $-\boxed{X}-$ est la porte quantique représentant l'opérateur de Pauli X. Une mesure d'un qubit dans la base standard est représentée par le motif $-\boxed{\nearrow}=$ (voir exemple figure 1.2).

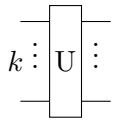
Du point de vue de l'expérimentateur, une porte quantique est un appareillage bien réel (par exemple un laser), qui va agir sur certaines des particules du système afin de leur appliquer un certain opérateur unitaire. Pour l'informaticien, une porte quantique est souvent assimilée avec l'opérateur unitaire qu'elle implémente et c'est ce que nous ferons généralement dans ce mémoire. Cependant, il s'agit là d'une vision idéale et simplifiée de la réalité car il faut garder à l'esprit que dans la phase actuelle de développement des ordinateurs quantiques, les portes quantiques ne sont pas vraiment fiables et fonctionnent avec un pourcentage d'erreur variable, mais non négligeable.

Figure 1.2 Circuit quantique représentant l'opérateur unitaire $(I \otimes I \otimes W)(I \otimes U \otimes U \otimes I)(V \otimes I)(U \otimes I \otimes U \otimes I)$ appliqué à l'état $|00\rangle \otimes |\psi\rangle$, suivi par une mesure des qubits dans la base standard. La double ligne en sortie des appareils de mesure transporte un bit classique, résultat de la mesure.



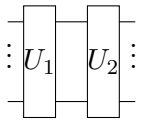
On peut démontrer que les mesures des qubits peuvent toujours être reportées en fin de circuit (voir [148, section 4.4]). Ainsi un circuit quantique peut être défini sans perte de généralité comme un circuit composé de portes quantiques avec des mesures d'un ou plusieurs qubits en fin de circuit. Formellement, un circuit composé uniquement de portes quantiques, ainsi que sa sémantique, peuvent être définis par induction de la façon suivante :

- Pour tout entier k non nul,



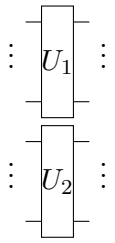
est un circuit quantique représentant un opérateur unitaire U d'arité k (*i.e.* agissant sur k qubits).

- Le circuit quantique —— représente l'identité I_2 d'arité 1.
- Composition séquentielle : si C_1 et C_2 sont des circuits quantiques représentant respectivement les opérateurs U_1 et U_2 de même arité k, alors



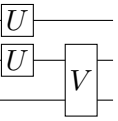
est un circuit quantique représentant l'opérateur U_2U_1 d'arité k.

- Composition parallèle : si C_1 et C_2 sont des circuits quantiques représentant respectivement les opérateurs U_1 d'arité k_1 et U_2 d'arité k_2, alors



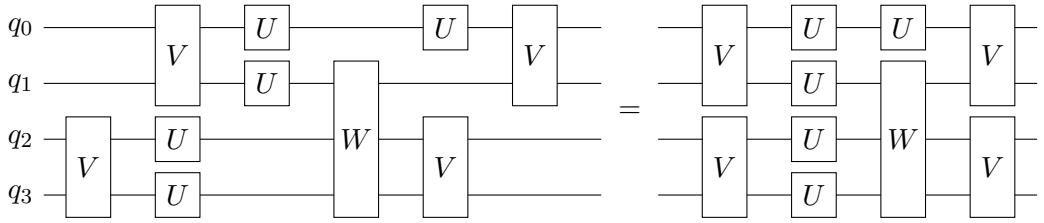
est un circuit quantique représentant l'opérateur $U_1 \otimes U_2$ d'arité $k_1 + k_2$.

Nous assimilerons un circuit quantique sans mesures avec l'opérateur unitaire qu'il représente. Ainsi, dans les chapitres qui suivent, nous parlerons par exemple de groupes (au sens mathématique) formé par tel ou tel type de circuit. La seule différence est l'ordre d'écriture des portes qui est inversée entre les deux représentations : un circuit quantique agit à droite sur un registre quantique tandis qu'un opérateur unitaire agit à gauche sur un ket. Nous écrivons par exemple :

$$(I \otimes V)(U \otimes U \otimes I)\,|\psi\rangle = \; |\psi\rangle$$  . (1.59)

La *longueur* d'un circuit quantique est le nombre de portes quantiques de ce circuit. Dans un circuit quantique, les portes consécutives portant sur des sous-ensembles de qubits deux à deux disjoints peuvent être appliquées en même temps, c'est à dire en parallèle. Le nombre minimal de regroupements d'opérations qu'on peut effectuer en parallèle s'appelle *la profondeur* du circuit (voir exemple figure 1.3). Cet indicateur est particulièrement important car il est relié à un phénomène nommé *décohérence* qui est un problème technique majeur pour les physiciens qui cherchent à mettre au point l'ordinateur quantique. Pour résumer, disons qu'il est très difficile d'isoler parfaitement un système quantique et que celui-ci va perdre rapidement son état de superposition

Figure 1.3 Un circuit quantique de longueur 10 et de profondeur 4.



par simple interaction (non désirée) avec son environnement. La décohérence peut donc complètement fausser les calculs. On voit qu'une faible profondeur de circuit implique un temps de calcul plus court ce qui permet de limiter l'effet de la décohérence. La longueur et la profondeur sont généralement les deux paramètres pris en compte pour décrire la complexité d'un circuit.

Nous décrivons maintenant les portes quantiques utilisées dans ce mémoire et les notations adoptées.

Portes unaires

Les *portes unaires* sont des portes qui agissent sur un seul qubit d'un registre quantique. Cela signifie que l'image d'un ket $|b_0 \dots b_{n-1}\rangle$ de la base standard par une porte unaire agissant sur q_i ne dépend que de b_i. De manière générale, quand on applique une porte quantique $U \in \mathrm{U}_2$ sur le qubit q_i d'un registre, son action sur le système est celui de l'opérateur unaire U_i de $\mathcal{H}^{\otimes n}$ défini par :

$$U_i = \underbrace{I \otimes \cdots \otimes I}_{i \text{ facteurs}} \otimes U \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i-1 \text{ facteurs}} = I^{\otimes i} \otimes U \otimes I^{\otimes n-i-1}. \tag{1.60}$$

Quand on applique simultanément la porte $U \in \mathrm{U}_2$ à plusieurs qubits, on définit un vecteur de bits v de $\mathbb{F}_2^n$ tel que, pour tout $i = 0, \dots, n-1$, on a $v_i = 1$ si et seulement si U est appliquée au qubit q_i. L'opérateur unitaire de $\mathcal{H}^{\otimes n}$ appliqué au système global est alors noté U_v et il est défini par :

$$U_v = U^{v_0} \otimes \cdots \otimes U^{v_{n-1}} = \prod_{i=0}^{n-1} U_i^{v_i}. \tag{1.61}$$

En particulier, si on note (e_i) la base canonique de $\mathbb{F}_2^n$, on a $U_{e_i} = U_i$.

Appliquons ces notations à des portes de Pauli X ou Z agissant en parallèle sur un registre de qubits. Pour $x \in \{0, 1\}$, on a $Z|x\rangle = (-1)^x |x\rangle$ et $X|x\rangle = |x \oplus 1\rangle$, où $\oplus$ désigne le XOR bit à bit, ou encore l'addition dans $\mathbb{F}_2$. Soit $|b\rangle$ un vecteur de la base standard (avec $b \in \mathbb{F}_2^n$). On a donc

$$Z_i |b\rangle = (-1)^{b_i} |b\rangle = (-1)^{e_i \cdot b} |b\rangle, \quad X_i |b\rangle = |b \oplus e_i\rangle, \tag{1.62}$$

ce qu'on peut généraliser en

$$Z_v |b\rangle = (-1)^{v \cdot b} |v\rangle, \quad X_v |b\rangle = |v \oplus b\rangle, \tag{1.63}$$

où l'opérateur « $\cdot$ » désigne le produit scalaire usuel. Ces formules apparaissent avec des notations similaires dès 1997 dans des travaux de Calderbank *et. al.* [46, section 2], [43, section 2], [44, Introduction].

Deux autres portes agissant sur un qubit jouent un rôle important dans le calcul quantique : les portes P et T. Elles sont définies par leur matrices dans la base standard :

$$P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\frac{\mathrm{i}\pi}{4}} \end{bmatrix}. \tag{1.64}$$

Ces portes, tout comme la porte Pauli Z, sont des *portes de changement de phase relative* car elles transforment l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ en l'état $|\psi'\rangle = \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\beta|1\rangle$ pour un certain réel φ. Dans la base standard, la matrice d'une porte de ce type est

$$\begin{bmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\varphi} \end{bmatrix} = \mathrm{e}^{\mathrm{i}\frac{\varphi}{2}} \begin{bmatrix} \mathrm{e}^{-\mathrm{i}\frac{\varphi}{2}} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\frac{\varphi}{2}} \end{bmatrix} = R_z(\varphi). \tag{1.65}$$

Il s'agit donc, à une phase globale près, d'une porte de rotation d'angle φ autour de l'axe $\hat{z}$. On remarque qu'on a les relations suivantes :

$$T^2 = P, \quad P^2 = Z, \quad PXP^{-1} = Y. \tag{1.66}$$

Portes binaires

Les portes binaires sont des portes qui font interagir deux qubits d'un registre quantique. Autrement dit, l'image d'un vecteur de base $|b\rangle$ par une porte binaire agissant sur deux qubits q_i et q_j d'un registre de n qubits ne dépend que des valeurs de b_i et de b_j. Une classe importante de portes binaires est celle des portes agissant sur un qubit, contrôlées par un autre qubit. Soit $U \in \mathrm{U}_2$ une porte quantique, on appelle *porte U contrôlée* par le qubit j ayant pour cible le qubit i, la porte binaire définie par son action sur un état de base $|b\rangle$ de la façon suivante : si $b_j = 1$ alors on applique U au qubit i, sinon on ne fait rien. Le qubit i est appelé le *qubit cible* et q_j est le *qubit de contrôle*. En notant cette porte $CU_{(i,j)}$, on a donc :

$$CU_{(i,j)}|b\rangle = U_i^{b_j}|b\rangle. \tag{1.67}$$

La porte X est aussi appelée porte NOT car elle transforme $|0\rangle$ en $|1\rangle$ et $|1\rangle$ en $|0\rangle$. Dans un circuit, elle est parfois notée $-\!\oplus\!-$ au lieu de $-\boxed{X}-$. Dans ce mémoire, deux cas particuliers de portes contrôlées seront étudiés plus en détail : les portes $CNOT$ et les portes CZ. Pour des raisons que nous évoquerons au chapitre 2, la porte $CNOT_{(i,j)}$ sera notée $X_{[i:j]}$. La porte $CZ_{(i,j)}$ sera notée simplement par $Z_{\{i,j\}}$. On a donc :

$$X_{[i:j]} = CNOT_{(i,j)} \quad \text{et} \quad Z_{\{i,j\}} = CZ_{(i,j)}. \tag{1.68}$$

La figure 1.4 montre comment sont représentées ces portes dans les circuits quantiques. La porte $X_{[i:j]}$ (pour $i < j$) est définie par :

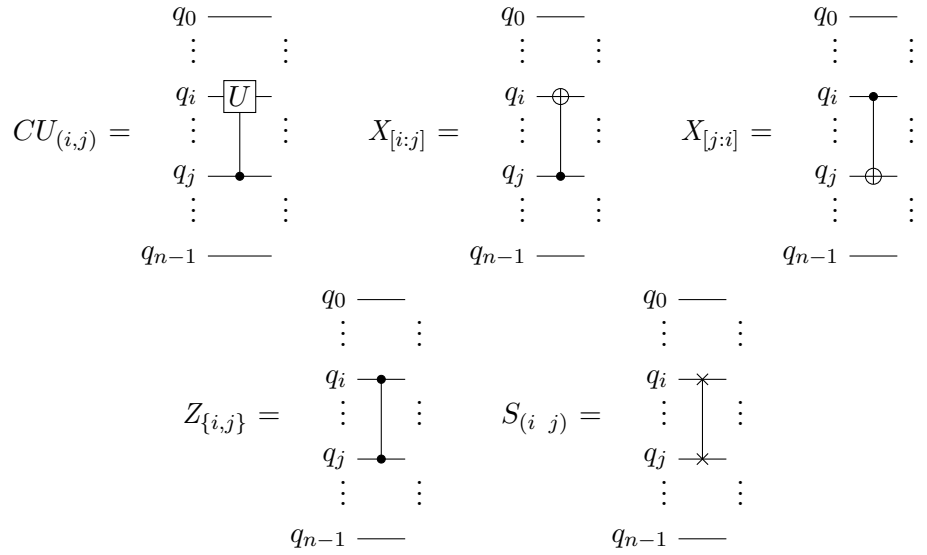
$$X_{[i:j]}|b\rangle = |b_0 \cdots b_i \oplus b_j \cdots b_j \cdots b_{n-1}\rangle = |b \oplus b_j e_i\rangle. \tag{1.69}$$

En effet, cette porte doit inverser le bit b_i si et seulement si b_j vaut 1, ce qui revient à remplacer b_i par $b_i \oplus b_j$, autrement dit remplacer le vecteur b de $\mathbb{F}_2^n$ par le vecteur $b \oplus b_j e_i$ (voir exemple figure 1.5).

La porte $Z_{\{i,j\}}$ est définie par :

$$Z_{\{i,j\}}|b\rangle = (-1)^{b_i b_j}|b\rangle. \tag{1.70}$$

Figure 1.4 Représentation dans un circuit quantique des portes contrôlées CU, $CNOT$ et CZ ainsi que des portes de $SWAP$.



En effet, cette porte multiplie le ket de base $|b\rangle$ par (-1) si le bit de contrôle b_j vaut 1 et si le bit cible b_i est également à 1. On voit que l'expression (1.70) est invariante par permutation de i et j, ce qui explique la notation symétrique $Z_{\{i,j\}}$ et le motif symétrique utilisé dans les circuits quantiques pour ces portes (voir figure 1.4).

La porte $CNOT$ est un cas particulier de porte X contrôlée : c'est la porte $X_{[1:0]}$ agissant sur un registre de 2 qubits. De même la porte CZ est la porte $Z_{\{0,1\}}$ agissant sur un registre deux qubits. On a donc, pour tout $x, y \in \{0, 1\}$:

$$CNOT\,|xy\rangle = |x\rangle\,|x \oplus y\rangle\,, \qquad CZ\,|xy\rangle = (-1)^{xy}\,|xy\rangle\,. \tag{1.71}$$

Les matrices de ces opérateurs dans la base standard sont :

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \tag{1.72}$$

Exemple 1.1. La construction de l'état $|GHZ_n\rangle$ (1.49) s'effectue assez simplement à l'aide d'une porte de Hadamard qui sert à créer de la superposition et de portes $CNOT$ qui permettent de mettre les bits à 1 (voir figure 1.6). En effet :

$$H_0\,|0\ldots0\rangle = \frac{1}{\sqrt{2}}(|0\ldots0\rangle + |10\ldots0\rangle)$$

et

$$X_{[n-1:n-2]}\ldots X_{[2:1]}X_{[1:0]}\,|10\ldots0\rangle = |1\ldots1\rangle\,.$$

On a donc :

$$|GHZ_n\rangle = X_{[n-1:n-2]}\ldots X_{[2:1]}X_{[1:0]}H_0\,|0\rangle^{\otimes n}\,. \tag{1.73}$$

Figure 1.5 La porte $X_{[0:2]}$ dans un circuit de 3 qubits et sa matrice dans la base standard de $\mathcal{H}^{\otimes 3}$.

$$X_{[0:2]} = \quad = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Figure 1.6 Un circuit de portes *CNOT* générant l'état $|GHZ_4\rangle$ à partir d'un état complètement factorisé.

$$|0\rangle - H \quad |0\rangle \quad |0\rangle \quad |0\rangle \qquad |GHZ_4\rangle$$

Les portes *SWAP* jouent un rôle important dans les circuits quantiques ; elles sont utilisées par exemple dans la transformation de Fourier quantique (voir par exemple [148, section 5.1]) et elles permettent aussi de simuler une porte non native dans un ordinateur quantique dont le graphe du réseau de qubits n'est pas complet (voir chapitre 2 , section 2.1.2). Une porte de *SWAP* entre les qubits i et j échange les valeurs de ces qubits quand elle est appliquée à un état de la base standard. Nous la notons $S_{(i\ j)}$, où $(i\ j)$ désigne la transposition du groupe symétrique $\mathfrak{S}_n$ [32] qui échange i et j. On a donc, pour $i < j$:

$$S_{(i\ j)} |b_0 \cdots b_i \cdots b_j \cdots b_{n-1}\rangle = |b_0 \cdots b_j \cdots b_i \cdots b_{n-1}\rangle . \tag{1.74}$$

Cette porte est symétrique (*i.e.* $S_{(i\ j)} = S_{(j\ i)}$) ce qui est cohérent avec la notation cyclique d'une transposition et sa représentation dans un circuit quantique (voir figure 1.4). Cette définition implique que dans un système de qubits dans un état complètement factorisé

$$|\psi\rangle = |\psi_0\rangle \otimes \cdots \otimes |\psi_i\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_{n-1}\rangle ,$$

on a :

$$S_{(i\ j)} |\psi\rangle = |\psi_0\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_i\rangle \otimes \cdots \otimes |\psi_{n-1}\rangle . \tag{1.75}$$

On en déduit que l'action par conjugaison d'une porte *SWAP* sur une porte unaire U_i est donnée par :

$$S_{(i\ j)} U_i S_{(i\ j)} = U_j. \tag{1.76}$$

Dans le cas particulier d'un registre de deux qubits, la porte $S_{(0\ 1)}$ est notée simplement

32. Voir annexe A, section A.4

SWAP et sa matrice dans la base standard est donc :

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{1.77}$$

Circuits quantiques équivalents

On dit que deux circuits sans mesures C_1 et C_2 sont *équivalents* (ou *égaux*) s'ils représentent le même opérateur unitaire. La figure 1.7 illustre les équivalences classiques qui suivent. Ces équivalences sont simples à démontrer : pour prouver que deux opérateurs U_1 et U_2 sont égaux, il suffit de comparer leur action sur un ket $|b\rangle$ de la base standard. On a ainsi :

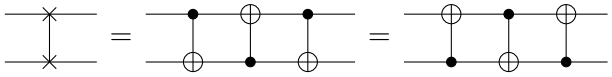
$$X_{[i:j]} = H_i H_j X_{[j:i]} H_j H_i, \tag{1.78}$$

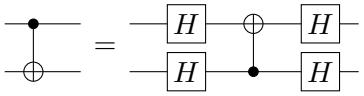
$$Z_{\{i,j\}} = H_i X_{[i:j]} H_i = H_j X_{[j:i]} H_j \tag{1.79}$$

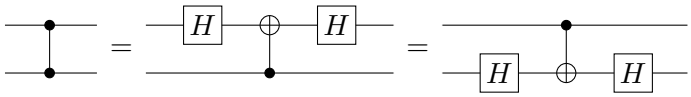
$$S_{(i\ \ j)} = X_{[i:j]} X_{[j:i]} X_{[i:j]} = X_{[j:i]} X_{[i:j]} X_{[j:i]} \tag{1.80}$$

En général, dans les ordinateurs quantiques actuels, toutes les portes ne sont pas implantées. On peut alors utiliser les égalités ci-dessus pour les simuler par d'autres portes qui, elles, sont implantées. Par exemple, dans les ordinateurs quantiques proposés par IBM en cloud computing [3], les portes de type *SWAP* ne sont pas implantées et le compilateur doit remplacer chacune de ces portes par trois portes de type *CNOT* en utilisant la formule (1.80).

Figure 1.7 Trois équivalences classiques de circuits.

$SWAP =$  (1.81)

$CNOT =$  (1.82)

$CZ =$  (1.83)

Théorèmes d'universalité

Les portes *CNOT* agissant sur un registre de n qubits (*i.e.* l'ensemble des portes $X_{[i:j]}$ pour $i, j = 0 \ldots, n-1$) sont d'une grande importance dans le calcul quantique. En effet, ces portes associées aux portes unaires constituent un ensemble de portes universelles pour le calcul quantique : toute transformation unitaire de $\mathcal{H}^{\otimes n}$ peut s'exprimer comme le produit d'un nombre fini de telles portes (voir [71] et [148, section 4.5.2]).

À partir de ce résultat, on peut démontrer que tout opérateur unitaire agissant sur un registre de n qubits peut être approché avec une erreur aussi petite que souhaitée par un produit de portes choisies dans l'ensemble $\{X_{[i:j]}, H_i, P_i, T_i\} \mid 0 \leqslant i, j < n\}$ [35].

L'erreur réalisée quand on remplace un opérateur unitaire U par un opérateur unitaire V, est définie par :

$$E(U,V) = \max_{|\psi\rangle} ||(U-V)\,|\psi\rangle\,|| \tag{1.84}$$

où le maximum est pris sur l'ensemble des vecteurs normalisés de $\mathcal{H}^{\otimes n}$. Pour résumer cela on dit que l'ensemble des portes $\{CNOT, H, P, T\}$ est universel pour le calcul quantique (voir [148, section 4.5.3]). L'avantage d'utiliser un nombre fini de portes différentes dans les circuits quantiques est qu'il est possible d'implanter ces portes de façon à résister aux erreurs (*fault tolerant quantum computing* en anglais, voir par exemple [148, section 10.6]). Notez qu'on peut remplacer les portes $CNOT$ par les portes CZ en raison de l'identité (1.79). D'autre part, les portes de phase (portes P) ne sont pas indispensables car $T^2 = P$. Généralement, on les inclut dans l'ensemble des portes universelles car l'ensemble $\{CNOT, H, P\}$ en constitue un sous-ensemble important appelé *portes de Clifford*. Cet ensemble sera étudié en détail au chapitre 4. On dit souvent que l'ensemble *Clifford + T* est universel pour le calcul quantique.

Pour terminer cette description des circuits quantiques, soulignons le fait que d'autres portes qui ne sont ni unaires, ni binaires sont également souvent utilisées. Ainsi en est-il des portes *multi-contrôlées* telle la porte de Tofolli qui est une porte NOT contrôlée par deux qubits ou bien des portes contrôlées dont la cible agit sur plusieurs qubits telle la porte de Fredkin qui est une porte $SWAP$ contrôlée par un qubit (voir [148, section 4.3] pour plus de précisions). Nous n'utiliserons pas ces portes dans ce mémoire.

Enfin, il convient de signaler que le formalisme des circuits quantiques n'est pas la seule façon de décrire la suite des opérations appliquées à un système quantique. Ainsi le calcul ZX (*ZX-calculus* en anglais) se présente comme un autre langage graphique dans lequel ces opérations sont représentées par des nœuds d'un graphe appelé *diagramme ZX*. Ces diagrammes sont munis de règles de réécriture permettant d'effectuer les différentes opérations directement dans le langage graphique [57, 110, 111].

1.3.2 Implantation des circuits quantiques

Ordinateurs quantiques

L'idée d'utiliser un ordinateur basé sur les principes de la mécanique quantique a été initialement suggérée par Feynman en 1982 [78]. Il remarque qu'il y a des difficultés fondamentales à simuler un système quantique sur un ordinateur classique en raison de l'explosion des ressources nécessaires et se demande s'il serait possible d'utiliser un ordinateur quantique afin de contourner ces difficultés. Depuis lors, différentes solutions techniques ont été proposées pour implémenter le qubit dans une machine quantique. Parmi les principales, citons : ions piégés [52], résonance magnétique nucléaire [84], spin nucléaire [70], spin d'un électron dans une boîte quantique (quantum dot) [126], circuit supraconducteur et jonctions de Josephson [144], ordinateur photonique (ou optique) [118] (voir [148, chapitre 7]) pour plus de détails).

Cependant, quarante ans plus tard, un ordinateur quantique fonctionnel n'est toujours pas construit même si de nombreux prototypes expérimentaux existent. L'un des principaux obstacles techniques est la décohérence : plus le nombre de qubits augmente plus le risque d'interaction avec l'environnement est élevé et ces interactions agissent sur le système comme des observateurs involontaires, modifiant son état et détruisant tout ou partie de la superposition. De plus, un équilibre subtil est à trouver car les qubits doivent être assez isolés pour limiter la décohérence mais aussi suffisamment accessibles pour pouvoir être manipulés (voir [148, p. 278]).

Actuellement deux technologies semblent se détacher du lot car elles offrent des perspectives de miniaturisation et donc un passage à l'échelle moins problématique (voir par exemple [147] : les circuits supraconducteurs à base de jonctions de Josephson choisis par de grandes entreprises comme IBM ou Google [168] et les spins d'électrons piégés dans le silicium [149, 181] qui ont la faveur d'Intel. En France, dans le cadre du PEPR Quantique, le CEA, l'INRIA et le CNRS mènent des recherches conjointes sur ces deux technologies au travers des projets *PRESQUILE* et *RobustSuperQ* [65].

Signalons qu'il existe des approches théoriques plus originales comme celle de l'ordinateur quantique topologique proposé par Kitaev [79]. Cet ordinateur semble être est le candidat idéal pour résister au bruit car il est basé sur l'utilisation de particules appelées *anyons non-abélien* dont l'état quantique n'est pas affecté par des perturbations locales. Cependant l'existence de ces particules reste théorique car elles n'ont encore jamais été observées.

Architecture et compilation

Du point de vue de l'informaticien, parmi les caractéristiques techniques essentielles des ordinateurs quantiques actuels, on peut citer :

- le nombre maximum de qubits autorisés pour un calcul,
- Les portes natives, c'est à dire les portes quantiques directement implantées par les physiciens dans cette machine,
- La topologie du réseau des qubits, c'est à dire les différentes interactions permises entre les qubits.
- Les indicateurs de fiabilité comme les taux d'erreurs sur les portes quantiques, sur les mesures et le temps de décohérence des qubits.

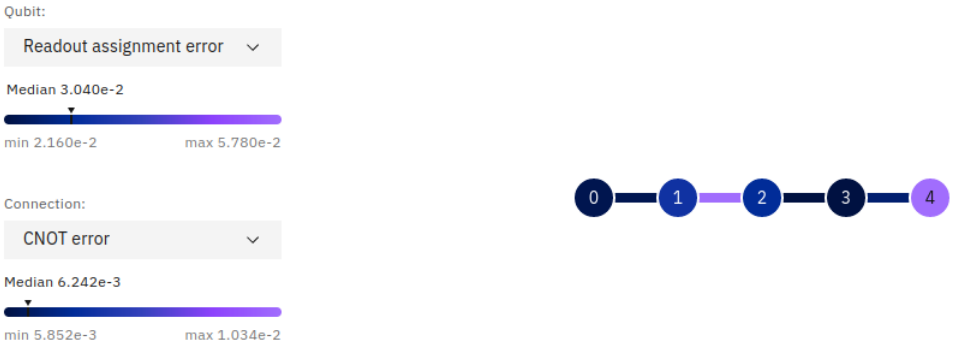
Les interactions permises entre les qubits sont données sous la forme d'un graphe appelé parfois *graphe de connectivité*, dont les sommets sont étiquetés par les qubits et les arêtes sont les paires de qubits qui peuvent interagir au moyen d'une porte binaire native, généralement une porte *CNOT* ou une porte *CZ* (voir exemple figure 1.8). Dans une machine où toutes les paires de qubits peuvent interagir, la topologie est qualifiée de *complète* (voir par exemple [180] et [160]). À l'opposé, si le graphe de connectivité G est en ligne (*i.e.* $G = \{\{0,1\},\{1,2\},\ldots,\{n-2,n-1\}\}$) on dit que la topologie est LNN (*Linear Nearest Neighbour*) [15, 183]. Dans ce cas seules les interactions entre deux qubits consécutifs sont possibles. Entre ces deux configurations extrêmes, il existe différentes topologies intermédiaires comme celles des machines quantiques d'IBM [3].

Toutes les portes d'un circuit quantique donné ne sont pas nécessairement des portes natives de l'ordinateur dans lequel on souhaite implanter ce circuit. Une porte qui n'est pas native doit pouvoir être simulée au moyen de portes natives. Par exemple, dans les ordinateurs quantiques d'IBM, la porte de Hadamard n'est pas native et doit être simulée en utilisant deux portes de rotations $R_z(\pi/2)$ et la porte $\sqrt{X}$ au moyen de l'identité $H = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}} R_z(\pi/2)\sqrt{X}R_z(\pi/2)$, avec $\sqrt{X} = \frac{1}{2}\begin{bmatrix} 1+\mathrm{i} & 1-\mathrm{i} \\ 1-\mathrm{i} & 1+\mathrm{i} \end{bmatrix}$. De même pour les portes *CZ* qui sont simulées grâce à l'identité (1.79).

La compilation dans les ordinateurs quantiques est le processus qui consiste à réécrire un circuit quantique à l'aide de portes natives dans l'architecture cible. Sur les

Figure 1.8 Graphes de connectivité de deux ordinateurs quantiques IBM.

Ordinateur ibmq-oslo, 7 qubits



Ordinateur ibmq-manila, 5 qubits, topologie LNN

ordinateurs d'IBM, ce processus est qualifié de *transpilation*. Nous verrons aux chapitres 2, 3 et 5 quelques exemples de circuits compilés sur ces ordinateurs. Selon le circuit à compiler et l'architecture de la machine, la différence de longueur entre le circuit compilé et le circuit avant compilation peut être importante. Cette inflation éventuelle du nombre de portes à la compilation est pénalisante en terme de fiabilité du calcul en raison du taux d'erreur des portes quantiques : actuellement les portes quantiques ne sont pas complètement fiables (voir exemple table 2.1) et la probabilité d'erreur d'un calcul augmente rapidement avec le nombre de portes d'un circuit.

Pour terminer cette introduction aux circuits quantiques, il convient de mentionner que des langages de programmation adaptés à l'informatique quantique ont été introduits parallèlement à l'apparition des premiers ordinateurs quantiques expérimentaux. On peut citer notamment Qiskit qui est un module Python développé autour des machines IBM permettant d'écrire, de compiler de d'exécuter des programmes [61]. Pour plus d'information sur ce sujet, on pourra par exemple consulter la thèse de De Boutray [62, Chapitre 2] ou bien [58].

1.4 Conclusion et perspectives

La phase actuelle de développement des ordinateurs quantiques a été qualifiée d'ère *NISQ* (*Noisy Intermediate Scale Quantum era*) par John Preskill en 2018. Cette ère est

caractérisée par des taux d'erreurs sur les portes qui restent importants, des temps de décohérence trop rapides et des processeurs comportant un trop petit nombre de qubits [158].

La solution proposée pour remédier aux erreurs est une approche basée sur les codes quantiques correcteurs d'erreurs qui permettent de lutter contre les erreurs de calcul provenant des portes ou contre les effets de la décohérence (voir par exemple un article tutoriel de Gottesman [88]). Il s'agit d'un champ de recherche initié par Calderbank, Shor et Steane (codes CSS [165, 167, 45]) qui continue d'être l'objet de nombreux travaux. Ces deux dernières années, des avancées importantes ont été réalisées dans ce domaine [153, 124, 123] (voir la page de l'INRIA [105] qui fait le point sur ce sujet).

Cependant, pour donner un ordre de grandeur, on estime qu'il faudrait entre 1 000 et 10 000 qubits physiques pour implanter un qubit logique de façon à corriger les erreurs [147, p. 41]. Bien que ces exigences soient encore loin d'être réalisées, elles ne sont pas nécessairement hors d'atteinte car les progrès actuels du matériel sont rapides. Ainsi Google, tout comme IBM, annoncent des processeurs à un million de qubits avant 2030.

En attendant la fin de l'ère NISQ et le début d'une nouvelle ère de l'informatique quantique, on peut simuler le calcul quantique au moyen de supercalculateurs classiques mais les possibilités sont limitées par l'importance des ressources en espace et en temps nécessaires : les meilleures machines actuelles telles la *Quantum Learning Machine* d'ATOS [152] plafonnent à 41 qubits et on estime la frontière des 50 qubits hors de portée de la simulation [158].

Dans l'optique de réduire le bruit dans les circuits quantiques, une approche complémentaire à celle des codes correcteurs d'erreurs est celle des techniques d'optimisation de circuit. Il s'agit de déterminer un circuit équivalent à un circuit donné qui contienne moins de portes. A l'instar des codes correcteurs d'erreurs, le problème de l'optimisation des circuits quantiques est un sujet central qui a fait l'objet de nombreuses recherches. En raison des théorèmes d'universalité mentionnés à la section 1.3.1, la plupart des résultats obtenus sont centrés sur l'optimisation de circuits formés par les portes de l'ensemble universel $\{CNOT, H, P, T\}$, citons par exemple [7, 8, 184]. Certains travaux utilisent le formalisme du ZX-calcul [73, 114] et d'autres incluent, en plus de l'ensemble Clifford + T, des portes de rotations $R_z\theta$ [145].

Une partie des résultats présentés dans ce mémoire concerne l'optimisation des circuits. Malgré cela, nos résultats ne sont pas vraiment dans le prolongement des travaux que nous venons de citer dans la mesure où nous ne proposons pas de méthodes générales d'optimisation des circuits Clifford + T. Il s'agit plus modestement de quelques méthodes traitant de circuits particuliers formés de portes de Clifford. Ces méthodes reposent essentiellement sur la structure de groupe de ces circuits. Dans le chapitre suivant nous commençons par nous intéresser aux circuits composés de portes $CNOT$.

Chapitre 2

Circuits quantiques composés de portes *CNOT*

Ce chapitre est consacré à l'étude des circuits quantiques composés exclusivement de portes *CNOT*. On présente quelques résultats concernant la structure algébrique de ce type de circuit et on montre comment ces résultats peuvent s'appliquer à des problèmes d'optimisation et de réduction de circuits.

Les portes *CNOT* sont omniprésentes en informatique quantique, en particulier en raison des théorèmes d'universalité mentionnés à la section 1.3.1) du chapitre 1 : on peut approcher avec une précision arbitraire n'importe quel opérateur unitaire par un circuit quantique composé uniquement des portes *CNOT*, Hadamard, Phase et de la porte T. Ainsi toutes les portes binaires peuvent être implantés à l'aide de la porte *CNOT* et de quelques portes unaires (voir exemples figure 1.7).

Les portes *CNOT* apparaissent également dans une classe importante de circuits que nous traitons en détail au chapitre 4 : les circuits stabilisateurs. Ces circuits sont engendrés par un sous-ensemble de l'ensemble des portes universelles qu'on appelle l'ensemble des portes de Clifford. Cet ensemble est obtenu en retirant la porte T à l'ensemble des portes universelles. Les circuits stabilisateurs (ou circuits de Clifford) possèdent des *formes normales*, c'est à dire des circuits équivalents ayant une forme simple et une longueur bornée. Ces formes normales comportent des sous-circuits composés uniquement de portes *CNOT*. En raison du taux d'erreur des portes *CNOT* dans les ordinateurs quantiques actuels (voir par exemple la table 2.1), il peut être utile de disposer de méthodes pour optimiser ou réduire le nombre de portes *CNOT* utilisées dans ces sous-circuits.

La correspondance entre les circuits de portes *CNOT* agissant sur un système de n qubits et les matrices inversibles $n \times n$ à coefficients dans $\mathbb{F}_2$ n'est pas une idée nouvelle, même si nous l'avons redécouverte indépendamment. Elle apparaît par exemple dans un papier de Patel, Markov et Hayes datant de 2004 [154]. Nous l'avons formalisée en terme d'isomorphisme et de présentation de groupe dans la section 2.2. Nous appliquons ensuite ce formalisme à des questions liées à l'optimisation ou à la réduction de circuits. Ainsi, dans la section 2.3.3, nous donnons un algorithme d'optimisation pour les circuits agissant sur un petit nombre de qubits. Enfin, la section 2.4 est consacrée à l'étude d'un cas particulier de circuit. La plupart des résultats de ce chapitre sont tirés du papier [19].

Table 2.1 Taux d'erreur des portes *CNOT* agissant sur les qubits i et j, avec $i, j \in \{0, 1, 2, 3, 4\}$. Les données proviennent de l'ordinateur quantique ibmq-manila (19 février 2023) et sont disponibles au public à l'adresse [3].

$X_{[i:j]}$	0	1	2	3	4
0		$6{,}226 \times 10^{-3}$			
1	$6{,}226 \times 10^{-3}$		$1{,}162 \times 10^{-2}$		
2		$1{,}162 \times 10^{-2}$		$6{,}746 \times 10^{-3}$	
3			$6{,}746 \times 10^{-3}$		$1{,}242 \times 10^{-2}$
4				$1{,}242 \times 10^{-2}$	

2.1 Propriétés des portes *CNOT* et *SWAP* et application à leur implantation

2.1.1 Propriétés algébriques des portes *CNOT* et *SWAP*

Pour tout entier $n \geqslant 2$, le sous-groupe du groupe unitaire engendré par l'ensemble des matrices $X_{[i:j]}$ sera noté $\langle CNOT \rangle_n$et le groupe engendré par les portes $S_{(i\ j)}$ sera noté $\langle SWAP \rangle_n$.

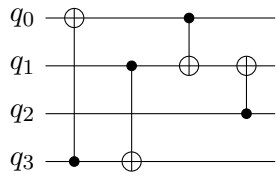
$$\langle CNOT \rangle_n = \left\langle X_{[i:j]} \mid 0 \leqslant i, j < n, i \neq j \right\rangle \tag{2.1}$$

$$\langle SWAP \rangle_n = \left\langle S_{(i\ j)} \mid 0 \leqslant i, j < n, i \neq j \right\rangle \tag{2.2}$$

La figure 2.1 montre un élément du groupe $\langle CNOT \rangle_4$ et un circuit le représentant.

Figure 2.1 Un opérateur du groupe $\langle CNOT \rangle_4$ et un circuit de portes *CNOT* représentant cet opérateur.

$X_{[1:2]}X_{[1:0]}X_{[3:1]}X_{[0:3]}$:

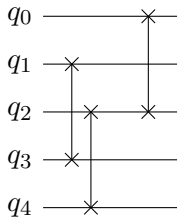


Le groupe symétrique $\mathfrak{S}_n$ étant engendré par les transpositions, il est clair que le groupe $\langle SWAP \rangle_n$ lui est isomorphe, la porte $S_{(i\ j)}$ correspondant à la transposition $(i\ j)$. De plus l'identité (1.80) implique que $\langle SWAP \rangle_n$ est un sous-groupe de $\langle CNOT \rangle_n$. Étant donné une permutation $\sigma \in \mathfrak{S}_n$, on notera S_σ l'opérateur unitaire de $\langle SWAP \rangle_n$ associé à σ par cet isomorphisme (voir exemple figure 2.2). Ainsi on peut penser l'opérateur S_σ comme étant n'importe quel circuit de portes *SWAP* tel que la permutation σ soit égale au produit des transpositions associées à chaque porte *SWAP*. On peut alors généraliser l'identité (1.74) à n'importe quel circuit de portes *SWAP* et on obtient :

$$S_\sigma \left| b_0 b_1 \cdots b_{n-1} \right\rangle = \left| b_{\sigma^{-1}(0)} b_{\sigma^{-1}(1)} \cdots b_{\sigma^{-1}(n-1)} \right\rangle . \tag{2.3}$$

Figure 2.2 Une permutation de $\mathfrak{S}_5$, l'opérateur de $\langle SWAP\rangle_5$ associé et un circuit quantique de portes *SWAP* représentant cet opérateur.

$$\sigma = (0\ 2\ 4)(1\ \ 3) \qquad S_\sigma = S_{(0\ \ 2)}S_{(2\ \ 4)}S_{(1\ \ 3)}$$



Proposition 2.1. *Les portes $X_{[i:j]}$ vérifient les identités suivantes.*

$$\textit{Involution : } X_{[i:j]}^2 = I \tag{2.4}$$

$$\textit{Commutativité : } (X_{[i:j]}X_{[k:\ell]})^2 = I \quad \textit{si } i \neq \ell \textit{ et } j \neq k \tag{2.5}$$

$$\textit{Relation de Chasles quadratique : } (X_{[i:j]}X_{[j:k]})^2 = (X_{[j:k]}X_{[i:j]})^2 = X_{[i:k]}, \quad i,j,k \textit{ distincts} \tag{2.6}$$

Démonstration. On prouve chaque identité $A = B$ en montrant que les actions des opérateurs A et B sur un vecteur $|b_0 \cdots b_{n-1}\rangle$ de la base standard sont les mêmes. On utilise pour cela l'identité (1.69). □

En utilisant les identités de la proposition 2.1, on obtient directement les relations de conjugaison dans le groupe $\langle CNOT\rangle_n$.

$$X_{[i:j]}X_{[j:k]}X_{[i:j]} = X_{[j:k]}X_{[i:k]} = X_{[i:k]}X_{[j:k]} \tag{2.7}$$

$$X_{[i:j]}X_{[k:i]}X_{[i:j]} = X_{[k:i]}X_{[k:j]} = X_{[k:j]}X_{[k:i]} \tag{2.8}$$

L'action du groupe $\langle SWAP\rangle_n$ sur le groupe $\langle CNOT\rangle_n$ par conjugaison est donnée par la proposition suivante.

Proposition 2.2. *Étant donné une permutation $\sigma \in \mathfrak{S}_n$ et deux entiers distincts i et j, on a :*

$$S_\sigma X_{[i:j]} S_\sigma^{-1} = X_{[\sigma(i):\sigma(j)]}. \tag{2.9}$$

Démonstration. Comme les transpositions engendrent le groupe symétrique [1], il suffit de prouver l'identité (2.9) dans le cas où σ est une transposition, c'est à dire quand $S_\sigma = S_{(k\ \ \ell)} = X_{[k:\ell]}X_{[\ell:k]}X_{[k:\ell]}$ pour deux entiers ℓ et k. On utilise alors les identités (1.80), (2.4), (2.5), (2.7) et (2.8). □

On remarque que l'identité (1.80) peut être généralisée comme suit.

Proposition 2.3. *Soit $\sigma \in \mathfrak{S}_n$ une permutation de type cyclique $\lambda = (n_1, \ldots, n_p)$ [2]. Tout circuit de portes SWAP agissant sur n qubits et représentant l'opérateur unitaire S_σ admet un circuit équivalent comportant $3(n-p)$ portes CNOT.*

1. Voir annexe A, théorème A.39
2. Voir annexe A, section A.4.3.

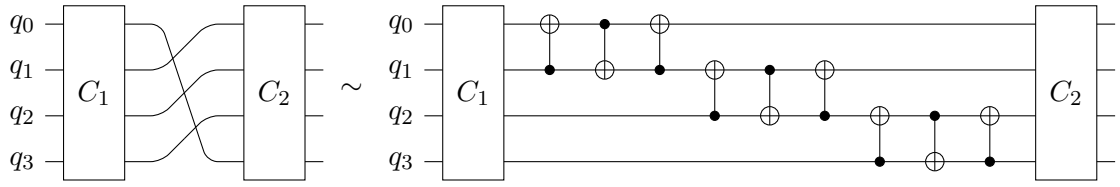
Démonstration. Soit $\sigma \in \mathfrak{S}_n$ une permutation de type cyclique $\lambda = (n_1, \ldots, n_p)$. On sait que σ se décompose en p cycles et que $\sum_{i=1}^{p} n_i = n$. Or un cycle $(j_1 \ldots j_\ell)$ de longueur ℓ peut être décomposé en un produit de $\ell - 1$ transpositions sous la forme

$$(j_1 \ldots j_\ell) = (j_1 \;\; j_2) \ldots (j_{\ell-1} \;\; j_\ell). \tag{2.10}$$

Donc σ se décompose en un produit de $\sum_{i=1}^{p}(n_i - 1) = n - p$ transpositions. L'opérateur unitaire S_σ peut donc être représenté par un circuit comportant $n - p$ portes *SWAP*. Comme chaque porte *SWAP* peut s'écrire avec 3 portes *CNOT* d'après (1.80), on a bien le résultat annoncé. □

La figure 2.3 illustre la proposition 2.3 dans le cas d'une permutation cyclique de 4 qubits.

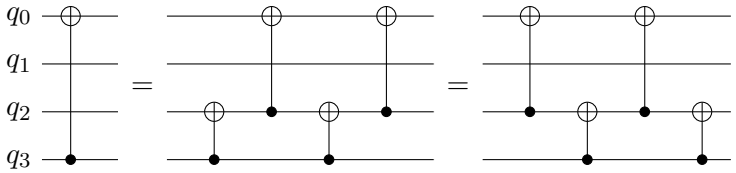
Figure 2.3 Une permutation cyclique des qubits entre deux circuits C_1 et C_2.



$$\sigma = (3\ 2\ 1\ 0) = (2\ \ 3)(1\ \ 2)(0\ \ 1), \quad S_\sigma = S_{(2\ \ 3)} S_{(1\ \ 2)} S_{(0\ \ 1)}$$

L'identité (2.6) porte sur 3 entiers distincts i, j, k. Elle met donc en jeu des portes *CNOT* qui interagissent avec 3 qubits particuliers d'un circuit quantique agissant sur n qubits (voir figure 2.4).

Figure 2.4 Utilisation de l'identité (2.6) sur un circuit du groupe $\langle CNOT \rangle_4$.



$$X_{[0:3]} = X_{[0:2]} X_{[2:3]} X_{[0:2]} X_{[2:3]} = X_{[2:3]} X_{[0:2]} X_{[2:3]} X_{[0:2]}$$

On remarque qu'il est possible de généraliser l'identité (2.6) à un nombre arbitraire de qubits. C'est l'objet de la proposition suivante.

Proposition 2.4. *Soit un système de n qubits, un entier p tel que $3 \leqslant p \leqslant n$ et $i_1, i_2, \ldots, i_p$ des entiers distincts. On a*

$$X_{[i_1:i_p]} = \left(X_{[i_1:i_2]} X_{[i_2:i_3]} \ldots X_{[i_{p-2}:i_{p-1}]} X_{[i_{p-1}:i_p]} X_{[i_{p-2}:i_{p-1}]} \ldots X_{[i_2:i_3]} \right)^2. \tag{2.11}$$

Démonstration. La preuve s'effectue par induction sur p. Le cas de base ($p = 3$) correspond simplement à l'identité (2.6). Effectuons un pas d'induction. Soient $p \geqslant 3$ et $p + 1$ entiers distincts $i_1, \ldots, i_{p+1}$. Par hypothèse de récurrence appliquée à $i_1, \ldots, i_{p-1}, i_{p+1}$ on a

$$X_{[i_1:i_{p+1}]} = \left(X_{[i_1:i_2]} X_{[i_2:i_3]} \ldots X_{[i_{p-2}:i_{p-1}]} X_{[i_{p-1}:i_{p+1}]} X_{[i_{p-2}:i_{p-1}]} \ldots X_{[i_2:i_3]} \right)^2.$$

Or, d'après l'identité (2.6), on a

$$X_{[i_{p-1}:i_{p+1}]} = X_{[i_{p-1}:i_p]} X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_p]} X_{[i_p:i_{p+1}]}$$

et $X_{[i_p:i_{p+1}]}$ commute avec $X_{[i_{p-2}:i_{p-1}]} \dots X_{[i_2:i_3]}$ d'après (2.5), donc

$$X_{[i_1:i_{p+1}]} = \left(X_{[i_1:i_2]} X_{[i_2:i_3]} \dots X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_p]} X_{[i_{p-2}:i_{p-1}]} \dots X_{[i_2:i_3]} X_{[i_p:i_{p+1}]} \right)^2.$$

En posant

$$R_1 = X_{[i_1:i_2]} X_{[i_2:i_3]} \dots X_{[i_{p-2}:i_{p-1}]} X_{[i_{p-1}:i_p]} X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_p]} X_{[i_{p-2}:i_{p-1}]} \dots X_{[i_2:i_3]}$$

on a donc

$$X_{[i_1:i_{p+1}]} = R_1 X_{[i_p:i_{p+1}]} R_1 X_{[i_p:i_{p+1}]}. \tag{2.12}$$

En utilisant à nouveau l'identité (2.5), on fait commuter les deux portes $X_{[i_p:i_{p+1}]}$ avec $X_{[i_1:i_2]}, X_{[i_2:i_3]}, \dots, X_{[i_{p-2}:i_{p-1}]}$ dans l'expression $X_{[i_p:i_{p+1}]} R_1 X_{[i_p:i_{p+1}]}$ et en posant

$$R_2 = X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_p]} X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_p]} X_{[i_p:i_{p+1}]}$$

il vient

$$X_{[i_p:i_{p+1}]} R_1 X_{[i_p:i_{p+1}]} = X_{[i_1:i_2]} X_{[i_2:i_3]} \dots X_{[i_{p-2}:i_{p-1}]} R_2 X_{[i_{p-2}:i_{p-1}]} \dots X_{[i_2:i_3]}. \tag{2.13}$$

Or, d'après (2.6), on a $R_2 = X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_{p+1}]}$ et en utilisant l'identité de conjugaison (2.7), il vient $R_2 = X_{[i_{p-1}:i_p]} X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_p]}$. En reportant ce résultat dans (2.13) on obtient

$$X_{[i_p:i_{p+1}]} R_1 X_{[i_p:i_{p+1}]} = X_{[i_1:i_2]} X_{[i_2:i_3]} \dots X_{[i_p:i_{p+1}]} X_{[i_{p-1}:i_p]} \dots X_{[i_2:i_3]} = R_1$$

donc, d'après (2.12), on a $X_{[i_1:i_{p+1}]} = R_1^2$ ce qui termine le pas d'induction. □

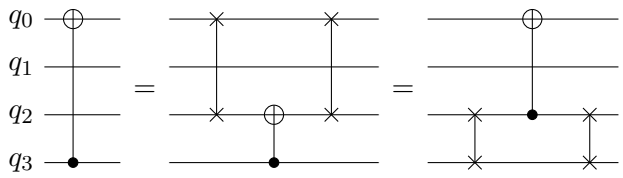
2.1.2 Implantation d'une porte *CNOT* dans un ordinateur quantique

Nous présentons ici quelques applications pratiques des propriétés établies dans la sous-section 2.1.1. Nous montrons sur un exemple comment ces propriétés permettent d'expliquer l'implantation des portes *CNOT* dans les machines quantiques d'IBM et nous proposons une utilisation pratique de la proposition 2.4.

La proposition 2.4 fournit directement une méthode simple pour adapter n'importe quelle porte *CNOT* aux contraintes de connectivité des qubits d'un ordinateur quantique. Ces contraintes sont représentées par un graphe dont les sommets sont étiquetés par les numéros des qubits. Il existe une arête $\{i, j\}$ entre deux sommets i et j si on peut faire interagir directement les qubits i et j pour exécuter une opération $X_{[i:j]}$ ou $X_{[j:i]}$ sur le système. On dira alors que les portes $X_{[i:j]}$ et $X_{[j:i]}$ sont natives.

Pour implanter une porte *CNOT* qui n'est pas native, une méthode courante est d'utiliser la formule de conjugaison (2.9) d'une porte *CNOT* par des portes *SWAP*. Par exemple le circuit de la figure 2.5 peut être vu comme une implantation de la porte *CNOT* non native $X_{[0:3]}$ dans une machine quantique où les portes $X_{[2:3]}$ et $X_{[0:2]}$ sont natives. Cependant, si chaque porte *SWAP* est implantée en utilisant trois portes *CNOT* au moyen de la relation de tresse (1.80) (c'est par exemple le cas sur les machines quantiques d'IBM), on peut utiliser moins de portes *CNOT* en utilisant la relation (2.11) au lieu de la relation (2.9). En effet supposons que l'on souhaite implanter la porte non native $X_{[i:j]}$. A cette fin, considérons un chemin $(i_1 = i, \dots, i_p = j)$ entre les

Figure 2.5 Utilisation de l'identité (2.9) sur un circuit de $\langle CNOT \rangle_4$.



$$X_{[0:3]} = S_{(0\ \ 2)} X_{[2:3]} S_{(0\ \ 2)} = S_{(2\ \ 3)} X_{[0:2]} S_{(2\ \ 3)}$$

qubits i et j (dans la pratique on utilise un chemin qui minimise les taux d'erreurs des portes $CNOT$). Une implantation de la porte $X_{[i:j]}$ basée sur l'identité (2.9) s'écrit

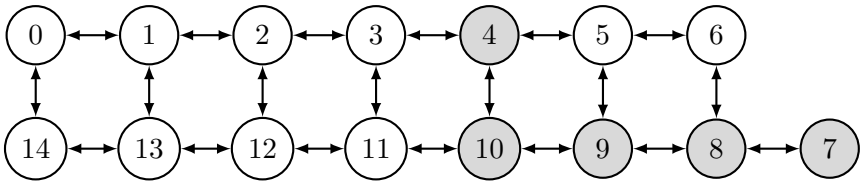
$$X_{[i:j]} = S_{(i_1\ \ i_2)} S_{(i_2\ \ i_3)} \dots S_{(i_{p-2}\ \ i_{p-1})} X_{[i_{p-1}:i_p]} \left(S_{(i_1\ \ i_2)} S_{(i_2\ \ i_3)} \dots S_{(i_{p-2}\ \ i_{p-1})} \right)^{-1}, \tag{2.14}$$

tandis qu'en utilisant l'identité (2.11) on obtient

$$X_{[i:j]} = \left(X_{[i_1:i_2]} X_{[i_2:i_3]} \dots X_{[i_{p-2}:i_{p-1}]} X_{[i_{p-1}:i_p]} X_{[i_{p-2}:i_{p-1}]} \dots X_{[i_2:i_3]} \right)^2. \tag{2.15}$$

Dans la première implantation on utilise un total de $(6p-11)$ portes $CNOT$ (on utilise 3 portes $CNOT$ pour chaque $SWAP$) alors que dans la seconde implantation le total est de $(4p-8)$ portes $CNOT$ (voir exemple figure 2.6).

Figure 2.6 Implantation de la porte $X_{[4:7]}$ dans l'ordinateur quantique de 15 qubits ibmq-16-melbourne.



Chemin choisi pour implanter $X_{[4:7]}$: $(4, 10, 9, 8, 7)$.

Implantation utilisant des portes $SWAP$ et l'identité (2.9) :

$$X_{[4:7]} = S_{(4\ \ 10)} S_{(10\ \ 9)} S_{(9\ \ 8)} X_{[8:7]} S_{(9\ \ 8)} S_{(10\ \ 9)} S_{(4\ \ 10)}$$

Implantation utilisant des portes $CNOT$ et l'identité (2.11) :

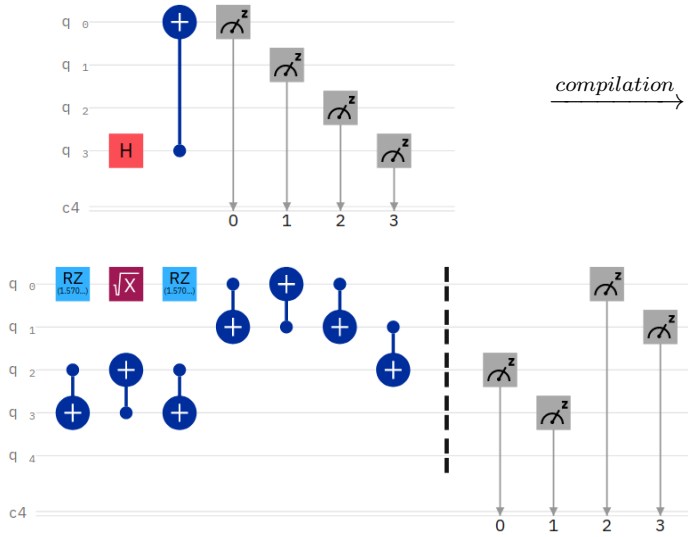
$$X_{[4:7]} = \left(X_{[4:10]} X_{[10:9]} X_{[9:8]} X_{[8:7]} X_{[9:8]} X_{[10:9]} \right)^2$$

Remarque 2.5. Si la porte $CNOT$ à implanter est située en fin de circuit juste avant d'effectuer les mesures, alors une implantation basée sur la conjugaison par des portes $SWAP$ peut être préférable à une solution basée sur l'identité (2.11). En effet, on peut dans ce cas éliminer les portes $SWAP$ qui sont situées juste avant les mesures et les remplacer par un post-traitement qui applique la permutation définie par ces portes $SWAP$ directement sur les résultats des mesures. Plus précisément, soit S_σ un circuit de portes $SWAP$ suivi par des mesures des n qubits tel que les résultats des mesures soient n bits d'un registre classique $R = c_0 \dots c_{n-1}$. On a $S_\sigma |b_0 \dots b_{n-1}\rangle = |b_{\sigma^{-1}(0)} \dots b_{\sigma^{-1}(n-1)}\rangle$ donc le bit c_i du registre R a pour valeur $b_{\sigma^{-1}(i)}$, autrement dit la valeur b_i est celle du

bit $c_{\sigma(i)}$ du registre R. On peut donc se passer des portes *SWAP* et mettre directement le résultat de la mesure du qubit i dans le bit $c_{\sigma(i)}$ du registre. Ce type d'optimisation est pratiqué par les compilateurs des ordinateurs quantiques d'IBM (voir exemple figure 2.7).

Figure 2.7 Compilation d'une porte *CNOT* dans l'ordinateur quantique d'IBM ibmq-bogota

Graphe de connectivité LNN : $\{\{0,1\},\{1,2\},\{2,3\},\{3,4\}\}$



Soit $|\psi\rangle = X_{[0:3]}H_3\,|0000\rangle$, on a :

$$|\psi\rangle = S_{(1\ 3)}S_{(0\ 2)}X_{[2:1]}S_{(0\ 2)}S_{(1\ 3)}H_3\,|0000\rangle$$
$$|\psi\rangle = S_{(1\ 3)}S_{(0\ 2)}X_{[2:1]}S_{(0\ 2)}S_{(1\ 3)}S_{(0\ 3)}S_{(1\ 2)}H_0S_{(1\ 2)}S_{(0\ 3)}\,|0000\rangle$$
$$|\psi\rangle = S_{(1\ 3)}S_{(0\ 2)}X_{[2:1]}S_{(2\ 3)}S_{(0\ 1)}H_0\,|0000\rangle$$

Les portes $S_{(1\ 3)}$ et $S_{(0\ 2)}$ en fin de circuit sont éliminées et remplacées par une permutation des valeurs du registre classique de 4 bits c_4.

2.2 Structure du groupe engendré par les portes *CNOT*

2.2.1 Isomorphisme avec un groupe classique

Notons $\mathrm{SL}_n(K)$ le groupe spécial linéaire sur un corps K. Soient deux entiers i et j tels que $0 \leqslant i, j \leqslant n-1$ et soit E_{ij} la matrice dont toutes les entrées sont nulles sauf l'entrée (i,j) qui est égale à 1. Pour $a \in K \setminus \{0\}$ et $i \neq j$, on pose :

$$T_{i,j}(a) = I + aE_{ij}. \tag{2.16}$$

Soit $(e_k)_{0\leqslant k<n}$ la base canonique de l'espace vectoriel K^n et $(e_k^*)_{0\leqslant k<n}$ sa base duale. Alors la matrice $T_{i,j}(a)$ représente dans cette base l'automorphisme $t_{i,j}(a) : u \to u + ae_j^*(u)e_i$ de K^n. Cet automorphisme est la *transvection* dirigée par la droite $\langle e_i\rangle$ qui fixe l'hyperplan $\langle e_k \mid k \neq j\rangle$. Ainsi les matrices $T_{i,j}(a)$ sont des matrices de transvection et il est bien connu que ces matrices engendrent le groupe $\mathrm{SL}_n(K)$. Une manière classique

de déterminer une décomposition d'une matrice de $\mathrm{SL}_n(K)$ en produit de transvections est d'appliquer la méthode d'élimination de Gauss-Jordan à cette matrice [5]. Cet algorithme est souvent utilisé pour calculer l'inverse d'une matrice mais il donne par la même occasion une décomposition en transvections de cette matrice.

Si $K = \mathbb{F}_2$ alors l'ensemble $\{T_{i,j}(a) \mid a \in K \setminus \{0\}\}$ se réduit aux $n(n-1)$ matrices $I + E_{ij}$ et on pose :

$$[i : j] = I + E_{ij}. \tag{2.17}$$

Comme toute matrice inversible à coefficients dans $\mathbb{F}_2$ a son déterminant égal à 1, alors les matrices $[i : j]$ engendrent le groupe linéaire $\mathrm{GL}_n(\mathbb{F}_2)$:

$$\mathrm{GL}_n(\mathbb{F}_2) = \langle [i : j] \mid 0 \leqslant i, j < n, i \neq j \rangle \,. \tag{2.18}$$

On rappelle que l'algorithme de Gauss-Jordan est basé sur le résultat suivant.

Proposition 2.6. *Multiplier à gauche (resp. à droite) une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$ par une matrice de transvection $[i : j]$ revient à ajouter la ligne j (resp. la colonne i) de A à sa ligne i (resp. sa colonne j).*

On rappelle également que la matrice de permutation associée à la permutation σ de $\mathfrak{S}_n$ est la matrice à coefficients dans $\mathbb{F}_2$ dont l'entrée (i, j) vaut 1 si et seulement si $\sigma(j) = i$. Par commodité on notera cette matrice de permutation comme la permutation et ainsi $(i\ \ j)$ désignera à la fois une transposition de $\mathfrak{S}_n$ et la matrice de permutation $n \times n$ qui lui est associée. En utilisant ces notations, on vérifie facilement que

$$(i\ \ j) = [i : j][j : i][i : j] = [j : i][i : j][j : i] \tag{2.19}$$

et on déduit de la proposition 2.6 les résultats classiques qui suivent.

Proposition 2.7. *Multiplier à gauche (resp. à droite) une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$ par une matrice de transposition $(i\ \ j)$ revient à échanger les lignes (resp. les colonnes) i et j de A.*

Multiplier à gauche une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$ par une matrice de permutation $\sigma \in \mathrm{GL}_n(\mathbb{F}_2)$ revient à appliquer la permutation σ aux lignes de A, c'est à dire remplacer chaque ligne i de A par la ligne $\sigma^{-1}(i)$.

Multiplier à droite une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$ par une matrice de permutation $\sigma \in \mathrm{GL}_n(\mathbb{F}_2)$ revient à appliquer la permutation σ^{-1} aux colonnes de A, c'est à dire remplacer chaque colonne j de A par la colonne $\sigma(j)$.

On a des résultats similaires à ceux des propositions 2.6 et 2.7, dans le cas d'un vecteur $u \in \mathbb{F}_2^n$:

$$[i : j][u_0 \dots u_i \dots u_j \dots u_{n-1}]^{\mathrm{t}} = [u_0 \dots u_i \oplus u_j \dots u_j \dots u_{n-1}]^{\mathrm{t}} \tag{2.20}$$

$$(i\ \ j)[u_0 \dots u_i \dots u_j \dots u_{n-1}]^{\mathrm{t}} = [u_0 \dots u_j \dots u_i \dots u_{n-1}]^{\mathrm{t}} \tag{2.21}$$

$$\sigma[u_0 \dots u_{n-1}]^{\mathrm{t}} = [u_{\sigma^{-1}(0)} \dots u_{\sigma^{-1}(n-1)}]^{\mathrm{t}} \tag{2.22}$$

En identifiant le vecteur $|b\rangle = |b_0 b_1 \cdots b_{n-1}\rangle$ de l'espace de Hilbert $\mathcal{H}^{\otimes n}$ avec le vecteur $b = [b_0 \dots b_{n-1}]^{\mathrm{t}}$ de $\mathbb{F}_2^n$, les résultats précédents permettent de réécrire les identités (1.69), (1.74) et (2.3) d'une façon plus concise et élégante :

$$X_{[i:j]}\,|b\rangle = |\ [i : j]b\ \rangle \tag{2.23}$$

$$S_{(i\ \ j)}\,|b\rangle = |\ (i\ \ j)b\ \rangle \tag{2.24}$$

$$S_\sigma\,|b\rangle = |\ \sigma b\ \rangle\,. \tag{2.25}$$

Ces différentes considérations nous amènent naturellement au théorème suivant.

Théorème 2.8. *Le groupe $\langle CNOT\rangle_n$ engendré par les portes CNOT agissant sur n qubits est isomorphe*[3] *à $\mathrm{GL}_n(\mathbb{F}_2)$. Le morphisme Φ qui envoie chaque porte $X_{[i:j]}$ sur la transvection $[i:j]$ est un isomorphisme explicite.*

Démonstration. La surjectivité de Φ vient du fait que le groupe $\mathrm{GL}_n(\mathbb{F}_2)$ est engendré par les transvections $[i:j]$. De plus, en utilisant la relation (2.23), on voit qu'un antécédent M par Φ d'une matrice quelconque A de $\mathrm{GL}_n(\mathbb{F}_2)$ doit vérifier la relation $M|b\rangle = |Ab\rangle$ pour tout vecteur de base $|b\rangle$, ce qui définit M de manière unique. Donc Φ est également injectif. □

Remarque 2.9. On note X_A l'antécédent d'une matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ quelconque par le morphisme Φ du théorème 2.8 :

$$\forall A \in \mathrm{GL}_n(\mathbb{F}_2),\ X_A = \Phi^{-1}(A) \tag{2.26}$$

Cette notation explique, a posteriori, la convention que nous avons adoptée au chapitre 1 (section 1.3) en désignant par $X_{[i:j]}$ la porte *CNOT* ayant le qubit i pour cible et le qubit j comme contrôle, choix qui est l'inverse de la convention généralement utilisée dans laquelle le premier indice désigne le contrôle. L'opérateur X_A désigne n'importe quel circuit $X_{[i_1:j_i]} \dots X_{[i_p:j_p]}$ de portes *CNOT* tel que la matrice A puisse s'écrire comme le produit des matrices de transvection $[i_1:j_i], \dots, [i_p:j_p]$. Avec cette notation, l'action de l'opérateur X_A sur un vecteur $|b\rangle$ de la base standard est définie par :

$$X_A|b\rangle = |Ab\rangle\,. \tag{2.27}$$

On remarque également que cette notation permet d'écrire $S_\sigma = X_\sigma$. Cependant on conservera la notation S_σ pour les éléments de $\langle SWAP\rangle_n$ car elle nous semble plus parlante.

Nous utiliserons parfois une notation plus compacte pour la conjugaison d'une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$ par une matrice de permutation σ :

$$A^\sigma = \sigma A \sigma^{-1}. \tag{2.28}$$

En utilisant cette notation et l'isomorphisme Φ, l'identité (2.9) montre que :

$$[i:j]^\sigma = [\sigma(i):\sigma(j)]. \tag{2.29}$$

De plus l'identité (2.9) se généralise en :

$$S_\sigma X_A S_{\sigma^{-1}} = X_{\sigma A \sigma^{-1}} = X_{A^\sigma}. \tag{2.30}$$

L'ordre de $\mathrm{GL}_n(\mathbb{F}_2)$ est bien connu et se calcule facilement : il suffit de compter le nombre de bases de l'espace vectoriel $\mathbb{F}_2^n$. D'après le théorème 2.8 on a donc :

Corollaire 2.10.

$$|\langle CNOT\rangle_n| = 2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (2^i - 1). \tag{2.31}$$

3. Voir annexe A, section A.1.3

Un résultat classique de la théorie des groupes énonce que le groupe projectif spécial linéaire $\mathrm{PSL}_n(K)$ est simple[4] dès que $n \geqslant 3$ (voir par exemple [179, chapitre 3]). Ce groupe est défini comme le groupe quotient $\mathrm{SL}_n(K)/\mathrm{Z}$ où Z est le sous-groupe des matrices scalaires de déterminant 1. Dans le cas où $K = \mathbb{F}_2$, la matrice identité est la seule matrice scalaire de déterminant 1. Ainsi $\mathrm{SL}_n(\mathbb{F}_2) = \mathrm{PSL}_n(\mathbb{F}_2)$ et on en déduit le théorème suivant.

Théorème 2.11. *Le groupe* $\langle CNOT \rangle_n$ *est simple si* $n \geqslant 3$.

Remarque 2.12. Si $n = 2$, le groupe $\langle CNOT \rangle_2$ est d'ordre 6 et il est isomorphe au groupe symétrique $\mathfrak{S}_3$[5], un isomorphisme explicite étant donné par $X_{[0:1]} \simeq (0\ 1)$, $X_{[1:0]} \simeq (1\ 2)$, $X_{[0:1]}X_{[1:0]} \simeq (0\ 1\ 2)$, $X_{[1:0]}X_{[0:1]} \simeq (0\ 2\ 1)$ et $X_{[0:1]}X_{[1:0]}X_{[0:1]} \simeq (0\ 2)$. Ainsi $\langle CNOT \rangle_2$ n'est pas un groupe simple puisque le groupe alterné[6] est toujours un sous groupe normal du groupe $\mathfrak{S}_n$.

Remarque 2.13. On peut remarquer que le groupe $\mathrm{GL}_p(\mathbb{F}_2)$ peut être assimilé à un sous groupe de $\mathrm{GL}_n(\mathbb{F}_2)$ si $p < n$. En effet, soit f le morphisme injectif de $\mathrm{GL}_p(\mathbb{F}_2)$ dans $\mathrm{GL}_n(\mathbb{F}_2)$ défini par $f(M) = \begin{bmatrix} M & 0 \\ 0 & I_{n-p} \end{bmatrix}$. On a $\mathrm{GL}_p(\mathbb{F}_2) \simeq \varphi(\mathrm{GL}_p(\mathbb{F}_2))$ et on peut considérer que $\mathrm{GL}_p(\mathbb{F}_2) \subset \mathrm{GL}_n(\mathbb{F}_2)$.

2.2.2 Présentation du groupe $\langle CNOT \rangle_n$ et système de réécriture

Dans "Lectures on Chevalley Groups" [169, chapitre 6], Steinberg donne une présentation[7] du groupe spécial linéaire sur un corps fini K en dimension $n \geqslant 3$. Il utilise la notation (a, b) pour le commutateur de deux éléments a et b d'un groupe, *i.e.* $(a, b) = a^{-1}b^{-1}ab$.

Théorème 2.14. *(Steinberg) Si* $n \geqslant 3$ *et* K *est un corps fini, les symboles* $x_{ij}(t)$, $(1 \leqslant i, j \leqslant n,\ i \neq j,\ t \in K)$ *soumis aux relations*

$$x_{ij}(t)x_{ij}(u) = x_{ij}(t+u), \tag{2.32}$$
$$(x_{ij}(t), x_{jk}(u)) = x_{ik}(tu) \text{ si } i, j, k \text{ sont distincts}, \tag{2.33}$$
$$(x_{ij}(t), x_{k\ell}(u)) = 1 \text{ si } j \neq k,\ i \neq \ell, \tag{2.34}$$

définissent le groupe $\mathrm{SL}_n(K)$.

En adaptant cette présentation au cas du corps à deux éléments, on obtient immédiatement une présentation du groupe $\langle CNOT \rangle_n$ pour tout $n \geqslant 3$.

Corollaire 2.15. *Si* $n \geqslant 3$, *une présentation du groupe* $\langle CNOT \rangle_n$ *est* $< \mathcal{S} \mid \mathcal{R} >$ *où* $\mathcal{S}$ *est l'ensemble des* $n(n-1)$ *symboles* x_{ij} $(0 \leqslant i, j \leqslant n-1,\ i \neq j)$ *et* $\mathcal{R}$ *est l'ensemble des relations :*

$$x_{ij}^2 = 1, \tag{2.35}$$
$$(x_{ij}x_{jk})^2 = x_{ik}, \quad i, j, k \text{ distincts} \tag{2.36}$$
$$(x_{ij}x_{k\ell})^2 = 1 \quad \text{si } i \neq \ell, j \neq k. \tag{2.37}$$

4. Voir annexe A, définition A.21
5. Voir annexe A, section A.4.4
6. Voir annexe A, section A.4.1
7. Voir annexe A, section A.5

Remarque 2.16. On retrouve dans le corollaire 2.15 les trois identités de la proposition 2.1. Cela implique que ces trois identités sont théoriquement suffisantes pour retrouver n'importe quelle identité entre des portes *CNOT*. Ainsi, on doit pouvoir retrouver l'identité de tresse (1.80) ($X_{[i:j]}X_{[j:i]}X_{[i:j]} = X_{[j:i]}X_{[i:j]}X_{[j:i]}$) à partir des identités (2.4), (2.5) et (2.6), ce qui ne semble pas évident. En fait, le calcul n'est pas immédiat et nous le présentons ci-dessous.

Dans un premier temps, on déduit de (2.35), (2.36) et (2.37) les relations de conjugaison similaires à (2.7) et (2.8) :

$$x_{ij}x_{jk}x_{ij} = x_{jk}x_{ik} = x_{ik}x_{jk}$$
$$x_{ij}x_{ki}x_{ij} = x_{ki}x_{kj} = x_{kj}x_{ki}.$$

Ensuite on obtient

$$\begin{aligned} x_{ji}x_{ij}x_{ji} &= x_{ji}(x_{ik}x_{kj})^2x_{ji} \\ &= (x_{ji}x_{ik}x_{kj}x_{ji})^2 \\ &= (x_{ji}x_{ik}x_{ji}\ x_{ji}x_{kj}x_{ji})^2 \\ &= (x_{ik}x_{jk}x_{ki}x_{kj})^2 \end{aligned}$$

et finalement

$$\begin{aligned} x_{ij}x_{ji}x_{ij}x_{ji}x_{ij} &= x_{ij}(x_{ik}x_{jk}x_{ki}x_{kj})^2x_{ij} \\ &= (x_{ij}x_{ik}x_{jk}x_{ki}x_{kj}x_{ij})^2 \\ &= (x_{ik}x_{ij}x_{jk}x_{ki}x_{ij}x_{kj})^2 \\ &= (x_{ik}x_{ij}x_{jk}x_{ij}\ x_{ij}x_{ki}x_{ij}x_{kj})^2 \\ &= (x_{ik}x_{ik}x_{jk}x_{ki}x_{kj}x_{kj})^2 \\ &= (x_{jk}x_{ki})^2 \\ &= x_{ji} \end{aligned}$$

Théorème 2.17. *Tout circuit de portes CNOT agissant sur n qubits peut être optimisé en utilisant le système de réécriture suivant (*$0 \leqslant i, j, k, \ell \leqslant n-1$*) :*

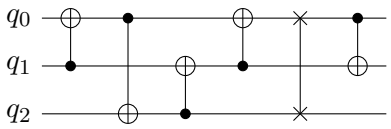
$$[i:j][i:j] = 1, \tag{2.38}$$
$$[i:j][j:k][i:j] = [j:k][i:k],\ [i:j][k:i][i:j] = [k:i][k:j], \tag{2.39}$$
$$[i:j][k:\ell] = [k:\ell][i:j] \text{ si } i \neq \ell \text{ et } j \neq k, \tag{2.40}$$
$$[i:j][j:i][i:j] = [j:i][i:j][j:i] = (i\ \ j), \tag{2.41}$$
$$(i\ \ j)[k:\ell] = [k:\ell]^{(i\ \ j)}(i\ \ j),\ [k:\ell](i\ \ j) = (i\ \ j)[k:\ell]^{(i\ \ j)}, \tag{2.42}$$
$$[k:\ell]^{(i\ \ j)} = [\tau(k):\tau(\ell)],\ \text{avec } \tau = (i\ \ j). \tag{2.43}$$

Démonstration. Les trois premières règles (2.38), (2.39) et (2.40) sont équivalentes aux trois identités du corollaire 2.15 et sont donc théoriquement suffisantes pour optimiser n'importe quel circuit de portes *CNOT*. Les trois dernières règles peuvent être déduites des trois premières. On les a ajouté par commodité (voir remarque 2.16). □

Actuellement, il n'existe pas d'algorithme expliquant comment employer ces règles afin d'optimiser un circuit donné. On peut certes automatiser quelques règles de réduction en recherchant dans un circuit donné les motifs correspondant au règles (2.38) et (2.39) mais les gains seront probablement très limités. Dans la pratique on se contente d'utiliser ces règles de réécriture de façon *ad hoc* dans le but d'essayer de réduire un circuit donné (voir exemple figure 2.8).

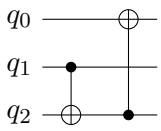
Figure 2.8 Optimisation d'un circuit de portes *CNOT* en utilisant un système de réécriture.

Circuit C à optimiser :



$$
\begin{aligned}
A &= [1:0](0\ \ 2)[0:1][1:2][2:0][0:1] \\
&\overset{(2.42)}{=} (0\ \ 2)[1:0]^{(0\ \ 2)}[0:1][1:2][2:0][0:1] \\
&\overset{(2.43)}{=} (0\ \ 2)[1:2][0:1][1:2][2:0][0:1] \\
&\overset{(2.39)}{=} (0\ \ 2)[0:1][0:2][2:0][0:1] \\
&\overset{(2.40)}{=} (0\ \ 2)[0:2][0:1][2:0][0:1] \\
&\overset{(2.41)}{=} [0:2][2:0][0:2]][0:2][0:1][2:0][0:1] \\
&\overset{(2.38)}{=} [0:2][2:0][0:1][2:0][0:1] \\
&\overset{(2.39)}{=} [0:2][2:0][2:0][2:1] \\
&\overset{(2.38)}{=} [0:2][2:1]
\end{aligned}
$$

Circuit optimisé $C' = C$:



2.3 Optimisation et réduction de circuits de portes *CNOT*

Nous commençons par préciser le vocabulaire et nous poursuivons par une revue sommaire (état de l'art) des principales *heuristiques* de décomposition d'une matrice de $\mathrm{GL}_n(\mathbb{F}_2)$ en transvections. Ces heuristiques sont des algorithmes polynomiaux efficaces donnant une décomposition non optimale d'une telle matrice. Nous présentons ensuite un algorithme d'optimisation de circuits basé sur l'utilisation du graphe de Cayley [8] du groupe $\mathrm{GL}_n(\mathbb{F}_2)$, utile pour les petits cas ($n \leqslant 6$).

2.3.1 Vocabulaire et notations

Soit $\mathrm{seqT} = (T_0, T_1, \ldots T_{\ell-1})$ une suite finie (éventuellement vide) de ℓ transvections. Nous dirons que seqT est une *décomposition de longueur* ℓ de la matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ si $A = \prod_{k=0}^{\ell-1} T_k$. En particulier la suite vide est une décomposition de longueur 0 de la matrice identité. Deux décompositions d'une même matrice A sont dites *équivalentes*.

Soit $\mathcal{G}$ un ensemble de transvections qui engendre le groupe $\mathrm{GL}_n(\mathbb{F}_2)$. Nous définissons la *taille* d'une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$ relativement à $\mathcal{G}$, notée $|A|_{\mathcal{G}}$, comme étant le minimum des longueurs des décompositions de A en transvections de $\mathcal{G}$. Dans la pratique, la partie génératrice de $\mathrm{GL}_n(\mathbb{F}_2)$ correspond (par le morphisme Φ du théorème 2.8) aux portes *CNOT* permises par le graphe de connectivité des qubits. Ainsi, pour le graphe

8. Voir annexe A, définition A.7 et figure A.1.

complet, $\mathcal{G}$ est l'ensemble des $n(n-1)$ transvections et, pour le graphe LNN, $\mathcal{G}$ est l'ensemble des transvections $[i : i+1]$ et $[i : i-1]$. Dans la suite de ce chapitre, nous considérons que le graphe est complet. Ainsi, pour tout i, j, on a $|[i : j]| = 1$. La *taille* de la matrice unitaire X_A de $\langle CNOT \rangle_n$, notée $|X_A|$, est définie comme étant la taille de A : c'est la longueur minimale d'un circuit de portes *CNOT* qui représente l'opérateur X_A.

Une décomposition d'une matrice A est *optimale* si sa longueur est égale à la taille de A. De la même façon, nous dirons qu'un circuit de portes *CNOT* représentant l'opérateur unitaire X_A est *optimal* si la longueur de ce circuit est égal à la taille de la matrice A.

Étant donné deux décompositions seqT et seqT$'$ d'une même matrice A, de longueurs respectives ℓ et ℓ', nous dirons que seqT$'$ est une *réduction* de seqT si $\ell' < \ell$. On a la même définition pour deux circuits équivalents de portes *CNOT*.

Optimiser une décomposition seqT, c'est déterminer une décomposition seqT$'$ équivalente à seqT qui soit optimale. *Réduire* une décomposition seqT, c'est déterminer une décomposition seqT$'$ équivalente à seqT qui soit de longueur strictement inférieure. De la même façon, réduire un circuit de portes *CNOT* c'est déterminer un circuit équivalent de longueur strictement inférieure et optimiser ce circuit consiste à déterminer un circuit équivalent qui soit optimal.

Finalement, nous définissons maxT(n) comme étant la taille maximale des éléments de $\mathrm{GL}_n(\mathbb{F}_2)$:

$$\mathrm{maxT}(n) = \max\{|A| : A \in \mathrm{GL}_n(\mathbb{F}_2)\}. \tag{2.44}$$

2.3.2 État de l'art des heuristiques de décomposition d'une matrice de $\mathrm{GL}_n(\mathbb{F}_2)$

Principe général des heuristiques de décomposition

Si l'on dispose d'un certain algorithme DECOMP-ALG permettant de décomposer une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$ en un produit de transvections alors on peut construire très simplement une heuristique de réduction d'un circuit de portes *CNOT*, de la façon suivante.

- Soit C un circuit quantique de n qubits composé de ℓ portes *CNOT*.
- Calculer la matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ associée à ce circuit en remplaçant chaque porte *CNOT* par la transvection correspondante et en multipliant ces matrices de transvections.
- Soit seqT $= ([i_0 : j_0], \ldots, [i_{\ell'-1} : j_{\ell'-1}])$ la décomposition de longueur ℓ' de la matrice A retournée par DECOMP-ALG(A).
- Si $\ell' < \ell$ alors retourner le circuit C' correspondant à seqT, sinon l'heuristique a échoué à réduire C.

Décomposition par l'algorithme de Gauss-Jordan

L'algorithme d'élimination de Gauss-Jordan (méthode du pivot de Gauss) est une méthode classique d'algèbre linéaire visant à calculer les solutions d'un système d'équations linéaires, à déterminer le rang d'une matrice ou à inverser une matrice carrée. Sa complexité asymptotique est $O(n^3)$ (voir [5] et [159]). Si on l'utilise pour inverser une matrice A de $\mathrm{GL}_n(\mathbb{F}_2)$, cet algorithme prend une forme très simple : on multiplie la

matrice A à gauche par une suite de transvections bien choisies de façon à obtenir la matrice identité. Le produit de ces transvections est alors égal à la matrice A.

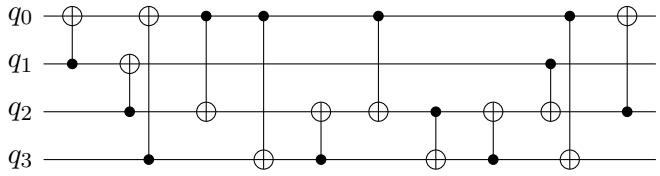
L'utilisation de cet algorithme comme heuristique de réduction est référencée dans [154]. Nous en donnons un exemple d'utilisation figure 2.9. Nous remarquons que cet algorithme classique fournit facilement une majoration du nombre $\mathrm{maxT}(n)$ (2.44). En effet, une matrice donnée de $\mathrm{GL}_n(\mathbb{F}_2)$ ayant n^2 entrées et l'algorithme procédant entrée par entrée, il effectue tout au plus n^2 additions de lignes. On a donc la proposition suivante.

Proposition 2.18.

(i) Tout circuit de portes CNOT pour n qubits possède un circuit équivalent composé de moins de n^2 portes.

(ii) $\mathrm{maxT}(n) \leqslant n^2$

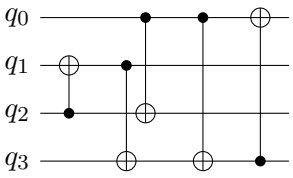
Figure 2.9 L'algorithme de Gauss-Jordan appliqué à la réduction d'un circuit de portes *CNOT*.

$\texttt{INPUT} : C =$ 

$A = [0:2][3:0][2:1][2:3][3:2][2:0][2:3][3:0][2:0][0:3][1:2][0:1]$

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} ; \ [0:3]A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} ; \ [3:1][2:0][3:0][0:3]A = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$A = [0:3][3:0][2:0][3:1][1:2]$

$\texttt{OUTPUT} : C' =$ 

Décomposition par l'algorithme de Patel-Markov-Hayes

Dans un article de 2004 [154], Patel, Markov et Hayes proposent un algorithme de décomposition d'une matrice de $\mathrm{GL}_n(\mathbb{F}_2)$ en produit de transvections permettant, en moyenne, une réduction sensible de la longueur de la décomposition donnée par l'algorithme de Gauss-Jordan. Cet algorithme de complexité asymptotique $O(n^3/\ln n)$ est décrit formellement de façon très détaillée dans [154] et un exemple complet de déroulement est fourni. L'idée générale est de procéder par regroupements de m colonnes consécutives de la matrice à décomposer, m désignant un entier non nul qui est le paramètre de l'algorithme. On peut voir l'algorithme de Gauss-Jordan comme un cas particulier de cet algorithme, celui où $m = 1$. Les auteurs obtiennent une amélioration de la borne supérieure de n^2 transvections de l'algorithme de Gauss-Jordan puisqu'ils

prouvent que leur algorithme permet une décomposition en $O(n^2/\ln n)$ transvections en choisissant $m = \alpha \log_2 n$ avec $0 < \alpha < 1$. On a donc :

$$\mathrm{maxT}(n) = O(n^2/\ln n). \tag{2.45}$$

Patel et ses coauteurs prouvent également que :

$$\mathrm{maxT}(n) = \Omega(n^2/\ln n). \tag{2.46}$$

La démonstration de ce dernier résultat étant courte et instructive, nous la rappelons ici. Il y a $n(n-1)$ portes *CNOT* différentes et en ajoutant l'identité nous obtenons un ensemble de $n(n-1)+1$ portes quantiques. L'ordre du groupe $\langle CNOT \rangle_n$ est strictement inférieur au nombre de circuits de portes *CNOT* de longueur inférieure ou égale à $\mathrm{maxT}(n)$. Or le nombre de ces circuits est lui même strictement inférieur à $(n(n-1)+1)^{\mathrm{maxT}(n)}$. On a donc, d'après la formule 2.31 : $(n(n-1)+1)^{\mathrm{maxT}(n)} > 2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(2^i-1)$. De plus $2^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(2^i-1) > 2^{n(n-1)}$, donc $(n(n-1)+1)^{\mathrm{maxT}(n)} > 2^{n(n-1)}$ et on en déduit l'inégalité $\mathrm{maxT}(n) > \dfrac{n^2-n}{\log_2(n^2-n+1)}$, d'où l'équation (2.46).

Remarque 2.19. L'inégalité (2.45) porte sur la longueur maximale des décompositions retournées et garantit donc seulement qu'une décomposition donnée ne sera pas "trop grande". Il n'y a aucune raison pour que cet algorithme retourne une décomposition optimale d'une matrice donnée. Considérons le contre-exemple suivant :

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

La décomposition retournée par l'algorithme de Patel-Markov-Hayes avec $m = 2$ a pour longueur 19 :

$$A = [1:0][2:0][5:0][4:0][1:3][3:1][4:1][5:4][2:3][3:2][3:4] \\ [4:3][5:4][4:5][2:4][0:1][1:4][1:3][0:2].$$

Cependant, nous verrons dans la section suivante (exemple 2.27) que cette matrice admet une décomposition de longueur 12, à savoir

$$A = [1:2][4:1][2:4][5:4][4:0][0:5][5:3][3:4][4:5][1:4][4:2][2:1].$$

Ainsi, même pour des petites valeurs de n, il est possible que la décomposition donnée par cet algorithme soit très loin d'être optimale.

Décomposition par l'algorithme GreedyGE

En septembre 2021, une équipe française propose une heuristique de décomposition d'une matrice de $\mathrm{GL}_n(\mathbb{F}_2)$ qui prolonge les idées développées dans [154] : l'algorithme GreedyGE (Greedy Gaussian Elimination) [40]. Cette fois-ci, la décomposition ne s'effectue plus en avançant par regroupement de colonnes, mais en prenant en compte

toute la matrice et en cherchant avant chaque opération de transvection deux lignes dont l'addition permettra de mettre à 0 le plus grand nombre possible de bits (voir exemple détaillé dans [40, section 3, Fig. 1]). Cet algorithme diminue d'environ 25% la longueur moyenne des décompositions données par l'algorithme de Patel *et al.* [154], tout en étant au moins aussi rapide.

2.3.3 Optimisation basée sur le graphe de Cayley du groupe linéaire

Principe de l'algorithme

Pour optimiser un circuit de portes *CNOT* de quelques qubits ($n \leqslant 6$), on commence par multiplier les matrices de transvections associées aux portes *CNOT* composant ce circuit et l'on obtient ainsi une matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$. On construit alors progressivement le graphe de Cayley [9] du groupe $\mathrm{GL}_n(\mathbb{F}_2)$ en effectuant un parcours en largeur de ce graphe : partant de la matrice identité (élément de taille 0), on construit d'abord les éléments de taille 1 (les $n(n-1)$ matrices de transvections), puis les éléments de taille 2, et ainsi de suite. Chaque matrice ainsi construite est stockée en mémoire avec une décomposition minimale en produit de transvections (sous la forme d'une simple chaîne de caractères par exemple). On continue ainsi jusqu'à obtenir la matrice A.

En pratique cette approche n'est réalisable que jusqu'à 5 ou 6 qubits sur un PC de base car la complexité en espace d'un tel algorithme est exponentielle en n comme l'indique la formule 2.31. En effet, dans le pire des cas, il faut construire entièrement le graphe de Cayley. De plus, il faut vérifier pour chaque nouvel élément potentiel du groupe, qu'il n'a pas déjà été construit (ligne 23 de l'algorithme 2.1). Dans le cas d'un algorithme naïf où l'on compare chaque nouvel élément potentiel avec chaque élément déjà construit, le temps de calcul d'une seule vérification est donc proportionnel à l'ordre du groupe, c'est à dire exponentiel en n. Il faut alors plusieurs heures de calcul sur un PC de base pour décomposer certaines matrices dans le cas où $n = 5$.

Optimisations mises en place

Nous remarquons qu'il est possible de diminuer le temps de calcul et l'espace mémoire nécessaire à l'approche naïve grâce aux deux optimisations suivantes, mises en place dans l'algorithme 2.1.

La première optimisation est basée sur la remarque suivante : quand on calcule les matrices de taille $k+2$ à partir des matrices de taille $k+1$, on peut se contenter de garder en mémoire uniquement les matrices de taille k, $k+1$ et $k+2$. En effet, soit A une matrice de taille $k+1$ déjà présente dans le graphe et T une matrice de transvection, on voit facilement que

$$|TA| \in \{|A|-1, |A|, |A|+1\}.$$

Ainsi l'algorithme 2.1 ne conserve en mémoire à chaque instant que trois lignes du graphe de Cayley, stockées dans des arbres $\mathcal{A}_0$, $\mathcal{A}_1$ et $\mathcal{A}_2$.

La seconde optimisation est basée sur l'utilisation d'une structure de donnée adaptée. En effet, on peut créer un ordre sur $\mathrm{GL}_n(\mathbb{F}_2)$ en associant à chaque matrice l'entier dont la représentation binaire est la séquence des n^2 bits de cette matrice. On peut alors utiliser un arbre AVL [2] pour stocker chaque matrice sous la forme d'un unique entier. Cela permet l'insertion et la recherche d'une matrice (lignes 23 et 25 de l'algorithme 2.1) en temps $O(\ln m)$ où m est le nombre de noeuds, autrement dit en temps $O(n^2)$ d'après

9. Voir annexe A, exemple A.1

Algorithme 2.1 OPTIMISER(n, A)

Entrée : un entier $n \geqslant 2$, une matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ qui n'est ni l'identité, ni une transvection

Sortie : une décomposition optimale de la matrice A

1: // Initialisation des trois arbres $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2$. L'arbre $\mathcal{A}_i$ $(i = 0, 1, 2)$ contient les matrices de taille $taille + i$.
2: Soient $\mathcal{A}_0$, $\mathcal{A}_1$ et $\mathcal{A}_2$ des arbres vides
3: $taille \leftarrow 0$
4: // Un noeud est un couple $(clé, valeur)$ avec $clé \in \mathrm{GL}_n(\mathbb{F}_2)$ et *valeur* une décomposition optimale de *clé*
5: $noeud \leftarrow (I, ())$// L'identité a une décomposition minimale vide
6: insérer$(\mathcal{A}_0, noeud)$
7: *transvections* $\leftarrow$ ensemble des matrices de transvection.
8: **pour tout** T dans *transvections* **faire**
9: $\quad noeud \leftarrow (T, (T))$
10: $\quad$ insérer$(\mathcal{A}_1, noeud)$
11: **fin pour**
12: **boucle**
13: $\quad$ // Calcul des matrices de taille $taille + 2$
14: $\quad$ **pour tout** *noeud* dans A_1 **faire**
15: $\quad\quad$ **pour tout** T dans *transvections* **faire**
16: $\quad\quad\quad matrice \leftarrow noeud.clé$
17: $\quad\quad\quad matrice \leftarrow T \times matrice$
18: $\quad\quad\quad decompo \leftarrow noeud.valeur$
19: $\quad\quad\quad$ ajouter$(decompo, T)$
20: $\quad\quad\quad$ **si** $matrice = A$ **alors**
21: $\quad\quad\quad\quad$ **retourner** $decompo$
22: $\quad\quad\quad$ **fin si**
23: $\quad\quad\quad$ **si** $matrice \notin \mathcal{A}_0 \cup \mathcal{A}_1 \cup \mathcal{A}_2$ **alors**
24: $\quad\quad\quad\quad nouveauNoeud \leftarrow (matrice, decompo)$
25: $\quad\quad\quad\quad$ insérer$(\mathcal{A}_2, nouveauNoeud)$
26: $\quad\quad\quad$ **fin si**
27: $\quad\quad$ **fin pour**
28: $\quad$ **fin pour**
29: $\quad taille \leftarrow taille + 1$
30: $\quad \mathcal{A}_0 \leftarrow \mathcal{A}_1$
31: $\quad \mathcal{A}_1 \leftarrow \mathcal{A}_2$
32: $\quad \mathcal{A}_2 \leftarrow$ arbre vide
33: **fin boucle**

la formule 2.31. Cette opération est beaucoup plus rapide que le temps de vérification en $O(\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_2)))$ nécessaire dans une implantation naïve.

Cependant, malgré ces optimisations, la complexité de l'algorithme 2.1 reste exponentielle en temps et en espace. Nous avons implanté cet algorithme en langage C sous la forme d'une commande `cnot_opt` dont le code source est disponible dans un dépôt Github [54]. En utilisant cette commande, on trouve une décomposition optimale de n'importe quelle matrice de $\mathrm{GL}_5(\mathbb{F}_2)$ en quelques secondes sur un PC de base. On peut faire de même pour les matrices de $\mathrm{GL}_6(\mathbb{F}_2)$ à condition de disposer d'une machine possédant quelques centaines de Go de mémoire ($|\mathrm{GL}_6(\mathbb{F}_2)| = 20\,158\,709\,760$ d'après la formule 2.31). Le cas $n = 7$ reste hors de portée de cette approche.

Répartition des matrices de $\mathrm{GL}_n(\mathbb{F}_2)$ selon leur taille

Table 2.2 Répartition des matrices de $\mathrm{GL}_n(\mathbb{F}_2)$ en fonction de leur taille. Les matrices de taille 1 sont les $n(n-1)$ transvections et les valeurs en gras correspondent aux $(n-1)!$ matrices de permutations associées aux cycles de longueur n.

taille	$n=2$	$n=3$	$n=4$	$n=5$
0	1	1	1	1
1	2	6	12	20
2	2	24	96	260
3	**1**	51	542	2 570
4		60	2 058	19 680
5		24	5 316	117 860
6		**2**	7 530	540 470
7			4 058	1 769 710
8			541	3 571 175
9			**6**	3 225 310
10				736 540
11				15 740
12				**24**
Ordre de $\mathrm{GL}_n(\mathbb{F}_2)$	6	168	20 160	9 999 360

La table 2.2 montre la répartition des matrices de $\mathrm{GL}_n(\mathbb{F}_2)$ selon leur taille pour les premières valeurs de n. Une observation se dégage immédiatement : les matrices de plus grande taille sont les matrices de permutations correspondant aux cycles de longueur n. On a donc :

$$\mathrm{maxT}(n) = 3(n-1), \quad n = 2, 3, 4, 5 \tag{2.47}$$

Nous avons pensé pouvoir étendre ce résultat à tout entier $n \geqslant 1$ et tenté en vain de le démontrer, avant d'avoir connaissance du résultat (2.46) de Patel *et al.* [154, Lemme 1] qui invalide cette conjecture. Nous vérifions que $\dfrac{n^2-n}{\log_2(n^2-n+1)} > 3(n-1)$ si $n > 29$. Ainsi, à partir de 30 qubits, il y a certainement des circuits de portes *CNOT* qui ne peuvent pas se réduire en un circuit de longueur inférieure à $3(n-1)$. Nous ignorons jusqu'à quelle valeur de n l'égalité (2.47) reste vraie.

2.4 Étude d'un cas particulier : inversion des bits d'une matrice de permutation

Nous proposons dans cette section un algorithme de décomposition d'un type particulier de matrices de $\mathrm{GL}_n(\mathbb{F}_2)$: les matrices obtenues en inversant tous les bits d'une matrice de permutation σ en dimension paire. Nous notons $\overline{\sigma}$ une telle matrice. Par exemple $\overline{(0\ 2)(1\ 3)} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ et $\overline{I_4} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$. Notez qu'en dimension impaire, la matrice $\overline{\sigma}$ n'est jamais inversible car chaque ligne (resp. chaque colonne) de cette matrice est la somme de toutes les autres.

2.4.1 Propriétés algébriques

On note 1_n la matrice $n \times n$ à coefficients dans $\mathbb{F}_2$ dont toutes les entrées valent 1. Soit M une matrice $n \times n$ à coefficients dans $\mathbb{F}_2$, on note $\overline{M}$ la matrice dont les entrées sont obtenues en inversant les entrées de M. On a donc

$$\overline{M} = M \oplus 1_n. \tag{2.48}$$

Proposition 2.20. *Soit n un entier pair non nul. Soient σ, σ_1 et σ_2 des matrices de permutation $n \times n$. On a les identités suivantes.*

$$\overline{I_n}^2 = I_n \tag{2.49}$$
$$\sigma \overline{I_n} \sigma^{-1} = \overline{I_n} \tag{2.50}$$
$$\overline{\sigma} = \sigma \overline{I_n} \text{ et } (\overline{\sigma})^{-1} = \sigma^{-1} \overline{I_n} \tag{2.51}$$
$$\overline{\sigma_1}\ \overline{\sigma_2} = \sigma_1 \sigma_2 \tag{2.52}$$

Démonstration. Preuve de (2.49) : $\overline{I_n}^2 = (I_n \oplus 1_n)^2 = I_n^2 \oplus 1_n^2$ et $1_n^2 = 0$ car n est impair, donc $\overline{I_n}^2 = I_n$.
Preuve de (2.50) : $\sigma \overline{I_n} \sigma^{-1} = \sigma(I_n \oplus 1_n)\sigma^{-1} = \sigma I_n \sigma^{-1} \oplus \sigma 1_n \sigma^{-1} = I_n \oplus 1_n = \overline{I_n}$.
Preuve de (2.51) : $\sigma \overline{I_n} = \sigma(I_n + 1_n) = \sigma I_n + \sigma 1_n = \sigma + 1_n = \overline{\sigma}$ donc
$(\overline{\sigma})^{-1} = (\overline{I_n})^{-1}\sigma^{-1} \overset{(2.50)}{=} \sigma^{-1}(\overline{I_n})^{-1} \overset{(2.49)}{=} \sigma^{-1}\overline{I_n}$.
Preuve de (2.52) : $\overline{\sigma_1}\ \overline{\sigma_2} = \sigma_1 \overline{I_n} \sigma_2 \overline{I_n} = \sigma_1 \sigma_2 \overline{I_n}^2 = \sigma_1 \sigma_2$. □

De la proposition 2.20, on déduit facilement la structure du groupe engendré par l'ensemble des matrices de permutation et des matrices de type $\overline{\sigma}$, $\sigma \in \mathfrak{S}_n$.

Proposition 2.21. *Si n est un entier pair non nul, le groupe engendré par les matrices de permutation $n \times n$ à coefficients dans $\mathbb{F}_2$ et la matrice $\overline{I_n}$ est isomorphe au produit direct des groupes $\mathfrak{S}_n$ et $(\mathbb{F}_2, \oplus)$. Un isomorphisme possible associe aux matrices de permutation σ le couple $(\sigma, 0)$ et aux matrices de type $\overline{\sigma}$ le couple $(\sigma, 1)$.*

Remarque 2.22. L'effet de la matrice $\overline{I_n}$ sur un vecteur $[b_0 \dots b_{n-1}]$ est facile à décrire : s'il y a un nombre impair de bits à 1 alors les bits sont inversés, sinon les bits sont inchangés. Nous verrons au chapitre 5 que la matrice $\overline{I_4}$ intervient dans la construction de circuits quantiques permettant de produire des états de 4 qubits maximalement intriqués.

2.4.2 Une décomposition de la matrice $\overline{I_n}$

Soient i, j, k des entiers distincts de $\{0, \dots, n-1\}$, La notation $[i : j : k]$ désigne le produit dans $\mathrm{GL}_n(\mathbb{F}_2)$ des trois matrices de transvection $[i : j]$, $[k : i]$ et $[j : k]$.

$$[i : j : k] = [i : j][k : i][j : k] \tag{2.53}$$

Proposition 2.23. *Soit $n = 2q$ un entier pair non nul. Si $n \geqslant 4$ on définit la matrice $B_n \in \mathrm{GL}_n(\mathbb{F}_2)$ par*

$$B_n = \prod_{i=0}^{q-2} [2i+1 : 2i+2 : 2i+3]$$

et on pose $B_2 = I_2$. On a alors

$$\overline{I_n} = B_n^{-1}(0\ \ 1)B_n. \tag{2.54}$$

Démonstration. On prouve le résultat par récurrence sur n. Pour $n = 2$, l'égalité (2.54) est vérifiée car $\overline{I_2} = (0\ \ 1)$. Supposons $n \geqslant 2$ et $\overline{I_n} = B_n^{-1}(0\ \ 1)B_n$. On utilise le morphisme f permettant d'injecter $\mathrm{GL}_n(\mathbb{F}_2)$ dans $\mathrm{GL}_{n+2}(\mathbb{F}_2)$ (voir remarque 2.13). On rappelle que f est défini pour toute matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ par $f(A) = \begin{bmatrix} A & 0 \\ 0 & I_2 \end{bmatrix}$. On a donc

$$f(\overline{I_n}) = \begin{bmatrix} \overline{I_n} & 0 \\ 0 & I_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 & \dots & 1 & 0 & 0 \\ 1 & 0 & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 1 & \vdots & \vdots \\ 1 & \dots & 1 & 0 & 0 & \vdots \\ 0 & \dots & \dots & 0 & 1 & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \end{bmatrix} \text{ et } f(\overline{I_n}) = f(B_n^{-1}(0\ \ 1)B_n).$$

En utilisant la proposition 2.6, on vérifie que

$$[n : n+1][n+1 : n-1][n-1 : n]f(\overline{I_n})[n-1 : n][n+1 : n-1][n : n+1] = \overline{I_{n+2}}.$$

Or $[n-1 : n][n+1 : n-1][n : n+1] = [n-1 : n : n+1]$ d'après (2.53), donc

$$\overline{I_{n+2}} = [n-1 : n : n+1]^{-1} f(\overline{I_n})[n-1 : n : n+1].$$

Ainsi $\overline{I_{n+2}} = [n-1 : n : n+1]^{-1} f(B_n^{-1}(0\ \ 1)B_n)[n-1 : n : n+1]$ et finalement $\overline{I_{n+2}} = B_{n+2}^{-1}(0\ \ 1)B_{n+2}$. □

2.4.3 Une décomposition des matrices de type $\overline{\sigma}$

La proposition 2.25 est une généralisation de la proposition 2.23. On en déduit un algorithme de décomposition des matrices de type $\overline{\sigma}$. Pour démontrer la proposition 2.25, on fait appel au lemme 2.24.

Lemme 2.24. *Soient $0 \leqslant i, j, k \leqslant n-1$ des entiers distincts. On a :*

$$[i : j : k](j\ \ k) = [j : k : i]^{-1} \tag{2.55}$$

$$(i\ \ j)[i : j : k] = [k : i : j]^{-1} \tag{2.56}$$

$$[i : j : k](i\ \ j) = [k : j : i]^{-1} \tag{2.57}$$

$$(j\ \ k)[i : j : k] = [k : j : i]^{-1} \tag{2.58}$$

Démonstration. On démontre uniquement l'identité (2.58). Les autres preuves sont similaires.

$$\begin{aligned}
(j\ \ k)[i:j:k] &= (j\ \ k)[i:j][k:i][j:k] \\
&\overset{(2.42)}{=} [i:j]^{(j\ \ k)}[k:i]^{(j\ \ k)}(j\ \ k)[j:k] \\
&\overset{(2.43)}{=} [i:k][j:i](j\ \ k)[j:k] \\
&\overset{(2.41)}{=} [i:k][j:i][j:k][k:j] \\
&\overset{(2.38)}{=} [j:i][j:i][i:k][j:i][j:k][k:j] \\
&\overset{(2.39)}{=} [j:i][i:k][j:k][j:k][k:j] \\
&\overset{(2.38)}{=} [j:i][i:k][k:j] \\
&= ([k:j][i:k][j:i])^{-1} \\
&= [k:j:i]^{-1}
\end{aligned}$$

□

Proposition 2.25. *Soit $n = 2q$ un entier pair non nul. Étant donné une matrice de permutation σ de $\mathrm{GL}_n(\mathbb{F}_2)$ différente de l'identité, on peut écrire la matrice $\overline{I_n}$ sous la forme*

$$\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \sigma\ \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}. \tag{2.59}$$

avec $M_1, M_1', \ldots, M_{q-1}, M_{q-1}'$ des matrices de type $[x:y:z]$ et $\varepsilon_1, \varepsilon_1', \ldots, \varepsilon_{q-1}, \varepsilon_{q-1}'$ des entiers dans $\{-1;1\}$.

Démonstration. Notons $\mathcal{P}_n^*$ l'ensemble des partitions décroissantes de l'entier n différentes de $(1,\ldots,1)$. Tout élément de $\mathcal{P}_n^*$ est le type cyclique d'une permutation [10] différente de l'identité. Soit $\lambda = (n_1, \ldots, n_p)$ un élément de $\mathcal{P}_n^*$, on note α_λ la permutation de $\mathfrak{S}_n$ (et la matrice de permutation de $\mathrm{GL}_n(\mathbb{F}_2)$) de type cyclique λ définie par

$$\alpha_\lambda = \underbrace{(0 \ldots n_1 - 1)}_{\text{cycle de longueur } n_1}\ \underbrace{(n_1 \ldots n_1 + n_2 - 1)}_{\text{cycle de longueur } n_2} \ldots \underbrace{(\sum_{i=1}^{p-1} n_i \cdots \sum_{i=1}^{p} n_i - 1)}_{\text{cycle de longueur } n_p} \tag{2.60}$$

Soit $n \geqslant 4$ et $\lambda \in \mathcal{P}_n^*$, on note λ' la partition de $\mathcal{P}_{n-2}^*$ obtenue à partir de λ de la façon suivante. Pour décrire cette opération on distingue le cas général et trois cas particuliers. Dans chaque cas, on donne également la relation entre $\alpha_{\lambda'}$ et α_λ. Notez que $\alpha_{\lambda'}$ est une permutation de $\mathfrak{S}_{n-2}$ mais on peut l'identifier à une permutation de $\mathfrak{S}_n$ en posant $\alpha_{\lambda'}(n-2) = n-2$ et $\alpha_{\lambda'}(n-1) = n-1$. De même on peut identifier la matrice de permutation $\alpha_{\lambda'}$ de $\mathrm{GL}_{n-2}(\mathbb{F}_2)$ à une matrice de permutation de $\mathrm{GL}_n(\mathbb{F}_2)$ en utilisant le morphisme injectif f de $\mathrm{GL}_{n-2}(\mathbb{F}_2)$ dans $\mathrm{GL}_n(\mathbb{F}_2)$ déjà utilisé dans la preuve de la proposition 2.23.

- Cas général : $n_p \geqslant 3$. On pose $\lambda' = (n_1, \ldots, n_p - 2)$, ainsi $\alpha_{\lambda'} = \alpha_\lambda(n-2\ \ n-1)(n-3\ \ n-2)$.
- Cas particulier A : $n_p = n_{p-1} = 1$. On pose $\lambda' = (n_1, \ldots, n_{p-2})$, ainsi $\alpha_{\lambda'} = \alpha_\lambda$.

10. Voir annexe A, section A.4.3

- Cas particulier B : $n_p = 1$ et $n_{p-1} > 1$. On pose $\lambda' = (n_1, \ldots, n_{p-2}, n_{p-1} - 1)$, ainsi $\alpha_{\lambda'} = \alpha_\lambda(n-3\ \ n-2)$.
- Cas particulier C : $n_p = 2$. On pose $\lambda' = (n_1, \ldots, n_{p-1})$, ainsi $\alpha_{\lambda'} = \alpha_\lambda(n-2\ \ n-1)$.

Sans perte de généralité, on peut prouver la proposition 2.25 uniquement dans le cas où la permutation σ est du type α_λ, avec $\lambda \in \mathcal{P}_n^*$. En effet, si σ est une permutation quelconque (différente de l'identité) de type cyclique $\lambda \in \mathcal{P}_n^*$, alors σ est dans la même classe de conjugaison que α_λ et on peut construire facilement une permutation γ telle que $\sigma = \gamma\alpha_\lambda\gamma^{-1}$. Ayant prouvé la proposition 2.25 pour α_λ, on pose $\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_\lambda \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}$ et puisque $\overline{I_n} \overset{2.50}{=} \left(\overline{I_n}\right)^\gamma$, on en déduit que $\overline{I_n} = \prod_{i=1}^{q-1} (M_i^{\varepsilon_i})^\gamma\ \sigma \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^\gamma$. Pour conclure, il suffit alors de remarquer que

$$([i:j:k]^\varepsilon)^\gamma = [\gamma(i):\gamma(j):\gamma(k)]^\varepsilon \tag{2.61}$$

pour toute permutation γ et tout entier $\varepsilon \in \{-1, 1\}$. Ainsi $\overline{I_n}$ peut se mettre sous la forme (2.59).

On prouve maintenant la proposition 2.25 dans le cas d'une permutation α_λ par récurrence sur $n \geqslant 2$ pair. Le cas de base est clair car il existe une seule partition de l'entier 2 différente de $(1,1)$, à savoir $\lambda = (2)$. Dans ce cas, $\alpha_\lambda = (01)$ et $\overline{I_2} = (01)$, ce qui est une écriture de I_2 de la forme (2.59), en utilisant la convention $\prod_{i=1}^{0} M_i^{\varepsilon_i} = \prod_{i=1}^{0} M_i'^{\varepsilon_i'} = I_2$. Effectuons un pas d'induction : soit $n \geqslant 2$ un entier pair et soit $\lambda \in \mathcal{P}_{n+2}^*$. Par hypothèse on a $\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_{\lambda'} \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}$ et d'après la proposition 2.23 on a $\overline{I_{n+2}} = [n-1:n:n+1]^{-1}\overline{I_n}[n-1:n:n+1]$ donc

$$\overline{I_{n+2}} = [n-1:n:n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_{\lambda'} \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}[n-1:n:n+1]. \tag{2.62}$$

On considère les différentes relations possibles entre $\alpha_{\lambda'}$ et α_λ en commençant par les trois cas particuliers A,B,C et en terminant par le cas général.

Dans le cas particulier A, on a $\alpha_{\lambda'} = \alpha_\lambda$, donc l'égalité (2.62) s'écrit

$$\overline{I_{n+2}} = [n-1:n:n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_\lambda \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}[n-1:n:n+1] \tag{2.63}$$

ce qui termine le pas d'induction.

Dans le cas particulier B, on a $\alpha_{\lambda'} = \alpha_\lambda(n-1\ \ n)$, donc l'égalité (2.62) s'écrit

$$\overline{I_{n+2}} = [n-1:n:n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_\lambda(n-1\ \ n) \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}[n-1:n:n+1]. \tag{2.64}$$

Soit $M = (n-1\ \ n) \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}[n-1:n:n+1]$, on a

$$M = \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n-1\ \ n)} (n-1\ \ n)[n-1:n:n+1]$$
$$\overset{2.56}{=} \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n-1\ \ n)} [n+1:n-1:n]^{-1}$$

donc l'égalité (2.64) devient

$$\overline{I_{n+2}} = [n-1:n:n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_\lambda \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n-1\ \ n)} [n+1:n-1:n]^{-1} \quad (2.65)$$

et on termine le pas d'induction en utilisant l'identité 2.61.

Dans le cas particulier C, on a $\alpha_{\lambda'} = \alpha_\lambda(n\ \ n+1)$, donc l'égalité (2.62) s'écrit

$$\overline{I_{n+2}} = [n-1:n:n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_\lambda(n\ \ n+1) \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'} [n-1:n:n+1]. \quad (2.66)$$

Soit $M = (n\ \ n+1) \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'} [n-1:n:n+1]$, on a

$$M = \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n\ \ n+1)} (n\ \ n+1)[n-1:n:n+1]$$
$$\overset{2.58}{=} \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n\ \ n+1)} [n+1:n:n-1]^{-1}$$

donc l'égalité (2.66) devient

$$\overline{I_{n+2}} = [n-1:n:n+1]^{-1} \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_\lambda \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n\ \ n+1)} [n+1:n:n-1]^{-1} \quad (2.67)$$

et on termine le pas d'induction en utilisant l'identité 2.61.

Dans le cas général, on commence par conjuguer chaque membre de l'égalité (2.62) par $(n \quad n+1)$ et on utilise l'invariance de $\overline{I_{n+2}}$ par conjugaison (2.50) pour obtenir

$$\begin{aligned}\overline{I_{n+2}} = (n\ \ n+1)[n-1:n:n+1]^{-1} &\prod_{i=1}^{q-1} M_i^{\varepsilon_i} \\ &\alpha_{\lambda'} \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'} [n-1:n:n+1](n\ \ n+1).\end{aligned} \quad (2.68)$$

En utilisant les identités 2.55 et 2.56 on obtient

$$\overline{I_{n+2}} = [n:n+1:n-1] \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \alpha_{\lambda'} \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'} [n:n+1:n-1]^{-1}. \quad (2.69)$$

Dans le cas général on a $\alpha_{\lambda'} = \alpha_\lambda(n\ \ n+1)(n-1\ \ n) = \alpha_\lambda(n-1\ \ n)(n+1\ \ n-1)$, donc

$$\begin{aligned}\overline{I_{n+2}} = [n:n+1:n-1] &\prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda(n-1\ \ n)(n+1\ \ n-1) \\ &\prod_{i=1}^{q-1} M_i'^{\varepsilon_i'} [n:n+1:n-1]^{-1}.\end{aligned} \quad (2.70)$$

Soit $M = (n-1\ \ n)(n+1\ \ n-1)\prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}[n : n+1 : n-1]^{-1}$. On a

$$\begin{aligned} M &= \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n-1\ \ n)(n+1\ \ n-1)} (n-1\ \ n)(n+1\ \ n-1)[n : n+1 : n-1]^{-1} \\ &\overset{2.56}{=} \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n-1\ \ n)(n+1\ \ n-1)} (n-1\ \ n)[n+1 : n-1 : n] \\ &\overset{2.58}{=} \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n-1\ \ n)(n+1\ \ n-1)} [n : n-1 : n+1]^{-1} \end{aligned}$$

donc l'égalité (2.70) devient

$$\overline{I_{n+2}} = [n : n+1 : n-1] \prod_{i=1}^{q-1} M_i^{\varepsilon_i} \alpha_\lambda \prod_{i=1}^{q-1} \left(M_i'^{\varepsilon_i'}\right)^{(n-1\ \ n)(n+1\ \ n-1)} [n : n-1 : n+1]^{-1} \quad (2.71)$$

et on termine le pas d'induction en utilisant l'identité 2.61. □

Le principal intérêt de la proposition 2.25 est de nous fournir une méthode pour décomposer une matrice de type $\overline{\sigma}$ en transvections, comme l'explique la proposition suivante.

Proposition 2.26. *Soit $n \geqslant 4$ un entier pair. Pour toute matrice de permutation σ différente de l'identité I_n, il existe $n-2$ matrices $M_1, \ldots, M_{n-2}$ de type $[x : y : z]$ et $n-2$ entiers $\varepsilon_i \in \{1, -1\}$ tels que*

$$\overline{\sigma} = \prod_{i=1}^{n-2} M_i^{\varepsilon_i}. \quad (2.72)$$

Démonstration. Soit σ une matrice de permutation de $\mathrm{GL}_n(\mathbb{F}_2)$ différente de I_n. En appliquant la proposition 2.25 à σ^{-1} on obtient $\overline{I_n} = \prod_{i=1}^{q-1} M_i^{\varepsilon_i}\ \sigma^{-1}\ \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}$, donc

$$\overline{\sigma} = \sigma\overline{I_n} = \prod_{i=1}^{q-1} (M_i^{\varepsilon_i})^\sigma \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'} = \prod_{i=1}^{q-1} (M_i^\sigma)^{\varepsilon_i} \prod_{i=1}^{q-1} M_i'^{\varepsilon_i'}$$ □

La preuve de la proposition 2.25 étant constructive, on obtient par la proposition 2.26 un algorithme de décomposition en transvections des matrices de type $\overline{\sigma}$ (voir exemple 2.27). Elles se décomposent ainsi toutes (sauf $\overline{I_n}$) en $3(n-2)$ transvections. On conjecture que cette décomposition est optimale.

Exemple 2.27. On déroule l'algorithme défini par les propositions 2.25 et 2.26 dans le cas où $n = 6$ sur la matrice

$$\overline{\sigma} = \overline{(0\ 3\ 5)(1\ 4\ 2)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

On a $\sigma^{-1} = (0\ 5\ 3)(1\ 2\ 4)$.
Soit $\lambda_6 = (3, 3)$ le type cyclique de σ^{-1}. On a $\alpha_{\lambda_6} = (0\ 1\ 2)(3\ 4\ 5)$.
Soit $\lambda_4 = \lambda_6'$ (cas général).

On a $\lambda_4 = (3,1)$ et $\alpha_{\lambda_4} = (0\ 1\ 2)(3) = \alpha_{\lambda_6}(4\ \ 5)(3\ \ 4) = \alpha_{\lambda_6}(3\ \ 4)(5\ \ 3)$.
Soit $\lambda_2 = \lambda_4'$ (cas particulier B). On a $\lambda_2 = (2)$ et $\alpha_{\lambda_2} = (0\ \ 1) = \alpha_{\lambda_4}(1\ \ 2)$.

On part de $\overline{I_2} = \alpha_{\lambda_2}$ et on calcule successivement une décomposition de $\overline{I_4}$ et $\overline{I_6}$:
$\overline{I_4} = [1:2:3]^{-1}\overline{I_2}[1:2:3] = [1:2:3]^{-1}\alpha_{\lambda_2}[1:2:3]$
$\overline{I_4} = [1:2:3]^{-1}\alpha_{\lambda_4}(1\ \ 2)[1:2:3] = [1:2:3]^{-1}\alpha_{\lambda_4}[3:1:2]^{-1}$
$\overline{I_6} = [3:4:5]^{-1}\overline{I_4}[3:4:5] = [3:4:5]^{-1}[1:2:3]^{-1}\alpha_{\lambda_4}[3:1:2]^{-1}[3:4:5]$
$\overline{I_6} = (4\ \ 5)[3:4:5]^{-1}[1:2:3]^{-1}\alpha_{\lambda_4}[3:1:2]^{-1}[3:4:5](4\ \ 5)$
$\overline{I_6} = [4:5:3][1:2:3]^{-1}\alpha_{\lambda_4}[3:1:2]^{-1}[4:5:3]^{-1}$
$\overline{I_6} = [4:5:3][1:2:3]^{-1}\alpha_{\lambda_6}(3\ \ 4)(5\ \ 3)[3:1:2]^{-1}[4:5:3]^{-1}$
$\overline{I_6} = [4:5:3][1:2:3]^{-1}\alpha_{\lambda_6}\left([3:1:2]^{-1}\right)^{(3\ \ 4)(5\ \ 3)}(3\ \ 4)(5\ \ 3)[4:5:3]^{-1}$
$\overline{I_6} = [4:5:3][1:2:3]^{-1}\alpha_{\lambda_6}\left([3:1:2]^{(3\ \ 4)(5\ \ 3)}\right)^{-1}(3\ \ 4)[5:3:4]$
$\overline{I_6} = [4:5:3][1:2:3]^{-1}\alpha_{\lambda_6}[5:1:2]^{-1}[4:3:5]^{-1}$

On détermine une permutation γ telle que $\sigma^{-1} = \alpha_{\lambda_6}^{\gamma}$: $\gamma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 3 & 1 & 2 & 4 \end{pmatrix}$.
$\overline{I_6} = (\overline{I_6})^{\gamma} = ([4:5:3][1:2:3]^{-1})^{\gamma}\sigma^{-1}([5:1:2]^{-1}[4:3:5]^{-1})^{\gamma}$
$\overline{I_6} = [2:4:1][5:3:1]^{-1}\sigma^{-1}[4:5:3]^{-1}[2:1:4]^{-1}$
$\overline{\sigma} = \sigma\overline{I_6} = ([2:4:1][5:3:1]^{-1})^{\sigma}[4:5:3]^{-1}[2:1:4]^{-1}$
$\overline{\sigma} = [1:2:4][0:5:4]^{-1}[4:5:3]^{-1}[2:1:4]^{-1}$
$\overline{\sigma} = [1:2][4:1][2:4][5:4][4:0][0:5][5:3][3:4][4:5][1:4][4:2][2:1]$

2.5 Conclusion et perspectives

Dans la section 2.1.2 nous avons abordé le problème de l'implantation d'une porte *CNOT* dans un ordinateur quantique en tenant compte des contraintes de connectivité entre les qubits. Ce problème est un cas particulier simple d'un problème plus général : le problème de l'implantation d'un circuit de portes *CNOT* dans un ordinateur quantique ayant un graphe de connectivité qui n'est pas complet. Ce problème a fait l'objet de nombreuses publications depuis les années 2000, par exemple [120, 138, 113, 146, 170, 89].

Concernant l'optimisation des circuits de portes *CNOT*, nous nous sommes placés dans le cas d'un ordinateur quantique dont le graphe de connectivité est complet, ce qui signifie d'un point de vue algébrique que la partie génératrice considérée pour le groupe $\langle CNOT\rangle_n$ est l'ensemble des $n(n-1)$ transvections $[i:j]$. Il ne s'agit pas seulement d'un cas idéal qui n'existerait pas dans la réalité. Actuellement certaines pistes sont explorées par les physiciens pour développer et perfectionner de telles machines (voir par exemple [160]), même si les ordinateurs quantiques qui ont la plus grande visibilité publique comme ceux proposés par IBM [3] ont des contraintes de connectivité plus ou moins fortes suivant les machines. En attendant de connaître les choix technologiques qui prévaudront dans les années à venir, rien n'interdit de développer des heuristiques de réduction de circuit ou des algorithmes d'optimisation pour le graphe complet : on pourra toujours chercher dans un second temps à adapter les circuits obtenus à un graphe de connectivité donné.

Actuellement, il n'existe pas à notre connaissance d'algorithme polynomial permettant d'écrire un élément de $\mathrm{GL}_n(\mathbb{F}_2)$, donné par un produit de transvections appartenant à une partie génératrice du groupe, en un produit de longueur minimale. Pourtant ce type d'algorithme existe pour certains groupes, par exemple pour le groupe symétrique

(voir chapitre 3 et [82]) et plus généralement pour les groupes de Coxeter [11] dont fait partie le groupe symétrique (voir par exemple [27, chapitre 3]). La recherche d'un algorithme polynomial permettant d'obtenir un mot réduit en utilisant les règles de réécriture énoncées dans le théorème 2.17 est une voie qui reste à explorer.

11. Voir annexe A, section A.5.3

Chapitre 3

Circuits quantiques composés de portes CZ et $CNOT$

Pour tout entier $n \geqslant 2$, on désigne par $\langle CZ, CNOT\rangle_n$ le groupe engendré par les portes CZ et $CNOT$ agissant sur n qubits. Dans le chapitre 2, nous avons remarqué que le groupe $\langle SWAP\rangle_n$ est un sous-groupe du groupe $\langle CNOT\rangle_n$. Ainsi le groupe engendré par les portes CZ et $SWAP$, noté $\langle CZ, SWAP\rangle_n$, est un sous-groupe du groupe $\langle CZ, CNOT\rangle_n$.

La première section de ce chapitre est consacrée à l'étude du groupe $\langle CZ, SWAP\rangle_n$. Après avoir établi sa structure, nous montrons qu'il existe un lien entre ce groupe et les groupes de Coxeter, puis nous appliquons les résultats obtenus à l'optimisation des circuits quantiques composés de portes CZ et $SWAP$. Notez que les démonstrations des deux principaux théorèmes de la première section (théorèmes 3.8 et 3.11) ont été reportées en annexe B. Ces démonstrations sont longues et techniques et nous avons souhaité donner plus de fluidité à la lecture. La plupart des résultats de cette première section sont tirés de [19].

Dans la seconde section, nous étudions le groupe $\langle CZ, CNOT\rangle_n$ et nous en déduisons une implantation des états de graphe basée sur l'utilisation de portes $CNOT$. Les états de graphe sont des états particuliers d'un système quantique qui jouent un rôle important dans la théorie de l'information quantique [140]. Nous en donnons une définition précise un peu plus loin dans le chapitre (définition 3.18). Ces états sont utilisés dans de nombreux domaines comme le calcul quantique basé sur la mesure, les codes quantiques correcteurs d'erreurs, l'étude de l'intrication ou les protocoles de partage de secret. Nous invitons le lecteur intéressé par ces différentes applications à lire la longue introduction de [97]) qui contient de très nombreuses références sur ces différents sujets. Pour des travaux plus récents (postérieurs à 2006) en lien avec les états de graphes, on pourra consulter par exemple [137, 109, 20] (sur le partage de secret), [177, 32, 39] (sur le calcul quantique basé sur la mesure) ou encore [81] (sur des liens entre les états de graphes et la géométrie algébrique). La plupart des résultats de la seconde section sont tirés de [16].

3.1 Étude du groupe engendré par les portes *CZ* et *SWAP* et application à l'optimisation des circuits

3.1.1 Structure du groupe engendré par les portes *CZ* et *SWAP*

Groupe engendré par les portes *CZ*

On rappelle (voir équation (1.70)) que l'action d'une porte $Z_{\{i,j\}}$ sur un ket de base $|b\rangle$ est donné par :

$$Z_{\{i,j\}} |b\rangle = (-1)^{b_i b_j} |b\rangle .$$

On voit alors que les opérateurs unitaires $Z_{\{i,j\}}$ sont des involutions et que leurs matrices dans la base standard sont diagonales. Elles commutent donc entre elles. Le groupe $\langle CZ\rangle_n$ engendré par ces portes est donc un groupe abélien isomorphe à $\mathbb{Z}_2^{\frac{n(n-1)}{2}}$. On a ainsi :

$$\langle CZ\rangle_n \simeq \mathbb{Z}_2^{\frac{n(n-1)}{2}}, \tag{3.1}$$

$$|\langle CZ\rangle_n| = 2^{\frac{n(n-1)}{2}}. \tag{3.2}$$

On note $\mathcal{G}_n$ l'ensemble des parties de l'ensemble formé de toutes les paires $\{i,j\}$:

$$\mathcal{G}_n = \mathcal{P}(\{\{i,j\} \mid 0 \leqslant i,j \leqslant n-1, i \neq j\}). \tag{3.3}$$

L'ensemble $\mathcal{G}_n$ est l'ensemble des graphes simples d'ordre n et on peut indexer les éléments de $\langle CZ\rangle_n$ par ceux de $\mathcal{G}_n$ en posant, pour tout $G \in \mathcal{G}_n$:

$$Z_G = \prod_{\{i,j\}\in G} Z_{\{i,j\}}. \tag{3.4}$$

L'action d'un élément $Z_G \in \langle CZ\rangle_n$ sur un ket $|b\rangle$ de la base standard est donnée par :

$$Z_G |b\rangle = (-1)^{\sum_{\{i,j\}\in G} b_i b_j} |b\rangle . \tag{3.5}$$

On en déduit que la matrice de Z_G dans la base standard est une matrice diagonale dont les éléments sur la diagonale sont 1 ou -1.

L'ensemble $\mathcal{G}_n$ muni de la différence symétrique (la réunion moins l'intersection), notée ici $\oplus$, est un groupe abélien et on a, pour tout $G, G' \in \mathcal{G}_n$,

$$Z_G Z_{G'} = Z_{G\oplus G'}. \tag{3.6}$$

Ainsi le groupe $\langle CZ\rangle_n$ est isomorphe au groupe $(\mathcal{G}_n, \oplus)$:

$$\langle CZ\rangle_n \simeq (\mathcal{G}_n, \oplus). \tag{3.7}$$

En utilisant cette indexation par des parties, la porte $Z_{\{i,j\}}$ devrait se noter $Z_{\{\{i,j\}\}}$ mais on conservera en général la notation $Z_{\{i,j\}}$ plus commode.

Remarque 3.1. On prendra garde au fait que Z_G désigne un opérateur de $\langle CZ\rangle_n$, c'est à dire un circuit de portes *CZ* alors que la notation Z_v (avec $v \in \mathbb{F}_2^n$) introduite au chapitre 1 (section 1.3.1) désigne un circuit de portes de Pauli Z.

À tout élément $G \in \mathcal{G}_n$ on fait correspondre une matrice symétrique à éléments dans $\mathbb{F}_2$ dont les entrées (i,j) valent 1 si et seulement si $\{i,j\} \in G$. Une telle matrice n'est autre que la matrice d'adjacence du graphe G, qui est dans ce cas symétrique et de diagonale nulle puisqu'il s'agit d'un graphe simple non orienté. L'ensemble de ces matrices forme un groupe additif qui est donc isomorphe à $\mathcal{G}_n$ et que nous noterons $\mathcal{B}_n^0$:

$$(\mathcal{G}_n, \oplus) \simeq (\mathcal{B}_n^0, \oplus). \tag{3.8}$$

Par cet isomorphisme, l'élément $\{\{i,j\}\}$ de $\mathcal{G}_n$ correspond à la matrice $E_{\{i,j\}}$ de $\mathcal{B}_n^0$ définie par

$$E_{\{i,j\}} = E_{ij} \oplus E_{ji}, \tag{3.9}$$

avec E_{ij} la matrice dont toutes les entrées sont nulles sauf l'entrée (i,j) qui est égale à 1. Par la suite, on pourra aussi bien indexer les éléments de $\langle CZ \rangle_n$ par des matrices de $\mathcal{B}_n^0$ que par des graphes de $\mathcal{G}_n$. Ainsi, on peut réécrire l'équation (3.4) en

$$Z_B = \prod_{i<j} Z_{\{i,j\}}^{B_{ij}} \tag{3.10}$$

et l'équation (3.5) en

$$Z_B \left|b\right\rangle = (-1)^{\sum_{i<j} B_{ij} b_i b_j} \left|b\right\rangle. \tag{3.11}$$

Enfin, à tout élément $B \in \mathcal{B}_n^0$, on associe la forme quadratique q_B définie pour tout vecteur $b \in \mathbb{F}_2^n$ par :

$$q_B(b) = \sum_{i<j} B_{ij} b_i b_j. \tag{3.12}$$

En utilisant cette forme quadratique, l'équation (3.11) s'écrit de façon plus compacte en :

$$Z_B \left|b\right\rangle = (-1)^{q_B(b)} \left|b\right\rangle. \tag{3.13}$$

Produit semi-direct de groupes

Pour toute permutation $\sigma \in \mathfrak{S}_n$ et tout graphe $G \in \mathcal{G}_n$, on note $\sigma(G)$ le graphe isomorphe à G tel que :

$$\sigma(G) = \{\{\sigma(i), \sigma(j)\} \mid \{i,j\} \in G\}. \tag{3.14}$$

Si B_G désigne la matrice d'adjacence de G alors la matrice d'adjacence de $\sigma(G)$ est obtenue en appliquant la permutation σ aux lignes et aux colonnes de B_G, donc :

$$B_{\sigma(G)} = \sigma B \sigma^{-1}, \tag{3.15}$$

où dans cette dernière expression σ désigne la matrice de permutation associée à la permutation σ.

Il s'avère que le groupe $\langle CZ \rangle_n$ est stable par conjugaison par tout élément du groupe $\langle SWAP \rangle_n$ ce qui va nous permettre de déterminer la structure de $\langle CZ, SWAP \rangle_n$.

Proposition 3.2. *Le groupe $\langle CZ \rangle_n$ est un sous-groupe normal de $\langle CZ, SWAP \rangle_n$. Pour tout graphe $G \in \mathcal{G}_n$, toute matrice $B \in \mathcal{B}_n^0$ et toute permutation $\sigma \in \mathfrak{S}_n$, l'action par conjugaison du groupe $\langle SWAP \rangle_n$ sur le groupe $\langle CZ \rangle_n$ est donnée par :*

$$S_\sigma Z_G S_\sigma^{-1} = Z_{\sigma(G)}, \tag{3.16}$$

$$S_\sigma Z_B S_\sigma^{-1} = Z_{\sigma B \sigma^{-1}}. \tag{3.17}$$

Démonstration. Pour démontrer l'identité (3.16), il suffit de comparer l'action de chaque membre de cette égalité sur un ket $|b\rangle$ de la base standard, en utilisant les identités (3.5) et (2.3). D'une part on a :

$$\begin{aligned} S_\sigma Z_G S_\sigma^{-1} |b\rangle &= S_\sigma Z_G |b_{\sigma(0)} \dots b_{\sigma(n-1)}\rangle \\ &= (-1)^{\sum_{\{i,j\}\in G} b_{\sigma(i)} b_{\sigma(j)}} S_\sigma |b_{\sigma(0)} \dots b_{\sigma(n-1)}\rangle \\ &= (-1)^{\sum_{\{i,j\}\in G} b_{\sigma(i)} b_{\sigma(j)}} |b\rangle . \end{aligned}$$

D'autre part on a :

$$\begin{aligned} Z_{\sigma(G)} |b\rangle &= (-1)^{\sum_{\{i,j\}\in \sigma(G)} b_i b_j} |b\rangle \\ &= (-1)^{\sum_{\{i,j\}\in G} b_{\sigma(i)} b_{\sigma(j)}} |b\rangle , \end{aligned}$$

ce qui prouve l'identité (3.16).

L'identité (3.17) se déduit de (3.16) en utilisant l'isomorphisme entre $\mathcal{B}_n^0$ et $\mathcal{G}_n$ ainsi que la formule (3.15). □

Théorème 3.3. *Pour tous les graphes $G, G' \in \mathcal{G}_n$ et toutes les permutations $\sigma, \sigma' \in \mathfrak{S}_n$ on a :*

$$Z_G S_\sigma Z_{G'} S_{\sigma'} = Z_{G\oplus\sigma(G')} S_{\sigma\sigma'} \tag{3.18}$$

Tout élément du groupe $\langle CZ, SWAP\rangle_n$ peut s'écrire de façon unique sous la forme ZS, c'est à dire comme le produit d'un élément du groupe $\langle CZ\rangle_n$ par un élément du groupe $\langle SWAP\rangle_n$. En conséquence le cardinal du groupe $\langle CZ, SWAP\rangle_n$ est :

$$|\langle CZ, SWAP\rangle_n| = n! 2^{\frac{n(n-1)}{2}}. \tag{3.19}$$

La multiplication définie par

$$(G, \sigma)(G', \sigma') = (G \oplus \sigma(G'), \sigma\sigma'), \tag{3.20}$$

confère au produit cartésien $\mathcal{G}_n \times \mathfrak{S}_n$ une structure de produit semi-direct de groupes[1] *et le groupe $\langle CZ, SWAP\rangle_n$ est isomorphe à ce produit semi-direct :*

$$\langle CZ, SWAP\rangle_n \simeq \mathcal{G}_n \rtimes \mathfrak{S}_n. \tag{3.21}$$

Démonstration. En utilisant l'identité (3.16) on a :

$$Z_G S_\sigma Z_{G'} S_{\sigma'} = Z_G S_\sigma Z_{G'} S_\sigma^{-1} S_\sigma S_{\sigma'} = Z_G S_\sigma Z_{\sigma(G')} S_{\sigma\sigma'},$$

ce qui prouve l'identité (3.18). En raisonnant par induction structurelle sur l'ensemble $\langle CZ, SWAP\rangle_n$, on en déduit que tout élément de $\langle CZ, SWAP\rangle_n$ peut s'écrire sous la forme $Z_G S_\sigma$, c'est à dire sous la forme ZS. De plus, si $Z_G S_\sigma = Z_{G'} S_{\sigma'}$, alors $Z_{G\oplus G'} = S_{\sigma'\sigma^{-1}}$ donc $Z_{G\oplus G'}$ est une matrice de permutation de U_{2^n}, ce qui prouve que $Z_{G\oplus G'} = I$ puisque la matrice de Z_G dans la base standard est une matrice diagonale. On en déduit que $G = G'$ puis que $\sigma = \sigma'$. Ainsi, la décomposition d'un élément de $\langle CZ, SWAP\rangle_n$ sous la forme ZS est unique.

Le fait que le groupe $\langle CZ\rangle_n$ soit un sous-groupe normal de $\langle CZ, SWAP\rangle_n$ et que tout élément de $\langle CZ\rangle_n$ puisse s'écrire de façon unique sous la forme ZS montre que le groupe

1. Voir annexe A, section A.3.3

$\langle CZ, SWAP\rangle_n$ est le produit semi-direct interne [2] de ses sous-groupes $\langle CZ\rangle_n$ et $\langle SWAP\rangle_n$, ce qui s'écrit $\langle CZ, SWAP\rangle_n \simeq \langle CZ\rangle_n \rtimes \langle SWAP\rangle_n$. Pour tout $\sigma \in \mathfrak{S}_n$, définissons $\Phi(\sigma)$, l'automorphisme de $\mathcal{G}_n$ tel que, pour tout $G \in \mathcal{G}_n$, on a $\Phi(\sigma)(G) = \sigma(G)$. Il est clair que Φ est un morphisme de $\mathfrak{S}_n$ dans le groupe des automorphismes de $\mathcal{G}_n$. On définit alors une multiplication dans le produit cartésien $\mathcal{G}_n \times \mathfrak{S}_n$ de la façon suivante :

$$(G, \sigma)(G', \sigma') = (G \oplus \sigma(G'), \sigma\sigma').$$

Muni de cette multiplication, le produit cartésien $\mathcal{G}_n \times \mathfrak{S}_n$ a une structure de produit semi-direct des groupes $\mathcal{G}_n$ et $\mathfrak{S}_n$. Ce groupe est noté $\mathcal{G}_n \rtimes_\Phi \mathfrak{S}_n$.

L'unicité de la forme ZS montre que le morphisme de $\langle CZ, SWAP\rangle_n$ vers $\mathcal{G}_n \rtimes_\Phi \mathfrak{S}_n$ qui, à tout élément $Z_G S_\sigma$, associe l'élément (G, σ) est un isomorphisme. □

Remarque 3.4. En utilisant une approche matricielle pour décrire les circuits de portes CZ, la formule 3.18 s'écrit :

$$Z_B S_\sigma Z_{B'} S_{\sigma'} = Z_{B \oplus \sigma B' \sigma^{-1}} S_{\sigma\sigma'}, \tag{3.22}$$

pour toutes les matrices $B, B' \in \mathcal{B}_n^0$ et toutes les permutations $\sigma, \sigma' \in \mathfrak{S}_n$.

3.1.2 Lien avec les groupes de Coxeter

Nous donnons ici deux présentations du groupe $\langle CZ, SWAP\rangle_n$ qui montrent que ce groupe peut être vu comme le quotient de groupes de Coxeter. Concernant les deux notions mises en jeu (présentation d'un groupe et groupes de Coxeter), nous invitons le lecteur à consulter l'annexe A, sections A.5 et A.5.3.

Les preuves que nous proposons sont basées sur les deux propriétés suivantes des présentations de groupe. La première propriété semble assez classique (voir par exemple [112]) et explique comment obtenir une présentation d'un groupe qui est le produit semi-direct de deux groupes dont les présentations sont connues. La seconde propriété est assez intuitive et formalise une méthode naturelle de réduction du nombre de générateurs d'une présentation dans certains cas. Dans un premier temps, nous montrons comment ces propriétés permettent de construire une présentation de $\langle CZ, SWAP\rangle_3$ puis nous généralisons la méthode.

Proposition 3.5 (voir [112])**.** *Soient $G_1 \simeq \langle \mathcal{S}_1 \mid \mathcal{R}_1\rangle$ et $G_2 \simeq \langle \mathcal{S}_2 \mid \mathcal{R}_2\rangle$ deux groupes donnés par une présentation. Le produit semi-direct $G_1 \rtimes_\Phi G_2$ admet comme présentation*

$$\langle \mathcal{S}_1 \cup \mathcal{S}_2 \mid \mathcal{R}_1 \cup \mathcal{R}_2 \cup \{g_2 g_1 g_2^{-1} \left(\Phi(g_2)(g_1)\right)^{-1} \mid g_1 \in \mathcal{S}_1, g_2 \in \mathcal{S}_2\}\rangle, \tag{3.23}$$

où Φ désigne le morphisme de G_2 dans $\mathrm{Aut}(G_1)$ définissant le produit semi-direct de G_1 et G_2.

Proposition 3.6. *Soit G un groupe admettant une présentation $\langle \mathcal{S} | \mathcal{R}\rangle$. On suppose que $\mathcal{S}$ est la réunion disjointe de $\mathcal{S}_1$ et $\mathcal{S}_2$ et que, pour chaque générateur g dans $\mathcal{S}_2$, on puisse déduire des relations de $\mathcal{R}$ une égalité $g = w_g$, où w_g est un élément du groupe libre engendré par $\mathcal{S}_1$. Soit $\mathcal{R}_2$ l'ensemble des relations de $\mathcal{R}$ qui s'écrivent avec au moins un élément de $\mathcal{S}_2$ et soit $\mathcal{R}_1 = \mathcal{R} \setminus \mathcal{R}_2$. On construit l'ensemble $\mathcal{R}_2'$ en remplaçant dans $\mathcal{R}_2$ chaque occurrence d'un élément de $\mathcal{S}_2$ par w_g. Alors le groupe G admet pour présentation $\langle \mathcal{S}_1 \mid \mathcal{R}_1 \cup \mathcal{R}_2'\rangle$.*

2. Voir annexe A, section A.3.2

Exemple 3.7. Le groupe $\mathcal{G}_3 \simeq \langle CZ \rangle_3$ est isomorphe à $\mathbb{Z}_2^3$ donc isomorphe au groupe $G_1 = \langle z_0, z_1, z_{02} \mid z_0^2, z_1^2, z_{02}^2, (z_0 z_{02})^2, (z_0 z_1)^2, (z_0 z_{02})^2 \rangle$. L'isomorphisme entre $\langle CZ \rangle_3$ et G_1 associe $Z_{\{0,1\}}$ à z_0, $Z_{\{1,2\}}$ à z_1 et $Z_{\{0,2\}}$ à z_{02}.

Le groupe symétrique $\mathfrak{S}_3 \simeq \langle SWAP \rangle_3$ est isomorphe au groupe $G_2 = \langle s_0, s_1 \mid s_0^2, s_1^2, (s_0 s_1)^3 \rangle$ [3]. L'isomorphisme entre $\langle SWAP \rangle_3$ et G_2 associe $S_{(0\ 1)}$ à s_0 et $S_{(1\ 2)}$ à s_1.

En appliquant la proposition 3.5, il résulte qu'une présentation de $\mathcal{G}_3 \rtimes \mathfrak{S}_3$, c'est à dire de $\langle CZ, SWAP \rangle_3$ est $\langle z_0, z_1, z_{02}, s_0, s_1 \mid \mathcal{R} \rangle$, avec

$$\mathcal{R} = \{z_0^2, z_1^2, z_{02}^2, (z_0 z_{02})^2, (z_0 z_1)^2, (z_0 z_{02})^2, (z_1 z_{02})^2, s_0^2, s_1^2, (s_0 s_1)^3, \\ (z_0 s_0)^2, (z_1 s_1)^2, s_1 z_0 s_1 z_{02}, s_0 z_1 s_0 z_{02}\}.$$

On utilise la proposition 3.6 avec $\mathcal{S}_1 = \{z_0, z_1, s_0, s_1\}$ et $\mathcal{S}_2 = \{z_{02}\}$. En effet, on remarque qu'à partir des relations $s_1 z_0 s_1 z_{02} = 1$ et $z_{02}^2 = 1$ on a : $z_{02} = s_1 z_0 s_1$. On pose donc

$$\mathcal{R}_1 = \{z_0^2, z_1^2, (z_0 z_1)^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 s_0)^2, (z_1 s_1)^2\}$$

et

$$\mathcal{R}_2 = \{z_{02}^2, (z_1 z_{02})^2, (z_0 z_{02})^2, s_1 z_0 s_1 z_{02}, s_0 z_1 s_0 z_{02}\}.$$

On a alors

$$\mathcal{R}_2' = \{(s_1 z_0 s_1)^2, (z_1 s_1 z_0 s_1)^2, (z_0 s_1 z_0 s_1)^2, s_1 z_0 s_1 s_1 z_0 s_1, s_0 z_1 s_0 s_1 z_0 s_1\}.$$

Puisque $s_1^2 = z_0^2 = 1$, on peut éliminer la relation $s_1 z_0 s_1 s_1 z_0 s_1$ de $\mathcal{R}_2'$. De plus la relation $s_0 z_1 s_0 s_1 z_0 s_1 = 1$ implique que $(z_1 s_1 z_0 s_1)^2 = (z_1 s_0)^4$. Ainsi $\langle CZ, SWAP \rangle_3$ est isomorphe à

$$\langle z_0, z_1, s_0, s_1 | z_0^2, z_1^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 z_1)^2, (z_0 s_0)^2, (z_1 s_1)^2, \\ (z_0 s_1)^4, (z_1 s_0)^4, s_0 s_1 z_0 s_1 s_0 z_1 \rangle. \tag{3.24}$$

On peut diminuer le nombre de relations dans cette présentation en remarquant qu'il y a des redondances. En effet, en utilisant les relations $z_0 = z_1^2 = 1$, $s_0^2 = s_1^2 = 1$, $(s_0 s_1)^3 = 1$, $(z_0 s_0)^2 = 1$, $(z_0 s_1)^4$ et $s_0 s_1 z_0 s_1 s_0 z_1 = 1$, on obtient :

$$\begin{aligned}(z_1 s_1)^2 &= (z_1 s_1)(z_1 s_1) \\ &= (s_0 s_1 z_0 s_1 s_0 s_1)(s_0 s_1 z_0 s_1 s_0 s_1) \\ &= s_0 s_1 z_0 s_0 z_0 s_0 s_1 s_0 \\ &= s_0 s_1 (z_0 s_0)^2 s_1 s_0 = 1,\end{aligned}$$

$(z_0 s_1)^4 = (z_0 s_1 z_0 s_1)^2 = (z_0 s_0 z_1 s_0)^2 = (s_0 z_0 z_1 s_0)^2 = s_0 (z_0 z_1)^2 s_0$ donc

$$(z_0 z_1)^2 = s_0 (z_0 s_1)^4 s_0 = 1,$$

et $(z_1 s_0)^4 = (z_1 s_0 z_1 s_0)^2 = (z_1 s_1 z_0 s_1)^2 = (s_1 z_1 z_0 s_1)^2 = s_1 (z_1 z_0)^2 s_1 = s_1 (z_0 z_1)^2 s_1 = 1$.

ce qui prouve que les relations $(z_1 s_1)^2 = 1$, $(z_0 z_1)^2 = 1$ et $(z_1 s_0)^4 = 1$ sont redondantes. On simplifie alors la présentation de $\langle CZ, SWAP \rangle_3$ en :

$$\langle z_0, z_1, s_0, s_1 | z_0^2, z_1^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 s_0)^2, (z_0 s_1)^4, s_0 s_1 z_0 s_1 s_0 z_1 \rangle.$$

3. voir annexe A, section A.5.3

On remarque qu'on peut à nouveau appliquer la proposition 3.6 afin d'éliminer le générateur z_1. En effet, comme $s_0 s_1 z_0 s_1 s_0 z_1 = 1$ et $z_1^2 = 1$ on a $z_1 = s_0 s_1 z_0 s_1 s_0$. On obtient alors :

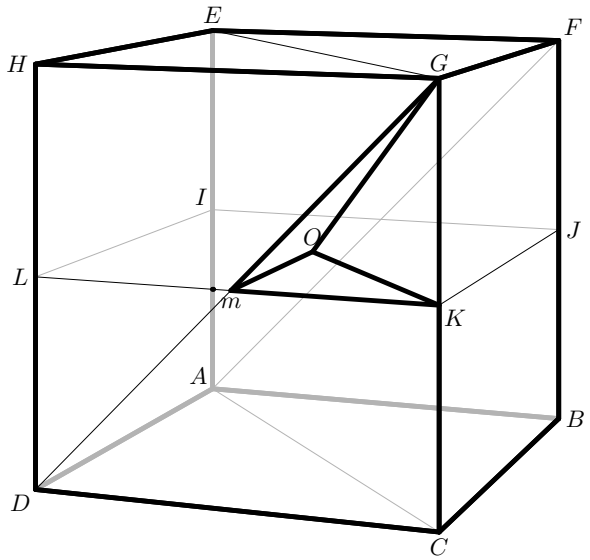
$$\langle CZ, SWAP\rangle_3 \simeq \langle z_0, s_0, s_1 | z_0^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 s_0)^2, (z_0 s_1)^4\rangle. \tag{3.25}$$

On renomme les symboles en posant $g_0 = z_0$, $g_1 = s_0$, $g_2 = s_1$ et on a finalement :

$$\langle CZ, SWAP\rangle_3 \simeq \langle g_0, g_1, g_2 | g_0^2, g_1^2, g_2^2, (g_1 g_2)^3, (g_0 g_1)^2, (g_0 g_2)^4\rangle. \tag{3.26}$$

Le groupe $\langle CZ\rangle_3$ est donc un groupe de Coxeter de matrice $M = \begin{bmatrix} 1 & 2 & 4 \\ 2 & 1 & 3 \\ 4 & 3 & 1 \end{bmatrix}$. Il s'agit du groupe des isométries laissant le cube invariant (voir figure 3.1). Ce groupe est d'ordre 48.

Figure 3.1 Le groupe $\langle CZ, SWAP\rangle_3$ est isomorphe au groupe des isométries laissant le cube invariant.



Le groupe des isométries laissant le cube $ABCDEFGH$ invariant est engendré par les trois symétries par rapports aux plans $(IJKL)$, $(EGCA)$ et $(DAFG)$.
L'angle entre les plans $(EGCA)$ et $(DAFG)$ vaut $\pi/3$ et peut se calculer par exemple à partir des deux vecteurs normaux $\overrightarrow{OG} \wedge \overrightarrow{OK}$ et $\overrightarrow{OG} \wedge \overrightarrow{Om}$ à ces plans (voir [162] pour plus de détails). L'angle entre les plans $(IJKL)$ et $(EGCA)$ vaut $\pi/2$ et celui entre les plans $(IJKL)$ et $(DAFG)$ vaut $\pi/4$. On a donc $(s_{(IJKL)} s_{(EGCA)})^2 = I$, $(s_{(EGCA)} s_{(DAFG)})^3 = I$ et $(s_{(IJKL)} s_{(DAFG)})^4 = I$ et les correspondances :

$$s_{(IJKL)} \simeq z_0 \simeq Z_{\{0,1\}},$$
$$s_{(EGCA)} \simeq s_0 \simeq S_{(0\ 1)},$$
$$s_{(DAFG)} \simeq s_1 \simeq S_{(1\ 2)}.$$

Théorème 3.8. *Soit un entier $n \geqslant 2$. Le groupe $\langle CZ, SWAP\rangle_n$ est isomorphe à la présentation $\langle z_0, \ldots, z_{n-2}, s_0, \ldots, s_{n-2} \mid \mathcal{R}\rangle$, où $\mathcal{R}$ est l'ensemble de relations :*

(i) *pour tout* $0 \leqslant i \leqslant n-2$, $z_i^2 = s_i^2 = 1$,

(ii) *pour tout* $0 \leqslant i < j \leqslant n-2$ *tel que* $j - i > 1$, $(s_i s_j)^2 = 1$,

(iii) *pour tout* $0 \leqslant i \leqslant n-3$, $(s_i s_{i+1})^3 = 1$,

(iv) *pour tout* $0 \leqslant i < j \leqslant n-2$, $(z_i z_j)^2 = 1$,

(v) *pour tout* $0 \leqslant i, j \leqslant n-2$ *tel que* $|i-j| \neq 1$, $(z_i s_j)^2 = 1$,

(vi) *pour tout* $0 \leqslant i, j \leqslant n-2$ *tel que* $|i-j| = 1$, $(z_i s_j)^4 = 1$,

(vii) *pour tout* $0 \leqslant i \leqslant n-3$, $s_i s_{i+1} z_i s_{i+1} s_i z_{i+1} = 1$.

Un isomorphisme explicite envoie chaque opérateur $Z_{\{i,i+1\}}$ *sur* z_i *et chaque opérateur* $S_{(i\ \ i+1)}$ *sur* s_i.

Démonstration. Voir annexe B, section B.1 □

Du théorème 3.8, on déduit le lien suivant entre le groupe $\langle CZ, SWAP\rangle_n$ et les groupes de Coxeter.

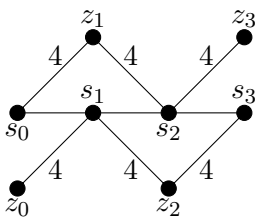
Corollaire 3.9. *Soit* $\mathcal{W}_n$ *le groupe de Coxeter engendré par les* $2(n-1)$ *éléments* $g_0, g_1, \ldots, g_{2(n-2)+1}$ *soumis aux relations encodées dans la matrice de Coxeter*

$$M_n = \begin{bmatrix} D & A & B & \cdots & B \\ A & \ddots & \ddots & \ddots & \vdots \\ B & \ddots & \ddots & \ddots & B \\ \vdots & \ddots & \ddots & \ddots & A \\ B & \cdots & B & A & D \end{bmatrix} \tag{3.27}$$

avec $A = \begin{bmatrix} 2 & 4 \\ 4 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$ *et* $D = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$.

Le groupe $\langle CZ, SWAP\rangle_n$ *est isomorphe au quotient* $\mathcal{W}_n/_{\mathcal{R}_n}$ *de* $\mathcal{W}_n$ *par les relations* $\mathcal{R}_n = \{g_{2i+1}g_{2i+3}g_{2i}g_{2i+3}g_{2i+1}g_{2i+2} = 1 \mid 0 \leqslant i \leqslant n-3\}$. *Un isomorphisme explicite envoie chaque opérateur* $Z_{\{i,i+1\}}$ *sur* g_{2i} *et chaque opérateur* $S_{(i\ \ i+1)}$ *sur* g_{2i+1}.

Exemple 3.10. Le groupe $\langle CZ, SWAP\rangle_5$ est isomorphe au groupe engendré par les éléments $\{z_0, s_0, z_1, s_1, z_2, s_2, z_3, s_3\}$ soumis aux relations $s_i^2 = z_i^2 = 1$, $(s_0s_1)^3 = (s_1s_2)^3 = (s_2s_3)^3 = 1$, $(s_0s_2)^2 = (s_0s_3)^2 = (s_1s_3)^2 = 1$, $(z_0s_1)^4 = (z_1s_0)^4 = (z_1s_2)^4 = (z_2s_1)^4 = (z_2s_3)^4 = (z_3s_2)^4 = 1$, $(z_0s_0)^2 = (z_0s_2)^2 = (z_0s_3)^2 = (z_1s_1)^2 = (z_1s_3)^2 = (z_2s_0)^2 = (z_2s_2)^2 = (z_3s_0)^2 = (z_3s_1)^2 = (z_3s_3)^2$, et $s_0s_1z_0s_1s_0s_1 = s_1s_2z_1s_2s_1z_2 = s_2s_3z_2s_3s_2z_3 = 1$. Le groupe $\langle CZ, SWAP\rangle_5$ est le quotient du groupe $\mathcal{W}_5$ ayant pour diagramme de Coxeter



par les relations $s_0s_1z_0s_1s_0z_1 = s_1s_2z_1s_2s_1z_2 = s_2s_3z_2s_3s_2z_3 = 1$.

On peut simplifier la présentation de $\langle CZ, SWAP\rangle_n$ donnée par le théorème 3.8, en généralisant la méthode que nous avons utilisée dans l'exemple 3.7 pour simplifier la présentation de $\langle CZ, SWAP\rangle_3$ donnée par l'équation (3.24). C'est l'objet du théorème qui suit.

Théorème 3.11. *Pour $n \geqslant 2$, le groupe $\langle CZ, SWAP\rangle_n$ est isomorphe à la présentation $\langle g_0, g_1, g_2, \ldots, g_{n-1} \mid \mathcal{R}_n\rangle$, où $\mathcal{R}_n$ est l'ensemble des relations suivantes :*

(i) Pour tout $0 \leqslant i \leqslant n-1$, $g_i^2 = 1$,

(ii) Pour tout $1 \leqslant i < j \leqslant n-1$ tel que $|i-j| > 1$, $(g_ig_j)^2 = 1$,

(iii) Pour tout $1 \leqslant i \leqslant n-2$, $(g_ig_{i+1})^3 = 1$,

(iv) Pour tout $i = 1, 3, \ldots n-1$, $(g_0g_i)^2 = 1$,

(v) $(g_0g_2)^4 = 1$,

(vi) $(g_0g_2g_3g_1g_2)^4 = 1$.

Un isomorphisme explicite envoie $Z_{\{0,1\}}$ sur g_0 et chaque $S_{(i\ \ i+1)}$ sur g_{i+1}.

Démonstration. Voir annexe B, section B.2 □

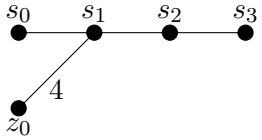
Du théorème 3.11, on déduit une autre façon d'envisager le groupe $\langle CZ, SWAP\rangle_n$ comme le quotient d'un groupe de Coxeter. En fait $\langle CZ, SWAP\rangle_n$ est le quotient d'un groupe de Coxeter engendré par n éléments, par une unique relation.

Corollaire 3.12. *Soit $\mathcal{C}_n$ le groupe de Coxeter engendré par les n éléments $g_0, g_1, \ldots, g_{n-1}$ soumis aux relations encodées dans la matrice de Coxeter*

$$N_n = \begin{bmatrix} 1 & 2 & 4 & 2 & \cdots & 2 \\ 2 & 1 & 3 & 2 & & \vdots \\ 4 & 3 & 1 & 3 & \ddots & \vdots \\ 2 & 2 & 3 & 1 & \ddots & 2 \\ \vdots & & \ddots & \ddots & \ddots & 3 \\ 2 & \cdots & \cdots & 2 & 3 & 1 \end{bmatrix}. \tag{3.28}$$

Le groupe $\langle CZ, SWAP\rangle_n$ est isomorphe au quotient $\mathcal{C}_n/_{(g_0g_2g_3g_1g_2)^4}$. Un isomorphisme explicite envoie $Z_{\{0,1\}}$ sur g_0 et chaque $S_{(i\ \ i+1)}$ sur g_{i+1}.

Exemple 3.13. Le groupe $\langle CZ, SWAP\rangle_5$ est isomorphe au quotient du groupe de Coxeter $\mathcal{C}_5$ ayant comme diagramme de Coxeter



par la relation $(z_0s_1s_2s_0s_1)^4$.

3.1.3 Optimisation de circuits composés de portes *CZ* et *SWAP*

Nous appliquons les résultats des sous-sections précédentes à la simplification de circuits, en tenant compte de la structure du réseau de qubits. En effet, si le graphe de connectivité n'est pas complet, il est nécessaire de simuler certaines portes à partir des portes natives (voir section 1.3.2) ce qui peut considérablement augmenter la taille du circuit. Nous considérons ici deux types de réseaux : le cas d'un graphe de connectivité complet et celui d'un graphe en ligne (topologie LNN).

Optimisation d'un circuit de portes *SWAP*

Afin d'illustrer comment les études algébriques précédentes permettent de trouver des algorithmes de simplification, nous commençons par présenter un des cas les plus simples de circuits quantiques : ceux qui sont composés uniquement de portes *SWAP*. En effet, le groupe $\langle SWAP\rangle_n$ est isomorphe au groupe symétrique $\mathfrak{S}_n$ (voir Sous-section 2.1.1) et c'est l'exemple le plus simple d'un sous-groupe de $\langle CZ, SWAP\rangle_n$ pour lequel le mécanisme de simplification peut être complètement décrit.

Dans le cas de la topologie du graphe complet, le procédé de décomposition d'une permutation en transpositions est bien connu : il suffit de décomposer la permutation en cycles puis chaque cycle en transpositions [4].

Dans le cas de la topologie du graphe en ligne, l'algorithme est plus subtil mais il est également classique. Le nombre minimal de facteurs dans un produit de transpositions du type $(i\ \ i+1)$ égal à σ est égal au nombre d'inversions de σ, c'est à dire le nombre de couples (i, j) tels que $i < j$ et $\sigma(i) > \sigma(j)$. Une décomposition comportant un nombre minimal de facteurs est dite *réduite* ou *optimale*. Sur le sujet des décompositions réduites dans le groupe symétrique, on pourra consulter par exemple la monographie très complète de Garsia [82].

Pour obtenir une décomposition optimale d'une permutation σ, on peut utiliser un algorithme basé sur le diagramme de Rothe [5] d'une permutation, algorithme décrit par Knuth dans [117, pp. 14,15]. Cette méthode étant classique, nous la rappelons brièvement sans démonstration. Le diagramme de Rothe d'une permutation $\sigma \in \mathfrak{S}_n$ est une matrice $n \times n$ dont les entrées (i, j) (i désignant le numéro de ligne et j le numéro de colonne) sont non vides si $(j, \sigma^{-1}(i))$ est une inversion de σ. Les entrées non vides d'une même colonne sont des entiers consécutifs croissants (du haut vers le bas) et l'entrée non vide la plus haute d'une colonne est égale au numéro de cette colonne. Une fois cette matrice construite, on obtient une décomposition réduite de σ en parcourant les entrées de la droite vers la gauche et du haut vers le bas (voir exemple figure 3.2).

Optimisation de circuits dans $\langle CZ, SWAP\rangle_n$ pour la topologie du graphe complet

Le théorème 3.3 permet de construire un algorithme de simplification de circuits constitués de portes *CZ* et *SWAP*. Le principe de cet algorithme est très simple : d'abord on applique la formule 3.22 autant de fois qu'il y a de portes dans le circuit afin d'obtenir un seul élément $Z_B S_\sigma$ (algorithme 3.1), puis on décompose σ en produit de transpositions en utilisant la formule (2.10) (voir exemple figure 3.3).

Proposition 3.14. *La complexité temporelle de l'algorithme* `C-to-ZS` *est* $O(\ell n)$.

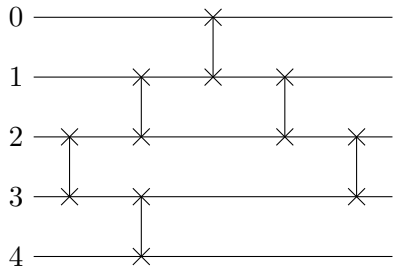
4. Voir annexe A, section A.4.2

5. Heinrich August Rothe (1773-1842), mathématicien allemand, travaux sur les séries de Taylor, les coefficients binomiaux et les permutations.

Figure 3.2 Une permutation, son diagramme de Rothe, une décomposition réduite et le circuit quantique associé. Dans cette figure, une permutation (agissant sur l'ensemble $\{0, \ldots, n-1\}$) est représentée par sa décomposition en cycles. Le symbole s_i désigne la transposition élémentaire $(i\ \ i+1)$.

$$\texttt{Rothe}((0\ \ 3)(2\ \ 4)) = \begin{bmatrix} 0 & 1 & 2 & \\ 1 & & & \\ 2 & & 3 & \\ & & & \\ & & & \end{bmatrix}$$

$$(0\ \ 3)(2\ \ 4) = s_2 s_1 s_0 s_1 s_3 s_2$$



Démonstration. Il y a ℓ portes dans le circuit en entrée et le temps de calcul pour chaque porte est au plus $O(n)$. □

Corollaire 3.15. *Tout circuit quantique de longueur ℓ composé de portes CZ et SWAP agissant sur n qubits peut être optimisé pour la topologie du graphe complet en temps $O(\ell n)$.*

Démonstration. Pour optimiser un tel circuit, on applique d'abord l'algorithme `C-to-ZS` de complexité $O(\ell n)$, puis on décompose σ en produit de transpositions ce qui a un coût de $O(n)$ opérations. Le circuit ainsi obtenu est de longueur minimale car si $Z_G S_\sigma = Z_{G_1} S_{\sigma_1} Z_{G_2} S_{\sigma_2}$ alors $|G| \leqslant |G_1| \oplus |G_2|$ et la longueur de σ (le nombre minimal de transpositions dans sa décomposition) est inférieure ou égale à la somme des longueurs de σ_1 et σ_2. □

Simplification de circuits dans $\langle CZ, SWAP\rangle_n$ pour la topologie LNN

Nous venons de voir que l'algorithme `C-to-ZS` fournit un circuit optimal dans le cas d'un ordinateur quantique ayant un graphe de connectivité complet. Cependant pour des raisons techniques les machines actuelles imposent souvent des conditions plus restrictives au réseau des qubits. Nous considérons maintenant le cas où seules les portes agissant sur deux qubits adjacents sont permises. Plus précisément, nous abordons le problème suivant : étant donné un circuit de $\langle CZ, SWAP\rangle_n$ comportant seulement des portes $Z_{\{i,i+1\}}$ et $S_{(i\ \ i+1)}$, trouver un algorithme efficace (*i.e.* ayant une complexité polynomiale raisonnable) permettant d'optimiser ce circuit, ou au moins d'en réduire le nombre de portes.

Algorithme 3.1 `C-to-ZS`

Entrée : C, un élément de $\langle CZ, SWAP\rangle_n$ donné par un produit $C = \prod_{k=1}^{\ell} M_k$ avec $M_k \in \{Z_{\{i,j\}}, S_{(i\ j)} \mid 0 \leqslant i, j \leqslant n-1\}$.
Sortie : $Z_B S_\sigma$, un élément de $\langle CZ, SWAP\rangle_n$ égal à C, avec $B \in \mathcal{B}_n^0$ et $\sigma \in \mathfrak{S}_n$.

```
B ← matrice nulle
σ ← permutation identité
pour k ← ℓ à 1 faire
    si M_k = S_(i j) alors
        échanger les lignes i et j de B
        échanger les colonnes i et j de B
        σ ← (i j)σ
    sinon // cas où M_k = Z_{i,j}
        inverser les bits B_ij et B_ji de la matrice B
    fin si
fin pour
retourner Z_B S_σ
```

Dans un premier temps on remarque qu'il existe un algorithme assez évident pour optimiser un tel circuit : on construit le graphe de Cayley du groupe $\langle CZ, SWAP\rangle_n$ à partir des générateurs $Z_{\{i,i+1\}}$ et $S_{(i\ i+1)}$ jusqu'à obtenir le circuit qu'on veut optimiser. On peut stocker chaque élément du graphe sous la forme d'un couple de matrices (B, σ) avec $B \in \mathcal{B}_n^0$ et $\sigma \in \mathfrak{S}_n$ et actualiser ce couple à chaque multiplication par un générateur en utilisant la formule (3.22). Clairement une telle approche est exponentielle en temps et en espace et n'est pas praticable dès que le nombre de qubits dépasse 6 ou 7 (voir chapitre 2, section 2.3.3).

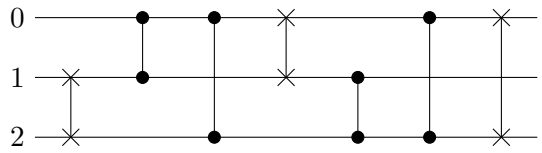
Dans le but de réduire le nombre de portes d'un circuit, une autre stratégie consiste à utiliser la présentation du groupe donnée par le théorème 3.8 ainsi que le lien entre $\langle CZ, SWAP\rangle_n$ et le groupe de Coxeter $\mathcal{W}_n$ établi dans le corollaire 3.9. Dans ce contexte on peut utiliser deux outils classiques : l'algorithme de Dehn [135] et l'algorithme de réduction d'un mot dans un groupe de Coxeter (voir par exemple [27]). Cette méthode a déjà été utilisée par Aytac et Husain [12] dans des recherches sur d'autres groupes de Coxeter dans le contexte des circuits quantiques.

Commençons par rappeler le principe de l'algorithme de Dehn. Le point de départ est une présentation finie d'un groupe G sous la forme $G \simeq \langle \mathcal{S} \mid \mathcal{R}\rangle$. On note $\tilde{\mathcal{R}}$ la fermeture de $\mathcal{R}$ par permutation cyclique des relations et de leur inverse. On considère un mot w réduit dans le groupe libre $\mathcal{F}_\mathcal{S}$ engendré par $\mathcal{S}$. L'algorithme de Dehn permet de construire une suite finie de mots $w_0 = w$, $w_1, w_2, \ldots, w_n$ de la façon suivante. S'il existe un facteur u dans w_i qui est le préfixe d'un mot $r = uv$ de $\tilde{\mathcal{R}}$ avec $|u| > |v|$, alors le facteur u de w_i est remplacé par v^{-1} et w_{i+1} est le mot réduit (dans le groupe libre) de ce mot. Sinon l'algorithme se termine. Évidemment la longueur des mots w_i est strictement décroissante, donc l'algorithme de Dehn permet de diminuer la longueur du mot initial w en un nombre fini d'étapes. Cependant le mot obtenu w_n n'est pas, à priori, de longueur optimale : il peut très bien exister un autre mot plus court qui représente le même élément de G.

Dans le cas du groupe $\langle CZ, SWAP\rangle_n$, on peut essayer d'améliorer cette méthode en mettant à profit la structure de Coxeter de $\mathcal{W}_n$. Soit un mot w sur l'alphabet des générateurs $Z_{\{i,i+1\}}$ et $S_{(i\ i+1)}$ de $\langle CZ, SWAP\rangle_n$ qui représente le circuit à réduire, on utilise successivement l'algorithme de réduction d'un mot dans le groupe de Coxeter

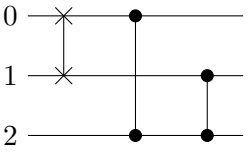
Figure 3.3 Optimisation d'un circuit de portes CZ et $SWAP$

Circuit en entrée de l'algorithme `C-to-ZS` :



$$\begin{aligned}
C &= S_{(0\ 2)}Z_{\{0,2\}}Z_{\{1,2\}}S_{(0\ 1)}Z_{\{0,2\}}Z_{\{0,1\}}S_{(1\ 2)} \\
&= S_{(0\ 2)}Z_{\{0,2\}}Z_{\{1,2\}}S_{(0\ 1)}Z_{\{0,2\}}Z_{\{0,1\}}S_{(1\ 2)} \\
&= S_{(0\ 2)}Z_{\{0,2\}}Z_{\{1,2\}}S_{(0\ 1)}Z_{\{0,2\}}Z_{\{0,1\}}S_{(1\ 2)} \\
&= S_{(0\ 2)}Z_{\{0,2\}}Z_{\{1,2\}}S_{(0\ 1)}Z_{\{\{0,2\},\{0,1\}\}}S_{(1\ 2)} \\
&= S_{(0\ 2)}Z_{\{0,2\}}Z_{\{1,2\}}Z_{\{\{1,2\},\{0,1\}\}}S_{(0\ 1)}S_{(1\ 2)} \\
&= S_{(0\ 2)}Z_{\{0,2\}}Z_{\{1,2\}}Z_{\{\{1,2\},\{0,1\}\}}S_{(0\ 1\ 2)} \\
&= S_{(0\ 2)}Z_{\{0,2\}}Z_{\{0,1\}}S_{(0\ 1\ 2)} \\
&= S_{(0\ 2)}Z_{\{\{0,2\},\{0,1\}\}}S_{(0\ 1\ 2)} \\
&= Z_{\{\{0,2\},\{1,2\}\}}S_{(0\ 2)}S_{(0\ 1\ 2)} \\
&= Z_{\{\{0,2\},\{1,2\}\}}S_{(0\ 1)}
\end{aligned}$$

Circuit en sortie de l'algorithme `C-to-ZS` :



$\mathcal{W}_5$ et l'algorithme de Dehn appliqué à la présentation de $\langle CZ, SWAP\rangle_n$ obtenue au théorème 3.8, jusqu'à stabilisation.

Exemple 3.16. Considérons le circuit qui implémente l'opérateur

$$C = Z_{\{0,1\}}Z_{\{3,4\}}S_{(1\ 2)}S_{(0\ 1)}Z_{\{1,2\}}Z_{\{3,4\}}S_{(0\ 1)}.$$

Soit l'élément $w = z_0z_3s_1s_0z_1z_3s_0$ associé à C dans la présentation décrite par le théorème 3.8. On utilise successivement les relations $(z_3z_1)^2$, $(z_3s_0)^2$, $(z_3s_1)^2$ et z_3^2 et w se réduit en $z_0s_1s_0z_1s_0$. On utilise alors l'algorithme de Dehn, en remarquant que $z_0s_1s_0z_1s_0$ est le préfixe de la relation $z_0s_1s_0z_1s_0s_1$, elle même obtenue par permutation circulaire à partir de $s_0s_1z_0s_1s_0z_1$. Donc l'élément $w = z_0s_1s_0z_1s_0$ se réduit en s_1 et on en déduit que $C = S_{(1\ 2)}$.

Cependant cette méthode n'est pas en général suffisante pour obtenir un circuit de longueur minimale comme le montre l'exemple suivant.

Exemple 3.17. Soit le circuit correspondant à l'opérateur

$$C = S_{(3\ 4)}S_{(2\ 3)}Z_{\{1,2\}}S_{(2\ 3)}S_{(3\ 4)}S_{(2\ 3)}Z_{\{1,2\}}S_{(2\ 3)}.$$

Considérons l'élément $w = s_3s_2z_1s_2s_3s_2z_1s_2$ associé à C dans la présentation 3.8. Cet élément est déjà réduit (minimal) dans $\mathcal{W}_5$. Cette minimalité peut être testée en appliquant l'algorithme de réduction dans les groupes de Coxeter décrit par exemple dans [27]. Cet algorithme est implémenté dans Sagemath [171] : il suffit d'entrer la matrice de Coxeter M_5 du groupe $\mathcal{W}_5$ et d'appeler la méthode `reduced_word()`.

Les seules relations qui peuvent être utilisées pour réduire w par l'algorithme de Dehn sont $(s_2s_3)^3$, $(z_1s_2)^4$, $(s_2z_1)^4$ et $s_1s_2z_1s_2s_1z_2$. Mais aucun facteur de $s_3s_2z_1s_2s_3s_2z_1s_2$ n'est le préfixe d'une relation $r = uv$ telle que $|u| > |v|$, donc le circuit ne peut pas être réduit en utilisant l'algorithme de Dehn. Dans ce cas, la stratégie consistant à appliquer successivement une réduction dans le groupe de Coxeter suivie par l'algorithme de Dehn ne permet pas de calculer un circuit plus court qui soit équivalent à C.

Néanmoins, à partir de $s_1s_2z_1s_2s_1z_2 = 1$, $s_i^2 = 1$ et $z_2^2 = 1$, on obtient $s_2z_1s_2 = s_1z_2s_1$, donc $w = s_3s_1z_2s_1s_3s_1z_2s_1$. En utilisant $(s_1s_3)^2 = 1$ et $s_1^2 = 1$, on a alors $w = s_3s_1z_2s_3z_2s_1$. Ainsi $C = S_{(3\ 4)}S_{(1\ 2)}Z_{\{2,3\}}S_{(3\ 4)}Z_{\{2,3\}}S_{(1\ 2)}$.

Notre dernier exemple montre comment traduire un circuit produisant un état de graphe pour la topologie en ligne en utilisant la présentation de $\langle CZ, SWAP\rangle_6$ donnée par le théorème 3.8 et l'heuristique Coxeter/Dehn. L'importance des états de graphe a été soulignée dans l'introduction de ce chapitre. Nous rappelons maintenant leur définition.

Définition 3.18. Un état de graphe d'un système de n qubits est un état

$$|G\rangle = Z_G\,|+\rangle^{\otimes n} \tag{3.29}$$

défini par un graphe $G \in \mathcal{G}_n$, avec $|+\rangle = H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Exemple 3.19. Soit $|G\rangle = Z_{\{0,2\}}Z_{\{1,3\}}Z_{\{0,4\}}Z_{\{2,4\}}Z_{\{0,5\}}Z_{\{2,5\}}|+\rangle^{\otimes 6}$ un état de graphe. Soit $C = Z_{\{0,2\}}Z_{\{1,3\}}Z_{\{0,4\}}Z_{\{2,4\}}Z_{\{0,5\}}Z_{\{2,5\}}$ le circuit à implémenter. On utilise dans un premier temps l'identité

$$Z_{\{i,j\}} = S_{(i\ i+1)}S_{(i+1\ i+2)}\cdots S_{(j-2\ j-1)}Z_{\{j-1,j\}}S_{(j-2\ j-1)}\cdots S_{(i+1\ i+2)}S_{(i\ i+1)}$$

afin d'écrire C avec les générateurs $Z_{\{i,i+1\}}$ et $S_{(i\ i+1)}$ permis par la topologie. Ainsi, l'élément associé à C dans la présentation décrite par le théorème 3.8 est :

$$w = s_0z_1s_0s_1z_2s_1s_0s_1s_2z_3s_2s_1s_0s_2z_3s_2s_0s_1s_2s_3z_4s_3s_2s_1s_0s_2s_3z_4s_3s_2 \text{ (30 portes).}$$

En utilisant la méthode `reduced_word()` de SageMath dans le groupe $\mathcal{W}_6$, on obtient $w = s_0z_1s_0s_1z_2s_1s_2z_3s_0s_1s_2s_3z_4z_3s_2s_3z_4s_2s_3s_1s_2s_0$ (22 portes). On applique ensuite l'algorithme de Dehn et à partir de la relation $s_1z_2s_1s_2z_1s_2$, elle même obtenue par permutation circulaire de $s_1s_2z_1s_2s_1z_2$. On a alors : $w = s_0z_1s_0s_2z_1z_3s_0s_1s_2s_3z_4z_3s_2s_3z_4s_2s_3s_1s_2s_0$ (20 portes). Finalement on applique à nouveau la réduction dans le groupe de Coxeter $\mathcal{W}_6$ et on observe alors que le mot est déjà réduit. Notez qu'il n'y a aucune garantie que le résultat final soit optimal. Dans le cas présent, le lecteur pourra vérifier (par exemple en utilisant l'algorithme `C-to-ZS`) que $C = S_0Z_1S_1S_2Z_3S_4Z_3S_2S_1S_0S_2Z_3S_4Z_1Z_3S_2$ (16 portes). Remarquez également que, l'algorithme de Dehn n'étant pas déterministe, l'algorithme Dehn/Coxeter ne l'est pas non plus. Dans notre exemple, le résultat final dépend également de l'ordre des portes $Z_{\{i,j\}}$ choisi au départ dans le circuit C.

Le nombre d'étapes de l'algorithme de Dehn appliqué à un mot w est majoré par $\ell = |w|$ puisqu'on diminue la longueur d'au moins 1 à chaque étape. Lors de chaque étape, le nombre d'opérations est borné par une fonction en $O(\ell^2\mathrm{Card}(\tilde{\mathcal{R}}))$. Dans le cas de la présentation 3.8, le nombre de relations qui ne sont pas des relations de commutation est linéaire en n et chacune de ces relations a une longueur au plus égale à 8. Pour les relations de commutations, vérifier si un facteur u d'un mot w est un préfixe de longueur trois d'une de ces relations peut se faire en temps constant. On voit donc

qu'à chaque étape de l'algorithme de Dehn, le nombre d'opérations de comparaison est $O(\ell n)$. Ainsi la complexité de l'algorithme de Dehn est $O(\ell^2 n)$ pour la topologie en ligne ce qui en fait un algorithme plutôt efficace. Concernant le calcul d'un mot minimal dans les groupes de Coxeter, des algorithmes polynomiaux efficaces sont connus (voir par exemple [27]). En conclusion, l'algorithme Coxeter/Dehn que nous venons de décrire permet de réduire un circuit donné en un temps de calcul raisonnable. Cependant cette méthode doit être considérée comme une simple heuristique puisque le résultat obtenu n'est généralement pas optimal.

3.2 Groupe engendré par les portes CZ et $CNOT$ et application aux états de graphe

3.2.1 Structure de produit semi-direct du groupe $\langle CZ, CNOT\rangle_n$

Règles de conjugaison par les portes $CNOT$

Soit $\langle Z, CZ\rangle_n$ le groupe engendré par les portes $\{Z_i, Z_{\{i,j\}} \mid 0 \leqslant i, j \leqslant n-1\}$. Ce groupe est un groupe commutatif isomorphe à $\mathbb{Z}_2^{\frac{n(n+1)}{2}}$ car les matrices unitaires qui l'engendrent sont des matrices qui commutent entre elles (elles sont diagonales) dont le carré est l'identité. Tout élément de ce groupe peut s'écrire sous la forme $Z_b Z_B$, avec $b \in \mathbb{F}_2^n$ et $B \in \mathcal{B}_n^0$ et on montre sans difficultés qu'une telle écriture est unique. Le produit de deux éléments de $\langle Z, CZ\rangle_n$ est donné par :

$$(Z_b Z_B)(Z_{b'} Z_{B'}) = Z_{b\oplus b'} Z_{B\oplus B'}. \tag{3.30}$$

La proposition qui suit donne les règles de conjugaison des générateurs de $\langle Z, CZ\rangle_n$ par les portes $CNOT$.

Proposition 3.20.

$$X_{[i:j]} Z_{\{i,j\}} X_{[i:j]} = Z_{\{i,j\}} Z_j \tag{3.31}$$
$$X_{[i:j]} Z_{\{i,k\}} X_{[i:j]} = Z_{\{i,k\}} Z_{\{j,k\}} \quad (i,j,k \text{ distincts}) \tag{3.32}$$
$$X_{[i:j]} Z_{\{p,q\}} X_{[i:j]} = Z_{\{p,q\}} \quad (p,q \neq i) \tag{3.33}$$
$$X_{[i:j]} Z_i X_{[i:j]} = Z_i Z_j \tag{3.34}$$
$$X_{[i:j]} Z_j X_{[i:j]} = Z_j \tag{3.35}$$
$$\tag{3.36}$$

Démonstration. On peut prouver chaque identité en comparant l'action du membre de gauche et du membre de droit sur un vecteur $|b\rangle$ de la base standard de $\mathcal{H}^{\otimes n}$. À cette fin, on utilise les identités (1.69), (1.62) et (1.70). Démontrons par exemple l'identité 3.32. Sans perte de généralité, supposons que $i < j$. On a :

$$\begin{aligned}
X_{[i:j]} Z_{\{i,k\}} X_{[i:j]} |b\rangle &= X_{[i:j]} Z_{\{i,k\}} X_{[i:j]} |b_0 \dots b_i \dots b_j \dots b_{n-1}\rangle \\
&= X_{[i:j]} Z_{\{i,k\}} |b_0 \dots b_i \oplus b_j \dots b_j \dots b_{n-1}\rangle \\
&= (-1)^{(b_i\oplus b_j)b_k} X_{[i:j]} |b_0 \dots b_i \oplus b_j \dots b_j \dots b_{n-1}\rangle \\
&= (-1)^{(b_i\oplus b_j)b_k} |b_0 \dots b_i \dots b_j \dots b_{n-1}\rangle \\
&= (-1)^{b_i b_k \oplus b_j b_k} |b\rangle \\
&= Z_{\{i,k\}} Z_{\{j,k\}} |b\rangle
\end{aligned}$$

□

On peut généraliser sans difficultés ces formules à la conjugaison d'un élément quelconque de $\langle Z, CZ\rangle_n$ par une porte $CNOT$.

Proposition 3.21. *Le groupe $\langle Z, CZ\rangle_n$ est un sous groupe normal de $\langle CZ, CNOT\rangle_n$. On a :*

$$X_{[i:j]}Z_vX_{[i:j]} = Z_{[j:i]v} \tag{3.37}$$
$$X_{[i:j]}Z_BX_{[i:j]} = Z_j^{B_{ij}}Z_{[j:i]B[i:j]} \tag{3.38}$$
$$X_{[i:j]}Z_vZ_BX_{[i:j]} = Z_{[j:i]v\oplus B_{ij}e_j}Z_{[j:i]B[i:j]} \tag{3.39}$$

Démonstration. L'identité (3.37) est la conséquence directe de (3.34) et de (3.35) car appliquer la transvection $[j:i]$ sur le vecteur v de $\mathbb{F}_2^n$ revient à ajouter son bit i à son bit j. Montrons l'identité (3.38). Soit B_i la matrice formée à partir de la ligne i et de la colonne i de B. On a donc $B_i = \sum_{k\neq i} B_{ik}E_{\{i,k\}}$ où $E_{\{i,k\}}$ est défini par l'égalité (3.9). Soit $B_i^c = B \oplus B_i$ et soit $B_i' = B_i \oplus B_{ij}E_{\{i,j\}}$, on a alors :

$$B = B_{ij}E_{\{i,j\}} \oplus B_i^c \oplus B_i'. \tag{3.40}$$

En utilisant la proposition 2.6, on vérifie que :

$$\begin{aligned}[j:i]E_{\{i,j\}}[i:j] &= E_{\{i,j\}},\\ [j:i]B_i^c[i:j] &= B_i^c,\\ [j:i]E_{\{i,k\}}[i:j] &= E_{\{i,k\}} \oplus E_{\{j,k\}} \text{ si } k \neq i,j.\end{aligned}$$

Donc

$$[j:i]B[i:j] = B_{ij}E_{\{i,j\}} \oplus B_i^c \oplus \sum_{k\neq i,j} B_{ik}(E_{\{i,k\}} \oplus E_{\{j,k\}}),$$

et ainsi :

$$Z_{[j:i]B[i:j]} = Z_{\{i,j\}}^{B_{ij}}Z_{B_i^c}\prod_{k\neq i,j}(Z_{\{i,k\}}Z_{\{j,k\}})^{B_{ik}}. \tag{3.41}$$

D'autre part on a : $X_{[i:j]}Z_BX_{[i:j]} = X_{[i:j]}Z_{\{i,j\}}^{B_{ij}}Z_{B_i^c}Z_{B_i'}X_{[i:j]}$, donc en utilisant (3.31), (3.32) et (3.33) on a :

$$X_{[i:j]}Z_BX_{[i:j]} = Z_{\{i,j\}}^{B_{ij}}Z_j^{B_{ij}}Z_{B_i^c}\prod_{k\neq i,j}(Z_{\{i,k\}}Z_{\{j,k\}})^{B_{ik}}. \tag{3.42}$$

On conclut en comparant (3.41) et (3.42). L'identité (3.39) se déduit facilement de (3.37) et de (3.38) puisque $Z_j^{B_{ij}} = Z_{B_{ij}e_j}$. □

On peut généraliser les identités (3.37) et (3.38) au cas d'une matrice unitaire quelconque X_A de $\langle CNOT\rangle_n$ (avec $A \in \mathrm{GL}_n(\mathbb{F}_2)$).

Proposition 3.22. *Pour tout vecteur $v \in \mathbb{F}_2^n$, toute matrice $B \in \mathcal{B}_n^0$ et toute matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ on a :*

$$X_AZ_vX_{A^{-1}} = Z_{(A^{-1})^{\mathrm{t}}v} \tag{3.43}$$
$$X_AZ_BX_{A^{-1}} = Z_{q_B(A^{-1})}Z_{(A^{-1})^{\mathrm{t}}BA^{-1}} \tag{3.44}$$

où q_B est la forme quadratique associée à B (voir équation (3.12)), $q_B(A)$ désigne le vecteur $[q_B(\mathrm{col}_0(A)), \ldots, q_B(\mathrm{col}_{n-1}(A))]^{\mathrm{t}}$ de $\mathbb{F}_2^n$ avec $\mathrm{col}_i(A)$ la colonne i de la matrice A.

Démonstration. Soit $A = \prod_{k=1}^{\ell}[i_k : j_k]$ une matrice de $\mathrm{GL}_n(\mathbb{F}_2)$. On remarque que $(A^{-1})^{\mathrm{t}} = \prod_{k=1}^{\ell}[j_k : i_k]$, donc l'identité (3.43) s'obtient en itérant (3.37). Démontrons l'identité (3.44). Comme $\langle Z, CZ\rangle_n$ est un sous groupe normal de $\langle CZ, CNOT\rangle_n$, il est clair que $X_A Z_B X_{A^{-1}}$ peut s'écrire sous la forme $Z_v Z_{B'}$ pour un certain vecteur v de $\mathbb{F}_2^n$ et une certaine matrice $B' \in \mathcal{B}_n^0$. De plus A se décompose en produit de transvections, donc en itérant l'identité 3.39, on a $B' = (A^{-1})^{\mathrm{t}} B A^{-1}$. Il reste donc à prouver que $v = q_B(A^{-1})$, soit que $v_i = q_B(\mathrm{col}_i(A^{-1}))$ pour tout $i = 0, \ldots, n-1$. Posons $|\psi_i\rangle = Z_v |e_i\rangle$ pour tout $i = 0, \ldots, n-1$. On a donc $|\psi_i\rangle = (-1)^{v_i} |e_i\rangle$. D'autre part, comme $Z_v = X_A Z_B X_{A^{-1}} Z_{B'}$, on a $|\psi_i\rangle = X_A Z_B X_{A^{-1}} Z_{B'} |e_i\rangle$. Or $Z_{B'} |e_i\rangle = (-1)^{q_{B'}(e_i)} |e_i\rangle = |e_i\rangle$ donc $|\psi_i\rangle = X_A Z_B X_{A^{-1}} |e_i\rangle = X_A Z_B |A^{-1} e_i\rangle$. Finalement $|\psi_i\rangle = (-1)^{q_B(\mathrm{col}_i(A^{-1}))} X_A |A^{-1} e_i\rangle = (-1)^{q_B(\mathrm{col}_i(A^{-1}))} |e_i\rangle$, ce qui prouve que $v_i = q_B(\mathrm{col}_i(A^{-1}))$. □

Remarque 3.23. L'identité 3.44 est une généralisation de l'identité 3.17. En effet, dans le cas où A est une matrice de permutation σ, on a $\sigma^{-1} = \sigma^{\mathrm{t}}$ (l'inverse d'une matrice de permutation est sa transposée) et $q_B(A^{-1})$ est le vecteur nul. Ainsi l'égalité $X_A Z_B X_{A^{-1}} = Z_{q_B(A^{-1})} Z_{(A^{-1})^{\mathrm{t}} B A^{-1}}$ s'écrit $S_\sigma Z_B S_{\sigma^{-1}} = Z_{\sigma B \sigma^{-1}}$.

La forme *ZX* pour les éléments du groupe $\langle CZ, CNOT\rangle_n$

En utilisant les identités (3.30) et (3.39), on construit l'algorithme `C-to-ZX` (algorithme 3.2) qui permet de mettre tout élément de $\langle CZ, CNOT\rangle_n$ donné par un produit de générateurs sous la forme ZX, c'est à dire sous la forme du produit d'un élément $Z_v Z_B$ de $\langle Z, CZ\rangle_n$ (avec $v \in \mathbb{F}_2^n$, $B \in \mathcal{B}_n^0$) par un élément X_A de $\langle CNOT\rangle_n$ (avec $A \in \mathrm{GL}_n(\mathbb{F}_2)$).

Algorithme 3.2 `C-to-ZX`

Entrée : C, un élément de $\langle CZ, CNOT\rangle_n$ donné par un produit $C = \prod_{k=1}^{\ell} M_k$ avec $M_k \in \{Z_{\{i,j\}}, X_{[i:j]} \mid 0 \leqslant i, j \leqslant n-1\}$.
Sortie : $Z_v Z_B X_A$, un élément de $\langle CZ, CNOT\rangle_n$ égal à C, avec $v \in \mathbb{F}_2^n$, $B \in \mathcal{B}_n^0$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$.

```
v ← vecteur nul
B ← matrice nulle
A ← matrice identité
pour k ← ℓ à 1 faire
    si M_k = X_[i:j] alors
        v_j ← v_i ⊕ v_j ⊕ B_ij
        ajouter la ligne i de B à sa ligne j
        ajouter la colonne i de B à sa colonne j
        ajouter la ligne j de A à sa ligne i
    sinon // cas où M_k = Z_{i,j}
        inverser les bits B_ij et B_ji de la matrice B
    fin si
fin pour
retourner Z_v Z_B X_A
```

Proposition 3.24. *Tout circuit de portes CZ et CNOT de longueur ℓ agissant sur n qubits admet un circuit équivalent comportant $O(n^2)$ portes du type CZ, CNOT et Pauli Z. Ce circuit peut être calculé en temps $O(\ell n)$.*

Démonstration. Il suffit d'appliquer l'algorithme `C-to-ZX` au circuit initial. Il y a ℓ portes dans le circuit en entrée et le temps de calcul pour chaque porte est au plus $O(n)$. La complexité temporelle de l'algorithme `C-to-ZX` est donc $O(\ell n)$. Une fois obtenue la forme ZX du circuit, on applique un algorithme de décomposition d'une matrice de $\mathrm{GL}_n(\mathbb{F}_2)$ en transvections (voir chapitre 2, section 2.3.2) afin d'obtenir le sous-circuit de portes $CNOT$ correspondant à la matrice unitaire X_A dans la forme $Z_v Z_B X_A$. □

Le théorème qui suit résume les résultats de la sous-section 3.2.1.

Théorème 3.25. *Tout élément de $\langle CZ, CNOT\rangle_n$ admet une unique décomposition sous la forme ZX, c'est à dire sous la forme*

$$Z_v Z_B X_A, \tag{3.45}$$

avec $v \in \mathbb{F}_2^n$, $B \in \mathcal{B}_n^0$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$. On a donc :

$$|\langle CZ, CNOT\rangle_n| = 2^{n^2} \prod_{i=1}^{n} (2^i - 1). \tag{3.46}$$

Le produit de deux éléments de $\langle CZ, CNOT\rangle_n$ est donné par :

$$(Z_v Z_B X_A)(Z_{v'} Z_{B'} X_{A'}) = Z_{v''} Z_{B''} X_{A''} \tag{3.47}$$

avec $v'' = v \oplus (A^{-1})^{\mathrm{t}} v' \oplus q_{B'}(A^{-1})$, $B'' = B \oplus (A^{-1})^{\mathrm{t}} B' A^{-1}$ et $A'' = AA'$.

Le groupe $\langle CZ, CNOT\rangle_n$ est le produit semi-direct interne de ses deux sous-groupes $\langle Z, CZ\rangle_n$ et $\langle CNOT\rangle_n$:

$$\langle CZ, CNOT\rangle_n \simeq \langle Z, CZ\rangle_n \rtimes \langle CNOT\rangle_n. \tag{3.48}$$

Démonstration. L'existence de la décomposition (3.45) se prouve en appliquant l'algorithme `C-to-ZX` à un élément $C \in \langle CZ, CNOT\rangle_n$ donné sous la forme d'un produit de portes CZ et $CNOT$. Montrons qu'une telle décomposition est unique. Supposons que $Z_v Z_B X_A = Z_{v'} Z_{B'} X_{A'}$. Si $A \neq A'$ alors il existe $u \in \mathbb{F}_2^n$ tel que $Au \neq A'u$, donc $|Au\rangle$ et $|A'u\rangle$ sont deux vecteurs distincts de la base standard. Or $Z_v Z_B X_A |u\rangle = Z_{v'} Z_{B'} X_{A'} |u\rangle$, donc $Z_v Z_B |Au\rangle = Z_{v'} Z_{B'} |A'u\rangle$. On a alors deux vecteurs différents de la base standard qui sont colinéaires ce qui n'est pas possible. Donc $A = A'$ et on en déduit que $Z_v Z_B = Z_{v'} Z_{B'}$. Ainsi $v = v'$ et $B = B'$.

L'ordre de $\langle CZ, CNOT\rangle_n$ s'obtient en multipliant l'ordre de chacun des sous-groupes $\langle Z, CZ\rangle_n$ et $\langle CNOT\rangle_n$ (voir formule (2.31)). L'identité (3.47) est une conséquence directe de (3.30), (3.43) et (3.44). La structure de produit semi-direct [6] est la conséquence de la proposition 3.21 ainsi que de l'existence et de l'unicité de la forme ZX. □

Remarque 3.26. La forme ZX est une généralisation de la forme ZS définie au théorème 3.3) : la forme ZX d'un circuit de $\langle CZ, SWAP\rangle_n$ est sa forme ZS puisque X_σ et S_σ sont deux notations de la même matrice unitaire (voir Remarque 2.9).

6. Voir annexe A, section A.3.2

3.2.2 Implémentation d'un état de graphe dans un ordinateur quantique

La longueur d'un circuit de portes CZ est au plus $\frac{n(n-1)}{2}$, donc en $O(n^2)$, alors qu'un circuit de portes $CNOT$ admet un circuit équivalent comportant $O(n^2/\ln n)$, obtenu par exemple par l'algorithme de Patel-Markov-Hayes [154] (voir chapitre 2, section 2.3.2). L'idée de base de cette sous-section est d'utiliser la formule de conjugaison (3.44) afin de transformer un circuit de portes CZ en un circuit équivalent dont la longueur est dominée par le nombre de portes $CNOT$. On peut espérer que pour certains circuits, cette transformation produise un circuit équivalent de longueur inférieure au circuit de départ.

Circuit équivalent à un circuit de portes CZ

Nous dirons qu'une matrice $B \in \mathcal{B}_n^0$ est *réduite* quand chaque colonne et chaque ligne de cette matrice contient au plus une entrée non nulle, c'est à dire quand le circuit de portes CZ associé à l'opérateur Z_B a une profondeur égale à 1. Cela signifie aussi que les sommets du graphe $G \in \mathcal{G}_n$ de matrice B ont pour degré 0 ou 1.

Lemme 3.27. *Pour toute matrice $B \in \mathcal{B}_n^0$, il existe une matrice triangulaire supérieure $A \in \mathrm{GL}_n(\mathbb{F}_2)$ et une matrice réduite $B_{red} \in \mathcal{B}_n^0$ telle que $B_{red} = A^{\mathrm{t}}BA$.*

Démonstration. On applique l'algorithme `B-to-B`$_{\mathrm{red}}$ (algorithme 3.3) à la matrice B. Cet algorithme construit étape par étape les matrices A et B_{red} par élimination gaussienne, c'est à dire en multipliant par des matrices de transvection bien choisies. □

Remarque 3.28. La matrice B peut être vue comme la matrice (dans la base canonique (e_i) de $\mathbb{F}_2^n$) d'une forme bilinéaire alternée f. Dans ce contexte, la relation de congruence $B_{\mathrm{red}} = A^{\mathrm{t}}BA$ entre les matrices B et B_{red} est la formule classique de changement de base pour les formes bilinéaires, A désignant la matrice de passage de l'ancienne base vers la nouvelle base. Si f est une forme bilinéaire alternée non dégénérée (*i.e.* B est de plein rang) sur un espace vectoriel V de dimension n alors il existe un algorithme classique permettant de démontrer que n est pair et de construire une base dite symplectique pour la forme f c'est à dire une base dans laquelle la matrice de f a la forme $\begin{bmatrix} 0_k & -I_k \\ I_k & 0_k \end{bmatrix}$ avec $n = 2k$ (voir par exemple [179, section 3.4.4]). Dans le cas où $V = \mathbb{F}_2^n$ et où B est inversible, cette matrice a la forme $\begin{bmatrix} 0_k & I_k \\ I_k & 0_k \end{bmatrix}$, elle est donc réduite selon notre définition. Cependant, il n'y a pas de garantie que la matrice A soit triangulaire supérieure. De plus, si B est une matrice définissant un circuit de portes CZ, elle peut être dégénérée. C'est pourquoi nous proposons un autre algorithme, l'algorithme `B-to-B`$_{\mathrm{red}}$, qui permet de construire une matrice réduite congruente à B, pour toute matrice $B \in \mathcal{B}_n^0$ (inversible ou non), et pour toute dimension $n \geqslant 2$ (paire ou non). L'exemple 3.29 propose un déroulement détaillé de cet algorithme.

Algorithme 3.3 `B-to-B`$_{\text{red}}$: réduction d'une matrice de $\mathcal{B}_n^0$

Entrée : B, une matrice de $\mathcal{B}_n^0$.
Sortie : B' une matrice réduite de $\mathcal{B}_n^0$ et A une matrice triangulaire supérieure de $\mathrm{GL}_n(\mathbb{F}_2)$ tels que $B' = A^{\mathrm{t}}BA$.

```
1:  B' ← B ;
2:  A ← matrice identité
3:  pivot ← tableau de booléens de taille n dont les valeurs sont initialisées à False
4:  pour j ← 0 à n − 1 faire
5:      si pivot[j] = False et Card{i | B'_ij = 1} ≠ 0 alors
6:          p ← min{i | B'_ij = 1};// Choix du pivot
7:          pivot[p] ← True;
8:          // Étape a : élimination des 1 restants dans la colonne j et la ligne j
9:          pour r ← p + 1 à n − 1 faire
10:             si B'_rj = 1 alors
11:                 B' ← [r : p]B'[p : r];
12:                 A ← A[p : r];
13:             fin si
14:         fin pour
15:         // Étape b : élimination des 1 restants dans la colonne p et la ligne p
16:         pour c ← j + 1 à n − 1 faire
17:             si B'_pc = 1 alors
18:                 B' ← [c : j]B'[j : c];
19:                 A ← A[j : c];
20:             fin si
21:         fin pour
22:     fin si
23: fin pour
24: retourner (B', A)
```

Exemple 3.29. Appliquons l'algorithme `B-to-B`$_{\text{red}}$ à la matrice

$$B = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Après avoir initialisé chaque entrée du tableau `pivot` à `False`, on décrit l'exécution de la boucle principale (lignes 4 à 23).

$\boxed{j = 0}$ Choix du pivot : $p \leftarrow 3$; `pivot`$[3] \leftarrow$ `True`;

Étape a : $[5:3]B[3:5] = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 0 & 1 & 1 & 0 & 1 & 1 \\ \mathbf{0} & 1 & 0 & 0 & 1 & 1 & 0 \\ \mathbf{1} & 1 & 0 & 0 & 1 & 0 & 0 \\ \mathbf{0} & 0 & 1 & 1 & 0 & 1 & 0 \\ \mathbf{0} & 1 & 1 & 0 & 1 & 0 & 1 \\ \mathbf{0} & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Étape b : $[4:0][1:0][5:3]B[3:5][0:1][0:4] = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 0 & 1 & \mathbf{0} & 0 & 1 & 1 \\ \mathbf{0} & 1 & 0 & \mathbf{0} & 1 & 1 & 0 \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 0 & 1 & \mathbf{0} & 0 & 1 & 0 \\ \mathbf{0} & 1 & 1 & \mathbf{0} & 1 & 0 & 1 \\ \mathbf{0} & 1 & 0 & \mathbf{0} & 0 & 1 & 0 \end{bmatrix}$

$\boxed{j=1}$ Choix du pivot : $p \leftarrow 2$; `pivot`$[2] \leftarrow$ `True` ;

Étape a :

$[6:2][5:2][4:0][1:0][5:3]B[3:5][0:1][0:4][2:5][2:6] = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & 0 & \mathbf{0} & 1 & 1 & 0 \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 1 & \mathbf{0} & 0 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & 1 & \mathbf{0} & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & 0 & \mathbf{0} & 1 & 0 & 0 \end{bmatrix}$

Étape b :

$[5:1][4:1][6:2][5:2][4:0][1:0][5:3]B[3:5][0:1][0:4][2:5][2:6][1:4][1:5] =$
$\begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 0 & 0 \end{bmatrix}$

$\boxed{j=2}$ `pivot`$[2] =$ `True`

$\boxed{j=3}$ `pivot`$[3] =$ `True`

$\boxed{j=4}$ Choix du pivot : $p \leftarrow 6$; `pivot`$[6] \leftarrow$ `True` ;

Étape a : B' reste inchangée
Étape b : B' reste inchangée

$\boxed{j=5}$ Colonne nulle

$\boxed{j=6}$ Choix du pivot : $p \leftarrow 4$; `pivot`$[4] \leftarrow$ `True` ;

Étape a : B' reste inchangée
Étape b : B' reste inchangée

$$\texttt{return}(B', A), \text{ avec } B' = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{bmatrix},$$

$$\text{et } A = [3:5][0:1][0:4][2:5][2:6][1:4][1:5] = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proposition 3.30. *Tout circuit de portes CZ agissant sur n qubits possède un circuit équivalent comportant $O(n^2/\ln n)$ portes du type CZ, CNOT ou Pauli Z.*

Démonstration. Soit un circuit de portes *CZ* et Z_B l'opérateur associé. En appliquant l'algorithme $\texttt{B-to-B}_{\text{red}}$ à la matrice B, on obtient une matrice réduite B_{red} et une matrice triangulaire supérieure $A \in \mathrm{GL}_n(\mathbb{F}_2)$ telles que $B_{\text{red}} = A^{\mathrm{t}}BA$. En utilisant l'identité (3.44), il vient $X_A Z_{B_{\text{red}}} {X_A}^{-1} = Z_{q_{B_{\text{red}}}(A^{-1})} Z_{(A^{-1})^{\mathrm{t}} B_{\text{red}} A^{-1}}$. Donc $Z_B = Z_v X_A Z_{B_{\text{red}}} X_A^{-1}$, avec $v = q_{B_{\text{red}}}(A^{-1})$. Le circuit quantique correspondant à l'opérateur $Z_{B_{\text{red}}}$ comporte au plus $\lfloor n/2 \rfloor$ portes *CZ* et le circuit quantique correspondant à l'opérateur Z_v comporte au plus n portes Pauli Z. En décomposant la matrice A en $O(n^2/\ln n)$ transvections par l'algorithme de Patel-Markov-Hayes [154], on obtient le résultat annoncé. □

Implémentation d'un état de graphe pour la topologie du graphe complet

Dans cette sous-section, nous montrons comment appliquer les résultats algébriques précédents aux circuits produisant des états de graphe. Notre objectif est de proposer une méthode qui permette de diminuer (par rapport à une implémentation naïve) le nombre de portes utilisées dans de ce type de circuit.

Théorème 3.31. *Tout état de graphe $|G\rangle$ (avec $G \in \mathcal{G}_n$) peut s'écrire sous la forme*

$$|G\rangle = Z_{\mathbf{v}} X_A Z_{G'} |+\rangle^{\otimes n}, \tag{3.49}$$

avec $v \in \mathbb{F}_2^n$, $A \in \mathrm{GL}_n(\mathbb{F}_2)$ une matrice triangulaire supérieure et $G' \in \mathcal{G}_n$ un graphe dont les sommets ont pour degré 0 ou 1.

Démonstration. Soit $G \in \mathcal{G}_n$ et $|G\rangle$ un état de graphe. Soit $B \in \mathcal{B}_n^0$ la matrice d'adjacence de G. En écrivant Z_B sous la forme $Z_B = Z_v X_A Z_{B_{\text{red}}} X_A^{-1}$, avec $v = q_{B_{\text{red}}}(A^{-1})$ (voir preuve de la proposition 3.30), on a : $|G\rangle = Z_v X_A Z_{B_{\text{red}}} X_{A^{-1}} H^{\otimes n} |0\rangle^{\otimes n}$. En utilisant l'identité (1.78) qui permet d'interchanger la cible et le contrôle d'une porte *CNOT*, on obtient : $H^{\otimes n} X_{A^{-1}} H^{\otimes n} = X_{A^{\mathrm{t}}}$. En effet, si $A = \prod_{k=1}^{\ell} [i_k : j_k]$ alors

$(A^{-1})^{\mathrm{t}} = \prod_{k=1}^{\ell}[j_k : i_k]$. On a donc : $|G\rangle = Z_v X_A Z_{B_{\mathrm{red}}} H^{\otimes n} X_{A^{\mathrm{t}}} |0\rangle^{\otimes n}$. Comme un circuit de portes *CNOT* laisse inchangé l'état $|0\rangle^{\otimes n}$, on obtient : $|G\rangle = Z_v X_A Z_{B_{\mathrm{red}}} H^{\otimes n} |0\rangle^{\otimes n}$. Soit G' le graphe de matrice B_{red}, alors les sommets de G ont un degré au plus 1 et $|G\rangle = Z_v X_A Z_{G'} |+\rangle^{\otimes n}$. □

Exemple 3.32. Soit $n = 7$ et

$$|G\rangle = Z_{\{0,3\}} Z_{\{0,5\}} Z_{\{1,2\}} Z_{\{1,3\}} Z_{\{1,6\}} Z_{\{2,4\}} Z_{\{2,5\}} Z_{\{3,4\}} Z_{\{5,6\}} |+\rangle^{\otimes 7}. \tag{3.50}$$

Écrivons l'état de graphe $|G\rangle$ sous la forme (3.49).

$$\text{On a } |G\rangle = Z_B |+\rangle^{\otimes 7}, \text{ avec } B = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

En utilisant le résultat de l'exemple 3.29 et le théorème 3.31, nous obtenons : $|G\rangle = Z_v X_A Z_{B_{\mathrm{red}}} |+\rangle^{\otimes n}$, avec

$$B_{\mathrm{red}} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

et

$$A = [3:5][0:1][0:4][2:5][2:6][1:4][1:5] = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Le graphe G' de matrice B_{red} est donc $G' = \{\{0,3\},\{1,2\},\{4,6\}\}$. Calculons le vecteur $v \in \mathbb{F}_2^n$ qui définit les portes de Pauli Z du circuit. On a :

$$A^{-1} = [1:5][1:4][2:6][2:5][0:4][0:1][3:5] = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

donc la forme quadratique $q_{B_{\text{red}}}$ est définie par : $q_{B_{\text{red}}}([x_0, x_1, x_2, x_3, x_4, x_5, x_6]^{\text{t}}) = x_0x_3 \oplus x_1x_2 \oplus x_4x_6$. Ainsi $q_{B_{\text{red}}}(A^{-1}) = [0, 0, 0, 0, 0, 1, 0]^{\text{t}}$ d'où $Z_v = Z_5$ et finalement :

$$|G\rangle = Z_5 X_{[3:5]} X_{[0:1]} X_{[0:4]} X_{[2:5]} X_{[2:6]} X_{[1:4]} X_{[1:5]} Z_{\{0,3\}} Z_{\{1,2\}} Z_{\{4,6\}} |+\rangle^{\otimes 7} . \tag{3.51}$$

Table 3.1 Gain moyen obtenu par une implémentation de l'état de graphe $|G\rangle$ basée sur la forme (3.49). Résultats basés sur des échantillons aléatoires de 200 états de graphe, où chaque graphe a n sommets et ℓ arêtes. Soit ℓ' le nombre de portes 2-qubits dans le circuit correspondant à la forme (3.49), le gain en pourcentage est défini comme étant le quotient $(\ell - \ell')/\ell$ si $\ell > \ell'$ et 0 sinon.

n \ ℓ	$0{,}2 \times max$	$0{,}4 \times max$	$0{,}6 \times max$	$0{,}8 \times max$	$max = n(n-1)/2$
5	0%	0%	1%	21%	20%
10	0%	0%	20%	41%	33%
20	0%	0%	31%	49%	54%
50	0%	12%	41%	56%	62%
100	0%	23%	48%	61%	72%
200	0%	31%	54%	66%	74%
300	0%	37%	58%	68%	79%

Dans l'exemple 3.32, la forme finale (3.51) obtenue pour l'état de graphe $|G\rangle$ comporte 10 portes binaires, ce qui est une porte de plus que la forme initiale (3.50). Cependant, en utilisant l'algorithme de Patel-Markov-Hayes pour décomposer la matrice A, la forme (3.49) conduit à un décompte du nombre de portes binaires en $O(n^2/\ln n)$ qui est asymptotiquement meilleur qu'une implémentation naïve basée sur la forme (3.29). On peut donc se demander dans quels cas et dans quelle mesure une implémentation d'un état de graphe basé sur la forme (3.49) est plus avantageuse qu'une implémentation basée sur la forme (3.29). La table 3.1 montre quelques résultats permettant d'évaluer de façon expérimentale l'utilité de la réécriture (3.49). Ces résultats ont été obtenus en utilisant une commande dont le code source est disponible dans un dépot Github [56] (commande `stabnf`). Il s'agit d'une implémentation en langage C de la transformation permettant d'obtenir (3.49) à partir de (3.29) suivie d'une décomposition de la matrice A par l'algorithme de Patel-Markov-Hayes. On observe que la formule donnée par le théorème 3.31 est utile dans de nombreux cas. Plus précisément, si l'on définit la *densité* d d'un état de graphe de n qubits comme étant le quotient $\frac{\ell}{n(n-1)/2}$, où ℓ est le nombre d'arête du graphe alors la méthode que nous proposons est efficace quelle que soit la dimension n à partir de $d = 0{,}6$.

Implémentation d'un état de graphe dans les ordinateurs quantiques d'IBM

Nous proposons quelques exemples permettant de vérifier que le pré-traitement basé sur la formule (3.49) d'un circuit produisant un état de graphe peut s'avérer utile lors d'une implémentation sur un véritable ordinateur quantique. Dans le cas des ordinateurs quantiques proposés en libre accès par IBM, la connectivité du réseau de qubits n'est pas complète. De plus, des portes très courantes comme les portes *CZ* ou les portes de Hadamard ne sont pas natives et doivent être simulées à partir d'autres portes natives.

Dans ce contexte, on peut se demander si l'approche précédente utilisant le théorème 3.31 est encore utile, c'est à dire si elle entraîne une réduction du nombre de portes après le processus de compilation du circuit (sa réécriture à partir de portes natives dans l'architecture cible).

Nous avons choisi d'implémenter l'état de graphe complet $|K_5\rangle$ dans la machine de 5 qubits ibmq-belem [3] :

$$|K_5\rangle = Z_{\{0,1\}} Z_{\{0,2\}} Z_{\{0,3\}} Z_{\{0,4\}} Z_{\{1,2\}} Z_{\{1,3\}} Z_{\{1,4\}} Z_{\{2,3\}} Z_{\{2,4\}} Z_{\{3,4\}} \, |+\rangle^{\otimes 5} . \tag{3.52}$$

Cet état est intéressant d'un point de vue théorique car il est LC-équivalent (Local Clifford équivalent), et donc SLOCC-équivalent à l'état intriqué $|\text{GHZ}\rangle_5 = \frac{1}{\sqrt{2}}(|00000\rangle + |11111\rangle)$ (voir [92] sur l'état $|\text{GHZ}\rangle$ et [95, section 4.1] pour une preuve de cette équivalence).

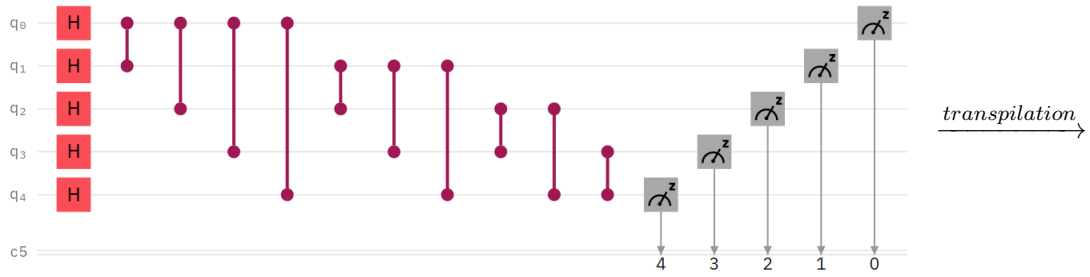
L'application du théorème 3.31 nous donne :

$$|K_5\rangle = Z_2 Z_3 X_{[3:4]} X_{[2:3]} X_{[1:2]} X_{[0:2]} X_{[2:4]} X_{[2:3]} Z_{\{0,1\}} Z_{\{2,3\}} \, |+\rangle^{\otimes 5} . \tag{3.53}$$

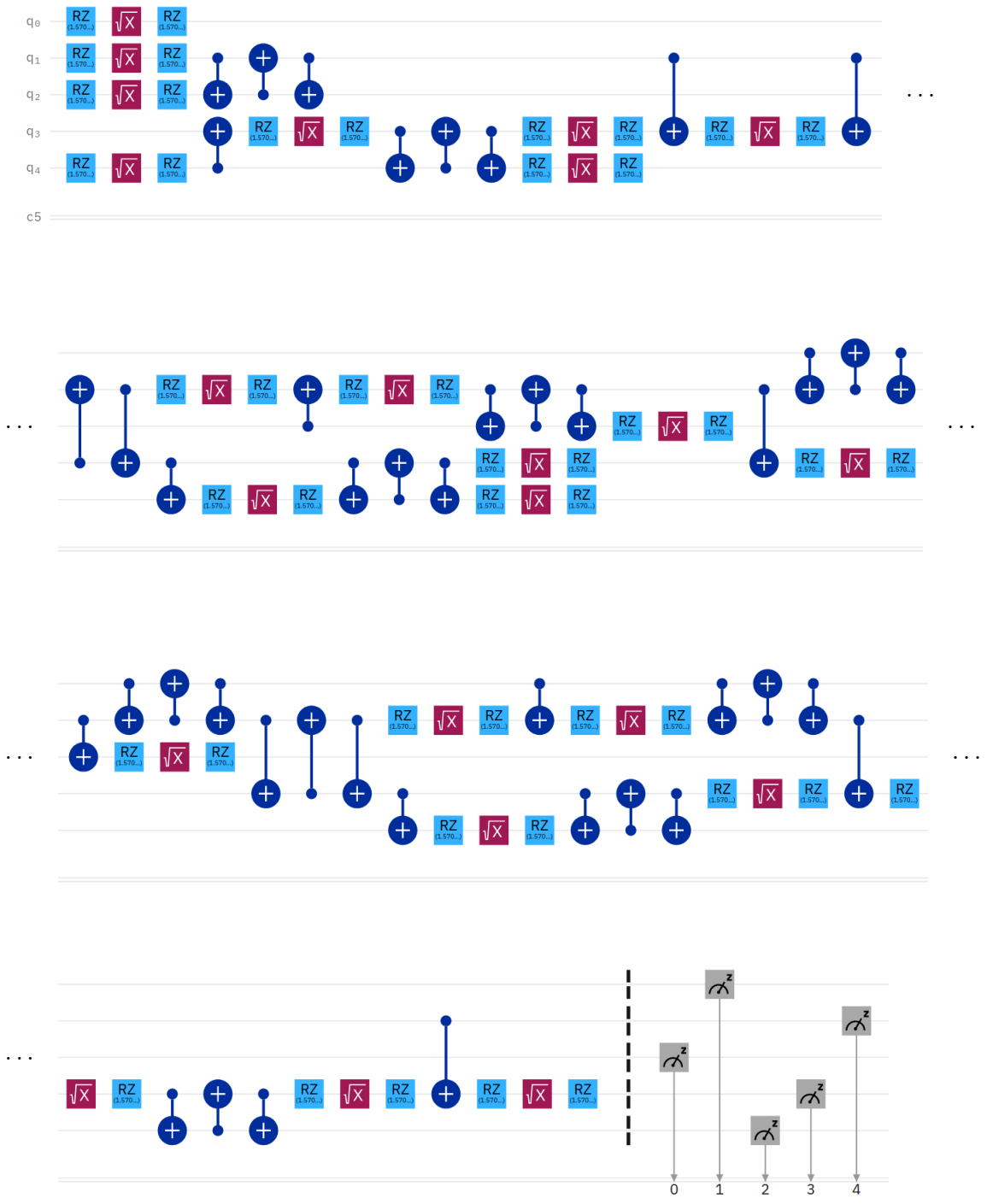
On observe qu'il y a 8 portes binaires dans la forme (3.53) contre 10 dans la forme (3.52), soit une réduction substantielle de 20%. Mais qu'en est-il de cette réduction quand on implémente ces deux circuits dans la machine ibmq-belem et que l'on compare le nombre de portes natives utilisées ? Dans l'ordinateur ibmq-belem, le graphe de connectivité des qubits est : $\{\{1,0\},\{1,2\},\{1,3\},\{3,4\}\}$. Ainsi les portes $X_{[2:3]}, X_{[0:2]}, X_{[2:4]}$ et $X_{[2:3]}$ ne sont pas natives et doivent être simulées (voir chapitre 2, section 2.1.2). Il en est de même des portes CZ et des portes de Hadamard (voir chapitre 1, section 1.3.2).

Nous présentons d'abord les circuits avant et après compilation correspondant à la formule (3.52).

`INPUT` : $|K_5\rangle = Z_{\{0,1\}} Z_{\{0,2\}} Z_{\{0,3\}} Z_{\{0,4\}} Z_{\{1,2\}} Z_{\{1,3\}} Z_{\{1,4\}} Z_{\{2,3\}} Z_{\{2,4\}} Z_{\{3,4\}} \, |+\rangle^{\otimes 5}$



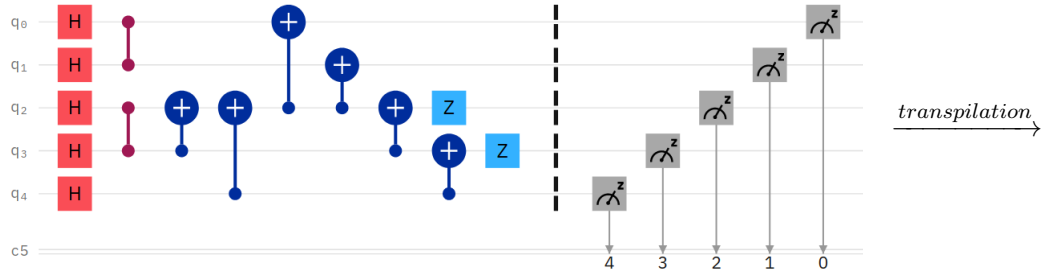
OUTPUT :



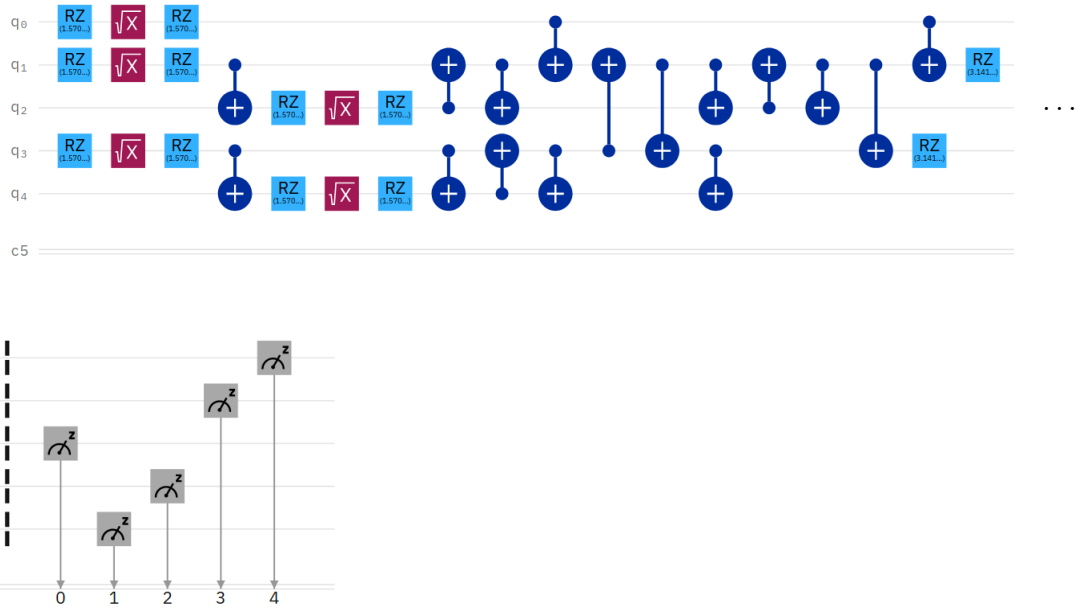
Une fois compilé, le circuit contient 43 portes *CNOT* et 69 portes simples.

Nous présentons maintenant les deux circuits (avant et après compilation) correspondant à la formule (3.53).

INPUT : $|K_5\rangle = Z_2 Z_3 X_{[3:4]} X_{[2:3]} X_{[1:2]} X_{[0:2]} X_{[2:4]} X_{[2:3]} Z_{\{0,1\}} Z_{\{2,3\}} |+\rangle^{\otimes 5}$



OUTPUT :



Nous constatons que le circuit compilé contient seulement 16 portes $CNOT$ et 17 portes simples. Notre méthode a permis, dans ce cas précis, une réduction de 63% du nombre de portes binaires.

La table 3.2 récapitule les gains obtenus, avant et après compilation des circuits, par l'utilisation de la forme (3.49) pour quatre états de graphe d'un système de 5 qubits (implantés dans la machine de 5 qubits ibmq-belem) et pour deux états de graphe d'un système de 7 qubits (implantés dans la machine de 15 qubits ibmq-melbourne). On observe une réduction significative du nombre de portes dans le circuit compilé et le gain obtenu après compilation est en général sensiblement plus important que le gain obtenu avant compilation.

Bien que ces résultats soient obtenus sur quelques états de graphes implémentés dans des ordinateurs quantiques particuliers, ils suggèrent que le théorème 3.31 peut avoir des applications utiles.

Table 3.2 Implémentation d'états de graphe dans deux ordinateurs quantiques. Gains obtenu par la forme (b) : $Z_v X_A Z_{B_{\text{red}}} |+\rangle^{\otimes n}$ par rapport à la forme (a) : $Z_B |+\rangle^{\otimes n}$ sur le nombre de portes binaires, avant compilation (INPUT) et après compilation (OUTPUT).

Implémentation dans l'ordinateur ibmq-belem (5 qubits)					
Ref.	INPUT			OUTPUT	
	Circuit	Portes	Gain	Portes	Gain
1(a)	$Z_{01}Z_{02}Z_{03}Z_{04}Z_{12}Z_{13}Z_{14}Z_{23}Z_{24}Z_{34}\|+\rangle^{\otimes 5}$	10	20%	43	63%
1(b)	$Z_2Z_3X_{34}X_{23}X_{12}X_{02}X_{24}X_{23}Z_{01}Z_{23}\|+\rangle^{\otimes 5}$	8		16	
2(a)	$Z_{02}Z_{03}Z_{04}Z_{13}Z_{14}Z_{23}Z_{24}Z_{34}\|+\rangle^{\otimes 5}$	8	25%	26	19%
2(b)	$Z_3X_{34}X_{23}X_{14}X_{03}Z_{02}Z_{13}\|+\rangle^{\otimes 5}$	6		21	
3(a)	$Z_{01}Z_{02}Z_{03}Z_{04}Z_{12}Z_{13}Z_{23}Z_{24}\|+\rangle^{\otimes 5}$	8	0%	35	40%
3(b)	$Z_2Z_3X_{23}X_{24}X_{12}X_{02}X_{04}X_{23}Z_{01}Z_{23}\|+\rangle^{\otimes 5}$	8		21	
4(a)	$Z_{01}Z_{02}Z_{04}Z_{12}Z_{13}Z_{23}Z_{34}\|+\rangle^{\otimes 5}$	7	14%	28	32%
4(b)	$Z_2X_{12}X_{02}X_{14}X_{03}Z_{01}Z_{24}\|+\rangle^{\otimes 5}$	6		19	
Implémentation dans l'ordinateur ibmq-melbourne (15 qubits)					
5(a)	$Z_{02}Z_{03}Z_{04}Z_{13}Z_{14}Z_{15}Z_{23}Z_{25}Z_{26}Z_{34}Z_{35}Z_{45}Z_{46}Z_{56}\|+\rangle^{\otimes 7}$	14	21%	41	22%
5(b)	$Z_3X_{34}X_{23}X_{35}X_{16}X_{06}X_{04}X_{03}Z_{02}Z_{13}Z_{46}\|+\rangle^{\otimes 7}$	11		32	
6(a)	$Z_{03}Z_{05}Z_{12}Z_{13}Z_{16}Z_{24}Z_{25}Z_{34}Z_{56}\|+\rangle^{\otimes 7}$	9	0%	33	18%
6(b)	$Z_5X_{35}X_{25}X_{26}X_{14}X_{01}X_{15}Z_{03}Z_{12}Z_{46}\|+\rangle^{\otimes 7}$	9		27	

3.3 Conclusion et perspectives

Nous venons d'étudier d'un point de vue algébrique certains circuits quantiques très simples formés de portes qui sont omniprésentes dans les algorithmes quantiques et nous avons montré comment l'analyse des structures algébriques mises en jeu permettaient de construire des algorithmes efficaces afin de réduire et, dans les cas les plus simples, d'optimiser ces circuits.

Nous avons pris en compte deux grands archétypes de réseaux de qubits, le cas du graphe complet et le cas LNN. Ce ne sont pas des cas purement théoriques car des ordinateurs quantiques expérimentaux ayant ce type de réseau ont déjà été construits (voir chapitre 1, section 1.3.2). Même si le réseau de qubits des machines expérimentales actuelles est souvent dans une configuration intermédiaire entre ces deux types de réseau (cas des machines d'IBM par exemple), on peut considérer les heuristiques basées sur la topologie du graphe complet comme des pré-traitements permettant dans certains cas une première diminution du nombre de portes avant d'essayer d'adapter le circuit à un graphe de connectivité donné. Ainsi, dans le cas des états de graphe, il semble qu'un pré-traitement basé sur un réseau complet (cas de la formule (3.49)) soit utile même pour une implantation dans un réseau de qubits qui lui n'est pas complet. Afin d'approfondir nos travaux, il serait intéressant de connaître les optimisations de circuit déjà implantées dans les compilateurs IBM mais le code source n'est malheureusement pas ouvert. Au vu des quelques expériences que nous avons réalisées il semble qu'une optimisation basée sur le théorème 3.31 n'ait pas été implémentée.

Dans le chapitre suivant nous poursuivons notre étude algébrique des circuits quantiques en enrichissant les circuits étudiés de deux types de portes simples : les portes de Hadamard et les portes de phase. Nous obtenons ainsi une classe de circuit bien connue : les circuits de Clifford.

Chapitre 4

Une forme générale des circuits de Clifford

Le formalisme du stabilisateur a été initialement introduit par Gottesman [85, 86] afin d'étudier une classe importante de codes quantiques correcteurs d'erreurs appelés *codes stabilisateurs*[1]. Ce formalisme est décrit en détail dans [148, section 10.5.1 et 10.5.2] mais on peut tenter de le résumer en deux idées principales expliquant son intérêt.

Soit $\mathcal{E}_n$ le groupe de Pauli pour n qubits (voir définition 4.1) et soit S un sous groupe de $\mathcal{E}_n$. On définit V_S, le sous-espace vectoriel stabilisé par S, comme étant l'ensemble des vecteurs de $\mathcal{H}^{\otimes n}$ qui sont stabilisés par chaque élément de S :

$$V_S = \{|\psi\rangle \in \mathcal{H}^{\otimes n} \mid \forall E \in S, E|\psi\rangle = |\psi\rangle\}. \tag{4.1}$$

On dit alors que S est le *stabilisateur* de V_S. La première idée du formalisme du stabilisateur est qu'on peut remplacer, dans certains cas, la description usuelle d'un état quantique au moyen de 2^n amplitudes complexes, par une description beaucoup plus compacte, en décrivant le groupe S par un ensemble de générateurs, chacun de ces générateurs étant complètement défini par la donnée de $2n+4$ bits (voir formule (4.3)).

La seconde idée principale est une conséquence de la première. Soit U un opérateur unitaire alors, pour tout $|\psi\rangle \in V_S$ et pour tout $E \in S$, on a

$$U|\psi\rangle = UE|\psi\rangle = UEU^{-1}U|\psi\rangle\,, \tag{4.2}$$

ce qui prouve que $U|\psi\rangle$ est stabilisé par UEU^{-1}. On en déduit que le stabilisateur de UV_S est le groupe USU^{-1}. Si de plus l'opérateur unitaire U normalise $\mathcal{E}_n$ (*i.e.* $U\mathcal{E}_nU^{-1} \subset \mathcal{E}_n$), alors l'espace UV_S est encore décrit par un sous-groupe de $\mathcal{E}_n$ et pour obtenir ses générateurs il suffit de conjuguer ceux de S par U.

Nous nous intéressons dans ce chapitre aux *circuits stabilisateurs*, une des applications de ce formalisme. Les circuits stabilisateurs sont des circuits quantiques composés uniquement de portes de Clifford (porte de Hadamard, portes de phase et portes $CNOT$) et de mesures d'observables du groupe de Pauli. On les utilise par exemple pour effectuer les phases d'encodage et de décodage de certains codes quantiques correcteurs d'erreurs [1, sections I,VI]. Ils participent donc au développement du calcul quantique résistant

1. Une définition précise de ces codes est donnée par exemple dans [148, section 10.5.5] mais cette définition n'est pas nécessaire à la compréhension du présent chapitre.

aux erreurs (voir [148, section 10.6] et [88]). Dans la suite on désigne par Stab_n le sous-groupe de U_{2^n} engendré par les portes de Clifford agissant sur n qubits. Le groupe Stab_n correspond donc aux circuits stabilisateurs sans mesures, d'où la notation utilisée. Un *état stabilisateur* est un état obtenu par l'action d'un circuit stabilisateur sur l'état $|0\rangle^{\otimes n}$. On montre qu'un tel état peut toujours être obtenu par l'action d'un élément de Stab_n sur $|0\rangle^{\otimes n}$ [1, théorème 1]. Dans ce qui suit, nous considérons uniquement des circuits stabilisateurs sans mesures et nous dirons que Stab_n est le groupe des circuits stabilisateurs.

Reprenons maintenant le formalisme du stabilisateur dans le cas où S est le sous-groupe du groupe de Pauli $\mathcal{E}_n$ engendré par les portes Pauli-Z (*i.e* : $S = \langle Z_i \mid i = 0, \ldots, n-1\rangle$). Alors le sous-espace V_S stabilisé par S est la droite de $\mathcal{H}^{\otimes n}$ engendrée par $|0\rangle^{\otimes n}$. Soit $U \in \mathrm{Stab}_n$, alors d'après l'égalité (4.2), $U|0\rangle^{\otimes n}$ dirige le sous espace stabilisé par USU^{-1}. Ainsi l'état stabilisateur $U|0\rangle^{\otimes n}$ est défini de façon compacte par la donnée de n éléments de $\mathcal{E}_n$: $UZ_0U^{-1}, \ldots, UZ_{n-1}U^{-1}$.

On voit donc que pour décrire complètement l'image d'un état stabilisateur par une porte de Clifford, il suffit de mettre à jour le stabilisateur de cet état en conjuguant chaque générateur du stabilisateur par l'opérateur unitaire correspondant, ce qui se fait en temps $O(n^2)$ par les formules (4.9), (4.10) et (4.11) que nous établirons après cette introduction. Cette possibilité de simuler efficacement ce type de calcul quantique (circuit stabilisateur agissant sur l'état $|0\rangle^{\otimes n}$) constitue en fait l'énoncé du théorème de Gottesman-Knill ([148, théorème 10.7]), qui apparaît dans la thèse de Gottesman [86, section 5.7].

Cependant cette simulation efficace sur un ordinateur classique est limitée à un type de circuit restreint puisque l'ensemble formé par les portes de Clifford n'est pas universel pour le calcul quantique (voir chapitre 1.3, section 1.3.1). Dans le cadre du calcul quantique le plus général, on peut être amené à utiliser des états stabilisateurs en entrée de circuits quantiques comportant d'autres types de portes. Il faut donc pouvoir implanter des états stabilisateurs dans de véritables ordinateurs quantiques. En raison des erreurs dans les portes quantiques des machines actuelles, il est important de minimiser ou de réduire le nombre de portes utilisées dans les circuits stabilisateurs.

Cette nécessité a conduit plusieurs équipes de chercheurs à construire, au cours des deux dernières décennies, des formes générales pour les circuits stabilisateurs sans mesures c'est à dire les circuits qui implantent les opérateurs de Stab_n. Ces formes sont qualifiées selon leur auteurs de formes *canoniques* [1, 36], *normales* [139] ou encore *pseudo normales* [73]. On pourrait définir une telle forme comme étant la concaténation d'un nombre N, indépendant de n, de circuits $C_1, \ldots, C_N$, chaque circuit C_i étant composé de portes du même type et la longueur de C_i étant majorée par une fonction en $O(n^2)$. Cette borne quadratique provient d'un algorithme de Gottesman [86, section 5.8], mentionné aussi dans [148] sous la forme d'un théorème [148, théorème 10.6] qui montre que n'importe quel opérateur unitaire qui normalise $\mathcal{E}_n$ peut s'écrire, à une phase globale près, sous la forme d'un produit de $O(n^2)$ portes de Clifford. Ainsi une forme générale dont le nombre de portes ne serait pas $O(n^2)$ n'aurait pas vraiment d'intérêt pour le problème d'optimisation qui nous intéresse ici.

Le *groupe de Clifford*, noté $\mathcal{C}_n$, est le normalisateur [2] du groupe de Pauli dans U_{2^n}. On démontre que Stab_n est inclus dans $\mathcal{C}_n$ (voir proposition 4.7) et que ces deux groupes sont en fait *presque* égaux (voir remarque 4.9). Dans ce chapitre, nous proposons une nouvelle forme générale pour les circuits de Clifford (*i.e.* les circuits implantant les opérateurs

2. Voir annexe A, section A.2.3

de $\mathcal{C}_n$). Pour résumer le principe, cette forme s'obtient à partir d'une décomposition d'un matrice *symplectique* (voir définition 4.11) en produit de matrices symplectiques particulières qui correspondent chacune à une porte quantique bien connue de $\mathcal{C}_n$.

Établir un lien entre le groupe de Clifford et le groupe symplectique n'est pas une idée nouvelle ; c'est en fait la méthode généralement utilisée pour construire des formes normales des circuits de Clifford. Dès 1997, Calderbank et Shor [44, 43] établissent un lien entre les codes quantiques correcteurs d'erreurs et la géométrie dans l'espace symplectique $\mathbb{F}_2^{2n}$. On trouve aussi à peu près au même moment, dans la thèse de Gottesman [86, section 3.4], l'expression de la forme bilinéaire alternée f (voir (4.19)) qui définit l'espace symplectique $\mathbb{F}_2^{2n}$. Cependant l'utilisation du groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ en lien avec les circuits de Clifford apparaît un peu plus tard en 2003 dans deux articles de Dehaene *et al.* [63, 64], suivis de différents travaux sur les formes normales [1, 139, 36].

Le plan du chapitre est le suivant. Dans la section 4.1, nous formalisons les notions que nous venons d'introduire (groupe symplectique, groupe de Clifford, circuit stabilisateur etc.) et nous explicitons le lien entre le groupe de Clifford $\mathcal{C}_n$ et le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$. Nous faisons également le bilan des formes normales connues. Dans les sections 4.2 et 4.3 nous proposons une nouvelle décomposition dans le groupe symplectique, puis nous l'utilisons dans la section 4.4 pour établir une forme générale pour les circuits de Clifford.

4.1 Notions de base et état de l'art

4.1.1 Notations

On rappelle ici quelques notations déjà utilisées et on en introduit de nouvelles.

- $\mathcal{B}_n$ désigne l'ensemble des matrices symétriques de dimensions $n \times n$ à coefficients dans $\mathbb{F}_2$,
- $\mathcal{B}_n^0$ est l'ensemble des matrices de $\mathcal{B}_n$ ayant une diagonale nulle.
- La matrice de dimensions $n \times n$ à entrées dans $\mathbb{F}_2$ dont toutes les entrées sont nulles sauf l'entrée (i, j) qui vaut 1 est notée E_{ij} et on pose $E_{\{i,j\}} = E_{ij} \oplus E_{ji}$.
- La base canonique de $\mathbb{F}_2^n$ est notée $(e_i)_{i=0,\dots,n-1}$ et les coordonnées de $u \in \mathbb{F}_2^n$ sont notées $u_0, \dots, u_{n-1}$. On a donc $u = \sum_i u_i e_i$.
- Soient K un corps, m un entier positif et u un vecteur de K^m (dans la pratique K désigne $\mathbb{F}_2$, $\mathbb{R}$ ou $\mathbb{C}$). La matrice diagonale D de dimensions $m \times m$ dont la diagonale est constituée des éléments de u se note $\mathrm{diag}(u)$.
- On désigne par ω le vecteur de $\mathbb{F}_2^n$ égal à $[1 \dots 1]^t$. On a donc : $I_n = \mathrm{diag}(\omega)$.
- Soit B une matrice de dimension $m \times m$ à coefficients dans K. Le vecteur colonne $b \in K^m$ tel que $b_i = B_{ii}$ pour $i = 0 \dots m-1$ se note $\overrightarrow{\mathrm{diag}}(B)$.
- La colonne j d'une matrice M se note $\mathrm{col}_j(M)$.
- La conjugaison d'une matrice carrée B par une matrice inversible A se note B^A : $B^A = ABA^{-1}$.

4.1.2 Groupe de Pauli et groupe de Clifford

Groupe de Pauli

Définition 4.1. Le groupe de Pauli pour n qubits, noté $\mathcal{E}_n$ est le sous-groupe du groupe unitaire U_{2^n} engendré par l'ensemble $\{X_i, Y_i, Z_i \mid i = 0 \dots n-1\}$ des portes de Pauli.

La proposition suivante est une conséquence directe des relations entre les opérateurs de Pauli ((1.30), (1.31) et (1.32)).

Proposition 4.2. *Tout élément E du groupe de Pauli $\mathcal{E}_n$ peut s'écrire de façon unique sous la forme*

$$E = \lambda X_u Z_v, \tag{4.3}$$

avec $\lambda \in \{\pm 1, \pm \mathrm{i}\}$ et $u, v \in \mathbb{F}_2^n$.

La multiplication de deux éléments E et E' ainsi que l'inverse d'un élément E de ce groupe sont donnés par

$$EE' = \lambda X_u Z_v \lambda' X_{u'} Z_{v'} = \lambda\lambda' (-1)^{u'\cdot v} X_{u\oplus u'} Z_{v\oplus v'}, \tag{4.4}$$

$$E^{-1} = (\lambda X_u Z_v)^{-1} = \lambda^{-1} (-1)^{u\cdot v} X_u Z_v, \tag{4.5}$$

où $u \cdot v$ désigne le produit scalaire usuel des vecteurs u et v, i.e. : $u \cdot v = \sum_i u_i v_i$.

Le théorème qui suit est une généralisation d'un exercice proposé dans [148, exercice 10.38], mais l'idée originale apparaît dans la thèse de Gottesman [86, pp.41,42], sous la forme d'un exemple. La preuve détaillée que nous donnons ici utilise la notion de groupe stabilisateur déjà évoquée en introduction.

Théorème 4.3. *Soient U_1 et U_2 deux matrices de U_{2^n} telles que, pour tout $i = 0, \dots, n-1$ on ait*

$$U_1 X_i U_1^{-1} = U_2 X_i U_2^{-1} \text{ et } U_1 Z_i U_1^{-1} = U_2 Z_i U_2^{-1}, \tag{4.6}$$

alors il existe un réel φ tel que $U_1 = \mathrm{e}^{\mathrm{i}\varphi} U_2$.

Démonstration. Soit S le groupe engendré par les matrices de Pauli $Z_0, \dots Z_{n-1}$. L'ensemble V_S des vecteurs de $\mathcal{H}^{\otimes n}$ qui sont fixés par tous les éléments de S est la droite dirigée par $|0 \dots 0\rangle$ (le groupe S s'appelle le stabilisateur de V_S). Pour tout $U \in \mathrm{U}_{2^n}$, tout vecteur $|\psi\rangle \in V_S$ et tout $E \in S$, on a $U|\psi\rangle = UE|\psi\rangle = UEU^{-1}U|\psi\rangle$, donc le stabilisateur de $U_1(V_S)$ est $U_1 S U_1^{-1}$ et le stabilisateur de $U_2(V_S)$ est $U_2 S U_2^{-1}$. Par hypothèse, on a $U_1 S U_1^{-1} = U_2 S U_2^{-1}$ et donc $U_1(V_S) = U_2(V_S)$. Comme l'espace $U_1(V_S)$ est une droite, on en déduit qu'il existe une phase φ tel que $U_1|0 \dots 0\rangle = \mathrm{e}^{\mathrm{i}\varphi} U_2|0 \dots 0\rangle$.

Soit $|b\rangle = |b_0 \dots b_{n-1}\rangle$ un vecteur quelconque de la base standard de $\mathcal{H}^{\otimes n}$, on a $|b\rangle = \prod_i X_i^{b_i}|0 \dots 0\rangle$, donc $U_1|b\rangle = (\prod_i U_1 X_i^{b_i} U_1^{-1}) U_1|0 \dots 0\rangle$. Or, pour tout i, on a $U_1 X_i U_1^{-1} = U_2 X_i U_2^{-1}$ d'où :

$$U_1|b\rangle = (\textstyle\prod_i U_2 X_i^{b_i} U_2^{-1}) U_1|0 \dots 0\rangle = \mathrm{e}^{\mathrm{i}\varphi} (\prod_i U_2 X_i^{b_i} U_2^{-1}) U_2|0 \dots 0\rangle = \mathrm{e}^{\mathrm{i}\varphi} U_2|b\rangle .$$

On en déduit que $U_1 = \mathrm{e}^{\mathrm{i}\varphi} U_2$. □

Corollaire 4.4. *Soit U une matrice unitaire de U_{2^n} pour laquelle il existe deux vecteurs $u = [u_0 \dots u_{n-1}]^{\mathrm{t}}$ et $v = [v_0 \dots v_{n-1}]^{\mathrm{t}}$ de $\mathbb{F}_2^n$ vérifiant, pour tout $i = 0, \dots, n-1$:*

$$U X_i U^{-1} = (-1)^{v_i} X_i \text{ et } U Z_i U^{-1} = (-1)^{u_i} Z_i. \tag{4.7}$$

Alors, il existe un réel φ tel que $U = \mathrm{e}^{\mathrm{i}\varphi} X_u Z_v$.

Démonstration. On a $X_u Z_v X_i (X_u Z_v)^{-1} = X_u Z_v X_i Z_v X_u = (-1)^{v_i} X_u Z_v Z_v X_i X_u = (-1)^{v_i} X_i$ et, par un calcul similaire $X_u Z_v Z_i (X_u Z_v)^{-1} = (-1)^{u_i} Z_i$. On conclut en utilisant le théorème 4.3. □

Groupe de Clifford

Définition 4.5 (Groupe de Clifford)**.** Le groupe de Clifford pour n qubits, noté $\mathcal{C}_n$, est le normalisateur du groupe de Pauli $\mathcal{E}_n$ dans le groupe unitaire U_{2^n}.

Définition 4.6 (Portes de Clifford)**.** L'ensemble des portes de Clifford pour n qubits, noté Cliff_n, est l'ensemble formé des portes de Hadamard, des portes de Phase et des portes *CNOT* agissant sur un système de n qubits :

$$\mathrm{Cliff}_n = \{P_i, H_i, X_{[i:j]} \mid 0 \leqslant i, j \leqslant n-1\}. \tag{4.8}$$

Proposition 4.7. *Les portes de Clifford normalisent le groupe de Pauli. Leur action sur un élément $X_u Z_v$ de $\mathcal{E}_n$ est donné par :*

$$H_i X_u Z_v H_i = (-1)^{u_i v_i} X_{u \oplus (u_i \oplus v_i) e_i} Z_{v \oplus (u_i \oplus v_i) e_i} \tag{4.9}$$

$$P_i X_u Z_v P_i = \mathrm{i}^{u_i} X_u Z_{v \oplus u_i e_i} \tag{4.10}$$

$$X_{[i:j]} X_u Z_v X_{[i:j]} = X_{[i:i]u} Z_{[j:i]v} \tag{4.11}$$

$$\forall A \in \mathrm{GL}_n(\mathbb{F}_2),\ X_A X_u Z_v X_A^{-1} = X_{Au} Z_{(A^{-1})^{\mathrm{t}} v} \tag{4.12}$$

Démonstration. La formule (4.9) est une conséquence des égalités $H_i X_i H_i = Z_i$ et $X_i Z_i = -Z_i X_i$. La formule (4.10) est une conséquence des égalités $P_i X_i P^{-1} = Y_i = \mathrm{i} X_i Z_i$ et $P_i Z_i = Z_i P_i$. La formule (4.11) est une conséquence des identités $X_{[i:j]} Z_i X_{[i:j]} = Z_i Z_j$ (3.34) et $X_{[i:j]} Z_j X_{[i:j]} = Z_j$ (3.35) ainsi que des égalités $X_{[i:j]} X_j X_{[i:j]} = X_j X_i$ et $X_{[i:j]} X_i X_{[i:j]} = X_i$ qu'on obtient en conjuguant les deux précédentes par $H_i H_j$. Enfin la formule (4.12) est une généralisation de (4.11) par induction sur la structure du groupe $\mathrm{GL}_n(\mathbb{F}_2)$ qui est engendré par les transvections. □

Définition 4.8 (Circuit stabilisateur)**.** On appelle circuit stabilisateur tout circuit agissant sur n qubits qui peut s'écrire uniquement avec des portes de Clifford. Pour cette raison, nous notons Stab_n le groupe engendré par les portes de Clifford :

$$\mathrm{Stab}_n = \langle \mathrm{Cliff}_n \rangle = \langle P_i, H_i, X_{[i:j]} \mid 0 \leqslant i, j \leqslant n-1 \rangle. \tag{4.13}$$

On remarque que les portes de Pauli ainsi que les portes *SWAP* et les portes *CZ* font partie de Stab_n en raison des identités $Z_i = P_i^2$, $X_i = H_i P_i^2 H_i$ et $Y_i = P_i X_i P_i^{-1} = P_i H_i P_i^2 H_i P_i^3$, ainsi que des identités (1.79) et (1.80).

Remarque 4.9. Le groupe de Clifford $\mathcal{C}_n$ n'est pas exactement le groupe engendré par les portes de Clifford. Le groupe de Clifford $\mathcal{C}_n$ est infini car toute matrice scalaire $\mathrm{e}^{\mathrm{i}\varphi} I$ normalise le groupe de Pauli. Le groupe Stab_n est un sous groupe fini de $\mathcal{C}_n$ dont le cardinal est $8 \times 2^{2n} |\mathrm{Sp}_{2n}(\mathbb{F}_2)| = 2^{n^2+2n+3} \prod_{j=1}^{n} (4^j - 1)$ [43, p.8] (dans cette formule 8×2^{2n} est le cardinal du groupe engendré par $\mathcal{E}_n$ et $\langle \mathrm{e}^{\frac{\mathrm{i}\pi}{4}} I \rangle$). En fait, les portes de Clifford engendrent *presque* le groupe de Clifford $\mathcal{C}_n$, dans le sens suivant : toute matrice unitaire qui normalise le groupe $\mathcal{E}_n$ peut s'écrire sous la forme $\mathrm{e}^{\mathrm{i}\varphi} \prod_{k=1}^{\ell} M_k$ avec $M_k \in \mathrm{Cliff}_n$ et φ un nombre réel. Il s'agit d'un théorème de Gottesman [148, théorème 10.6] que nous redémontrerons à partir de nos propres méthodes (voir section 4.4, théorème 4.43).

Définition 4.10. On appelle état stabilisateur, l'état d'un système de n qubits obtenu par l'action d'un circuit stabilisateur (*i.e.* : un élément de Stab_n) sur l'état $|0\rangle^{\otimes n}$.

4.1.3 Un lien entre le groupe de Clifford et le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$

Groupe symplectique sur $\mathbb{F}_2$

Définition 4.11. Le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ en dimension $2n$ sur le corps $\mathbb{F}_2$ est l'ensemble des matrices M de dimensions $2n \times 2n$ vérifiant l'égalité

$$M^{\mathrm{t}}\Omega M = \Omega \tag{4.14}$$

avec

$$\Omega = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}. \tag{4.15}$$

Le groupe $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ est un sous-groupe de $\mathrm{GL}_{2n}(\mathbb{F}_2)$ et une matrice de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ est dite *matrice symplectique*.

Proposition 4.12. *Soient A, B, C, D des matrices $n \times n$ sur $\mathbb{F}_2$. La matrice $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ est symplectique si et seulement si les trois conditions suivantes sont vérifiées :*

(i) $A^t D + C^t B = I$,

(ii) $A^t C = C^t A$,

(iii) $B^t D = D^t A$.

Démonstration. Il suffit d'effectuer la multiplication $M^{\mathrm{t}}\Omega M$ par blocs et d'utiliser l'égalité (4.14). □

Le groupe de Pauli $\mathcal{E}_n$ et l'espace symplectique $\mathbb{F}_2^{2n}$

Soient $u, v \in \mathbb{F}_2^n$, notons $\begin{bmatrix} u \\ v \end{bmatrix}$ le vecteur de l'espace vectoriel $\mathbb{F}_2^{2n}$ obtenu en juxtaposant les composantes des vecteurs u et v :

$$\begin{bmatrix} u \\ v \end{bmatrix} = [u_0, \ldots, u_{n-1}, v_0, \ldots, v_{n-1}]^{\mathrm{t}}. \tag{4.16}$$

Le centre $\mathcal{Z}$ du groupe de Pauli est formé des matrices du groupe de Pauli qui commutent avec toutes les autres, donc

$$\mathcal{Z} = \{\pm I, \pm \mathrm{i} I\} \tag{4.17}$$

et d'après (4.4) et (4.5), le groupe quotient $\mathcal{E}_n/\mathcal{Z}$ est isomorphe au groupe (additif) $\mathbb{F}_2^{2n}$. Soit $E = \lambda X_u Z_v$ un élément de $\mathcal{E}_n$, on note $\tilde{p}$ la projection canonique de $\mathcal{E}_n$ dans $\mathcal{E}_n/\mathcal{Z}$, et on identifie $\tilde{p}(E)$ (noté aussi $\tilde{E}$) avec le vecteur $\begin{bmatrix} u \\ v \end{bmatrix}$ de $\mathbb{F}_2^{2n}$:

$$E = \lambda X_u Z_v \implies \tilde{p}(E) = \tilde{E} \simeq \begin{bmatrix} u \\ v \end{bmatrix}. \tag{4.18}$$

On considère f, la forme bilinéaire alternée sur $\mathbb{F}_2^{2n}$ définie par :

$$f\left(\begin{bmatrix}u\\v\end{bmatrix},\begin{bmatrix}u'\\v'\end{bmatrix}\right) = u\cdot v' \oplus v\cdot u'. \tag{4.19}$$

En identifiant $\mathbb{F}_2^{2n}$ à $\mathcal{E}_n/\mathcal{Z}$, on écrira parfois $f(\tilde{E},\tilde{E}')$ au lieu de $f\left(\begin{bmatrix}u\\v\end{bmatrix},\begin{bmatrix}u'\\v'\end{bmatrix}\right)$. On remarque que la base canonique $(e_i)_{i=0,\dots,2n-1}$ de $\mathbb{F}_2^{2n}$ vérifie

$$f(e_i,e_j) = 1 \iff |i-j| = n, \tag{4.20}$$

et on la qualifie alors de *base symplectique* pour f. La matrice symplectique Ω (4.15) est aussi la matrice de la forme alternée f dans la base symplectique (e_i) puisqu'on a :

$$[u^{\mathrm{t}}\ v^{\mathrm{t}}]\begin{bmatrix}0 & I_n\\ I_n & 0\end{bmatrix}\begin{bmatrix}u'\\v'\end{bmatrix} = u\cdot v' \oplus v\cdot u'. \tag{4.21}$$

On verra que cette matrice Ω joue un rôle important dans les algorithmes exposés section 4.3.

On rappelle que le commutateur $[E,E']$ de deux éléments E et E' d'un groupe est défini par

$$[E,E'] = EE'E^{-1}E'^{-1}. \tag{4.22}$$

Dans le cas du groupe de Pauli, il s'exprime simplement à l'aide de la forme f (4.23). L'identité (4.23) montre que deux éléments du groupe de Pauli commutent si et seulement si leur images dans $\mathbb{F}_2^{2n}$ sont des vecteurs orthogonaux pour f. Cette observation apparaît dans [148, p. 447] où la matrice Ω est explicitée, sans toutefois mentionner le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$.

Proposition 4.13. *Soient $E = \lambda X_u Z_v$ et $E' = \lambda' X_{u'} Z_{v'}$ deux éléments du groupe de Pauli $\mathcal{E}_n$, on a :*

$$[E,E'] = (-I)^{f(\tilde{E},\tilde{E}')} = (-I)^{u\cdot v'\oplus v\cdot u'}. \tag{4.23}$$

Démonstration. La preuve de l'identité (4.23) consiste en un calcul direct visant à réduire le produit $EE'E^{-1}E'^{-1}$ à l'aide des formules (1.30) et (4.4). □

Morphisme entre $\mathcal{C}_n$ et $\mathrm{Sp}_{2n}(\mathbb{F}_2)$

Définition 4.14 (Morphisme Φ)**.** On définit Φ, le morphisme de $\mathcal{C}_n$ dans $\mathrm{GL}(\mathbb{F}_2^{2n})$ tel que, pour tout $C\in\mathcal{C}_n$ et pour tout $\begin{bmatrix}u\\v\end{bmatrix}\in\mathbb{F}_2^{2n}$, on a :

$$\Phi(C)\begin{bmatrix}u\\v\end{bmatrix} = \begin{bmatrix}u'\\v'\end{bmatrix} \iff \exists\lambda\in\{\pm1,\pm\mathrm{i}\}, CX_uZ_vC^{-1} = \lambda X_{u'}Z_{v'}. \tag{4.24}$$

En identifiant $\mathbb{F}_2^{2n}$ à $\mathcal{E}_n/\mathcal{Z}$, on a donc :

$$\Phi(C)\tilde{E} = \tilde{p}(CEC^{-1}). \tag{4.25}$$

On rappelle que le groupe des isométries de f est le groupe des applications linéaires de l'espace $\mathbb{F}_2^{2n}$ qui conservent la forme f. Il est bien connu que ce groupe est isomorphe au groupe $\mathrm{Sp}_{2n}(\mathbb{F}_2)$: à chaque isométrie on associe sa matrice dans la base symplectique (e_i) qui est une matrice de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ (voir par exemple [179]). Il apparaît que, pour toute matrice $C \in \mathcal{C}_n$, $\Phi(C)$ est une isométrie pour la forme f.

Proposition 4.15. *Pour toute matrice C du groupe de Clifford $\mathcal{C}_n$, l'application linéaire $\Phi(C)$ conserve la forme f.*

Démonstration. Soit $C \in \mathcal{C}_n$ et deux vecteurs $\begin{bmatrix} u \\ v \end{bmatrix}$ et $\begin{bmatrix} u' \\ v' \end{bmatrix}$ de $\mathbb{F}_2^{2n}$. On pose $E = X_u Z_v$ et $E' = X_{u'} Z_{v'}$ et on identifie $\begin{bmatrix} u \\ v \end{bmatrix}$ et $\begin{bmatrix} u' \\ v' \end{bmatrix}$ avec $\tilde{E}$ et $\tilde{E}'$ respectivement. Montrons que $f(\tilde{E}, \tilde{E}') = f(\Phi(C)\tilde{E}), \Phi(C)\tilde{E}')$.

On a $EE'E^{-1}E'^{-1} = (-I)^{f(\tilde{E},\tilde{E}')}$ et en conjuguant chaque membre de cette égalité par C, on obtient : $[CEC^{-1}, CE'C^{-1}] = (-I)^{f(\tilde{E},\tilde{E}')}$. Or, d'après l'identité (4.23), on a $[CEC^{-1}, CE'C^{-1}] = (-I)^{f(\tilde{p}(CEC^{-1}),\, \tilde{p}(CE'C^{-1}))}$ et en utilisant l'identité (4.25), il vient $[CEC^{-1}, CE'C^{-1}] = (-I)^{f(\Phi(C)\tilde{E},\, \Phi(C)\tilde{E}')}$.

D'où l'égalité $f(\tilde{E}, \tilde{E}') = f(\Phi(C)\tilde{E}), \Phi(C)\tilde{E}')$. □

Définition 4.16 (Morphisme $\overline{\Phi}$)**.** Le morphisme du groupe de Clifford $\mathcal{C}_n$ dans le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ qui associe, à toute matrice $C \in \mathcal{C}_n$, la matrice de $\Phi(C)$ dans la base canonique de $\mathbb{F}_2^{2n}$ est noté $\overline{\Phi}$. Pour tout $j = 0, \ldots, n-1$, on a donc :

$$\mathrm{col}_j(\overline{\Phi}(M)) = \begin{bmatrix} u \\ v \end{bmatrix} \iff \exists \lambda \in \{\pm 1, \pm \mathrm{i}\},\ MX_jM^{-1} = \lambda X_u Z_v \tag{4.26}$$

$$\mathrm{col}_{j+n}(\overline{\Phi}(M)) = \begin{bmatrix} u \\ v \end{bmatrix} \iff \exists \lambda \in \{\pm 1, \pm \mathrm{i}\},\ MZ_jM^{-1} = \lambda X_u Z_v \tag{4.27}$$

Proposition 4.17. *Le noyau de $\overline{\Phi}$ est $\{\mathrm{e}^{\mathrm{i}\varphi} X_u Z_v \mid \varphi \in \mathbb{R},\ u, v \in \mathbb{F}_2^n\}$.*

Démonstration. Soit $C = \mathrm{e}^{\mathrm{i}\varphi} X_u Z_v$, alors, pour tout $i = 0, \ldots, n-1$, on a d'après (4.4) : $CX_iC^{-1} = \pm X_i$ et $CZ_iC^{-1} = \pm Z_i$ donc d'après (4.26) et (4.27), on en déduit que $\overline{\Phi}(C) = I_{2n}$, donc $C \in \mathrm{Ker}(\overline{\Phi})$.

Réciproquement, soit $C \in \mathrm{Ker}(\overline{\Phi})$, alors pour tout $i = 0, \ldots, n-1$ on a, d'après (4.26) et (4.27) : $CX_iC^{-1} = \lambda_i X_i$ et $CZ_iC^{-1} = \lambda'_i Z_i$ avec $\lambda_i, \lambda'_i \in \{\pm 1, \pm \mathrm{i}\}$. Comme $(CX_iC^{-1})^2 = (\lambda_i X_i)^2$, on a $\lambda_i = \pm 1$, et de même $\lambda'_i = \pm 1$. Posons, pour tout $i = 1, \ldots, n-1$: $\lambda_i = (-1)^{v_i}$ et $\lambda'_i = (-1)^{u_i}$. Alors, d'après le corollaire 4.4, il existe un réel φ tel que $C = \mathrm{e}^{\mathrm{i}\varphi} X_u Z_v$. □

Pour alléger la notation, on pose, pour toute matrice $C \in \mathcal{C}_n$:

$$\overline{C} = \overline{\Phi}(C). \tag{4.28}$$

L'ensemble des images par $\overline{\Phi}$ des portes de Clifford dans le groupe symplectique est noté $\overline{\mathrm{Cliff}}_n$. On a donc :

$$\overline{\mathrm{Cliff}}_n = \overline{\Phi}(\mathrm{Cliff}_n) = \{\overline{P}_i, \overline{H}_i, \overline{X}_{[i:j]} \mid 0 \leqslant i, j \leqslant n-1\}. \tag{4.29}$$

On se référera parfois à ces matrices symplectiques particulières sous le terme *matrices symplectiques de Clifford*.

En utilisant les formules (4.26) et (4.27) ainsi que les règles de conjugaison données par la proposition 4.7, on calcule les images par $\overline{\Phi}$ des matrices usuelles de Stab_n. On a récapitulé les résultats dans la table 4.1 (un tableau similaire est donné dans [161, table I, p.6]).

Table 4.1 Images dans le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ des matrices usuelles de Stab_n.

Pour $0 \leqslant i, j \leqslant n-1$, $a, b \in \mathbb{F}_2^n$, $A \in \mathrm{GL}_n(\mathbb{F}_2)$, $B \in \mathcal{B}_n^0$ et σ une matrice de permutation de $\mathfrak{S}_n$, on a :

$$\overline{P}_i = \begin{bmatrix} I & 0 \\ \mathrm{diag}(e_i) & I \end{bmatrix} \qquad \overline{P}_b = \begin{bmatrix} I & 0 \\ \mathrm{diag}(b) & I \end{bmatrix}$$

$$\overline{H}_i = \begin{bmatrix} \mathrm{diag}(e_i \oplus \omega) & \mathrm{diag}(e_i) \\ \mathrm{diag}(e_i) & \mathrm{diag}(e_i \oplus \omega) \end{bmatrix} \qquad \overline{H}_a = \begin{bmatrix} \mathrm{diag}(a \oplus \omega) & \mathrm{diag}(a) \\ \mathrm{diag}(a) & \mathrm{diag}(a \oplus \omega) \end{bmatrix}$$

$$\overline{X}_{[i:j]} = \begin{bmatrix} [i:j] & 0 \\ 0 & [j:i] \end{bmatrix} \qquad \overline{X}_A = \begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix}$$

$$\overline{S}_{(i\ \ j)} = \begin{bmatrix} (i\ \ j) & 0 \\ 0 & (i\ \ j) \end{bmatrix} \qquad \overline{S}_\sigma = \begin{bmatrix} \sigma & 0 \\ 0 & \sigma \end{bmatrix}$$

$$\overline{Z}_{\{i,j\}} = \begin{bmatrix} I & 0 \\ E_{\{i,j\}} & I \end{bmatrix} \qquad \overline{Z}_B = \begin{bmatrix} I & 0 \\ B & I \end{bmatrix}$$

Remarque 4.18. On observe que :

- La matrice $\overline{P}_i$ est la matrice de transvection $[i+n : i]$ de $\mathrm{GL}_{2n}(\mathbb{F}_2)$ (voir chapitre 2, section 2.2.1).
- La matrice $\overline{P}_b$ est un produit de matrices de transvections : $\overline{P}_b = \prod_i [i+n : i]^{b_i}$.
- La matrice $\overline{H}_i$ est la matrice de la transposition de $\mathfrak{S}_{2n}$ qui échange i et $i+n$: $\overline{H}_i = (i\ \ i+n)$.
- La matrice $\overline{H}_a$ est un produit de matrices de transpositions : $H_a = \prod_i (i\ \ i+n)^{a_i}$.
- La matrice Ω définie par (4.15) est l'image par $\overline{\Phi}$ de l'opérateur unitaire qui applique à chaque qubit une porte de Hadamard H. On a donc

$$\overline{\Phi}(\textstyle\prod_i H_i) = \overline{H}_\omega = \Omega = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}. \tag{4.30}$$

De la table 4.1 et des remarques 4.18, on déduit la proposition suivante qui sera utilisée dans la section 4.3.3 (proposition 4.37).

Proposition 4.19. *Soit W une matrice symplectique de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$, et soient des entiers i, j distincts tels que $0 \leqslant i, j \leqslant n-1$.*

- *Multiplier à gauche W par $\overline{P}_i$ revient à ajouter la ligne i de W à sa ligne $i+n$.*
- *Multiplier à gauche W par $\overline{H}_i$ revient à échanger les lignes i et $i+n$ de W.*
- *Multiplier à gauche W par $\overline{X}_{[i:j]}$ revient à ajouter la ligne j de W à sa ligne i et la ligne $i+n$ de W à sa ligne $j+n$.*

4.1.4 État de l'art des décompositions dans le groupe symplectique et des formes normales

Dans [64, théorème 4], Dehaene *et al.* montrent que toute matrice symplectique W peut s'écrire sous la forme

$$W = \begin{bmatrix} A_1 & 0 \\ 0 & (A_1^{-1})^{\mathrm{t}} \end{bmatrix} \begin{bmatrix} I & B_1 \\ 0 & I \end{bmatrix} \begin{bmatrix} \mathrm{diag}(a \oplus \omega) & \mathrm{diag}(a) \\ \mathrm{diag}(a) & \mathrm{diag}(a \oplus \omega) \end{bmatrix} \begin{bmatrix} I & B_2 \\ 0 & I \end{bmatrix} \begin{bmatrix} A_2 & 0 \\ 0 & (A_2^{-1})^{\mathrm{t}} \end{bmatrix}, \tag{4.31}$$

avec $A_1, A_2 \in \mathrm{GL}_n(\mathbb{F}_2)$, $a \in \mathbb{F}_2^n$ et $B_1, B_2 \in \mathcal{B}_n$.

Dans un article de 2004 [1], Gottesman et Aaronson montrent que tout circuit composé uniquement de portes de l'ensemble Cliff_n peut s'écrire sous la forme

$$\textit{-H-CNOT-P-CNOT-P-CNOT-H-P-CNOT-P-CNOT-}, \tag{4.32}$$

dans laquelle chaque H désigne un sous-circuit composé de portes de Hadamard, chaque P un sous-circuit composé de portes de phase et chaque $CNOT$ un sous-circuit de portes contrôle NOT (deux symboles identiques désignent des circuits différents mais constitués du même type de portes). C'est à notre connaissance la première forme générale pour les circuits de portes de Clifford.

En 2018 [139], Maslov et Roetteler améliorent ce résultat et proposent la forme générale suivante :

$$\textit{-CNOT-P-CNOT-P-H-P-CNOT-P-CNOT-}. \tag{4.33}$$

Dans cette forme, chaque sous-circuit de portes $CNOT$ correspond à une matrice triangulaire supérieure dans $\mathrm{GL}_n(\mathbb{F}_2)$ (voir chapitre 2, théorème 2.8), c'est à dire que chaque porte $X_{[i:j]}$ est telle que $i < j$. Pour arriver à cette expression, ces auteurs utilisent une décomposition de Bruhat du groupe symplectique (voir [139, section V] pour une définition de cette notion). Ils montrent que toute matrice symplectique $W \in \mathrm{Sp}_{2n}(\mathbb{F}_2)$ peut s'écrire sous la forme

$$W = \begin{bmatrix} A_1 & 0 \\ 0 & (A_1^{-1})^{\mathrm{t}} \end{bmatrix} \begin{bmatrix} I & B_1 \\ 0 & I \end{bmatrix} \begin{bmatrix} \mathrm{diag}(a \oplus \omega) & \mathrm{diag}(a) \\ \mathrm{diag}(a) & \mathrm{diag}(a \oplus \omega) \end{bmatrix} \begin{bmatrix} \sigma & 0 \\ 0 & \sigma \end{bmatrix} \begin{bmatrix} I & B_2 \\ 0 & I \end{bmatrix} \begin{bmatrix} A_2 & 0 \\ 0 & (A_2^{-1})^{\mathrm{t}} \end{bmatrix} \tag{4.34}$$

avec A_1, A_2 des matrices triangulaires supérieures de $\mathrm{GL}_n(\mathbb{F}_2)$ (à comparer avec (4.31) où A_1 et A_2 sont quelconques), B_1, B_2 dans $\mathcal{B}_n$ et σ une matrice de permutation. À partir de (4.33), Maslov et Roetteler déduisent la forme suivante qui est, selon eux, le principal résultat de leur article :

$$\textit{-CNOT-CZ-P-H-P-CZ-CNOT-}. \tag{4.35}$$

Plus récemment, en mars 2020, Bravyi et Maslov utilisent la décomposition de Bruhat de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ [36, section 2.2] afin de construire la première forme réellement *canonique* pour les matrices de Stab_n, dans le sens où chaque matrice $C \in \mathrm{Stab}_n$ admet une décomposition unique sous cette forme (nous donnons le résultat avec nos propres notations pour les matrices) :

$$C = P_b Z_B X_A H_a S_\sigma E P_{b'} Z_{B'} X_{A'} \tag{4.36}$$

avec $E \in \mathcal{E}_n$ et où certaines conditions sur les différentes portes permettent d'assurer l'unicité [36, théorème 1]. Ces auteurs en déduisent la forme suivante (sans unicité cette fois) pour tout circuit implantant un opérateur de Stab_n :

$$\textit{-X-Z-P-CNOT-CZ-H-CZ-H-P-}. \tag{4.37}$$

où X (resp. Z) désigne un sous circuit de portes de Pauli X (resp. de portes de Pauli Z).

À notre connaissance, la dernière forme générale proposée pour les circuits stabilisateurs est celle de Duncan *et al.* en mai 2020 [73, section 6] :

$$\text{-}H\text{-}P\text{-}CZ\text{-}CNOT\text{-}H\text{-}CZ\text{-}P\text{-}H\text{-}. \tag{4.38}$$

Cette forme, qualifiée de pseudo-normale par ses auteurs, est obtenue par une nouvelle méthode basée sur le calcul ZX (voir chapitre 1, section 1.3) et non plus sur des décompositions dans le groupe $\mathrm{Sp}_{2n}(\mathbb{F}_2)$.

4.2 La forme $\overline{PZX}$ dans le groupe symplectique

Dans cette section, nous étudions le sous-groupe du groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ engendré par les matrices du type $\overline{P}_b$, $\overline{Z}_B$ et $\overline{X}_A$ avec $b \in \mathbb{F}_2^n$, $B \in \mathcal{B}_n^0$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$ (voir table 4.1).

4.2.1 Structure de produit semi-direct d'un sous-groupe de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$

Le sous-groupe du groupe de Clifford engendré par les portes de phase P et les portes CZ est noté $\langle P, CZ\rangle_n$. Son image dans le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ par le morphisme $\overline{\Phi}$ est noté $\langle \overline{P}, \overline{CZ}\rangle_n$:

$$\langle \overline{P}, \overline{CZ}\rangle_n = \left\{ \begin{bmatrix} I & 0 \\ B & I \end{bmatrix} \mid B \in \mathcal{B}_n \right\}. \tag{4.39}$$

Si $B \in \mathcal{B}_n$, on pose

$$\overline{PZ}_B = \begin{bmatrix} I & 0 \\ B & I \end{bmatrix}. \tag{4.40}$$

Avec cette notation on a,

$$\overline{PZ}_B \overline{PZ}_{B'} = \begin{bmatrix} I & 0 \\ B & I \end{bmatrix} \begin{bmatrix} I & 0 \\ B' & I \end{bmatrix} = \begin{bmatrix} I & 0 \\ B \oplus B' & I \end{bmatrix} = \overline{PZ}_{B \oplus B'} \tag{4.41}$$

avec $B, B' \in \mathcal{B}_n$ et

$$\overline{PZ}_B = \overline{P}_b \overline{Z}_{B \oplus \mathrm{diag}(b)}, \tag{4.42}$$

avec $b = \overrightarrow{\mathrm{diag}}(B)$.

L'image dans le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ du groupe $\langle CNOT\rangle_n$ par le morphisme $\overline{\Phi}$ est noté $\langle \overline{CNOT}\rangle_n$ et on a :

$$\langle \overline{CNOT}\rangle_n = \left\{ \begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix} \mid A \in \mathrm{GL}_n(\mathbb{F}_2) \right\}. \tag{4.43}$$

Le sous-groupe du groupe de Clifford engendré par les portes de phase P, les portes CZ et les portes $CNOT$ est noté $\langle P, CZ, CNOT\rangle_n$. Son image dans le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ par le morphisme $\overline{\Phi}$ est notée $\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n$. La proposition qui suit met en évidence la structure du groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n$.

Proposition 4.20. *Le groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n$ est le sous-groupe du groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ formé par l'ensemble des matrices symplectiques de la forme $\begin{bmatrix} M & 0 \\ Q & R \end{bmatrix}$.*

Tout élément de $\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n$ peut s'écrire de façon unique comme le produit d'un élément du groupe $\langle \overline{P}, \overline{CZ}\rangle_n$ et d'un élément du groupe $\langle \overline{CNOT}\rangle_n$, c'est à dire sous la forme

$$\overline{PZ}_B \overline{X}_A = \begin{bmatrix} I & 0 \\ B & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix} \tag{4.44}$$

avec $B \in \mathcal{B}_n$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$.

Le groupe $\langle \overline{P}, \overline{CZ}\rangle_n$ est un sous-groupe normal du groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n$ et le groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n$ est le produit semi-direct interne du groupe $\langle \overline{P}, \overline{CZ}\rangle_n$ par le groupe $\langle \overline{CNOT}\rangle_n$:

$$\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n \simeq \langle \overline{P}, \overline{CZ}\rangle_n \rtimes \langle \overline{CNOT}\rangle_n. \tag{4.45}$$

Le produit de deux éléments du groupe $\langle \overline{P}, \overline{CZ}\rangle_n \rtimes \langle \overline{CNOT}\rangle_n$ est donné par :

$$(\overline{PZ}_B \overline{X}_A)(\overline{PZ}_{B'} \overline{X}_{A'}) = \overline{PZ}_{B \oplus (A^{-1})^{\mathrm{t}} B' A^{-1}} \overline{X}_{AA'}. \tag{4.46}$$

Démonstration. Soit $W = \begin{bmatrix} M & 0 \\ Q & R \end{bmatrix}$ une matrice symplectique. D'après la proposition 4.12, on a $M^{\mathrm{t}}R \oplus Q^{\mathrm{t}}0 = I$, donc $M, R \in \mathrm{GL}_n(\mathbb{F}_2)$ et $R = (M^{\mathrm{t}})^{-1}$. Ainsi

$$W = \begin{bmatrix} M & 0 \\ Q & (M^{-1})^{\mathrm{t}} \end{bmatrix} = \begin{bmatrix} I & 0 \\ QM^{-1} & I \end{bmatrix} \begin{bmatrix} M & 0 \\ 0 & (M^{-1})^{\mathrm{t}} \end{bmatrix}.$$

De plus $M^{\mathrm{t}}Q = Q^{\mathrm{t}}M$ car W est symplectique donc $Q^{\mathrm{t}} = M^{\mathrm{t}}QM^{-1}$. Soit $B = QM^{-1}$, alors $B^{\mathrm{t}} = (M^{-1})^{\mathrm{t}}Q^{\mathrm{t}} = (M^{-1})^{\mathrm{t}}M^{\mathrm{t}}QM^{-1} = QM^{-1}$, donc $B^{\mathrm{t}} = B$. Ainsi

$$W = \begin{bmatrix} I & 0 \\ B & I \end{bmatrix} \begin{bmatrix} M & 0 \\ 0 & (M^{-1})^{\mathrm{t}} \end{bmatrix},$$

avec $B \in \mathcal{B}_n$ et W est le produit d'un élément du groupe $\langle \overline{P}, \overline{CZ}\rangle_n$ et d'un élément du groupe $\langle \overline{CNOT}\rangle_n$.

Cette décomposition est unique car si $\begin{bmatrix} I & 0 \\ B & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix} = \begin{bmatrix} I & 0 \\ B' & I \end{bmatrix} \begin{bmatrix} A' & 0 \\ 0 & (A'^{-1})^{\mathrm{t}} \end{bmatrix}$ alors $\begin{bmatrix} I & 0 \\ B' \oplus B & I \end{bmatrix} = \begin{bmatrix} A'A^{-1} & 0 \\ 0 & (A'^{-1})^{\mathrm{t}} A^{\mathrm{t}} \end{bmatrix}$, donc $A = A'$ et $B = B'$.

Le groupe $\langle \overline{P}, \overline{CZ}\rangle_n$ est un sous-groupe normal du groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT}\rangle_n$ car

$$\begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix} \begin{bmatrix} I & 0 \\ B & I \end{bmatrix} \begin{bmatrix} A^{-1} & 0 \\ 0 & A^{\mathrm{t}} \end{bmatrix} = \begin{bmatrix} I & 0 \\ (A^{-1})^{\mathrm{t}} B A^{-1} & I \end{bmatrix}$$

et la matrice $(A^{-1})^{\mathrm{t}} B A^{-1}$ est symétrique puisque $B \in \mathcal{B}_n$. En utilisant la définition du produit semi-direct interne [3] et les résultats précédents, on obtient directement la propriété (4.45). La formule (4.46) s'obtient en écrivant

$$(\overline{PZ}_B \overline{X}_A)(\overline{PZ}_{B'} \overline{X}_{A'}) = \overline{PZ}_B (\overline{X}_A \overline{PZ}_{B'} \overline{X}_{A^{-1}}) \overline{X}_A \overline{X}_{A'}$$

puis en effectuant un produit matriciel par blocs. □

3. Voir annexe A, section A.3.2

4.2.2 Algorithme de mise en forme $\overline{PZX}$

Définition 4.21. On dit qu'un élément de $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ est en forme $\overline{PZX}$ quand il est écrit sous la forme

$$\overline{P}_b \overline{Z}_B \overline{X}_A = \begin{bmatrix} I & 0 \\ \mathrm{diag}(b) & I \end{bmatrix} \begin{bmatrix} I & 0 \\ B & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix}, \tag{4.47}$$

avec $b \in \mathbb{F}_2^n$, $B \in \mathcal{B}_0^n$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$.

Le corollaire suivant est une conséquence immédiate de la proposition 4.20 et de l'identité (4.42).

Corollaire 4.22. *Tout élément du groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ peut s'écrire de façon unique sous la forme $\overline{PZX}$.*

Dans la pratique, pour mettre en forme $\overline{PZX}$ un élément du groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ donné comme un produit de générateurs, on utilise l'algorithme `C-to-PZX` (algorithme 4.1).

Algorithme 4.1 `C-to-PZX`

Entrée : $\overline{C}$, un élément de $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ donné par un produit $\overline{C} = \prod_{k=1}^{\ell} \overline{M}_k$ avec $\overline{M}_k \in \{\overline{P}_i, \overline{Z}_{\{i,j\}}, \overline{X}_{[i:j]} \mid 0 \leqslant i, j < n,\ i \neq j\}$.
$\overline{PZX}_{\mathrm{in}} = \overline{P}_b \overline{Z}_B \overline{X}_A$, un élément de $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ en forme $\overline{PZX}$.
Sortie : $\overline{PZX}_{\mathrm{out}}$, un élément de $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ en forme $\overline{PZX}$ tel que $\overline{PZX}_{\mathrm{out}} = \overline{C}\ \overline{PZX}_{\mathrm{in}}$.

1: $B' \leftarrow B \oplus \mathrm{diag}(b)$;
2: **pour** $k \leftarrow \ell$ **à** 1 **faire**
3: **si** $\overline{M}_k = \overline{P}_i$ **alors**
4: $B'_{i,i} \leftarrow B'_{i,i} \oplus 1$
5: **sinon si** $\overline{M}_k = \overline{Z}_{\{i,j\}}$ **alors**
6: $B'_{i,j} \leftarrow B'_{i,j} \oplus 1$
7: $B'_{j,i} \leftarrow B'_{j,i} \oplus 1$
8: **sinon**
9: // cas où $M_k = X_{[i:j]}$
10: $B' \leftarrow [j:i]B'[i:j]$
11: $A \leftarrow [i:j]A$
12: **fin si**
13: **fin pour**
14: $b' \leftarrow \overrightarrow{\mathrm{diag}}(B')$
15: **retourner** $\overline{PZX}_{\mathrm{out}} = \overline{P}_{b'} \overline{Z}_{B' \oplus \mathrm{diag}(b')} \overline{X}_A$

Proposition 4.23. *La complexité temporelle de l'algorithme* `C-to-PZX` *est $O(\ell n)$.*

Démonstration. Il y a ℓ matrices symplectiques $\overline{M}_k$ dans le produit $\overline{C}$ en entrée et pour chacune de ces matrices, on effectue au plus $3n$ additions (XOR) bit à bit. En effet, la multiplication par une matrice de transvection (lignes 10 et 11) consiste à additionner deux lignes de bits. □

Proposition 4.24. *Soit un élément $\overline{C}$ du groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ donné sous la forme d'un produit $\overline{C} = \prod_{k=1}^{\ell} \overline{M}_k$ avec $\overline{M}_k \in \{\overline{P}_i, \overline{Z}_{\{i,j\}}, \overline{X}_{[i:j]}\}$, alors l'algorithme* `C-to-PZX` *permet de mettre $\overline{C}$ en forme $\overline{PZX}$ en temps $O(\ell n)$.*

Démonstration. On utilise l'algorithme $\overline{\texttt{C-to-PZX}}$ avec en entrée $\overline{C} = \prod_{k=1}^{\ell} \overline{M}_k$ et $\overline{PZX}_{\text{in}} = I_{2n}$ (*i.e.*, $b = 0$, $B = 0$ et $A = I_n$). □

Remarque 4.25. Dans le cas particulier où l'algorithme $\overline{\texttt{C-to-PZX}}$ est utilisé avec des entrées $\overline{C}$ et $\overline{PZX}_{\text{in}}$ sans portes de phase, *i.e.* : $\overline{M}_k \in \{\overline{Z}_{\{i,j\}}, \overline{X}_{[i:j]} \mid 0 \leqslant i, j < n,\ i \neq j\}$ et $\overline{PZX}_{\text{in}} = \overline{Z}_B \overline{X}_A$, alors la sortie $\overline{PZX}_{\text{out}}$ est sous la forme $\overline{Z}_{B'} \overline{X}_{A'}$. Il s'agit donc dans ce cas de la version symplectique de l'algorithme `C-to-ZX` décrit au chapitre 3 (algorithme 3.2).

4.3 La forme $\overline{PZX}$ généralisée dans le groupe symplectique

Définition 4.26. On dit qu'un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ est en forme gen$\overline{PZX}$ (forme $\overline{PZX}$ généralisée) quand il est écrit sous la forme

$$\overline{H}_a \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A, \tag{4.48}$$

avec $a, d, b \in \mathbb{F}_2^n$, $D, B \in \mathcal{B}_0^n$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$.

En notation matricielle, cette forme s'écrit ainsi :

$$\begin{bmatrix} \mathrm{diag}(a \oplus \omega) & \mathrm{diag}(a) \\ \mathrm{diag}(a) & \mathrm{diag}(a \oplus \omega) \end{bmatrix} \begin{bmatrix} I & 0 \\ D \oplus \mathrm{diag}(d) & I \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} I & 0 \\ B \oplus \mathrm{diag}(b) & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix}. \tag{4.49}$$

On utilisera parfois des cas particuliers de la forme gen$\overline{PZX}$ obtenus en donnant des valeurs particulières aux vecteurs a, d, b ou aux matrices D, B, A. Ainsi la notation gen$\overline{PZX}_{\{a=0\}}$ désignera la forme gen$\overline{PZX}$ telle que $a = 0$ et la notation gen$\overline{PZX}_{\{a=0,\ d=0\}}$ désignera la forme gen$\overline{PZX}$ telle que $a = 0$ et $d = 0$. Avec ces notations, on remarque que la forme $\overline{PZX}$ est bien un cas particulier de la forme gen$\overline{PZX}$: il s'agit en fait de la forme particulière gen$\overline{PZX}_{\{a=[1\ldots1]^{\mathrm{t}},\ d=0,\ D=0\}}$ puisque dans ce cas $\overline{Z}_D = \overline{P}_d = I_{2n}$, $\overline{H}_a = \Omega$ et $\Omega^2 = I_{2n}$.

4.3.1 Formules de conjugaison et propriétés utilisées

L'algorithme de mise en forme $\overline{PZX}$ généralisée (exposé dans la sous-section suivante) est basé sur quelques règles de conjugaison dans le groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ ainsi que sur l'utilisation de différentes routines, dont l'algorithme $\overline{\texttt{C-to-PZX}}$. Dans la proposition 4.27, nous récapitulons les différentes formules de conjugaison utilisées. Nous donnons ensuite plusieurs propositions qui décrivent des algorithmes de transformation d'écriture de certains éléments de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$. Ces algorithmes interviendront sous forme de routines dans l'algorithme de mise en forme $\overline{PZX}$ généralisée, cela afin d'alléger sa description et de factoriser le code.

Proposition 4.27. *Soient i, j, k des entiers distincts de $\{0, \ldots, n-1\}$. Dans le groupe*

symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$*, on a les règles de conjugaison suivantes.*

$$\overline{S}_{(i\ \ j)}\overline{H}_i\overline{S}_{(i\ \ j)} = \overline{H}_j \tag{4.50}$$
$$\overline{X}_{[i:j]}\overline{X}_{[j:k]}\overline{X}_{[i:j]} = \overline{X}_{[j:k]}\overline{X}_{[i:k]} = \overline{X}_{[i:k]}\overline{X}_{[j:k]} \tag{4.51}$$
$$\overline{X}_{[j:i]}\overline{X}_{[i:j]}\overline{X}_{[j:i]} = \overline{S}_{(i\ \ j)} \tag{4.52}$$
$$\overline{X}^{\Omega}_{[i:j]} = \overline{X}_{[j:i]} \tag{4.53}$$
$$\overline{X}^{\Omega}_{A} = \overline{X}_{(A^{-1})^{\mathrm{t}}} \tag{4.54}$$
$$\overline{H}_i\overline{X}_{[i:j]}\overline{H}_i = \overline{H}_j\overline{X}_{[j:i]}\overline{H}_j = \overline{Z}_{\{i,j\}} \tag{4.55}$$
$$\overline{X}_{[i:j]}\overline{P}_i\overline{X}_{[i:j]} = \overline{P}_i\overline{P}_j\overline{Z}_{\{i,j\}} \tag{4.56}$$
$$\overline{X}_{[i:j]}\overline{P}_j\overline{X}_{[i:j]} = \overline{P}_j \tag{4.57}$$
$$\overline{S}_{(i\ \ j)}\overline{P}_b\overline{S}_{(i\ \ j)} = \overline{P}_{(i\ \ j)b} \tag{4.58}$$
$$\overline{S}_{(i\ \ j)}\overline{Z}_B\overline{S}_{(i\ \ j)} = \overline{Z}_{(i\ \ j)B(i\ \ j)} \tag{4.59}$$
$$\overline{P}^{\Omega}_i\overline{P}_i\overline{P}^{\Omega}_i = \overline{H}_i \tag{4.60}$$
$$\overline{P}^{\Omega}_i\overline{Z}_{\{i,j\}}\overline{P}^{\Omega}_i = \overline{P}_j\overline{Z}_{\{i,j\}}\overline{X}_{[i:j]} \tag{4.61}$$
$$\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_{\{i,k\}}\overline{Z}^{\Omega}_{\{i,j\}} = \overline{Z}_{\{i,k\}}\overline{X}_{[j:k]} \tag{4.62}$$
$$\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_{\{i,j\}}\overline{Z}^{\Omega}_{\{i,j\}} = \overline{H}_i\overline{H}_j\overline{S}_{(i\ \ j)} \tag{4.63}$$
$$\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_j\overline{Z}^{\Omega}_{\{i,j\}} = \overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{P}_j \tag{4.64}$$

Démonstration. Les quatre premières identités (4.50), (4.51), (4.52) et (4.53) sont obtenues respectivement à partir des identités (1.76), (2.7), (1.80) et (1.78) en utilisant le morphisme $\overline{\Phi}$ (définition 4.16).

L'identité (4.54) généralise l'identité (4.53) en utilisant une décomposition de la matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ en produit de transvections et en remarquant que si $A = \prod_{k=1}^{\ell}[i_k : j_k]$ alors $(A^{-1})^{\mathrm{t}} = \prod_{k=1}^{\ell}[j_k : i_k]$.

L'identité (4.55) est la version symplectique de l'identité (1.79) :

$$Z_{\{i,j\}} = H_iX_{[i:j]}H_i = H_jX_{[j:i]}H_j.$$

Pour prouver l'identité (4.56), on remarque que

$$\begin{aligned}\overline{X}_{[i:j]}\overline{P}_i\overline{X}_{[i:j]} &= \begin{bmatrix}[i:j] & 0\\ 0 & [j:i]\end{bmatrix}\begin{bmatrix}I & 0\\ \mathrm{diag}(e_i) & I\end{bmatrix}\begin{bmatrix}[i:j] & 0\\ 0 & [j:i]\end{bmatrix}\\ &= \begin{bmatrix}I & 0\\ [j:i]\mathrm{diag}(e_i)[i:j] & I\end{bmatrix}\end{aligned}$$

puis on utilise l'interprétation de la multiplication par une matrice de transvection à droite et à gauche (proposition 2.6) pour obtenir

$$[j:i]\mathrm{diag}(e_i)[i:j] = \mathrm{diag}(e_i \oplus e_j) \oplus E_{\{i,j\}}$$

et on a ainsi

$$\begin{bmatrix}I & 0\\ [j:i]\mathrm{diag}(e_i)[i:j] & I\end{bmatrix} = \overline{P}_i\overline{P}_j\overline{Z}_{\{i,j\}}.$$

L'identité (4.57) se démontre de la même façon que (4.56).

L'identité (4.58) se démontre de façon similaire à l'identité (4.56). On écrit tout d'abord

$$\begin{aligned}\overline{S}_{(i\ j)}\overline{P}_b\overline{S}_{(i\ j)} &= \begin{bmatrix}(i\ j) & 0\\ 0 & (i\ j)\end{bmatrix}\begin{bmatrix}I & 0\\ \mathrm{diag}(b) & I\end{bmatrix}\begin{bmatrix}(i\ j) & 0\\ 0 & (i\ j)\end{bmatrix}\\ &= \begin{bmatrix}I & 0\\ (i\ j)\mathrm{diag}(b)(i\ j) & I\end{bmatrix}\end{aligned}$$

puis on remarque que $(i\ j)\mathrm{diag}(b)(i\ j) = \mathrm{diag}((i\ j)b)$ (voir corollaire 2.7 sur l'effet de la multiplication par une matrice de transposition).

L'identité (4.59) se démontre simplement en effectuant une multiplication matricielle par bloc dans $\mathrm{Sp}_{2n}(\mathbb{F}_2)$.
Un calcul direct montre que $(HP)^3 = (PH)^3 = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}I_2$, donc pour tout $i = 0, \ldots, n-1$ on a $(H_iP_i)^3 = (P_iH_i)^3 = \mathrm{e}^{\mathrm{i}\frac{\pi}{4}}I_{2^n}$. En utilisant le morphisme $\overline{\Phi}$, on a alors $(\overline{H}_i\overline{P}_i)^3 = I_{2n}$ dans le groupe symplectique. Ainsi $(\overline{H}_i\overline{P}_i\overline{H}_i)\overline{P}_i(\overline{H}_i\overline{P}_i\overline{H}_i) = \overline{H}_i$ et on en déduit (4.60).

Pour prouver l'identité (4.61), on utilise d'abord l'identité (4.55) :

$$\overline{P}_i^{\Omega}\overline{Z}_{\{i,j\}}\overline{P}_i^{\Omega} = \overline{H}_i\overline{P}_i\left(\overline{H}_i\overline{Z}_{\{i,j\}}\overline{H}_i\right)\overline{P}_i\overline{H}_i = \overline{H}_i\overline{P}_i\overline{X}_{[i:j]}\overline{P}_i\overline{H}_i.$$

Or, d'après (4.56), on a $\overline{P}_i\overline{X}_{[i:j]}\overline{P}_i = \overline{X}_{[i:j]}\overline{P}_j\overline{Z}_{\{i,j\}}$ donc

$$\begin{aligned}\overline{P}_i^{\Omega}\overline{Z}_{\{i,j\}}\overline{P}_i^{\Omega} &= \overline{H}_i\left(\overline{X}_{[i:j]}\overline{P}_j\overline{Z}_{\{i,j\}}\right)\overline{H}_i\\ &= \left(\overline{H}_i\overline{X}_{[i:j]}\overline{H}_i\right)\left(\overline{H}_i\overline{P}_j\overline{H}_i\right)\left(\overline{H}_i\overline{Z}_{\{i,j\}}\overline{H}_i\right)\end{aligned}$$

Finalement, en utilisant l'identité (4.55) et en notant que $\overline{H}_i$ et $\overline{P}_j$ commutent, on obtient

$$\overline{P}_i^{\Omega}\overline{Z}_{\{i,j\}}\overline{P}_i^{\Omega} = \overline{Z}_{\{i,j\}}\overline{P}_j\overline{X}_{[i:j]} = \overline{P}_j\overline{Z}_{\{i,j\}}\overline{X}_{[i:j]}.$$

Prouvons l'identité (4.62) :

$$\begin{aligned}\overline{Z}_{\{i,j\}}^{\Omega}\overline{Z}_{\{i,k\}}\overline{Z}_{\{i,j\}}^{\Omega} &= \left(\overline{H}_i\overline{H}_j\overline{Z}_{\{i,j\}}\overline{H}_j\overline{H}_i\right)\overline{Z}_{\{i,k\}}\left(\overline{H}_i\overline{H}_j\overline{Z}_{\{i,j\}}\overline{H}_j\overline{H}_i\right)\\ &\overset{(4.55)}{=} \left(\overline{H}_i\overline{X}_{[j:i]}\overline{H}_i\right)\overline{Z}_{\{i,k\}}\left(\overline{H}_i\overline{X}_{[j:i]}\overline{H}_i\right)\\ &= \overline{H}_i\overline{X}_{[j:i]}\left(\overline{H}_i\overline{Z}_{\{i,k\}}\overline{H}_i\right)\overline{X}_{[j:i]}\overline{H}_i\\ &\overset{(4.55)}{=} \overline{H}_i\overline{X}_{[j:i]}\overline{X}_{[i:k]}\overline{X}_{[j:i]}\overline{H}_i\\ &\overset{(4.51)}{=} \overline{H}_i\overline{X}_{[i:k]}\overline{X}_{[j:k]}\overline{H}_i\\ &= \left(\overline{H}_i\overline{X}_{[i:k]}\overline{H}_i\right)\overline{X}_{[j:k]}\\ &\overset{(4.55)}{=} \overline{Z}_{\{i,k\}}\overline{X}_{[j:k]}.\end{aligned}$$

Prouvons l'identité (4.63) :

$$\begin{aligned}
\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_{\{i,j\}}\overline{Z}^{\Omega}_{\{i,j\}} &= \left(\overline{H}_i\overline{H}_j\overline{Z}_{\{i,j\}}\overline{H}_j\overline{H}_i\right)\overline{Z}_{\{i,j\}}\left(\overline{H}_i\overline{H}_j\overline{Z}_{\{i,j\}}\overline{H}_j\overline{H}_i\right)\\
&\overset{(4.55)}{=} \left(\overline{H}_i\overline{X}_{[j:i]}\overline{H}_i\right)\overline{Z}_{\{i,j\}}\left(\overline{H}_i\overline{X}_{[j:i]}\overline{H}_i\right)\\
&= \overline{H}_i\overline{X}_{[j:i]}\left(\overline{H}_i\overline{Z}_{\{i,j\}}\overline{H}_i\right)\overline{X}_{[j:i]}\overline{H}_i\\
&\overset{(4.55)}{=} \overline{H}_i\overline{X}_{[j:i]}\overline{X}_{[i:j]}\overline{X}_{[j:i]}\overline{H}_i\\
&\overset{(4.52)}{=} \overline{H}_i\overline{S}_{(i\ \ j)}\overline{H}_i\\
&= \overline{H}_i\overline{H}_j\overline{S}_{(i\ \ j)}.
\end{aligned}$$

Prouvons l'identité (4.64) :

$$\begin{aligned}
\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_j\overline{Z}^{\Omega}_{\{i,j\}} &= \left(\overline{H}_i\overline{H}_j\overline{Z}_{\{i,j\}}\overline{H}_j\overline{H}_i\right)\overline{P}_j\left(\overline{H}_i\overline{H}_j\overline{Z}_{\{i,j\}}\overline{H}_j\overline{H}_i\right)\\
&\overset{(4.55)}{=} \left(\overline{H}_i\overline{X}_{[j:i]}\overline{H}_i\right)\overline{P}_j\left(\overline{H}_i\overline{X}_{[j:i]}\overline{H}_i\right)\\
&= \overline{H}_i\left(\overline{X}_{[j:i]}\overline{P}_j\overline{X}_{[j:i]}\right)\overline{H}_i\\
&\overset{(4.56)}{=} \overline{H}_i\left(\overline{P}_i\overline{P}_j\overline{Z}_{\{i,j\}}\right)\overline{H}_i\\
&= \overline{P}^{\Omega}_i\overline{P}_j\left(\overline{H}_i\overline{Z}_{\{i,j\}}\overline{H}_i\right)\\
&\overset{(4.55)}{=} \overline{P}^{\Omega}_i\overline{P}_j\overline{X}_{[i:j]}\\
&\overset{(4.57)}{=} \overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{P}_j
\end{aligned}$$

□

Proposition 4.28. *Soit $\overline{F}$ un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ en forme $\mathrm{gen}\overline{PZX}$ et soit a' un vecteur de $\mathbb{F}_2^n$. On peut mettre $\overline{H}_{a'}\overline{F}$ sous la forme $\mathrm{gen}\overline{PZX}$ en temps $O(n)$.*

Démonstration. Il s'agit simplement d'additionner le vecteur a' avec le vecteur a définissant $\overline{H}_a$ dans la forme $\overline{F}$. □

Proposition 4.29. *Soit $\overline{F}$ un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ en forme $\mathrm{gen}\overline{PZX}_{\{a=0\}}$ et soit d' un vecteur de $\mathbb{F}_2^n$. On peut mettre $\overline{P}_{d'}\overline{F}$ sous la forme $\mathrm{gen}\overline{PZX}_{\{a=0\}}$ en temps $O(n)$.*

Démonstration. Il s'agit simplement d'additionner le vecteur d' avec le vecteur d définissant $\overline{P}_d$ dans la forme $\overline{F}$. □

Proposition 4.30. *Soit $\overline{F}$ un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ en forme $\mathrm{gen}\overline{PZX}_{\{a=0,\ d=0\}}$ et soit i un entier tel que $0 \leqslant i \leqslant n-1$. On peut mettre $\overline{P}^{\Omega}_i\overline{F}$ sous la forme $\mathrm{gen}\overline{PZX}_{\{a=0\}}$ en temps $O(n^2)$.*

Démonstration. Posons $\overline{F} = \overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A$. On commence par modifier l'écriture de $\overline{P}^{\Omega}_i\overline{F}$ de la façon suivante.

$$\begin{aligned}
\overline{P}^{\Omega}_i\overline{F} &= \overline{P}^{\Omega}_i\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A\\
&= \left(\overline{P}^{\Omega}_i\overline{Z}_D\overline{P}^{\Omega}_i\right)\overline{P}^{\Omega}_i\Omega\overline{P}_b\overline{Z}_B\overline{X}_A\\
&= \left(\overline{P}^{\Omega}_i\overline{Z}_D\overline{P}^{\Omega}_i\right)\Omega\overline{P}_i\overline{P}_b\overline{Z}_B\overline{X}_A\\
&= \left(\overline{P}^{\Omega}_i\overline{Z}_D\overline{P}^{\Omega}_i\right)\Omega\overline{P}_{b\oplus e_i}\overline{Z}_B\overline{X}_A
\end{aligned} \tag{4.65}$$

On pose alors $D_i = \{\{p,q\} \in D \mid i \in \{p,q\}\}$ et $\Lambda_i = \{k \mid \{i,k\} \in D\}$. On a donc $\overline{Z}_{D_i} = \prod_{k\in\Lambda_i} \overline{Z}_{\{i,k\}}$ et $\overline{Z}_D = \overline{Z}_{D\oplus D_i}\overline{Z}_{D_i}$. En remarquant que $\overline{Z}_{D\oplus D_i}$ et $\overline{P}_i^\Omega$ commutent, on a

$$\begin{aligned}\overline{P}_i^\Omega \overline{Z}_D \overline{P}_i^\Omega &= \overline{Z}_{D\oplus D_i}\left(\overline{P}_i^\Omega \overline{Z}_{D_i}\overline{P}_i^\Omega\right)\\ &= \overline{Z}_{D\oplus D_i}\prod_{k\in\Lambda_i}\overline{P}_i^\Omega\overline{Z}_{\{i,k\}}\overline{P}_i^\Omega\\ &\overset{(4.61)}{=} \overline{Z}_{D\oplus D_i}\prod_{k\in\Lambda_i}\overline{P}_k\overline{Z}_{\{i,k\}}\overline{X}_{[i:k]},\end{aligned}$$

et en reportant dans (4.65), il vient

$$\overline{P}_i^\Omega\overline{F} = \left(\overline{Z}_{D\oplus D_i}\prod_{k\in\Lambda_i}\overline{P}_k\overline{Z}_{\{i,k\}}\overline{X}_{[i:k]}\right)\Omega\overline{P}_{b\oplus e_i}\overline{Z}_B\overline{X}_A.$$

On utilise maintenant l'algorithme $\overline{\texttt{C-to-PZX}}$: soit

$$\overline{P}_{d'}\overline{Z}_{D'}\overline{X}_{A'} = \overline{\texttt{C-to-PZX}}\left(\textstyle\prod_{k\in\Lambda_i}\overline{P}_k\overline{Z}_{\{i,k\}}\overline{X}_{[i:k]}, I_{2n}\right),$$

on a alors

$$\begin{aligned}\overline{P}_i^\Omega\overline{F} &= \overline{Z}_{D\oplus D_i}\overline{P}_{d'}\overline{Z}_{D'}\overline{X}_{A'}\Omega\overline{P}_{b\oplus e_i}\overline{Z}_B\overline{X}_A\\ &= \overline{P}_{d'}\overline{Z}_{D\oplus D_i\oplus D'}\overline{X}_{A'}\Omega\overline{P}_{b\oplus e_i}\overline{Z}_B\overline{X}_A\\ &\overset{(4.54)}{=} \overline{P}_{d'}\overline{Z}_{D\oplus D_i\oplus D'}\Omega\overline{X}_{(A'^{-1})^{\mathrm{t}}}\overline{P}_{b\oplus e_i}\overline{Z}_B\overline{X}_A,\end{aligned} \tag{4.66}$$

avec $A' = \prod_{k\in\Lambda_i}[i:k]$, donc $(A'^{-1})^{\mathrm{t}} = \prod_{k\in\Lambda_i}[k:i]$.

On utilise à nouveau l'algorithme $\overline{\texttt{C-to-PZX}}$: soit

$$\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'} = \overline{\texttt{C-to-PZX}}\left(\textstyle\prod_{k\in\Lambda_i}[k:i], \overline{P}_{b\oplus e_i}\overline{Z}_B\overline{X}_A\right),$$

on a alors

$$\overline{P}_i^\Omega\overline{F} = \overline{P}_{d'}\overline{Z}_{D\oplus D_i\oplus D'}\Omega\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'}$$

ce qui est la forme souhaitée.

Le temps de calcul des différentes étapes permettant de mettre $\overline{P}_i^\Omega\overline{F}$ en forme $\mathrm{gen}\overline{PZX}_{\{a=0\}}$ est dominé par l'addition de matrices de $\mathcal{B}_n^0$ (4.66) qui se fait en temps $O(n^2)$ ainsi que par l'utilisation de l'algorithme $\overline{\texttt{C-to-PZX}}$ dont la complexité temporelle est $O(\ell n)$, avec ℓ désignant la longueur du produit de portes de Clifford en entrée (voir algorithme 4.1). On remarque que l'ensemble Λ_i contient au maximum n entiers, donc la complexité de l'utilisation de l'algorithme $\overline{\texttt{C-to-PZX}}$ dans ce contexte est $O(n^2)$. On voit donc que la complexité de l'algorithme constitué par les différentes étapes permettant de mettre $\overline{P}_i^\Omega\overline{F}$ en forme $\mathrm{gen}\overline{PZX}_{\{a=0\}}$ est $O(n^2)$. □

Corollaire 4.31. *Soit $\overline{F}$ un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ en forme $\mathrm{gen}\overline{PZX}_{\{a=0\}}$ et soit un entier i tel que $0 \leqslant i \leqslant n-1$. On peut mettre $\overline{P}_i^\Omega\overline{F}$ sous la forme $\mathrm{gen}\overline{PZX}$ en temps $O(n^2)$.*

Démonstration. Posons $\overline{F} = \overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A$, on a :

$$\overline{P}_i^\Omega\overline{F} = \overline{P}_i^\Omega\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A.$$

On doit distinguer deux cas selon les valeurs de d_i.

- Si $d_i = 0$, alors $\overline{P}_i^{\Omega}$ et $\overline{P}_d$ commutent, donc

$$\overline{P}_i^{\Omega}\overline{F} = \overline{P}_d\left(\overline{P}_i^{\Omega}\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A\right).$$

  On applique la proposition 4.30 à l'expression $\overline{P}_i^{\Omega}\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A$ de façon à l'écrire sous la forme $\overline{P}_{d'}\overline{Z}_{D'}\Omega\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'}$. On obtient alors

$$\begin{aligned}\overline{P}_i^{\Omega}\overline{F} &= \overline{P}_d\overline{P}_{d'}\overline{Z}_{D'}\Omega\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'}\\ &= \overline{P}_{d\oplus d'}\overline{Z}_{D'}\Omega\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'}\end{aligned}$$

  et $\overline{P}_i^{\Omega}\overline{F}$ est sous la forme gen$\overline{PZX}$.

- Si $d_i = 1$, alors $\overline{P}_i^{\Omega}$ et $\overline{P}_d$ ne commutent pas et on a

$$\overline{P}_i^{\Omega}\overline{F} = \left(\overline{P}_i^{\Omega}\overline{P}_d\overline{P}_i^{\Omega}\right)\overline{P}_i^{\Omega}\overline{Z}_D\Omega\overline{P}_b\overline{Z}_BX_A. \tag{4.67}$$

  En écrivant $\overline{P}_d = \overline{P}_i\overline{P}_{d\oplus e_i}$ et en utilisant l'identité (4.60) on obtient

$$\overline{P}_i^{\Omega}\overline{P}_d\overline{P}_i^{\Omega} = \overline{P}_i^{\Omega}\overline{P}_i\overline{P}_i^{\Omega}\overline{P}_{d\oplus e_i} = \overline{H}_i\overline{P}_{d\oplus e_i}$$

  donc

$$\overline{P}_i^{\Omega}\overline{F} = \overline{H}_i\overline{P}_{d\oplus e_i}\left(\overline{P}_i^{\Omega}\overline{Z}_D\Omega\overline{P}_b\overline{Z}_BX_A\right).$$

  On applique la proposition 4.30 à l'expression $\overline{P}_i^{\Omega}\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A$ afin de l'écrire sous la forme $\overline{P}_{d'}\overline{Z}_{D'}\Omega\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'}$. On obtient alors

$$\begin{aligned}\overline{P}_i^{\Omega}\overline{F} &= \overline{H}_i\overline{P}_{d\oplus e_i}\overline{P}_{d'}\overline{Z}_{D'}\Omega\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'}\\ &= \overline{H}_i\overline{P}_{d\oplus e_i\oplus d'}\overline{Z}_{D'}\Omega\overline{P}_{b'}\overline{Z}_{B'}\overline{X}_{A'}\end{aligned}$$

  et $\overline{P}_i^{\Omega}\overline{F}$ est écrit sous la forme gen$\overline{PZX}$.

La complexité temporelle de l'algorithme constitué par ces différentes étapes est la même que dans la proposition 4.30, à savoir $O(n^2)$. □

Proposition 4.32. *Soit $\overline{F}$ un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ en forme gen$\overline{PZX}_{\{a=0\}}$ et soient deux entiers distincts i, j tels que $0 \leqslant i, j \leqslant n-1$. On peut mettre $\overline{X}_{[i:j]}\overline{F}$ sous la forme gen$\overline{PZX}_{\{a=0\}}$ en temps $O(n)$.*

De plus, si $\overline{F}$ est en forme gen$\overline{PZX}_{\{a=0,\, d=0\}}$, alors le même algorithme permet d'écrire $\overline{X}_{[i:j]}\overline{F}$ sous la forme gen$\overline{PZX}_{\{a=0,\, d=0\}}$.

Démonstration. Posons $\overline{F} = \overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A$, on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{X}_{[i:j]}\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A.$$

On utilise l'algorithme $\overline{\texttt{C}}$-to-$\overline{\texttt{PZX}}$ une première fois : soit

$$\overline{P}_{d'}\overline{Z}_{D'}\overline{X}_{[i:j]} = \overline{\texttt{C}}\text{-to-}\overline{\texttt{PZX}}\left(\overline{X}_{[i:j]}, \overline{P}_d\overline{Z}_D\right),$$

on a

$$\begin{aligned}\overline{X}_{[i:j]}\overline{F} &= \overline{P}_{d'}\overline{Z}_{D'}\overline{X}_{[i:j]}\Omega\overline{P}_b\overline{Z}_B\overline{X}_A\\ &\overset{(4.53)}{=} \overline{P}_{d'}\overline{Z}_{D'}\Omega\overline{X}_{[j:i]}\overline{P}_b\overline{Z}_B\overline{X}_A.\end{aligned}$$

On utilise l'algorithme $\overline{\texttt{C-to-PZX}}$ une seconde fois : soit

$$\overline{P}_{b'}\overline{Z}_{b'}\overline{X}_{A'} = \overline{\texttt{C-to-PZX}}\left(\overline{X}_{[j:i]}, \overline{P}_d\overline{Z}_D\overline{X}_A\right),$$

on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{P}_{d'}\overline{Z}_{D'}\Omega\overline{P}_{b'}\overline{Z}_{b'}\overline{X}_{A'},$$

ce qui est une expression en forme gen$\overline{PZX}_{\{a=0\}}$.

Dans le cas où $d = 0$, on a lors de la première utilisation de $\overline{\texttt{C-to-PZX}}$:

$$\overline{\texttt{C-to-PZX}}\left(\overline{X}_{[i:j]}, \overline{Z}_D\right) = \overline{Z}_{[j:i]D[i:j]}\overline{X}_{[i:j]}$$

(voir algorithme 4.1). Après la seconde utilisation de $\overline{\texttt{C-to-PZX}}$, on obtient

$$\overline{X}_{[i:j]}\overline{F} = \overline{Z}_{[j:i]D[i:j]}\Omega\overline{P}_{b'}\overline{Z}_{b'}\overline{X}_{A'},$$

ce qui est une expression en forme gen$\overline{PZX}_{\{a=0,\ d=0\}}$.

La complexité de l'algorithme constitué par les différentes étapes permettant d'écrire $\overline{X}_{[i:j]}\overline{F}$ sous la forme gen$\overline{PZX}_{\{a=0\}}$ est celle de l'algorithme $\overline{\texttt{C-to-PZX}}$ qui est en temps $O(\ell n)$ avec ℓ désignant la longueur du produit de portes de Clifford en entrée (voir algorithme 4.1). Ici $\ell = 1$ car le produit en entrée est réduit à une seule porte ($\overline{X}_{[i:j]}$ ou $\overline{X}_{[j:i]}$), donc la complexité temporelle est $O(n)$. □

Table 4.2 Routines utilisées par l'algorithme de mise en forme $\overline{PZX}$ généralisée

Prop.	Routine	Input 1 : $\overline{C}$	Input 2 : $\overline{F}_{\text{in}}$	Output : $\overline{F}_{\text{out}}$ tel que $\overline{F}_{\text{out}} = \overline{C}\ \overline{F}_{\text{in}}$	Temps
4.28	merge-H	$\overline{H}_a$	gen$\overline{PZX}$	gen$\overline{PZX}$	$O(n)$
4.29	merge-P	$\overline{P}_d$	gen$\overline{PZX}_{\{a=0\}}$	gen$\overline{PZX}_{\{a=0\}}$	$O(n)$
4.30	merge-PΩ1	$\overline{P}_i^{\Omega}$	gen$\overline{PZX}_{\{a=0,\ d=0\}}$	gen$\overline{PZX}_{\{a=0\}}$	$O(n^2)$
4.31	merge-PΩ2	$\overline{P}_i^{\Omega}$	gen$\overline{PZX}_{\{a=0\}}$	gen$\overline{PZX}$	$O(n^2)$
4.32	merge-CX	$\overline{X}_{[i:j]}$	gen$\overline{PZX}_{\{a=0\}}$	gen$\overline{PZX}_{\{a=0\}}$	$O(n)$
4.32	merge-CX	$\overline{X}_{[i:j]}$	gen$\overline{PZX}_{\{a=0,\ d=0\}}$	gen$\overline{PZX}_{\{a=0,\ d=0\}}$	$O(n)$

Dans la table 4.2, on fait correspondre à chacune des propositions de la présente sous-section, une routine qui consiste simplement à appliquer la proposition à un élément du type $\overline{C}\ \overline{F}$ (*i.e.* mettre $\overline{C}\ \overline{F}$ en forme $\overline{PZX}$ généralisée), où $\overline{C}$ est la matrice symplectique définie dans la proposition et $\overline{F}$ un élément déjà en forme $\overline{PZX}$ généralisée. Les différentes routines ainsi définies sont appelées par l'algorithme de mise en forme $\overline{PZX}$ généralisée, décrit dans la sous-section suivante (algorithme 4.2 et théorème 4.33).

4.3.2 Mise en forme $\overline{PZX}$ généralisée d'un produit de matrices

L'algorithme 4.2 montre de façon schématique comment mettre en forme $\overline{PZX}$ généralisée un produit de matrices symplectiques prises dans l'ensemble $\overline{\text{Cliff}}_n$ (4.29). Le détail des différentes opérations à réaliser est donné dans la preuve du théorème 4.33.

Théorème 4.33. *Soit $\overline{F}$ un élément du groupe $\text{Sp}_{2n}(\mathbb{F}_2)$ en forme gen$\overline{PZX}$, alors pour toute matrice $\overline{M} \in \overline{\text{Cliff}}_n$, on peut mettre $\overline{M}\ \overline{F}$ sous la forme gen$\overline{PZX}$ en temps $0(n^2)$.*

Algorithme 4.2 $\overline{\texttt{C}}$`-to-gen`$\overline{\texttt{PZX}}$

Entrée : $\overline{C}$, un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ donné par un produit $\overline{C} = \prod_{k=1}^{\ell} \overline{M}_k$ avec $\overline{M}_k \in \overline{\mathrm{Cliff}}_n$.
$\overline{F}_{\mathrm{in}}$, un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ sous la forme gen$\overline{PZX}$.
Sortie : $\overline{F}_{\mathrm{out}}$, un élément de $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ sous la forme gen$\overline{PZX}$ tel que $\overline{F}_{\mathrm{out}} = \overline{C}\,\overline{F}_{\mathrm{in}}$.

1: $\overline{F}_{\mathrm{out}} \leftarrow \overline{F}_{\mathrm{in}}$
2: **pour** $k \leftarrow \ell$ **à** 1 **faire**
3: $\quad \overline{F}_{\mathrm{out}} \leftarrow \overline{M}_k \overline{F}_{\mathrm{out}}$
4: $\quad$ Mettre $\overline{F}_{\mathrm{out}}$ sous la forme gen$\overline{PZX}$// voir preuve du théorème 4.33
5: **fin pour**
6: **retourner** $\overline{F}_{\mathrm{out}}$

Démonstration. Soit $\overline{F} = \overline{H}_a \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A$. On distingue trois cas selon les valeurs possibles de $\overline{M}$: $\overline{M} = \overline{H}_i$ (cas 1), $\overline{M} = \overline{P}_i$ (cas 2) et $\overline{M} = \overline{X}_{[i:j]}$ (cas 3). Seul le premier cas est trivial. Dans les autres cas, on distingue plusieurs sous cas selon les valeurs des vecteurs et matrices définissant $\overline{F}$ (les vecteurs a, d, b de $\mathbb{F}_2^n$ et les matrices B, D, A de dimensions $n \times n$).

`Cas 1 :` Si $\overline{M} = \overline{H}_i$ alors

$$\overline{H}_i \overline{F} = \overline{H}_{e_i} \overline{H}_a \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A.$$

Soit $\overline{F}_1 = \text{merge-H}(\overline{H}_{e_i}, \overline{H}_a \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A)$, alors

$$\overline{H}_i \overline{F} = \overline{F}_1$$

et $\overline{H}_i \overline{F}$ est en forme gen$\overline{PZX}$.

`Cas 2 :` Si $\overline{M} = \overline{P}_i$ alors

$$\overline{P}_i \overline{F} = \overline{P}_i \overline{H}_a \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A.$$

`Cas 2.1` : $a_i = 0$. Dans ce cas $\overline{P}_i$ et $\overline{H}_a$ commutent, donc

$$\overline{P}_i \overline{F} = \overline{H}_a \overline{P}_i \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A.$$

Soit $\overline{F}_1 = \text{merge-P}(\overline{P}_i, \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A)$, alors

$$\overline{P}_i \overline{F} = \overline{H}_a \overline{F}_1.$$

Comme $\overline{F}_1$ est en forme gen$\overline{PZX}_{\{a=0\}}$, alors $\overline{P}_i \overline{F}$ est en forme gen$\overline{PZX}$.

`Case 2.2` : $a_i = 1$. Dans ce cas $\overline{P}_i$ et $\overline{H}_a$ ne commutent pas et on a

$$\begin{aligned} \overline{P}_i \overline{F} &= \overline{H}_a (\overline{H}_a \overline{P}_i \overline{H}_a) \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A \\ &= \overline{H}_a \left(\overline{P}_i^{\Omega} \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A \right) \end{aligned}$$

Soit $\overline{F}_1 = \text{merge-P}\Omega 2(\overline{P}_i^{\Omega}, \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A)$, on a

$$\overline{P}_i \overline{F} = \overline{H}_a \overline{F}_1.$$

Soit $\overline{F}_2 = \text{merge-H}(\overline{H}_a, \overline{F}_1)$, on a alors

$$\overline{P}_i\overline{F} = \overline{F}_2$$

et $\overline{P}_i\overline{F}$ est en forme gen$\overline{PZX}$.

`Cas 3 :` Si $\overline{M} = \overline{X}_{[i:j]}$ alors

$$\begin{aligned}\overline{X}_{[i:j]}\overline{F} &= \overline{X}_{[i:j]}\overline{H}_a\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A \\ &= \overline{H}_a\left(\overline{H}_a\overline{X}_{[i:j]}\overline{H}_a\right)\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A \end{aligned} \tag{4.68}$$

On distingue quatre cas selon les valeurs de (a_i, a_j).

`Cas 3.1` : $(a_i, a_j) = (0, 0)$. Dans ce cas $\overline{H}_a\overline{X}_{[i:j]}\overline{H}_a = \overline{X}_{[i:j]}$ et l'égalité (4.68) s'écrit

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\left(\overline{X}_{[i:j]}\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A\right)$$

Soit $\overline{F}_1 = \text{merge-CX}(\overline{X}_{[i:j]}, \overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A)$, alors $\overline{F}_1$ est en forme gen$\overline{PZX}_{\{a=0\}}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{F}_1$$

donc $\overline{X}_{[i:j]}\overline{F}$ est en forme gen$\overline{PZX}$.

`Cas 3.2` : $(a_i, a_j) = (1, 1)$. Dans ce cas $\overline{H}_a\overline{X}_{[i:j]}\overline{H}_a = \overline{X}^{\Omega}_{[i:j]} \overset{(4.53)}{=} \overline{X}_{[j:i]}$ et l'égalité (4.68) s'écrit

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\left(\overline{X}_{[j:i]}\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A\right)$$

Soit $\overline{F}_1 = \text{merge-CX}(\overline{X}_{[j:i]}, \overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A)$, alors $\overline{F}_1$ est en forme gen$\overline{PZX}_{\{a=0\}}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{F}_1$$

donc $\overline{X}_{[i:j]}\overline{F}$ est en forme gen$\overline{PZX}$.

`Cas 3.3` : $(a_i, a_j) = (1, 0)$. Dans ce cas $\overline{H}_a\overline{X}_{[i:j]}\overline{H}_a = \overline{H}_i\overline{X}_{[i:j]}\overline{H}_i \overset{(4.55)}{=} \overline{Z}_{\{i,j\}}$. L'égalité (4.68) s'écrit alors

$$\begin{aligned}\overline{X}_{[i:j]}\overline{F} &= \overline{H}_a\overline{Z}_{\{i,j\}}\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A \\ &= \overline{H}_a\overline{P}_d\overline{Z}_{D\oplus\{\{i,j\}\}}\Omega\overline{P}_b\overline{Z}_B\overline{X}_A\end{aligned}$$

et $\overline{X}_{[i:j]}\overline{F}$ est en forme gen$\overline{PZX}$.

`Cas 3.4` : $(a_i, a_j) = (0, 1)$.

Dans ce cas $\overline{H}_a\overline{X}_{[i:j]}\overline{H}_a = \overline{H}_j\overline{X}_{[i:j]}\overline{H}_j \overset{(4.55)}{=} \overline{H}_j\overline{H}_i\overline{Z}_{\{i,j\}}\overline{H}_i\overline{H}_j = \overline{Z}^{\Omega}_{\{i,j\}}$ et l'égalité (4.68) s'écrit

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}_D\Omega\overline{P}_b\overline{Z}_B\overline{X}_A. \tag{4.69}$$

Nous distinguons alors deux sous-cas selon les valeurs de $D_{i,j}$, l'entrée (i, j) de la matrice D.

`Cas 3.4.1` : $D_{i,j} = 0$. Dans ce cas l'égalité (4.69) s'écrit

$$\begin{aligned}\overline{X}_{[i:j]}\overline{F} &= \overline{H}_a\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}}\right)\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_D\overline{Z}^{\Omega}_{\{i,j\}}\right)\Omega\overline{Z}_{\{i,j\}}\overline{P}_b\overline{Z}_B\overline{X}_A \\ &= \overline{H}_a\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}}\right)\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_D\overline{Z}^{\Omega}_{\{i,j\}}\right)\Omega\overline{P}_b\overline{Z}_{B\oplus\{\{i,j\}\}}\overline{X}_A\end{aligned} \tag{4.70}$$

Soit $D_i = \{\{p,q\} \in D \mid i \in \{p,q\}\}$ et $\Lambda_i = \{k \mid \{i,k\} \in D\}$. Comme $D_{i,j} = 0$ alors $D_i \cap D_j = \emptyset$, $j \notin \Lambda_i$ et $i \notin \Lambda_j$.

$$\begin{aligned}
\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_D\overline{Z}^{\Omega}_{\{i,j\}} &= \overline{Z}_{D\oplus D_i\oplus D_j}\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_{D_i}\overline{Z}_{D_j}\overline{Z}^{\Omega}_{\{i,j\}} \\
&= \overline{Z}_{D\oplus D_i\oplus D_j}\overline{Z}^{\Omega}_{\{i,j\}}\left(\prod_{k\in\Lambda_i}\overline{Z}_{\{i,k\}}\right)\left(\prod_{k\in\Lambda_j}\overline{Z}_{\{j,k\}}\right)\overline{Z}^{\Omega}_{\{i,j\}} \\
&\overset{(4.62)}{=} \overline{Z}_{D\oplus D_i\oplus D_j}\left(\prod_{k\in\Lambda_i}\overline{Z}_{\{i,k\}}\overline{X}_{[j:k]}\right)\left(\prod_{k\in\Lambda_j}\overline{Z}_{\{j,k\}}\overline{X}_{[i:k]}\right)
\end{aligned}$$

On applique alors l'algorithme $\overline{\texttt{C-to-PZX}}$ dans le cas particulier où les entrées ne contiennent pas de portes de phase (voir Remarque 4.25) : soit

$$\overline{Z}_{D'}\overline{X}_{A'} = \overline{\texttt{C-to-PZX}}\left(\left(\prod_{k\in\Lambda_i}\overline{Z}_{\{i,k\}}\overline{X}_{[j:k]}\right)\left(\prod_{k\in\Lambda_j}\overline{Z}_{\{j,k\}}\overline{X}_{[i:k]}\right), I_{2n}\right),$$

on a alors

$$\begin{aligned}
\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_D\overline{Z}^{\Omega}_{\{i,j\}} &= \overline{Z}_{D\oplus D_i\oplus D_j}\overline{Z}_{D'}\overline{X}_{A'} \\
&= \overline{Z}_{D''}\overline{X}_{A'}
\end{aligned}$$

avec $D'' = D \oplus D_i \oplus D_j \oplus D'$ et $A' = \left(\prod_{k\in\Lambda_i}[j:k]\right)\left(\prod_{k\in\Lambda_j}[i:k]\right)$. En reportant dans (4.70), on obtient

$$\begin{aligned}
\overline{X}_{[i:j]}\overline{F} &= \overline{H}_a\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}}\right)\overline{Z}_{D''}\overline{X}_{A'}\Omega\overline{P}_b\overline{Z}_{B\oplus\{\{i,j\}\}}\overline{X}_A \\
&\overset{(4.54)}{=} \overline{H}_a\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}}\right)\overline{Z}_{D''}\Omega\overline{X}_{(A'^{-1})^{\mathrm{t}}}\overline{P}_b\overline{Z}_{B\oplus\{\{i,j\}\}}\overline{X}_A
\end{aligned}$$

avec $(A'^{-1})^{\mathrm{t}} = \left(\prod_{k\in\Lambda_i}[k:j]\right)\left(\prod_{k\in\Lambda_j}[k:i]\right)$.
On utilise l'algorithme $\overline{\texttt{C-to-PZX}}$ avec en entrée $\overline{C} = \overline{X}_{(A'^{-1})^{\mathrm{t}}} = \left(\prod_{k\in\Lambda_i}\overline{X}_{[k:j]}\right)\left(\prod_{k\in\Lambda_j}\overline{X}_{[k:i]}\right)$ et $\overline{PZX}_{\mathrm{in}} = \overline{P}_b\overline{Z}_{B\oplus\{\{i,j\}\}}\overline{X}_A$: soit

$$\overline{P}_{b''}\overline{Z}_{B''}\overline{X}_{A''} = \overline{\texttt{C-to-PZX}}\left(\left(\prod_{k\in\Lambda_i}\overline{X}_{[k:j]}\right)\left(\prod_{k\in\Lambda_j}\overline{X}_{[k:i]}\right), \overline{P}_b\overline{Z}_{B\oplus\{\{i,j\}\}}\overline{X}_A\right),$$

on a alors

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}}\right)\overline{Z}_{D''}\Omega\overline{P}_{b''}\overline{Z}_{B''}\overline{X}_{A''} \tag{4.71}$$

Il reste alors à distinguer différents cas selon les valeurs du couple (d_i, d_j).

- Si $(d_i, d_j) = (0,0)$, alors $\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}} = \overline{P}_d$ et l'égalité (4.71) s'écrit

  $$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{P}_d\overline{Z}_{D''}\Omega\overline{P}_{b''}\overline{Z}_{B''}\overline{X}_{A''}$$

  donc $\overline{X}_{[i:j]}\overline{F}$ est en forme gen$\overline{PZX}$.

- Si $(d_i, d_j) = (0, 1)$ alors

$$\begin{aligned}\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}} &= \overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_j\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_{d\oplus e_j}\\ &\overset{(4.64)}{=} \overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{P}_j\overline{P}_{d\oplus e_j}\\ &= \overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{P}_d\end{aligned}$$

  et l'égalité (4.71) devient

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{P}^{\Omega}_i\left(\overline{X}_{[i:j]}\overline{P}_d\overline{Z}_{D''}\Omega\overline{P}_{b''}\overline{Z}_{B''}\overline{X}_{A''}\right).$$

  Soit $\overline{F}_1 = \text{merge-CX}(\overline{X}_{[i:j]}, \overline{P}_d\overline{Z}_{D''}\Omega\overline{P}_{b''}\overline{Z}_{B''}\overline{X}_{A''})$, alors $\overline{F}_1$ est en forme gen$\overline{PZX}_{\{a=0\}}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{P}^{\Omega}_i\overline{F}_1.$$

  Soit $\overline{F}_2 = \text{merge-P}\Omega 2(\overline{P}^{\Omega}_i, \overline{F}_1)$, alors $\overline{F}_2$ est en forme gen$\overline{PZX}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{F}_2.$$

  Soit $\overline{F}_3 = \text{merge-H}(\overline{H}_a, \overline{F}_2)$, alors $\overline{F}_3$ est en forme gen$\overline{PZX}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{F}_3.$$

- Si $(d_i, d_j) = (1, 0)$, on procède comme dans le cas précédent en échangeant i et j car $\overline{Z}_{\{i,j\}} = \overline{Z}_{\{j,i\}}$.

- Si $(d_i, d_j) = (1, 1)$ alors

$$\begin{aligned}\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}^{\Omega}_{\{i,j\}} &= \overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_j\overline{P}_{d\oplus e_i\oplus e_j}\overline{P}_i\overline{Z}^{\Omega}_{\{i,j\}}\\ &= \left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_j\overline{Z}^{\Omega}_{\{i,j\}}\right)\overline{P}_{d\oplus e_i\oplus e_j}\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_i\overline{Z}^{\Omega}_{\{i,j\}}\right)\\ &\overset{(4.64)}{=} \left(\overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{P}_j\right)\overline{P}_{d\oplus e_i\oplus e_j}\left(\overline{P}^{\Omega}_j\overline{X}_{[j:i]}\overline{P}_i\right)\\ &\overset{(4.57)}{=} \left(\overline{P}^{\Omega}_i\overline{X}_{[i:j]}\right)\overline{P}_j\overline{P}_{d\oplus e_i\oplus e_j}\overline{P}_i\left(\overline{P}^{\Omega}_j\overline{X}_{[j:i]}\right)\\ &= \left(\overline{P}^{\Omega}_i\overline{X}_{[i:j]}\right)\overline{P}_d\left(\overline{P}^{\Omega}_j\overline{X}_{[j:i]}\right)\end{aligned}$$

  et l'égalité (4.71) devient

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\left(\overline{P}^{\Omega}_i\overline{X}_{[i:j]}\right)\overline{P}_d\left(\overline{P}^{\Omega}_j\overline{X}_{[j:i]}\right)\overline{Z}_{D''}\Omega\overline{P}_{b''}\overline{Z}_{B''}\overline{X}_{A''}.$$

  Soit $\overline{F}_1 = \text{merge-CX}(\overline{X}_{[j:i]}, \overline{Z}_{D''}\Omega\overline{P}_{b''}\overline{Z}_{B''}\overline{X}_{A''})$, alors $\overline{F}_1$ est en forme gen$\overline{PZX}_{\{a=0,\ d=0\}}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{P}_d\overline{P}^{\Omega}_j\overline{F}_1.$$

  Soit $\overline{F}_2 = \text{merge-P}\Omega 1(\overline{P}^{\Omega}_j, \overline{F}_1)$, alors $\overline{F}_2$ est en forme gen$\overline{PZX}_{\{a=0\}}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{P}_d\overline{F}_2.$$

  Soit $\overline{F}_3 = \text{merge-P}(\overline{P}_d, \overline{F}_2)$, alors $\overline{F}_3$ est en forme gen$\overline{PZX}_{\{a=0\}}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{P}^{\Omega}_i\overline{X}_{[i:j]}\overline{F}_3.$$

Soit $\overline{F}_4 = \text{merge-CX}(\overline{X}_{[i:j]}, \overline{F}_3)$, alors $\overline{F}_4$ est en forme gen$\overline{PZX}_{\{a=0\}}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{P}_i^{\Omega}\overline{F}_4.$$

Soit $\overline{F}_5 = \text{merge-P}\Omega 2(\overline{P}_i^{\Omega}, \overline{F}_4)$, alors $\overline{F}_5$ est en forme gen$\overline{PZX}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_a\overline{F}_5.$$

Soit $\overline{F}_6 = \text{merge-H}(\overline{H}_a, \overline{F}_5)$, alors $\overline{F}_6$ est en forme gen$\overline{PZX}$ et on a

$$\overline{X}_{[i:j]}\overline{F} = \overline{F}_6.$$

`Cas 3.4.2` : $D_{i,j} = 1$. Soit $D' = D \oplus \{\{i,j\}\}$, alors $D'_{i,j} = 0$. On a $\overline{Z}_D = \overline{Z}_{\{i,j\}}\overline{Z}_{D'}$ et l'égalité (4.69) devient

$$\begin{aligned}
\overline{X}_{[i:j]}\overline{F} &= \overline{H}_a\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_{\{i,j\}}\overline{P}_d\overline{Z}_{D'}\Omega\overline{P}_b\overline{Z}_B\overline{X}_A \\
&= \overline{H}_a\left(\overline{Z}^{\Omega}_{\{i,j\}}\overline{Z}_{\{i,j\}}\overline{Z}^{\Omega}_{\{i,j\}}\right)\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}_{D'}\Omega\overline{P}_b\overline{Z}_B\overline{X}_A \\
&\overset{(4.63)}{=} \overline{H}_a\left(\overline{H}_i\overline{H}_j\overline{S}_{(i\ \ j)}\right)\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}_{D'}\Omega\overline{P}_b\overline{Z}_B\overline{X}_A \\
&= \overline{H}_{a\oplus e_i\oplus e_j}\overline{S}_{(i\ \ j)}\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_d\overline{Z}_{D'}\Omega\overline{P}_b\overline{Z}_B\overline{X}_A
\end{aligned}$$

On utilise les formules de conjugaison par une matrice $\overline{S}_{(i\ \ j)}$ (équations (4.58) et (4.59)) pour obtenir

$$\overline{X}_{[i:j]}\overline{F} = \overline{H}_{a\oplus e_i\oplus e_j}\overline{Z}^{\Omega}_{\{i,j\}}\overline{P}_{(i\ \ j)d}\overline{Z}_{(i\ \ j)D'(i\ \ j)}\Omega\overline{P}_{(i\ \ j)b}\overline{Z}_{(i\ \ j)B(i\ \ j)}\overline{X}_{(i\ \ j)A} \tag{4.72}$$

Soit $D'' = (i\ \ j)D'(i\ \ j)$, alors $D''_{i,j} = 0$ (car $D'_{i,j} = 0$) et on remarque que l'égalité (4.72) a la même forme que l'égalité (4.69). On peut donc procéder comme dans le cas 3.4.1 pour mettre $\overline{X}_{[i:j]}\overline{F}$ en forme gen$\overline{PZX}$.

Dans chacun des cas décrits ci-dessus, le nombre d'opérations nécessaires pour mettre $\overline{M}\ \overline{F}$ en forme gen$\overline{PZX}$ est dominé par le coût d'utilisation des algorithmes merge-*, qui vaut tout au plus $O(n^2)$, et de l'algorithme $\overline{\texttt{C}}$`-to-`$\overline{\texttt{PZX}}$ dont la complexité est $O(\ell n)$, avec ℓ désignant le nombre de matrices M_k dans le produit de matrices symplectiques en entrée (voir algorithme 4.1). L'algorithme $\overline{\texttt{C}}$`-to-`$\overline{\texttt{PZX}}$ est utilisé dans le cas 3.4.1 sur des produits de matrices comportant $O(n)$ facteurs donc dans ce cas son coût d'utilisation est $O(n^2)$. On voit donc que le nombre d'opérations nécessaires pour écrire $\overline{MF}$ en forme gen$\overline{PZX}$ est $O(n^2)$. □

Du théorème 4.33, on déduit les corollaires suivants.

Corollaire 4.34. *La complexité de l'algorithme* $\overline{\texttt{C}}$`-to-gen`$\overline{\texttt{PZX}}$ *est* $O(\ell n^2)$.

Corollaire 4.35. *Soit* $\overline{C}$ *un élément de* $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ *donné par un produit* $\overline{C} = \prod_{k=1}^{\ell}\overline{M}_k$ *avec* $\overline{M}_k \in \overline{\mathrm{Cliff}}_n$, *on peut mettre* $\overline{C}$ *sous la forme* gen$\overline{PZX}$ *en temps* $O(\ell n^2)$.

Démonstration. On applique l'algorithme $\overline{\texttt{C}}$`-to-gen`$\overline{\texttt{PZX}}$ avec en entrée $\overline{C} = \prod_{k=1}^{\ell}\overline{M}_k$ et $\overline{F}_{\text{in}} = I_{2n}$. □

4.3.3 Mise en forme $\overline{PZX}$ généralisée d'une matrice symplectique quelconque

Pour mettre en forme $\overline{PZX}$ généralisée une matrice symplectique quelconque, on commence par l'écrire sous la forme $\left(\prod_{k=1}^{\ell} \overline{M}_k\right) \overline{F}$ où $\overline{F}$ est en forme $\overline{PZX}$ et $\overline{M}_k \in \overline{\mathrm{Cliff}}_n$, puis on applique l'algorithme `C-to-gen`$\overline{\texttt{PZX}}$.

Lemme 4.36. *Soit $W \in \mathrm{Sp}_{2n}(\mathbb{F}_2)$ et soient M, N, Q, R des matrices de dimensions $n \times n$ telles que $W = \begin{bmatrix} M & N \\ Q & R \end{bmatrix}$. Soient k et j deux entiers tels que $0 \leqslant k \leqslant n-1$ et $2 \leqslant j \leqslant n$. Supposons que les colonnes $0, \ldots, j-2$ de la matrice N sont nulles et que la colonne $j-1$ de N soit le vecteur e_k. Alors la ligne k de la matrice R a ses $j-1$ premiers éléments nuls : $R_{k,0} = \cdots = R_{k,j-2} = 0$.*

Démonstration. La ligne $j-1$ de $N^{\mathrm{t}}R$ est égale à la ligne k de R. Soit $[c_0, \ldots, c_{n-1}]^{\mathrm{t}}$ la colonne $j-1$ de $N^{\mathrm{t}}R$. Comme les lignes $0, \ldots, j-2$ de la matrice N^{t} sont nulles, alors $c_0 = \cdots = c_{j-2} = 0$. La matrice W étant symplectique, $N^{\mathrm{t}}R$ est une matrice symétrique (voir proposition 4.12) donc $R_{k,0} = c_0, \ldots, R_{k,j-2} = c_{j-2}$. Ainsi la ligne k de la matrice R a ses $j-1$ premiers éléments nuls. □

Proposition 4.37. *Toute matrice symplectique W peut s'écrire en temps $O(n^3)$ sous la forme*

$$W = \left(\prod_{k=1}^{\ell} \overline{M}_k\right) \begin{bmatrix} M & 0 \\ Q & R \end{bmatrix} \tag{4.73}$$

où ℓ est un entier inférieur à $n(n+1)$, $\overline{M}_k \in \overline{\mathrm{Cliff}}_n$, M, Q, R sont des matrices de dimensions $n \times n$, et 0 est la matrice nulle.

Démonstration. Soit W une matrice symplectique, on construit une suite de matrices symplectiques $W_0 = \begin{bmatrix} M_0 & N_0 \\ Q_0 & R_0 \end{bmatrix}, \ldots, W_n = \begin{bmatrix} M_n & N_n \\ Q_n & R_n \end{bmatrix}$ de la manière suivante. On pose $W_0 = W$ et pour tout $j = 0, \ldots, n-1$, on obtient W_{j+1} à partir de W_j par les opérations suivantes. Soit $W_j = \begin{bmatrix} M_j & N_j \\ Q_j & R_j \end{bmatrix}$, on considère la colonne j de la matrice N_j et l'ensemble Λ_j des entiers i tels que l'entrée (i, j) de la matrice N_j soit égale à 1. On distingue 3 cas selon le cardinal de $|\Lambda_j|$.

- Si $|\Lambda_j| = 0$, on pose $W_{j+1} = W_j$.
- Si $|\Lambda_j| = 1$, soit k l'unique élément de Λ_j, alors la colonne j de la matrice N_j est le vecteur e_k. On distingue alors deux sous-cas.
  - Si l'entrée (k, j) de la matrice R_j vaut 0, on échange les lignes k et $k+n$ de la matrice W_j, ce qui revient à multiplier W_j à gauche par la matrice $\overline{H}_k$ (voir proposition 4.19). Posons $W_{j+1} = \overline{H}_k W_j = \begin{bmatrix} M_{j+1} & N_{j+1} \\ Q_{j+1} & R_{j+1} \end{bmatrix}$, alors la colonne j de la matrice N_{j+1} est le vecteur nul.
  - Si l'entrée (k, j) de la matrice R_j vaut 1, on ajoute la ligne k de W_j à la ligne $k+n$ de W_j, ce qui revient à multiplier W_j à gauche par la matrice $\overline{P}_k$ (voir proposition 4.19). Posons $W'_j = \overline{P}_k W_j = \begin{bmatrix} M'_j & N'_j \\ Q'_j & R'_j \end{bmatrix}$, alors l'entrée

(k,j) de la matrice R'_j vaut 0. On échange alors les lignes k et $k+n$ de la matrice W'_j, ce qui revient à multiplier W'_j à gauche par la matrice $\overline{H}_k$. Posons $W_{j+1} = \overline{H}_k W'_j = \overline{H}_k \overline{P}_k W_j = \begin{bmatrix} M_{j+1} & N_{j+1} \\ Q_{j+1} & R_{j+1} \end{bmatrix}$, alors la colonne j de la matrice N_{j+1} est le vecteur nul.

- Si $|\Lambda_j| \geqslant 2$, on commence par choisir au hasard un élément de Λ_j : soit k cet élément, alors l'entrée (k,j) de la matrice N_j vaut 1 et nous utilisons cette entrée comme pivot afin de mettre à 0 les autres entrées non nulles de la colonne j de N_j. Posons $W'_j = \left(\prod_{i\in\Lambda_j, i\neq k} \overline{X}_{[i:k]}\right) W_j$ et $W'_j = \begin{bmatrix} M'_j & N'_j \\ Q'_j & R'_j \end{bmatrix}$, alors, d'après la proposition 4.19, la colonne j de N'_j est le vecteur e_k. On procède alors comme dans le cas où $|\Lambda_j| = 1$ pour construire W_{j+1} à partir de W'_j. On obtient ainsi une matrice W_{j+1} telle que la colonne j de la matrice N_{j+1} est le vecteur nul.

En utilisant le lemme 4.36, on démontre par récurrence que, pour tout $j = 1, \ldots, n$, la sous-matrice N_j de W_j a ses colonnes $0, \ldots, j-1$ qui sont nulles. Ainsi $W_n = \begin{bmatrix} M_n & 0 \\ Q_n & R_n \end{bmatrix}$. A la fin du processus on a donc

$$\begin{bmatrix} M_n & 0 \\ Q_n & R_n \end{bmatrix} = \Pi_{n-1} \ldots \Pi_0 W$$

où, pour tout $j = 0, \ldots, n-1$, le symbole Π_j désigne un produit d'au plus $n+1$ matrices symplectiques de Clifford choisies à l'étape j du processus. Ainsi on a :

$$W = (\Pi_0)^{-1} \ldots (\Pi_{n-1})^{-1} \begin{bmatrix} M_n & 0 \\ Q_n & R_n \end{bmatrix}.$$

Les matrices symplectiques de Clifford étant leur propre inverse, W s'écrit bien sous la forme (4.73).

Le nombre d'opérations (additions dans $\mathbb{F}_2$) nécessaires pour mettre W sous la forme (4.73) est $O(n^3)$ car le nombre maximal de facteurs de l'ensemble $\overline{\mathrm{Cliff}}_n$ présents dans le produit $(\Pi_0)^{-1} \ldots (\Pi_{n-1})^{-1}$ est $n(n+1)$ et chaque facteur a un coût de $O(n)$ opérations (additions ou échange de lignes d'une matrice symplectique). □

Corollaire 4.38. *Les matrices symplectiques de Clifford engendrent le groupe symplectique* $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ *:*

$$\mathrm{Sp}_{2n}(\mathbb{F}_2) = \langle \overline{\mathrm{Cliff}}_n \rangle. \tag{4.74}$$

Le morphisme $\overline{\Phi}$ *(voir définition 4.16) est surjectif :*

$$\mathrm{Sp}_{2n}(\mathbb{F}_2) = \overline{\Phi}(\mathrm{Stab}_n). \tag{4.75}$$

Démonstration. Soit W une matrice symplectique, en utilisant la proposition 4.37 on écrit W sous la forme

$$W = \left(\prod_{k=1}^{\ell} \overline{M}_k\right) \begin{bmatrix} M & 0 \\ Q & R \end{bmatrix}$$

et par la proposition 4.20, la matrice $\begin{bmatrix} M & 0 \\ Q & R \end{bmatrix}$ appartient au groupe $\langle \overline{P}, \overline{CZ}, \overline{CNOT} \rangle_n$ qui est inclus dans $\langle \overline{\mathrm{Cliff}}_n \rangle$ puisque $\overline{Z}_{\{i,j\}} = \overline{H}_i \overline{X}_{[i:j]} \overline{H}_i$ (4.55). □

Théorème 4.39. *Toute matrice symplectique peut s'écrire en forme* gen$\overline{PZX}$ *en temps* $O(n^4)$.

Démonstration. Soit W une matrice symplectique, en utilisant la proposition 4.37 on écrit W sous la forme

$$W = \left(\prod_{k=1}^{\ell} \overline{M}_k\right) \begin{bmatrix} M & 0 \\ Q & R \end{bmatrix}$$

puis par la proposition 4.22, on écrit $\begin{bmatrix} M & 0 \\ Q & R \end{bmatrix}$ sous la forme $\overline{PZX}$ qui est un cas particulier de la forme gen$\overline{PZX}$. On utilise ensuite l'algorithme `C-to-genPZX` dont la complexité est $O(\ell n^2)$, avec ici $\ell \leqslant n(n+1)$. □

4.4 La forme PZX généralisée dans le groupe de Clifford

Définition 4.40. On dit qu'un élément C du groupe de Clifford $\mathcal{C}_n$ est en forme genPZX (forme PZX généralisée) quand il est écrit sous la forme

$$H_a Z_u P_d Z_D H_\omega Z_v P_b Z_B X_A, \tag{4.76}$$

avec $a, u, d, v, b \in \mathbb{F}_2^n$, $D, B \in \mathcal{B}_0^n$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$.

Soit C un produit de portes de Clifford. On peut utiliser le morphisme $\overline{\Phi}$ (définition 4.16) et la forme gen$\overline{PZX}$ de $\overline{\Phi}(C)$ pour mettre C en forme genPZX.

Théorème 4.41. *Soit* $C \in \mathrm{Stab}_n$, *donné sous la forme d'un produit de portes de Clifford :* $C = \prod_{k=1}^{\ell} M_k$ *avec* $M_k \in \mathrm{Cliff}_n$. *À une phase près, on peut mettre* C *en forme* genPZX *en temps* $O(\ell n^2 + n^3)$ *: il existe un réel* φ *et un élément* C' *du groupe de Clifford en forme* genPZX *tels que* $C = \mathrm{e}^{\mathrm{i}\varphi} C'$.

Démonstration. Soit $C = \prod_{k=1}^{\ell} M_k$ et $\overline{C} = \overline{\Phi}(C) = \prod_{k=1}^{\ell} \overline{M}_k$. On écrit $\overline{C}$ en forme gen$\overline{PZX}$ par l'algorithme `C-to-genPZX` (algorithme 4.2) dont le coût en temps est $O(\ell n^2)$. Soit $\overline{C} = \overline{H}_a \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A$, on pose $C_1 = H_a P_d Z_D H_\omega P_b Z_B X_A$, alors $\overline{\Phi}(C_1) = \overline{C} = \overline{\Phi}(C)$, donc les éléments C et C_1 sont égaux, à un élément du groupe $\mathrm{Ker}(\overline{\Phi})$ près. Ainsi $C = C_1 E$, avec $E \in \mathrm{Ker}(\overline{\Phi})$. Or $\mathrm{Ker}(\overline{\Phi}) = \{\mathrm{e}^{\mathrm{i}\varphi} X_u Z_v \mid \varphi \in \mathbb{R},\ u, v \in \mathbb{F}_2^n\}$ (proposition 4.17) donc $\mathrm{Ker}(\overline{\Phi})$ est stable par conjugaison par les éléments de $\mathcal{C}_n$ et en particulier par $P_b Z_B X_A$. On en déduit qu'il existe deux vecteurs $u, v \in \mathbb{F}_2^n$ et un réel φ tels que

$$C = \mathrm{e}^{\mathrm{i}\varphi} H_a P_d Z_D H_\omega X_u Z_v P_b Z_B X_A. \tag{4.77}$$

Il reste alors à déterminer u et v. De l'égalité (4.77), on tire

$$\mathrm{e}^{\mathrm{i}\varphi} X_u Z_v = H_\omega Z_D P_d^3 H_a (\prod_{k=1}^{\ell} M_k) X_{A^{-1}} Z_B P_b^3.$$

On calcule alors l'action de $C_2 = H_\omega Z_D P_d^3 H_a (\prod_{k=1}^{\ell} M_k) X_{A^{-1}} Z_B P_b^3$ par conjugaison sur les X_i, Z_i (pour $i = 0, \ldots, n-1$) en utilisant les règles de calcul données dans la proposition 4.7. A cette fin, on commence par décomposer la matrice $A \in \mathrm{GL}_n(\mathbb{F}_2)$ en produit de transvections par l'algorithme de Patel-Markov-Hayes [154] dont le coût est $O(n^3/\ln n)$ et on déduit une décomposition de A^{-1} en produit de transvections, donc une décomposition de $X_{A^{-1}}$ en produit de portes $X_{[i:j]}$. La décomposition des

autres matrices présentes dans le produit définissant C_2 en produit de portes de Clifford est triviale. On obtient ainsi une décomposition de C_2 en produit d'éléments de Cliff_n en temps $O(n^3/\ln)$. Le nombre de portes de Cliff_n présentes dans ce produit est $O(\ell + n^2)$ et comme la conjugaison d'un élément de $\mathcal{E}_n$ par une porte de Clifford se fait en temps constant (voir les formules (4.9), (4.10), (4.11)), on en déduit que le coût algorithmique de la conjugaison par C_2 d'une porte de Pauli X_i ou Z_i est $O(\ell + n^2)$. Ainsi, on voit que le coût total en temps pour les $2n$ portes de Pauli X_i et Z_i est $O(n\ell + n^3)$. Une fois effectués ces $2n$ calculs, on détermine les vecteurs u et v en remarquant que, pour tout i, on a : $C_2 X_i C_2^{-1} = (X_u Z_v) X_i (X_u Z_v)^{-1} = (-1)^{v_i} X_i$ et $C_2 Z_i C_2^{-1} = (X_u Z_v) Z_i (X_u Z_v)^{-1} = (-1)^{u_i} Z_i$.

Partant de l'égalité (4.77), on obtient $C = \mathrm{e}^{\mathrm{i}\varphi} H_a P_d Z_D Z_u H_\omega Z_v P_b Z_B X_A$ en observant que $H_\omega X_u H_\omega = Z_u$. Finalement, puisque les matrices $P_d Z_D$ et Z_u commutent (ce sont des matrices diagonales), on a $C = \mathrm{e}^{\mathrm{i}\varphi} H_a Z_u P_d Z_D H_\omega Z_v P_b Z_B X_A$, qui est la forme souhaitée. Le coût total en temps pour mettre C sous cette forme est la somme du coût de l'utilisation de l'algorithme $\overline{\texttt{C-to-genPZX}}$ et du coût de calcul des vecteurs u et v, soit au final $O(\ell n^2 + n^3)$. Notez que la valeur de φ reste inconnue. □

Remarque 4.42. Le théorème 4.41 permet de retrouver un théorème de Van den Nest [174, théorème 1] qui s'énonce ainsi : tout état stabilisateur (définition 4.10) peut s'écrire comme un état de graphe (définition 3.18) à un produit de portes de Clifford locales près (les portes $\{P_i, H_i \mid i = 0, \ldots, n-1\}$). En effet, soit $C\,|0\rangle^{\otimes n}$ un état stabilisateur, avec $C \in \mathrm{Stab}_n$. En mettant C en forme genPZX on a :

$$\begin{aligned} C\,|0\rangle^{\otimes n} &= H_a Z_u P_d Z_D H_\omega Z_v P_b Z_B X_A\,|0\rangle^{\otimes n} \\ &= (H_a Z_u P_d) Z_D H_\omega\,|0\rangle^{\otimes n}\,. \end{aligned}$$

Le théorème 4.3 montre qu'un élément du groupe unitaire U_{2^n} est déterminé, à une phase près, par son action sur le groupe de Pauli $\mathcal{E}_n$. Dans le cas particulier d'une matrice C du groupe de Clifford $\mathcal{C}_n$, cette action est définie par la donnée, pour tout générateur $G \in \{X_i, Z_i \mid i = 0, \ldots, n-1\}$ du groupe de Pauli, de deux vecteurs u, v de $\mathbb{F}_2^n$ et d'un scalaire $\lambda \in \{\pm 1, \pm \mathrm{i}\}$ tel que $CGC^{-1} = \lambda X_u Z_v$. Autrement dit, la connaissance de la matrice symplectique associée à $C \in \mathcal{C}_n$ par le morphisme $\overline{\Phi}$ (définition 4.16), ainsi que la donnée supplémentaire de $2n$ scalaires de l'ensemble $\{\pm 1, \pm \mathrm{i}\}$ déterminent une matrice de Clifford C à une phase près. Le nombre de bits qui déterminent C à une phase près est donc égal à $2n \times (2n+2) = 4n^2 + 4n$. On peut alors se demander si ces informations permettent à elles seules de donner une expression de C en fonction des matrices de Cliff_n, à savoir les matrices P_i, H_i et $X_{[i:j]}$.

Dans sa thèse [86, section 5.8], Gottesman donne une réponse positive à cette question et fournit un algorithme (décrit également dans [148, exercice 10.40]) permettant de construire un circuit stabilisateur (voir définition 4.8) composé de $O(n^2)$ portes de Clifford dont l'action est équivalente à celle de C à une phase près. Les méthodes que nous venons de développer (théorèmes 4.39 et 4.41) nous permettent également de proposer une réponse à cette question. C'est l'objet du théorème qui suit.

Théorème 4.43. *Soit $C \in \mathcal{C}_n$, donné par son action sur le groupe de Pauli $\mathcal{E}_n$. A une phase près, on peut mettre C en forme* genPZX *en temps $O(n^4)$.*

Démonstration. Soit $C \in \mathcal{C}_n$. Par hypothèse, on connaît la matrice symplectique $\overline{\Phi}(C)$ et on pose, pour tout $i = 0, \ldots, 2n-1$: $\mathrm{col}_i(\overline{\Phi}(C)) = \begin{bmatrix} a^{(i)} \\ b^{(i)} \end{bmatrix}$ avec $a^{(i)}, b^{(i)} \in \mathbb{F}_2^n$.

On connaît également également $2n$ scalaires $\lambda_0, \ldots, \lambda_{n-1}, \lambda'_0, \ldots, \lambda'_{n-1}$ dans $\{\pm 1, \pm \mathrm{i}\}$ tels que, pour tout $i = 0, \ldots, n-1$, on a : $CX_iC^{-1} = \lambda_i X_{a^{(i)}} Z_{b^{(i)}}$ et $CZ_iC^{-1} = \lambda'_i X_{a^{(i+n)}} Z_{b^{(i+n)}}$. On a donc

$$CX_uZ_vC^{-1} = \prod_i \lambda_i^{u_i} \lambda_i'^{v_i} X_{u'} Z_{v'}, \tag{4.78}$$

avec $\begin{bmatrix} u' \\ v' \end{bmatrix} = \overline{\Phi}(C) \begin{bmatrix} u \\ v \end{bmatrix}$.

On commence par mettre $\overline{C}$ en forme gen$\overline{PZX}$ en temps $O(n^4)$ en utilisant le théorème 4.39 et on pose : $\overline{C} = \overline{H}_a \overline{P}_d \overline{Z}_D \Omega \overline{P}_b \overline{Z}_B \overline{X}_A$. On procède alors comme dans la preuve du théorème 4.41 : soit $C_1 = H_a P_d Z_D H_\omega P_b Z_B X_A$, alors $\overline{\Phi}(C_1) = \overline{C} = \overline{\Phi}(C)$ donc il existe deux vecteurs $u, v \in \mathbb{F}_2^n$ et un réel φ tels que

$$C = \mathrm{e}^{\mathrm{i}\varphi} H_a P_d Z_D H_\omega X_u Z_v P_b Z_B X_A.$$

On a donc $\mathrm{e}^{\mathrm{i}\varphi} X_u Z_v = (H_\omega Z_D P_d^3 H_a) C (X_{A^{-1}} Z_B P_b^3)$ et il reste à déterminer u et v. A cette fin, on calcule l'action de

$$C_2 = (H_\omega Z_D P_d^3 H_a) C (X_{A^{-1}} Z_B P_b^3)$$

par conjugaison sur les X_i, Z_i (pour $i = 1, \ldots, n$) en procédant de façon similaire à la méthode utilisée dans la preuve du théorème 4.41 et en utilisant l'identité (4.78). Une fois effectués ces $2n$ calculs, on détermine les vecteurs u et v en remarquant que, pour tout i, on a : $C_2 X_i C_2^{-1} = (X_u Z_v) X_i (X_u Z_v)^{-1} = (-1)^{v_i} X_i$ et $C_2 Z_i C_2^{-1} = (X_u Z_v) Z_i (X_u Z_v)^{-1} = (-1)^{u_i} Z_i$.

Le coût en temps de ces différentes opérations est dominé par la mise en forme gen$\overline{PZX}$ de $\overline{C}$ dont la complexité est $O(n^4)$. □

4.5 Conclusion et perspectives

L'équation (4.76) montre qu'un opérateur unitaire en forme genPZX peut s'implanter comme un circuit quantique ayant la forme :

$$\textit{-CNOT-CZ-P-Z-H-CZ-P-Z-H-} \tag{4.79}$$

où P désigne un sous-circuit de portes de phase ne comportant tout au plus qu'une porte de phase par qubit, c'est à dire un sous-circuit de profondeur 1, que nous appelons *couche* par commodité. On peut comparer cette forme avec les formes déjà existantes (listées dans la section 4.1.4) que nous récapitulons ci-dessous :

-H-CNOT-P-CNOT-P-CNOT-H-P-CNOT-P-CNOT- Gottesman et Aaronson, 2004 [1] (4.80)

-CNOT-CZ-P-H-P-CZ-CNOT- Maslov et Roetteler, 2018 [139] (4.81)

-X-Z-P-CNOT-CZ-H-CZ-H-P- Bravyi et Maslov, 2020 [36] (4.82)

-H-P-CZ-CNOT-H-CZ-P-H- Duncan *et al.*, 2020 [73] (4.83)

Dans cette liste, nous considérons que les deux dernières formes (4.82) et (4.83) sont les meilleures en terme de nombre de portes binaires utilisées car elles ne contiennent qu'un seul sous-circuit de portes *CNOT* et deux sous-circuits de portes *CZ*, ce qui est aussi le cas de la forme (4.79) que nous proposons.

Dans la forme (4.82) le dernier sous-circuit de portes de phase P peut contenir jusqu'à trois portes P par qubit et peut donc s'écrire -*Z*-*P*- où P représente une seule couche de portes de phase. Il en est de même pour les deux sous-circuits de portes de phase dans la forme (4.83). On peut donc réécrire les deux circuits (4.82) et (4.83) :

-*X*-*Z*-*P*-*CNOT*-*CZ*-*H*-*CZ*-*H*-*Z*-*P*-	Bravyi et Maslov, 2020
-*H*-*Z*-*P*-*CZ*-*CNOT*-*H*-*CZ*-*Z*-*P*-*H*-	Duncan *et al.*, 2020

où -*P*- désigne maintenant une seule couche de portes P. Avec cette réécriture, on voit maintenant que le nombre de couches de portes agissant sur 1 qubit est égal à 7 dans ces deux circuits alors qu'il n'est que de 6 dans la forme (4.79). En ce sens, on peut considérer que la forme (4.79) constitue une légère simplification par rapport aux formes (4.82) et (4.82). Cependant, il ne s'agit pas d'une amélioration sensible.

Dans un article de 2018, Calderbank *et al.* [161, théorème 23] montrent que toute matrice $W \in \mathrm{Sp}_{2n}(\mathbb{F}_2)$ peut s'écrire sous la forme :

$$W = \begin{bmatrix} A_1 & 0 \\ 0 & (A_1^{-1})^{\mathrm{t}} \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} I & B_1 \\ 0 & I \end{bmatrix} \begin{bmatrix} L_{n-k} & U_k \\ U_k & L_{n-k} \end{bmatrix} \begin{bmatrix} I & B_2 \\ 0 & I \end{bmatrix} \begin{bmatrix} A_2 & 0 \\ 0 & (A_2^{-1})^{\mathrm{t}} \end{bmatrix}, \quad (4.84)$$

avec $U_k = \mathrm{diag}(I_k, 0_{n-k})$ et $L_{n-k} = \mathrm{diag}(0_k, I_{n-k})$, $A_1, A_2 \in \mathrm{GL}_n(\mathbb{F}_2)$ et $B_1, B_2 \in \mathcal{B}_n$. Cette décomposition est utilisée dans le cadre du calcul quantique résistant aux erreurs afin de déterminer comment implanter les opérateurs de Clifford sur les qubits d'un code donné [161, section II.E] (voir aussi [148, chapitre 10] pour une introduction aux codes correcteurs d'erreurs).

La forme gen$\overline{PZX}$ d'une matrice $W \in \mathrm{Sp}_{2n}(\mathbb{F}_2)$ est donnée par l'équation (4.49) que nous rappelons :

$$W = \begin{bmatrix} \mathrm{diag}(a \oplus \omega) & \mathrm{diag}(a) \\ \mathrm{diag}(a) & \mathrm{diag}(a \oplus \omega) \end{bmatrix} \begin{bmatrix} I & 0 \\ D' & I \end{bmatrix} \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} \begin{bmatrix} I & 0 \\ B' & I \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & (A^{-1})^{\mathrm{t}} \end{bmatrix}. \quad (4.85)$$

avec $D', B' \in \mathcal{B}_n$ et $A \in \mathrm{GL}_n(\mathbb{F}_2)$. On peut se demander si cette nouvelle décomposition dans $\mathrm{Sp}_{2n}(\mathbb{F}_2)$, qui est similaire à (4.84) mais plus simple (une seule matrice $\overline{X}_A$), pourrait ou non permettre une implantation plus économique (moins de portes quantiques) des opérateurs de Clifford dans l'espace de Hilbert des qubits encodés. Nous reviendrons sur cette question dans de prochaines recherches.

Chapitre 5

Émergence de l'intrication dans les circuits composés de portes *CZ* et *CNOT*

Le rôle de l'intrication comme ressource fondamentale en information quantique a été souligné dans le chapitre introductif de cette thèse (chapitre 1, section 1.2.2). Dans ce dernier chapitre, nous proposons quelques constructions d'état quantiques intriqués possédant des propriétés intéressantes du point de vue de l'information quantique. Nous montrons qu'un circuit de portes *CZ* ou de portes *CNOT* prenant en entrée un état complètement factorisé peut produire des états intriqués remarquables. Cette étude concerne essentiellement les petites dimensions ($n \leqslant 5$) et même dans ce cas, il ne s'agit pas d'une étude exhaustive mais plus modestement de quelques exemples illustrant l'intérêt de ces circuits comme moyen pratique de générer de l'intrication. La plupart des résultats de ce dernier chapitre sont tirés de [19], [18] et [17]. Dans la suite de cette introduction, nous présentons sommairement les outils mathématiques que nous avons utilisés pour décrire et classifier les états intriqués.

Une grande partie du travail des physiciens et des mathématiciens à propos de l'intrication est d'établir une classification des états intriqués afin de mieux comprendre ce phénomène non classique. Dans ce chapitre nous nous basons sur la classification SLOCC des états intriqués déjà définie au chapitre 1 : les états sont classés dans l'espace de Hilbert $\mathcal{H}^{\otimes n}$ d'après leur orbite sous l'action du groupe $\mathrm{G}_{\mathrm{SLOCC}} = \mathrm{GL}_2(\mathbb{C})^n$, ou bien dans l'espace projectif $\mathbb{P}(\mathcal{H}^{\otimes n})$ sous l'action de $\mathrm{G}'_{\mathrm{SLOCC}} = \mathrm{SL}_2(\mathbb{C})^n$.

Afin d'établir cette classification on peut s'appuyer sur la théorie classique des invariants dont l'origine date du milieu du 19$^{\mathrm{e}}$ siècle avec les travaux fondateurs de Boole [31] et Cayley [49] (voir à ce propos l'introduction du chapitre 2 de [132]). C'est Klyachko [116] qui, le premier, a eu l'idée d'appliquer cette théorie à la description de l'intrication d'un système quantique. Le principe général de cette méthode est de classifier les formes binaires multilinéaires en évaluant certains polynômes qui sont invariants ou covariants sous l'action du groupe $\mathrm{G}_{\mathrm{SLOCC}}$. En effet on peut associer à toute forme binaire multilinéaire

$$A = \sum_{0 \leqslant b_0, \ldots, b_{n-1} \leqslant 1} \alpha_{b_0 \ldots b_{n-1}} x_{b_0}^{(0)} \cdots x_{b_{n-1}}^{(n-1)}, \tag{5.1}$$

un état quantique $|\psi\rangle$ de l'espace $\mathcal{H}^{\otimes n}$ défini par

$$|\psi\rangle = \sum_{0 \leqslant b_0,\ldots,b_{n-1} \leqslant 1} \alpha_{b_0 \ldots b_{n-1}} |b_0 \cdots b_{n-1}\rangle , \tag{5.2}$$

et réciproquement.

Un invariant est un polynôme en les 2^n variables $\alpha_{b_0 \ldots b_{n-1}}$, noté $P(A)$, qui est un invariant relatif par l'action du groupe $\mathrm{G_{SLOCC}}$, c'est à dire tel que, pour tout $g = (g_0, \ldots, g_{n-1})$ dans $\mathrm{G_{SLOCC}}$, on ait :

$$P(g.A) = \det(g_0)^{w_0} \times \cdots \times \det(g_{n-1})^{w_{n-1}} P(A), \tag{5.3}$$

où $g.A$ désigne la forme associée à l'état $(g_0 \otimes \cdots \otimes g_{n-1}) |\psi\rangle$ et où les w_i sont des entiers qui ne dépendent que de $P(A)$.

Un covariant est un polynôme en les variables $\alpha_{b_0,\ldots,b_{n-1}}$ et en les variables auxiliaires $\mathbf{x}^{(i)} = (x_0^{(i)}, x_1^{(i)})$ (avec $i = 0 \ldots n-1$), noté $P(A; \mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(n-1)})$, qui est un invariant relatif par l'action simultanée du groupe $\mathrm{G_{SLOCC}}$ sur A et sur les vecteurs $\mathbf{x}^{(i)}$. Cette action est définie pour tout $g = (g_0, \ldots, g_{n-1})$ dans $\mathrm{G_{SLOCC}}$ par

$$g.P(A; \mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(n-1)}) = P(g.A; g_0^{-1}\mathbf{x}^{(0)}, \ldots, g_{n-1}^{-1}\mathbf{x}^{(n-1)}). \tag{5.4}$$

Ainsi P est covariant si et seulement si

$$P(g.A; g_0^{-1}\mathbf{x}^{(0)}, \ldots, g_{n-1}^{-1}\mathbf{x}^{(n-1)}) = \det(g_0)^{w_0} \times \cdots \times \det(g_{n-1})^{w_{n-1}} P(A; \mathbf{x}^{(0)}, \ldots, \mathbf{x}^{(n-1)}) \tag{5.5}$$

On voit donc que les polynômes invariants sont des polynômes covariants particuliers dans lesquels les degrés des variables $\mathbf{x}^{(i)}$ sont nuls.

La forme A est le premier polynôme covariant et les générateurs de l'algèbre des covariants peuvent être obtenus en théorie par un algorithme dû à Cayley qui est basé sur des opérations de transvections entre polynômes. Cependant cet algorithme n'est utilisable dans la pratique que jusqu'à 4 qubits en raison du nombre de générateurs qui devient trop important (voir [132, chapitre 2]). En annexe C, on explique comment calculer quelques générateurs dans le cas $n = 4$. Cette approche a été mise en oeuvre par Luque, Thibon et Briand [37, 133, 132] puis par Luque et Holweck [100, 101, 102] et a permis une description complète des orbites jusqu'à 4 qubits.

Une approche complémentaire à celle utilisant les polynômes covariants s'appuie sur des outils mathématiques faisant appel à la géométrie algébrique. On décrit les orbites sous l'action de $\mathrm{G'_{SLOCC}}$ en terme de variétés algébriques dans l'espace projectif $\mathbb{P}(\mathcal{H}^{\otimes n})$ associé à l'espace de Hilbert. En effet, l'adhérence d'une orbite (au sens de la topologie de Zariski [1]) est une variété projective de $\mathbb{P}(\mathcal{H}^{\otimes n})$ et on peut donc décrire les états intriqués en fonction des propriétés géométriques de cette variété. Cette description géométrique de l'intrication a été développée notamment par Holweck, Luque et Thibon [100, 101, 102] et mise en oeuvre par Holweck et Jaffali dans l'étude de l'intrication dans les algorithmes quantiques [107]. Pour une introduction assez complète et pédagogique aux éléments de géométrie algébrique (notamment aux variétés algébriques) utilisés dans cette approche, le lecteur pourra consulter avec profit la thèse de Jaffali [106, section 2.1].

Parmi les polynômes invariants utilisés pour décrire l'intrication, il en est un auquel nous nous attacherons particulièrement ici : il s'agit de l'hyperdéterminant défini par

1. Dans cette topologie, les fermés sont les variétés algébriques.

Gelfand *et al.* [83] dans une approche basée sur des travaux de Cayley [47, 48]. On peut le voir comme une généralisation du déterminant classique à des hypermatrices (ensemble de valeurs indexées par plus de deux indices) et il peut être défini de façon géométrique, analytique ou algébrique (voir [83, p. 444]).

Soit $|\psi\rangle = \sum_{b_0,b_1,\ldots,b_{n-1}\in\{0,1\}} \alpha_{b_0b_1\ldots b_{n-1}} |b_0b_1\ldots b_{n-1}\rangle$ le vecteur d'état d'un système de n-qubits dans l'espace de Hilbert $\mathcal{H}^{\otimes n} \simeq (\mathbb{C}^2)^{\otimes n}$, alors l'hyperdéterminant au format 2^n, notée dans cette thèse Δ_n, est un polynôme homogène à coefficients dans $\mathbb{Z}$ en les 2^n variables $\alpha_{b_0b_1\ldots b_{n-1}}$. Il est invariant (au signe près) par permutation des qubits. C'est aussi un invariant relatif par l'action du groupe $\mathrm{G_{SLOCC}}$, ce qui implique qu'une action du groupe LU sur le système multiplie ce polynôme par un produit de déterminants de matrices unitaires dont la valeur se trouve sur le cercle unité. Ainsi, le module de l'hyperdéterminant est invariant sous l'action de LU.

Du point de vue de la géométrie algébrique, l'équation $\Delta_n = 0$ définit une hypersurface dans l'espace dual de l'espace projectif $\mathbb{P}(\mathcal{H}^{\otimes n})$. Cette hypersurface est la variété duale X^* de la variété de Segre X des états complètement factorisés, c'est à dire la fermeture (au sens de Zariski) de l'ensemble des hyperplans tangents à X. Nous renvoyons le lecteur intéressé par davantage de détails mathématiques vers la thèse de Jaffali [106], sections 2.1.3 et 2.1.8.

L'idée originale d'utiliser l'hyperdéterminant pour classifier l'intrication revient à Miyake [143, 141]. Dans [141], Miyake considère qu'un état est génériquement intriqué si et seulement si $\Delta_n \neq 0$ et il propose d'utiliser la valeur de $|\Delta_n|$ comme une mesure possible de l'intrication.

Ce chapitre est découpé en trois sections. Dans les deux premières sections, nous nous intéressons à l'apparition d'états intriqués remarquables quand des circuits d'un certain type agissent sur un état complètement factorisé. Dans la première section, il s'agit des circuits du groupe $\langle CZ, SWAP\rangle_n$ et dans la seconde section, des circuits du groupe $\langle CNOT\rangle_n$. La troisième section traite de la production d'états maximalement intriqués de 4 qubits, c'est à dire d'états qui maximisent $|\Delta_4|$.

5.1 Intrication dans les circuits de portes *CZ* et *SWAP*

5.1.1 *LU*-équivalence avec l'état $|GHZ_n\rangle$

Bien que le groupe $\langle CZ, SWAP\rangle_n$ ne contienne que deux types de portes quantiques, il permet de générer un état équivalent à $|GHZ_n\rangle$ en partant d'un état complètement factorisé. Notez que les portes $SWAP$ ne sont pas utiles ici car elles ne génèrent aucune intrication. Plus précisément, nous montrons le résultat suivant.

Proposition 5.1. *L'état*

$$\frac{1}{\sqrt{2^n}} Z_{\{\{0,1\},\{0,2\},\cdots,\{0,n-1\}\}} \left(|0\rangle + |1\rangle\right)^{\otimes n} \tag{5.6}$$

est LU-équivalent à $|GHZ_n\rangle$.

Démonstration. Soit $G = \{\{0,1\},\{0,2\},\cdots,\{0,n-1\}\}$ et soit $|G\rangle$ l'état de graphe défini par G (voir définition 3.18), c'est à dire $|G\rangle = Z_G H^{\otimes n} |0\ldots0\rangle$. On a ainsi, d'après l'identité (3.5)

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{0\leqslant b_0,\ldots,b_{n-1}\leqslant 1} (-1)^{b_0(b_1+\cdots+b_{n-1})} |b_0\cdots b_{n-1}\rangle\,, \tag{5.7}$$

ce qui peut s'écrire également

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{0 \leqslant b_1,\ldots,b_{n-1} \leqslant 1} \left(|0 b_1 \cdots b_{n-1}\rangle + (-1)^{b_1+\cdots+b_{n-1}} |1 b_1 \cdots b_{n-1}\rangle \right). \tag{5.8}$$

Nous allons démontrer que l'état $|G\rangle$ est en fait LU-équivalent à $|GHZ_n\rangle$. En appliquant la porte de Hadamard sur le qubit $\ell > 0$, il vient :

$$\begin{aligned}(I_{2^\ell} \otimes H \otimes I_{2^{n-\ell-1}})\,|G\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{0 \leqslant b_1,\ldots,b_{\ell-1},b_{\ell+1}\ldots b_{n-1} \leqslant 1} (|0 b_1 \cdots b_{\ell-1} 0 b_{\ell+1} \cdots b_{n-1}\rangle \\ +(-1)^{b_1+\cdots+b_{\ell-1}+b_{\ell+1}+\cdots+b_{n-1}} |1 b_1 \cdots b_{\ell-1} 1 b_{\ell+1} \cdots b_{n-1}\rangle).\end{aligned} \tag{5.9}$$

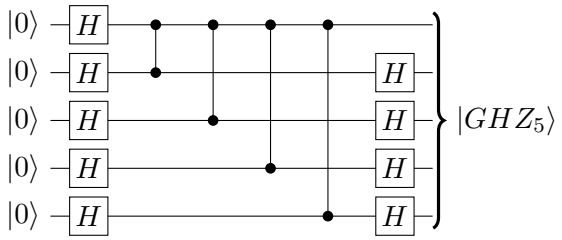
Ainsi, en itérant sur tous les qubits, sauf le qubit 0, on obtient

$$\left(I_2 \otimes H^{\otimes n-1}\right) |G\rangle = |GHZ_n\rangle\,, \tag{5.10}$$

ce qui montre que l'état $|G\rangle$ est LU-équivalent à $|GHZ_n\rangle$. □

Remarque 5.2. L'état mentionné dans la proposition 5.1 est un cas particulier d'état de graphe dit *en étoile* ou *étoilé*, dans lequel on a pris le qubit 0 comme centre (voir définition 3.18). Bien entendu, l'équivalence LU avec $|GHZ_n\rangle$ ne dépend pas du centre choisi et on peut facilement adapter la démonstration pour n'importe quel centre. Cette équivalence semble bien connue (voir par exemple [75, 96, 94]) mais, paradoxalement, nous n'en avons pas trouvé de démonstration dans la littérature. Dans la démonstration que nous proposons, nous nous basons sur une indication de preuve donnée dans [97, p. 37]. La figure 5.1 illustre la proposition 5.1 dans le cas où $n = 5$.

Figure 5.1 L'état intriqué $|GHZ_5\rangle$ généré à partir d'un circuit de $\langle CZ\rangle_5$ appliqué à un état complètement factorisé. Les 5 premières portes H permettent de créer de la superposition, les portes CZ créent de l'intrication et les 4 dernières portes H permettent d'atteindre l'état $|GHZ_5\rangle$ dans l'orbite LU de l'état de graphe étoilé (5.6)



Dans l'annexe D, nous prouvons que l'état $|GHZ_n\rangle$ n'est génériquement intriqué au sens de Miyake [141] que si $n \leqslant 3$. En fait, nous verrons plus loin que les seuls opérateurs du groupe $\langle CZ, SWAP\rangle_n$ ne permettent pas de créer un état génériquement intriqué si $n \geqslant 4$.

5.1.2 Équivalence SLOCC avec $|\mathrm{W}_3\rangle$

Nous montrons ici que le groupe $\langle CZ, SWAP\rangle_n$ n'est pas assez riche pour générer tous les types d'intrication à partir d'un état complètement factorisé. À cette fin, nous donnons un contre-exemple en prouvant qu'il n'est pas possible de générer un état

SLOCC-équivalent à $|W_3\rangle$. Nous utilisons la méthode proposée par Klyachko dans [116]. Cette méthode est basée sur la théorie algébrique des invariants. Les états appartenant à une même orbite sont caractérisés par leurs valeurs sur une liste de polynômes covariants.

Dans le cas de 3 qubits, la description des orbites SLOCC s'appuie sur la classification des formes binaires trilinéaires établie par Le Paige en 1881 [121, 122]. Cette classification est décrite dans [132, section 3.5] et nous la rappelons ici. Soit $|\psi\rangle = \sum_{0\leqslant i,j,k\leqslant 1} \alpha_{ijk} |ijk\rangle$ un état de 3 qubits. Le premier covariant est la forme trilinéaire associée à $|\psi\rangle$:

$$A = \sum_{i,j,k\in\{0,1\}} \alpha_{ijk} x_i y_j z_k. \tag{5.11}$$

Partant de A, on calcule trois formes quadratiques :

$$B_x(x_0, x_1) = \begin{vmatrix} \frac{\partial^2 A}{\partial y_0 \partial z_0} & \frac{\partial^2 A}{\partial y_0 \partial z_1} \\ \frac{\partial^2 A}{\partial y_1 \partial z_0} & \frac{\partial^2 A}{\partial y_1 \partial z_1} \end{vmatrix}, \tag{5.12}$$

$$B_y(y_0, y_1) = \begin{vmatrix} \frac{\partial^2 A}{\partial x_0 \partial z_0} & \frac{\partial^2 A}{\partial x_0 \partial z_1} \\ \frac{\partial^2 A}{\partial x_1 \partial z_0} & \frac{\partial^2 A}{\partial x_1 \partial z_1} \end{vmatrix}, \tag{5.13}$$

$$B_z(z_0, z_1) = \begin{vmatrix} \frac{\partial^2 A}{\partial x_0 \partial y_0} & \frac{\partial^2 A}{\partial x_0 \partial y_1} \\ \frac{\partial^2 A}{\partial x_1 \partial y_0} & \frac{\partial^2 A}{\partial x_1 \partial y_1} \end{vmatrix}. \tag{5.14}$$

Le catalectican C est la forme trilinéaire définie par :

$$C(x_0, x_1, y_0, y_1, z_0, z_1) = \begin{vmatrix} \frac{\partial A}{\partial x_0} & \frac{\partial A}{\partial x_1} \\ \frac{\partial B_x}{\partial x_0} & \frac{\partial B_x}{\partial x_1} \end{vmatrix} = \begin{vmatrix} \frac{\partial A}{\partial y_0} & \frac{\partial A}{\partial y_1} \\ \frac{\partial B_y}{\partial y_0} & \frac{\partial B_y}{\partial y_1} \end{vmatrix} = \begin{vmatrix} \frac{\partial A}{\partial z_0} & \frac{\partial A}{\partial z_1} \\ \frac{\partial B_z}{\partial z_0} & \frac{\partial B_z}{\partial z_1} \end{vmatrix}. \tag{5.15}$$

Les trois formes quadratiques B_x, B_y et B_z ont le même discriminant qui n'est autre que Δ_3, l'hyperdéterminant de Cayley au format $2 \times 2 \times 2$ (au sens de Gelfand *et al.* [83]) de la forme trilinéaire A :

$$\begin{aligned} \Delta_3(|\psi\rangle) \;=\; & (\alpha_{000}\alpha_{111} - \alpha_{001}\alpha_{110} - \alpha_{010}\alpha_{101} + \alpha_{011}\alpha_{100})^2 \\ & -4\,(\alpha_{000}\alpha_{011} - \alpha_{001}\alpha_{010})\,(\alpha_{100}\alpha_{111} - \alpha_{101}\alpha_{110})\,. \end{aligned} \tag{5.16}$$

Les polynômes A, B_x, B_y, B_z, C et Δ_3 sont les générateurs de l'algèbre des polynômes covariants et Δ_3 est l'unique générateur de l'algèbre des polynômes invariants.

Pour caractériser l'orbite de $|W_3\rangle$, nous avons besoin de seulement deux polynômes : C et Δ_3. Les états qui sont SLOCC-équivalents à $|GHZ_3\rangle$ sont caractérisés par $\Delta_3 \neq 0$ tandis que les états qui sont SLOCC-équivalents à $|W_3\rangle$ sont caractérisés par $C \neq 0$ et $\Delta_3 = 0$ [100]. Pour les autres orbites, on a : $\Delta_3 = C = 0$.

Soit $G \in \mathcal{G}_3$, on remarque que :

$$Z_G = \mathrm{diag}([1, 1, 1, \varepsilon_{\{1,2\}}, 1, \varepsilon_{\{0,2\}}, \varepsilon_{\{0,1\}}, \varepsilon_{\{0,1\}}\varepsilon_{\{0,2\}}\varepsilon_{\{1,2\}}]) \tag{5.17}$$

avec $\varepsilon_{\{i,j\}} = -1$ si $\{i, j\} \in G$ et $\varepsilon_{\{i,j\}} = 1$ sinon. Considérons les états

$$|\varphi_G\rangle = Z_G \sum_{0\leqslant i,j,k\leqslant 1} a_i b_j c_k |ijk\rangle = Z_G(a_0|0\rangle + a_1|1\rangle)(b_0|0\rangle + b_1|1\rangle)(c_0|0\rangle + c_1|1\rangle) \tag{5.18}$$

résultant de l'action de l'opérateur Z_G sur un état complètement factorisé. Après calcul, on obtient :

$$C(|\varphi_G\rangle) = a_0b_0c_0a_1b_1c_1(2 - \varepsilon_{\{0,1\}} - \varepsilon_{\{0,2\}} - \varepsilon_{\{1,2\}} + \varepsilon_{\{0,1\}}\varepsilon_{\{0,2\}}\varepsilon_{\{1,2\}})P \tag{5.19}$$

où $P = \sum_{i_0,i_1,i_2} a_{i_0}b_{i_1}c_{i_2}(-1)^{\mathrm{card}\{j|i_j=1\}} \left(\prod_{\{j,k\}|i_j+i_k>0} \varepsilon_{\{j,k\}} \right) x_{i_0}y_{i_1}z_{i_2}$ est une forme trilinéaire non nulle et

$$\Delta_3(|\varphi_G\rangle) = 4(a_0b_0c_0a_1b_1c_1)\varepsilon_{\{0,1\}}\varepsilon_{\{0,2\}}\varepsilon_{\{1,2\}}(2-\varepsilon_{\{0,1\}}-\varepsilon_{\{0,2\}}-\varepsilon_{\{1,2\}}+\varepsilon_{\{0,1\}}\varepsilon_{\{0,2\}}\varepsilon_{\{1,2\}}). \tag{5.20}$$

On voit donc que si Δ_3 s'annule pour $|\varphi_G\rangle$, alors il en est de même pour C, ce qui entraîne le résultat suivant :

Proposition 5.3. *L'état résultant de l'application d'un opérateur de $\langle CZ, SWAP\rangle_3$ sur un état complètement factorisé d'un système de 3 qubits ne peut être SLOCC-équivalent à $|W_3\rangle$.*

Cependant nous observons qu'il est possible d'atteindre l'orbite SLOCC de $|W_3\rangle$ à partir d'un élément de l'orbite LU de $|GHZ_3\rangle$. En effet, considérons l'état

$$|\varphi_1\rangle = \frac{1}{\sqrt{8}} \left(R_y(\frac{\pi}{4})HX \otimes R_y(\frac{\pi}{4}) \otimes HX \right) Z_{\{0,1\}}Z_{\{1,2\}}(|0\rangle + |1\rangle)^3 \tag{5.21}$$

qui est dans l'orbite LU de $|GHZ_3\rangle$ d'après la proposition 5.1. Après calcul, on obtient

$$\Delta_3 \left(Z_{\{0,1\}} |\varphi_1\rangle \right) = 0 \text{ et } C \left(Z_{\{0,1\}} |\varphi_1\rangle \right) \neq 0, \tag{5.22}$$

ce qui prouve que $Z_{\{0,1\}} |\varphi_1\rangle$ est dans l'orbite SLOCC de $|W_3\rangle$.

5.1.3 Système de quatre qubits

Le problème de la classification des états d'un système de 4 qubits est plus complexe que pour 3 qubits. Nous utilisons ici la classification établie en 2002 par Verstraete et al. [176] qui a été corrigée en 2006 par Chterental et Djokovic [51] : l'espace de Hilbert $\mathcal{H}^{\otimes 4}$ a une infinité d'orbites sous l'action du groupe $\mathrm{G_{SLOCC}}$ et ces orbites ont été classifiées en 9 familles, dont 6 sont décrites par des paramètres. Plus précisément, toute orbite contient, à une permutation des qubits près, au moins un représentant dans l'une de ces familles et deux états appartenant à deux familles différentes ne sont jamais SLOCC-équivalents [51, théorème 3.6]. Parmi ces 9 familles, une seule est générique : un état quantique dans la situation la plus générale est SLOCC-équivalent (à une permutation des qubits près) à 192 états de la famille G_{abcd}. Cette famille est définie par la forme normale

$$\begin{aligned} G_{abcd} \quad = \quad & \tfrac{a+d}{2}\left(|0000\rangle + |1111\rangle\right) + \tfrac{a-d}{2}\left(|0011\rangle + |1100\rangle\right) \\ & + \tfrac{b+c}{2}\left(|0101\rangle + |1010\rangle\right) + \tfrac{b-c}{2}\left(|0110\rangle + |1001\rangle\right), \end{aligned} \tag{5.23}$$

où les 4 paramètres a, b, c, et d sont indépendants (voir [176, théorème 2] et [102, section III.A]).

Pour déterminer la famille de Verstraete à laquelle appartient un état donné $|\psi\rangle = \sum_{0\leqslant i,j,k,\ell\leqslant 1} \alpha_{ijk\ell} |ijk\ell\rangle$, nous utilisons un algorithme décrit dans [102, section V]. Comme dans le cas des 3 qubits, cet algorithme est basé sur l'évaluation de certains polynômes covariants. Nous rappelons que l'algèbre des polynômes SLOCC-invariants est engendrée par les quatre polynômes suivants [133] :

- l'invariant de plus petit degré

$$B = \sum_{0\leqslant i_1,i_2,i_3\leqslant 1} (-1)^{i_1+i_2+i_3} \alpha_{0i_1i_2i_3}\alpha_{1(1-i_1)(1-i_2)(1-i_3)}, \tag{5.24}$$

- deux polynômes de degré 4

$$L = \begin{vmatrix} \alpha_{0000} & \alpha_{0010} & \alpha_{0001} & \alpha_{0011} \\ \alpha_{1000} & \alpha_{1010} & \alpha_{1001} & \alpha_{1011} \\ \alpha_{0100} & \alpha_{0110} & \alpha_{0101} & \alpha_{0111} \\ \alpha_{1100} & \alpha_{1110} & \alpha_{1101} & \alpha_{1111} \end{vmatrix} \tag{5.25}$$

et

$$M = \begin{vmatrix} \alpha_{0000} & \alpha_{0001} & \alpha_{0100} & \alpha_{0101} \\ \alpha_{1000} & \alpha_{1001} & \alpha_{1100} & \alpha_{1101} \\ \alpha_{0010} & \alpha_{0011} & \alpha_{0110} & \alpha_{0111} \\ \alpha_{1010} & \alpha_{1011} & \alpha_{1110} & \alpha_{1111} \end{vmatrix}, \tag{5.26}$$

- et un polynôme de degré 6 défini par $D_{xy} = -\det(B_{xy})$ où B_{xy} est la matrice 3×3 satisfaisant

$$\left[x_0^2, x_0x_1, x_1^2\right] B_{xy} \begin{bmatrix} y_0^2 \\ y_0y_1 \\ y_1^2 \end{bmatrix} = \det\left(\frac{\partial^2}{\partial z_i \partial t_j} A\right) \tag{5.27}$$

avec $A = \sum_{0\leqslant i,j,k,\ell\leqslant 1} \alpha_{ijk\ell} x_i y_j z_k t_\ell$ la forme trilinéaire associée à $|\psi\rangle$.

Le *cône nilpotent* est l'ensemble des états annulant tous les invariants. C'est donc la variété algébrique définie par l'annulation des 4 polynômes générateurs : $B = L = M = D_{xy} = 0$. Le cône nilpotent est la réunion de 31 orbites sous l'action de $\mathrm{G}'_{\mathrm{SLOCC}}$. Ces orbites sont réparties en 9 strates, les états d'une même strate ont le même type de Verstraete et deux états de strates différentes ont des types de Verstraete différents (la correspondance est donnée dans [101], table VIII page 45).

Pour effectuer notre classification, nous allons aussi utiliser un autre invariant

$$N = -L - M = \begin{vmatrix} \alpha_{0000} & \alpha_{1000} & \alpha_{0001} & \alpha_{1001} \\ \alpha_{0100} & \alpha_{1100} & \alpha_{0101} & \alpha_{1101} \\ \alpha_{0010} & \alpha_{1010} & \alpha_{0011} & \alpha_{1011} \\ \alpha_{0110} & \alpha_{1110} & \alpha_{0111} & \alpha_{1111} \end{vmatrix}, \tag{5.28}$$

et nous aurons besoin des polynômes covariants $\overline{\mathcal{G}}$, $\mathcal{G}$, $\mathcal{H}$, $\mathcal{K}_3$, $\mathcal{K}_5$ et $\mathcal{L}$ (voir [102]) dont nous rappelons la définition en annexe C.

Nous rappelons maintenant le principe de l'algorithme décrit dans [102]. Une première classification est obtenue en recherchant les racines des trois quartiques

$$Q_1 = x^4 - 2Bx^3y + (B^2 + 2L + 4M)x^2y^2 + 4(D_{xy} - B(M + \frac{1}{2}L))xy^3 + L^2y^4, \tag{5.29}$$

$$Q_2 = x^4 - 2Bx^3y + (B^2 - 4L - 2M)x^2y^2 + (4D_{xy} - 2MB)xy^3 + M^2y^4, \tag{5.30}$$

et

$$Q_3 = x^4 - 2Bx^3y + (B^2 + 2L - 2M)x^2y^2 - (2(L+M)B - 4D_{xy})xy^3 + N^2y^4. \quad (5.31)$$

Dans le cas d'un état nilpotent, les trois quartiques sont égales à x^4. Pour déterminer à quelle strate appartient un état nilpotent, on applique un algorithme décrit dans [101], basé sur le calcul de 8 polynômes covariants $A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F$ et P_L dont la définition est donnée en annexe C. On obtient ainsi la strate du cône nilpotent à laquelle cet état appartient et on lit le type de Verstraete de l'état en se reportant à [101], table VIII page 45.

Si l'état n'est pas nilpotent, nous déterminons les racines d'une quartique $Q = \alpha x^4 - 4\beta x^3y + 6\gamma x^2y^2 - 4\delta xy^3 + \omega y^4$ en testant l'annulation des polynômes covariants

$$I_2 = \alpha\omega - 4\beta\delta + 3\gamma^2, \quad (5.32)$$

$$I_3 = \alpha\gamma\omega - \alpha\delta^2 - \omega\beta^2 - \gamma^3 + 2\beta\gamma\delta, \quad (5.33)$$

$$\Delta = I_2^3 - 27I_3^2, \quad (5.34)$$

$$Hess = \begin{vmatrix} \frac{\partial^2}{\partial x^2}Q & \frac{\partial^2}{\partial x\partial y}Q \\ \frac{\partial^2}{\partial x\partial y}Q & \frac{\partial^2}{\partial y^2}Q \end{vmatrix}, \quad (5.35)$$

et

$$T = \begin{vmatrix} \frac{\partial}{\partial x}Q & \frac{\partial}{\partial y}Q \\ \frac{\partial}{\partial x}Hess(Q) & \frac{\partial}{\partial y}Hess(Q) \end{vmatrix}. \quad (5.36)$$

L'interprétation des valeurs des covariants en termes de racines des quartiques est résumée dans la table 5.1 (voir par exemple [150]). Remarquez que les valeurs des invariants

Table 5.1 Racines d'une quartique

Covariants	*Interprétation*
$\Delta \neq 0$	Quatre racines distinctes
$\Delta = 0$ et $T \neq 0$	Exactement une racine double
$T = 0$ et $I_2 \neq 0$	Deux racines doubles distinctes
$I_2 = I_3 = 0$ et $Hess \neq 0$	Une racine triple
$Hess = 0$	Une racine quadruple

I_2, I_3 et Δ sont les mêmes pour les trois quartiques. De plus Δ est l'hyperdéterminant au format $2 \times 2 \times 2 \times 2$ au sens de Gelfand et al. [83] de la forme A (voir [102]), c'est à dire que $\Delta = \Delta_4$. Notez également que

$$Q_1(G_{abcd}) = (x - a^2)(x - b^2)(x - c^2)(x - d^2). \quad (5.37)$$

Une fois la configuration des racines identifiée, on obtient le type de Verstraete de l'état $|\psi\rangle$ en calculant les valeurs de certains des covariants $\overline{\mathcal{G}}$, $\mathcal{G}$, $\mathcal{H}$, $\mathcal{K}_3$, $\mathcal{K}_5$ et $\mathcal{L}$ puis en se reportant à la classification décrite dans [102, p. 32].

Appliquons maintenant cet algorithme à un état

$$|\varphi_G\rangle = Z_G(a_0|0\rangle + a_1|1\rangle)(b_0|0\rangle + b_1|1\rangle)(c_0|0\rangle + c_1|1\rangle)(d_0|0\rangle + d_1|1\rangle) \quad (5.38)$$

résultant de l'application d'un opérateur Z_G de $\langle CZ\rangle_4$ sur un état complètement factorisé de 4 qubits. Nous devons traiter les 64 opérateurs de $\langle CZ\rangle_4$. Voici la liste des résultats obtenus (où l'on a posé $a_0b_0c_0d_0a_1b_1c_1d_1 = \frac{1}{16}\diamond$).

(i) Si $G = \emptyset$ alors $|\varphi_G\rangle$ est un état complètement factorisé.

(ii) Si $G = \{\{i, j\}\}$ pour $i, j = 0, \ldots, 3$, $i \neq j$ (6 cas), alors $|\varphi_G\rangle$ appartient au cône nilpotent et chaque quartique est égale à x^4. L'état $|\varphi_G\rangle$ est partiellement factorisé en le produit d'un état qui est SLOCC-équivalent à une paire EPR (pour les qubits i, j) par deux autres particules indépendantes.

(iii) Si $G = \{\{i, j\}, \{i, k\}\}$ pour i, j, k distincts (12 cas), alors $|\varphi_G\rangle$ est dans le cône nilpotent et chaque quartique est égale à x^4. L'état $|\varphi_G\rangle$ se factorise en le produit d'un état qui est SLOCC-équivalent à $|GHZ_3\rangle$ (pour les qubits i, j, k) par un qubit indépendant.

(iv) Si $G = \{\{i, j\}, \{k, \ell\}\}$ avec $\{i, j\} \cap \{k, \ell\} = \emptyset$ (3 cas) alors une des quartiques est égale à $x^3(x - 4 \diamond y)$ et les deux autres sont égales à $(x - \frac{1}{4} \diamond y)^4$. Pour des valeurs génériques des paramètres on a $\diamond \neq 0$, ce qui implique que $|\varphi_G\rangle$ se factorise en deux états de 2-qubits qui sont chacun SLOCC-équivalents à une paire EPR. Prenons par exemple le cas où $G = \{\{1, 2\}, \{3, 4\}\}$, les autres cas étant symétriques. Dans ce cas, on a $Q_1 = x^3(x - 4 \diamond y)$ et $\mathcal{C} = \mathcal{D} = \mathcal{K}_5 = \mathcal{L} = 0$. D'après les résultats de [102], cela implique que $|\varphi_G\rangle$ est dans la même orbite que G_{a000} avec $a = \frac{1}{2}\sqrt{\diamond}$.

(v) Si $G = \{\{i, j\}, \{j, k\}, \{i, k\}\}$ avec i, j, k distincts (4 cas) alors $|\varphi_G\rangle$ appartient au cône nilpotent et chaque quartique est égale à x^4. L'état $|\varphi_G\rangle$ se factorise en le produit d'un état SLOCC-équivalent à $|GHZ_3\rangle$ (sur les qubits i, j, k) par un qubit indépendant.

(vi) Si $G = \{\{i, j\}, \{j, k\}, \{k, \ell\}\}$ avec $\{i, j, k, \ell\} = \{0, 1, 2, 3\}$ (12 cas) alors une des quartiques est égale à $x^2(x^2 + \frac{1}{4} \diamond^2 y^2)$ et les deux autres sont égales à $(x^2 - \frac{1}{16}\diamond^2)^2$. Pour des valeurs génériques des paramètres on a $\diamond \neq 0$ donc une quartique a une racine double nulle ainsi que deux racines simples et les deux autres quartiques ont deux racines doubles. Prenons par exemple le cas où $G = \{\{3, 2\}, \{2, 1\}, \{1, 0\}\}$ dans lequel $Q_1 = x^2(x^2 + \frac{1}{4} \diamond^2 y^2)$. Selon l'algorithme décrit dans [102], nous devons calculer les valeurs des covariants $\mathcal{K}_3$ et $\mathcal{L}$ pour l'état $|\varphi_G\rangle$. Ces deux covariants étant dans ce cas des polynômes nuls, on en déduit que $|\varphi_G\rangle$ est dans une orbite dégénérée de G_{abcd}. Plus précisément, l'état $|\varphi_G\rangle$ est équivalent à G_{ab00} avec $a = \frac{1+\mathrm{i}}{2}\sqrt{\diamond}$ et $b = \frac{1-\mathrm{i}}{2}\sqrt{\diamond}$.

(vii) Si $E = \{\{i, j\}, \{i, k\}, \{i, \ell\}\}$ avec $\{i, j, k, \ell\} = \{0, 1, 2, 3\}$ (4 cas) alors les trois quartiques sont égales à $x^2(x + \frac{1}{2}\diamond)^2$. Selon [102], on détermine le type de Verstraete de $|\varphi_G\rangle$ en évaluant $\overline{\mathcal{G}}$, $\mathcal{G}$, $\mathcal{H}$ et $\mathcal{L}$. Comme ces quatre covariants sont nuls sur cet état, on en déduit que $|\varphi_G\rangle$ est dans l'orbite de G_{aa00} avec $a = \frac{1+\mathrm{i}}{2}\sqrt{\diamond}$. Cet état appartient également à la variété définie par $L = M = D_{xy} = 0$.

(viii) Si $G = \{\{i, j\}, \{i, k\}, \{i, \ell\}, \{j, k\}\}$ avec $\{i, j, k, l\} = \{0, 1, 2, 3\}$ (12 cas) alors une des quartiques est égale à $x^2(x - \frac{1}{2} \diamond y)(x + \frac{1}{2} \diamond y)$ et les deux autres sont égales à $(x^2 + \frac{1}{16} \diamond^2 y^2)^2$. Prenons le cas où $G = \{\{3, 2\}, \{3, 1\}, \{3, 0\}, \{1, 0\}\}$, les autres cas étant similaires. D'après [102], on doit calculer les valeurs de $\mathcal{K}_3$ et $\mathcal{L}$. Comme ces deux covariants sont nuls, on en déduit que $|\varphi_G\rangle$ est SLOCC-équivalent à G_{ab00} avec $a = \frac{1}{2}\sqrt{\diamond}$ et $b = \mathrm{i}a$. De plus, on remarque qu'il appartient à la variété définie par $L = 0$.

(ix) Si $G = \{\{i, j\}, \{j, k\}, \{k, \ell\}, \{\ell, i\}\}$ avec $\{i, j, k, \ell\} = \{0, 1, 2, 3\}$ (3 cas) alors une des quartiques est égale à $x^2(x^2 + \frac{1}{4}y^2\diamond^2)$ et les autres sont égales à $(x^2 - \frac{1}{16}y^2\diamond^2)^2$.

Considérons le cas où $G = \{\{3,1\},\{2,1\},\{2,0\},\{3,0\}\}$. D'après [102], on doit calculer les valeurs de $\mathcal{K}_3$ et $\mathcal{L}$. Comme ces deux covariants sont nuls, on en déduit que $|\varphi_G\rangle$ est SLOCC-équivalent à G_{ab00} avec $a = \frac{1+\mathrm{i}}{2\sqrt{2}}\sqrt{\diamond}$ et $b = \frac{1-\mathrm{i}}{2\sqrt{2}}\sqrt{\diamond}$. De plus, on remarque qu'il appartient à la variété définie par $L = 0$.

(x) Si $G = \{\{i,j\} \mid 0 \leqslant i < j \leqslant 3\} \backslash \{\{k,\ell\}\}$ avec $k \neq \ell$ (6 cas) alors une des quartiques est égale à $x^2(x^2 - \frac{1}{4}\diamond^2 y^2)$ tandis que les deux autres sont égales à $(x^2 + \frac{1}{16}\diamond^2 y^2)^2$. Sans perte de généralité, supposons que $G = \{\{3,2\},\{3,1\},\{3,0\},\{2,1\},\{2,0\}\}$, les autres cas s'obtenant par symétrie (permutation des qubits). On a alors $Q_1 = x^2(x^2 - \frac{1}{4}\exp(2i\diamond)y^2)$. Selon [102], on calcule $\mathcal{K}_3$ et $\mathcal{L}$. Comme ces deux covariants sont nuls pour $|\varphi_G\rangle$, on en déduit que $|\varphi_G\rangle$ est équivalent à un état dégénéré du type G_{abcd}. Plus précisément, il est équivalent à G_{ab00} avec $a = \sqrt{2}\sqrt{\diamond}$ et $b = -\mathrm{i}a$.

(xi) Si $G = \{\{i,j\} \mid 0 \leqslant i < j \leqslant 3\}$ alors $L = M = 0$ et les trois quartiques sont égales à $x^2(x - \frac{1}{2}\diamond y)^2$. Selon [102], nous calculons alors les valeurs des quatre covariants $\overline{\mathcal{G}}$, $\mathcal{G}$, $\mathcal{H}$, et $\mathcal{L}$. Comme ils sont tous nuls, on en déduit que $|\varphi_G\rangle$ est équivalent à un état dégénéré du type G_{abcd}. Plus précisément, il est équivalent à G_{aa00} avec $a = \frac{1}{\sqrt{2}}\sqrt{\diamond}$.

En considérant que G est l'ensemble des arêtes d'un graphe de 4 sommets, les cas (i) à (v) ci-dessus correspondent à des graphes non connexes et à des états $|\varphi_G\rangle$ factorisés (partiellement ou complètement). Les autres cas correspondent à des graphes connexes et à des état dégénérés du type G_{abcd}, certains étant factorisés. Ainsi les états $|\varphi_G\rangle$ ne sont jamais des états génériques de la famille G_{abcd}.

Dans le cas d'un système de 4 qubits, tout état génériquement intriqué au sens de Miyake (*i.e.* $\Delta_4 \neq 0$) est SLOCC-équivalent (à une permutation près des qubits) à un état de la famille G_{abcd} de Verstraete. En effet, pour les états des 8 autres familles, l'hyperdéterminant Δ_4 s'annule (voir [133, annexe A]). De plus, pour tout état G_{abcd}, on a :

$$\Delta_4(G_{abcd}) = \frac{1}{256}V(a^2,b^2,c^2,d^2)^2, \tag{5.39}$$

où V est le déterminant de Vandermonde en dimension 4 [133]. On voit donc qu'un état générique au sens de Verstraete *et al.* est génériquement intriqué au sens de Miyake et réciproquement. En résumé, on a le résultat suivant.

Théorème 5.4. *Un circuit de $\langle CZ, SWAP\rangle_4$ prenant en entrée un état complètement factorisé de 4 qubits ne peut pas produire d'états génériquement intriqués.*

Notez que l'état $|GHZ_4\rangle$ est SLOCC-équivalent à un état du type G_{aa00} [102] tout comme l'état $|\varphi_G\rangle$ dans le cas (vii) ci-dessus. De plus, en choisissant $a_i = b_i = c_i = d_i = \frac{1}{\sqrt{2}}$ (avec $i \in \{0,1\}$), il est possible de créer un état LU-équivalent à $|GHZ_4\rangle$ (voir proposition 5.1).

L'état $|W_4\rangle = \frac{1}{2}(|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle$ appartient au cône nilpotent (voir [101, p.21]). Comme tous les états $|\varphi_G\rangle$ appartenant au cône nilpotent sont des états complètement ou partiellement factorisés et que la propriété d'être factorisé est une propriété SLOCC-invariante, on en déduit qu'un état $|\varphi_G\rangle$ ne peut être SLOCC-équivalent à $|W_4\rangle$, tout comme dans le cas de trois qubits avec $|W_3\rangle$.

5.1.4 Cinq qubits et au-delà

Dans le cas de 5 qubits ou plus, les outils permettant une classification de l'intrication sont beaucoup plus limités. En effet la description de l'algèbre des polynômes covariants en terme de générateurs est hors de portée et certains invariants comme l'hyperdéterminant sont trop grands pour être calculés [134]. On rappelle que l'importance de l'hyperdéterminant vient du fait qu'il s'annule dès qu'un système n'est pas génériquement intriqué [141]. Même si l'hyperdéterminant est très difficilement calculable, sa nullité peut être testée plus facilement car elle peut être interprétée en terme de solutions d'un système d'équations polynomiales [83, p.445]. Dans le cas de 5 qubits, si $A = \sum_{0\leqslant i,j,k,\ell,m\leqslant 1} \alpha_{ijk\ell n} x_i y_j z_k t_\ell s_m$ est la forme de base associée à un état de 5 qubits $|\varphi\rangle = \sum_{0\leqslant i,j,k,\ell,m\leqslant 1} \alpha_{ijk\ell m}|ijk\ell m\rangle$, la condition $\Delta_5(|\varphi\rangle) = 0$ signifie que le système

$$S_\varphi = \{A = \frac{d}{dx_0}A = \frac{d}{dx_1}A = \frac{d}{dy_0}A = \frac{d}{dy_1}A = \cdots = \frac{d}{ds_0}A = \frac{d}{ds_1}A = 0\} \tag{5.40}$$

a une solution $\hat{x}_0, \hat{x}_1, \hat{y}_0, \hat{y}_1, \ldots, \hat{s}_0, \hat{s}_1$ en les variables $x_0, x_1, y_0, y_1, \ldots, s_0, s_1$ telle que $(\hat{x}_0, \hat{x}_1), (\hat{y}_0, \hat{y}_1), \ldots, (\hat{s}_0, \hat{s}_1) \neq (0, 0)$. Une telle solution est dite non triviale. Nous procédons de façon exhaustive en exhibant une solution non triviale pour chacun des 1024 systèmes S_{φ_G} avec

$$|\varphi_G\rangle = Z_G(a_0|0\rangle + a_1|1\rangle)(b_0|0\rangle + b_1|1\rangle)(c_0|0\rangle + c_1|1\rangle)(d_0|0\rangle + d_1|1\rangle)(e_0|0\rangle + e_1|1\rangle). \tag{5.41}$$

On considère l'action par conjugaison du groupe $\mathfrak{S}_5$ sur $\langle CZ\rangle_5$ définie par $\sigma \cdot Z_G = Z_{\sigma(G)}$ (3.14). On calcule qu'il y a 34 orbites pour cette action. Comme $Z_{\sigma(G)} = S_\sigma Z_G S_\sigma^{-1}$ et Δ_5 est invariant (au signe près) par permutation des qubits, on en déduit qu'il suffit de donner une solution non triviale pour chaque représentant des 34 orbites. Pour chaque représentant, nous avons trouvé (en utilisant Maple) une solution non triviale telle que $x_1 = y_1 = z_1 = t_1 = s_1 = 1$. Ces solutions sont données dans les trois tableaux en annexe E. On en déduit la proposition suivante.

Proposition 5.5. *Un circuit de $\langle CZ, SWAP\rangle_5$ prenant en entrée un état complètement factorisé ne peut pas produire un état génériquement intriqué.*

En principe on peut appliquer la même stratégie pour plus de 5 qubits et nous conjecturons que le résultat est encore vrai.

Conjecture 5.6. *Si $n \geqslant 4$, un circuit de $\langle CZ, SWAP\rangle_n$ agissant sur un état complètement factorisé ne peut pas produire un état génériquement intriqué.*

5.2 Intrication dans les circuits de portes *CNOT* de 3 ou 4 qubits

Au chapitre 1, nous avons observé que l'état $|GHZ_n\rangle$ peut se construire très simplement en faisant agir un circuit de portes *CNOT* sur un état complètement factorisé (voir exemple 1.1). Dans cette section, nous étudions plus en détail l'apparition d'états intriqués de 3 ou 4 qubits dans ce type de circuit.

5.2.1 Le groupe $\langle CNOT\rangle_3$ et les états intriqués de 3 qubits

Nous allons prouver que le groupe $\langle CNOT\rangle_3$ agissant sur un état complètement factorisé est assez puissant pour produire n'importe quel type d'intrication. Dans le cas de 3 qubits, la description des orbites SLOCC s'appuie sur la méthode de classification des formes binaires trilinéaires établie par Le Paige [121, 122] : les états d'une même orbite sont caractérisés par leurs valeurs sur les polynômes covariants B_x, B_y, B_z, C et Δ_3 dont la définition a été rappelée dans la section 5.1.2.

À chaque état de trois qubits $|\psi\rangle = \sum_{i,j,k\in\{0,1\}} \alpha_{ijk}\,|ijk\rangle$, on associe un vecteur de 5 bits

$$V[|\psi\rangle] = [[B_x(|\psi\rangle)], [B_y(|\psi\rangle)], [B_z(|\psi\rangle)], [C(|\psi\rangle)], [\Delta_3(|\psi\rangle)]] \tag{5.42}$$

où $[P(|\psi\rangle)] = 0$ si $P(|\psi\rangle) = 0$ et $[P(|\psi\rangle)] = 1$ si $P(|\psi\rangle) \neq 0$. La connaissance du vecteur $V[|\psi\rangle]$ est suffisante pour déterminer l'orbite d'un état $|\psi\rangle$ (voir [100]) et les résultats sont résumés dans la table 5.2.

Table 5.2 Les orbites SLOCC d'un système de trois qubits.

Orbites	Représentants $\|\psi\rangle$	$V[\|\psi\rangle]$
$\mathcal{O}_{VI}$	$\|GHZ_3\rangle$	$[1,1,1,1,1]$
$\mathcal{O}_{V}$	$\|W_3\rangle$	$[1,1,1,1,0]$
$\mathcal{O}_{IV}$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|110\rangle)$	$[0,0,1,0,0]$
$\mathcal{O}_{III}$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|101\rangle)$	$[0,1,0,0,0]$
$\mathcal{O}_{II}$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|011\rangle)$	$[1,0,0,0,0]$
$\mathcal{O}_{I}$	$\|000\rangle$	$[0,0,0,0,0]$

On vérifie qu'il est très simple de construire des représentants des orbites VI, IV, III et II, à partir d'un circuit de $\langle CNOT\rangle_3$ agissant sur un état factorisé. On a en effet :

$$\begin{aligned}
|GHZ_3\rangle &= X_{[2:1]}X_{[1:0]}H_0\,|000\rangle \quad \text{(orbit } \mathcal{O}_{VI}\text{)},\\
\frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) &= X_{[1:0]}H_0\,|000\rangle \quad \text{(orbit } \mathcal{O}_{IV}\text{)},\\
\frac{1}{\sqrt{2}}(|000\rangle + |101\rangle) &= X_{[2:0]}H_0\,|000\rangle \quad \text{(orbit } \mathcal{O}_{III}\text{)},\\
\frac{1}{\sqrt{2}}(|000\rangle + |011\rangle) &= X_{[2:1]}H_1\,|000\rangle \quad \text{(orbit } \mathcal{O}_{II}\text{)}.
\end{aligned}$$

Afin de produire un état SLOCC-équivalent à $|W_3\rangle$ (orbite $\mathcal{O}_V$) on voit d'après la table 5.2 qu'il faut réussir à construire un état $|\psi\rangle$ tel que

$$\Delta_3(|\psi\rangle) = 0 \text{ et } C(x_0,x_1,y_0,y_1,z_0,z_1) \neq\ 0.$$

Il apparaît qu'une telle construction est possible en utilisant uniquement des portes quantiques de l'ensemble standard des portes universelles (Clifford + T). Cette construction est décrite dans la proposition 5.7 et est illustrée par la figure 5.2.

Proposition 5.7. *Soit $X_{[i:j:k]} = X_{[i:j]}X_{[k:i]}X_{[j:k]}$, avec i,j,k des entiers distincts de $\{0,1,2\}$ et $k \neq 2$. L'état*

$$X_{[i:j:k]}(T\otimes T\otimes P)H^{\otimes 3}\,|000\rangle \tag{5.43}$$

est SLOCC-équivalent à $|W_3\rangle$.

Démonstration. Soit $q = \mathrm{e}^{\frac{\mathrm{i}\pi}{4}}$ et soit

$$|\psi_{(k_0,k_1,\ldots,k_7)}\rangle = \frac{1}{\sqrt{8}}\left(q^{k_0}|000\rangle + q^{k_1}|001\rangle + \cdots + q^{k_7}|111\rangle\right)$$

où k_i est un entier. Un calcul simple montre que $(T\otimes T\otimes P)H^{\otimes 3}|000\rangle = |\psi_{(0,2,1,3,1,3,2,4)}\rangle$. On évalue ensuite les polynômes Δ_3 (5.16) et C (5.15) pour l'état

$$|\psi'\rangle = X_{[i:j:k]}|\psi_{(0,2,1,3,1,3,2,4)}\rangle\,.$$

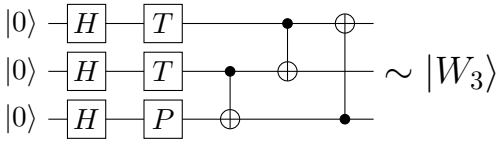
Si $k \neq 2$, on vérifie que $\Delta_3(|\psi'\rangle) = 0$ et $C(|\psi'\rangle) \neq 0$ (voir résultats table 5.3). □

Table 5.3 Valeurs de C pour l'état $X_{[i:j:k]}|\psi_{(0,2,1,3,1,3,2,4)}\rangle$, avec $k \neq 2$

$[i:j:k]$	$X_{[i:j:k]}\|\psi_{(0,2,1,3,1,3,2,4)}\rangle$	$C(x_0,x_1,y_0,y_1,z_0,z_1)$
$[0:2:1]$	$\|\psi_{(0,2,3,3,4,2,1,1)}\rangle$	$\frac{1}{8}\left((1+\mathrm{i})x_0y_0z_0 + (1+\mathrm{i})x_0y_0z_1 + (1-\mathrm{i})x_1y_0z_0 + (1-\mathrm{i})x_1y_0z_1\right)$
$[1:2:0]$	$\|\psi_{(0,2,1,3,1,3,2,4)}\rangle$	$\frac{1}{8}\left((1+\mathrm{i})x_0y_0z_0 + (1+\mathrm{i})x_0y_0z_1 + (1-\mathrm{i})x_0y_1z_0 + (1-\mathrm{i})x_0y_1z_1\right)$
$[2:0:1]$	$\|\psi_{(0,4,2,2,3,1,3,1)}\rangle$	$\frac{1}{8}\left((1+\mathrm{i})x_0y_0z_0 + (1-\mathrm{i})x_0y_0z_1 + (1+\mathrm{i})x_0y_1z_0 + (1-\mathrm{i})x_0y_1z_1\right)$
$[2:1:0]$	$\|\psi_{(0,4,3,1,2,2,3,1)}\rangle$	$\frac{1}{8}\left((1+\mathrm{i})x_0y_0z_0 + (1-\mathrm{i})x_0y_0z_1 + (1+\mathrm{i})x_1y_0z_0 + (1-\mathrm{i})x_1y_0z_1\right)$

Remarque 5.8. Le calcul de Δ_3 et C pour l'état $X_{[i:j:k]}(T\otimes T\otimes P)H^{\otimes 3}|000\rangle$ avec $k = 2$ donne $\Delta_3 \neq 0$ et $C \neq 0$. Donc, dans ce cas, cet état est équivalent à $|GHZ_3\rangle$.

Figure 5.2 Un circuit de $\langle CNOT\rangle_3$ générant un état SLOCC-équivalent à $|W_3\rangle$.



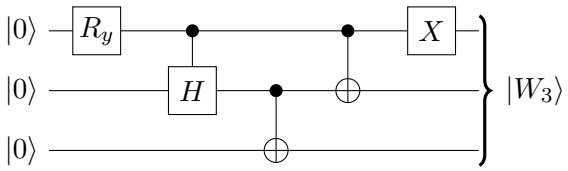
L'état en sortie est :
$|\psi_{(0,2,3,3,4,2,1,1)}\rangle = X_{[0:2:1]}|\psi_{(0,2,1,3,1,3,2,4)}\rangle = X_{[0:2]}X_{[1:0]}X_{[2:1]}(T\otimes T\otimes P)H^{\otimes 3}|000\rangle$.

Remarque 5.9. La dimension de l'espace de Hilbert $\mathcal{H}^{\otimes 3}$ étant seulement 8, il est encore possible de calculer des matrices A, B, C de dimension 2×2 et de déterminant égal à 1 ainsi qu'un nombre complexe a tels que $(A\otimes B\otimes C)|\psi_{(0,2,3,3,4,2,1,1)}\rangle = a|W_3\rangle$. Cela peut être fait en résolvant un système de 8 équations algébriques grâce à un logiciel de calcul formel. Nous vérifions que les matrices $A = \begin{bmatrix} 3\mathrm{i} & 1 \\ \frac{1}{2} & -\frac{1}{2}\mathrm{i}\end{bmatrix}$, $B = 2^{\frac{1}{4}}\begin{bmatrix} -\mathrm{i}\sqrt{2} & 2 \\ 0 & \frac{1}{2}\mathrm{i}\end{bmatrix}$, $C = \begin{bmatrix} \mathrm{i} & \mathrm{i} \\ \frac{1}{2}\mathrm{i} & -\frac{1}{2}\mathrm{i}\end{bmatrix}$ et le complexe $a = 2^{\frac{1}{4}}\frac{\sqrt{3}}{\sqrt{2}}\mathrm{e}^{\frac{\mathrm{i}\pi}{4}}$ constituent une solution possible du système.

Les résultats de cette section sont résumés par le théorème suivant.

Théorème 5.10. *Un circuit de portes CNOT agissant sur un état complètement factorisé de* 3 *qubits peut produire tous les types d'état intriqués dans la classification de l'intrication par l'action du groupe* $\mathrm{G}_{\mathrm{SLOCC}}$.

Figure 5.3 Circuit quantique produisant l'état $|W_3\rangle$. L'angle de la rotation est égal à $2\cos^{-1}(\frac{1}{\sqrt{3}})$.



5.2.2 Implantation d'états SLOCC-équivalents à $|W_3\rangle$

Dans un article publié en 2020 [157], Pérez-Salinas *et al.* montrent que tout état $|\psi\rangle$ de 3 qubits est LU-équivalent, à une phase près, à un état sous la forme suivante, appelée forme canonique :

$$|\tilde{\psi}\rangle = \lambda_0 |000\rangle + \lambda_1 e^{i\varphi_1} |100\rangle + \lambda_2 e^{i\varphi_2} |101\rangle + \lambda_3 e^{i\varphi_3} |110\rangle + \lambda_4 e^{i\varphi_4} |111\rangle , \qquad (5.44)$$

avec $\lambda_i \in \mathbb{R}$. Selon ces chercheurs, l'intérêt de cette forme canonique est de permettre de calculer expérimentalement une valeur approchée de $|\Delta_3|$ pour un état $|\psi\rangle$ donné. En effet, $|\Delta_3(|\psi\rangle)| = |\Delta_3(|\tilde{\psi}\rangle)|$ car les états $|\psi\rangle$ et $|\tilde{\psi}\rangle$ sont LU-équivalents. L'application de la formule (5.16) permettant de calculer Δ_3 donne $\Delta_3(|\tilde{\psi}\rangle) = (e^{i\varphi_4}\lambda_0\lambda_4)^2$. Ainsi la valeur de $|\Delta_3(|\psi\rangle)|$ est donnée par le produit $P_{000}P_{111}$, avec P_{ijk} la probabilité d'obtenir ijk lors de la mesure du système dans la base standard.

Soit $|\psi\rangle$ un état SLOCC équivalent à $|W_3\rangle$. D'après la classification de l'intrication des états de trois qubits résumée dans la table 5.2, l'hyperdéterminant doit s'annuler pour $|\psi\rangle$. Ainsi, en mettant cet état sous forme canonique et en mesurant les qubits dans la base standard, on devrait trouver théoriquement un produit $P_{000}P_{111}$ égal à zéro. Cependant, quand on implante un circuit produisant théoriquement $|\psi\rangle$ dans un ordinateur quantique expérimental, il est très probable, en raison du bruit dans le circuit, que l'état en sortie ne soit pas exactement l'état $|\psi\rangle$. Ainsi le produit $P_{000}P_{111}$ mesuré dans le circuit ne sera sans doute pas nul comme le prévoit la théorie. Pour illustrer cet effet du bruit, nous avons mis les états $|W_3\rangle$ et $|\psi_{(0,2,3,3,4,2,1,1)}\rangle$ (figure 5.2) sous forme canonique, puis nous avons implémenté les circuits correspondant dans l'ordinateur quantique ibmq-quito [3].

Il est facile de vérifier que l'état $|W_3\rangle$ peut être produit par le circuit quantique de la figure 5.3. Dans ce circuit, l'angle θ de la rotation autour de l'axe $\hat{y}$ est égal à $2\cos^{-1}(\frac{1}{\sqrt{3}})$ et la matrice de rotation est donc :

$$R_y(\theta) = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & -\sqrt{2} \\ \sqrt{2} & 1 \end{bmatrix}.$$

Nous observons que pour mettre $|W_3\rangle$ sous la forme (5.44), il suffit de retirer la porte *NOT* à la fin de ce circuit. On pose :

$$|\tilde{\psi}_1\rangle = X_0 |W_3\rangle = \frac{1}{\sqrt{3}}(|000\rangle + |101\rangle + |110\rangle). \qquad (5.45)$$

Soit un opérateur unitaire générique $U(\vec{\theta})$ défini par

$$U(\vec{\theta}) = \begin{bmatrix} \cos(\theta_0/2) & -e^{i\theta_1}\sin(\theta_0/2) \\ e^{i\theta_2}\sin(\theta_0/2) & e^{i(\theta_1+\theta_2)}\cos(\theta_0/2) \end{bmatrix} \tag{5.46}$$

avec $\vec{\theta}$ le triplet de réels $(\theta_0, \theta_1, \theta_2)$. Pour mettre $|\psi_{(0,2,3,3,4,2,1,1)}\rangle$ en forme canonique, on détermine $\vec{\theta}_A, \vec{\theta}_B$ et $\vec{\theta}_C$ tels que $|\tilde{\psi}\rangle = (U(\vec{\theta}_A) \otimes U(\vec{\theta}_B) \otimes U(\vec{\theta}_C)) |\psi\rangle$ soit sous la forme (5.44) à une phase près. A l'aide d'un système de calcul formel, on obtient

$$U(\vec{\theta}_A) = R_x(\pi/2) = \begin{bmatrix} \frac{\sqrt{2}}{2} & -i\frac{\sqrt{2}}{2} \\ -i\frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2} \end{bmatrix}, \quad U(\vec{\theta}_B) = I, \quad U(\vec{\theta}_C) = H,$$

et

$$|\tilde{\psi}_2\rangle = (R_x(\pi/2) \otimes I \otimes H) |\psi_{(0,2,3,3,4,2,1,1)}\rangle = e^{i\frac{\pi}{4}} \left(\frac{1}{2}|000\rangle - \frac{1}{2}|101\rangle + \frac{\sqrt{2}}{2}|110\rangle \right). \tag{5.47}$$

On obtient ainsi un nouvel état équivalent à $|W_3\rangle$ qui s'écrit comme superposition de seulement trois états de base.

Les deux histogrammes de la figure 5.4 montrent clairement un bruit non négligeable dans les deux circuits, avec l'apparition de certaines mesures qu'on ne devrait pas obtenir en théorie. En particulier, le produit $P_{000}P_{111}$ n'est pas nul et on obtient, après 2000 mesures, les résultats suivants.

- Pour l'état $|\tilde{\psi}_1\rangle$ (premier circuit) :

$$P_{000} \simeq 634/2000, \qquad P_{111} \simeq 51/2000, \qquad P_{000}P_{111} \simeq 0{,}008\,083\,5$$

- Pour l'état $|\tilde{\psi}_2\rangle$ (deuxième circuit) :

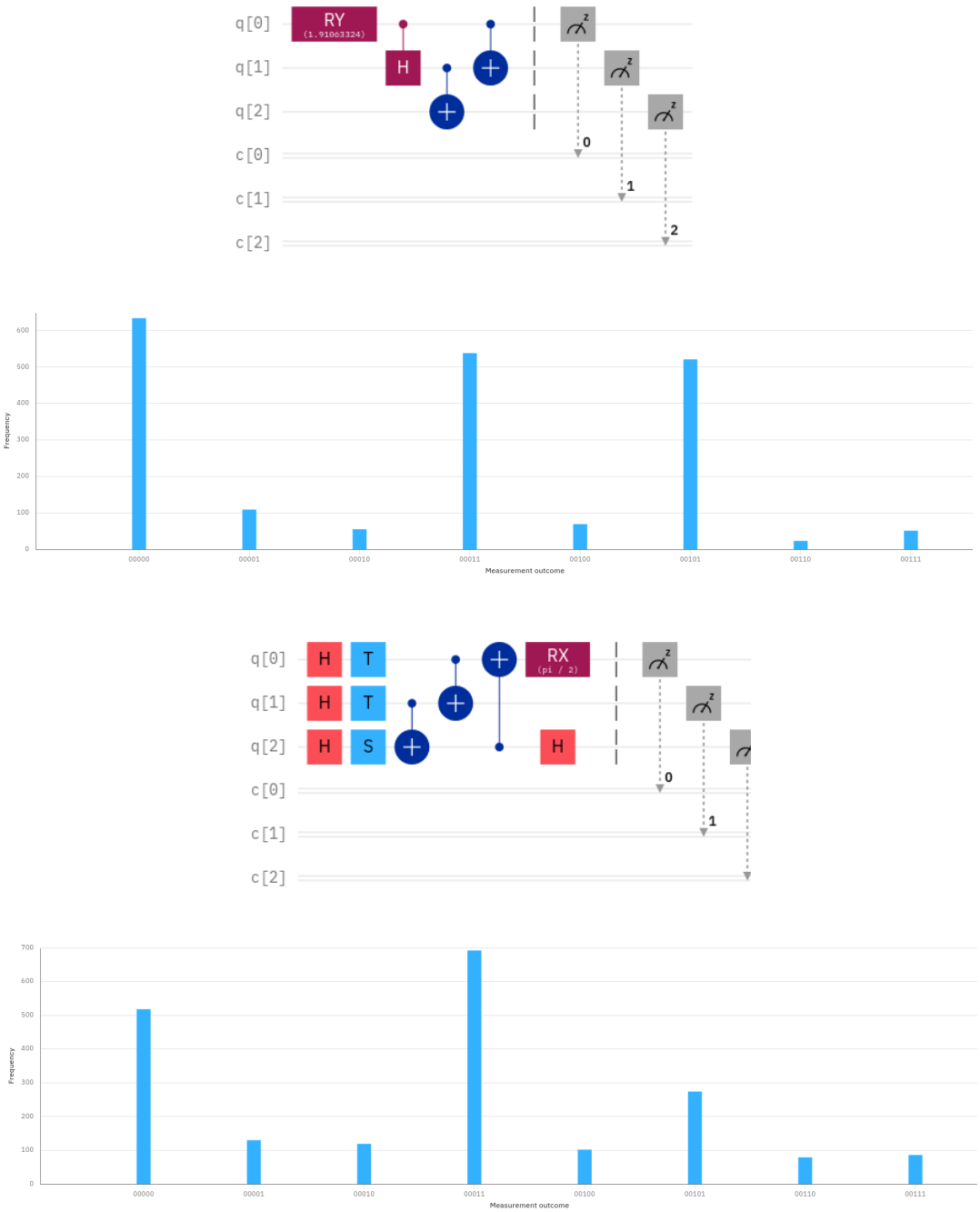
$$P_{000} \simeq 518/2000, \qquad P_{111} \simeq 86/2000, \qquad P_{000}P_{111} \simeq 0{,}011\,137.$$

Ces exemples suggèrent que, dans l'ère NISQ, il peut être difficile de produire de façon fiable un état du type $|W_3\rangle$ dans un ordinateur quantique, même quand cet état est créé par un circuit de longueur très modérée. D'un point de vue algébrique, ce n'est pas étonnant : l'ensemble des états génériquement intriqués (*i.e.* n'annulant pas Δ_3) est dense dans l'espace de Hilbert, alors que l'état $|W_3\rangle$ appartient à l'hypersurface définie par l'annulation de Δ_3. Ainsi, une petite variation des amplitudes complexes engendrée par les erreurs sur les portes donne un état qui n'annule plus l'hyperdéterminant.

5.2.3 Le groupe $\langle CNOT \rangle_4$ et les états intriqués de 4 qubits

Nous avons déjà rappelé au début de la section 5.1.3 quelques outils mathématiques permettant une classification des états d'un système de 4 qubits basée sur l'action du groupe G_{SLOCC}. Nous utilisons ici ces outils dans la recherche de deux types d'états intriqués d'un système de 4 qubits : les états génériquement intriqués et les états SLOCC équivalents à $|W_4\rangle$.

Figure 5.4 Circuits implémentant deux états SLOCC-équivalents à $|W_3\rangle$ dans l'ordinateur quantique ibmq-quito. Le premier circuit produit l'état $|\tilde{\psi}_1\rangle$ (5.45) et le second l'état $|\tilde{\psi}_2\rangle$ (5.47) (dans ce dernier circuit l'opérateur de changement de phase P est désigné par S). Notez que l'état de base $|b_0b_1b_2\rangle$ est noté $00b_2b_1b_0$ sur les histogrammes.



État génériquement intriqué de 4 qubits

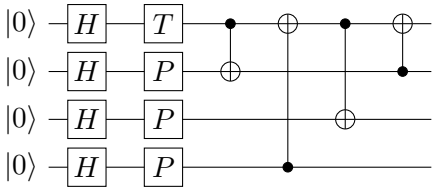
Dans [141], Miyake définit un état intriqué générique d'un système de n qubits comme état un état $|\psi\rangle$ tel que $\Delta_n(|\psi\rangle) \neq 0$. Dans le cas d'un système de 3 qubits, il est bien connu que $\Delta_3(|GHZ_3\rangle) \neq 0$ (voir table 5.2). En utilisant la formule (5.16) on vérifie facilement que $\Delta_3(|GHZ_3\rangle) = \frac{1}{4}$. Ainsi l'état $|GHZ_3\rangle$ est un état génériquement intriqué au sens de Miyake. L'état $|GHZ_4\rangle$ est l'état de la famille G_{abcd} tel que $a = d = \frac{1}{\sqrt{2}}$ et $b = c = 0$ (voir équation (5.23)). Il s'agit donc d'un état dégénéré du type G_{a000} et $\Delta_4(|GHZ_4\rangle) = 0$ (voir formule (5.39)). Ainsi, contrairement à ce qu'on pourrait attendre, le résultat pour trois qubits concernant le type d'intrication de l'état GHZ ne s'étend pas à 4 qubits puisque $|GHZ_4\rangle$ n'est pas génériquement intriqué. On peut même généraliser ce résultat et nous montrons dans l'annexe D que $\Delta(|GHZ_n\rangle) = 0$, pour tout $n > 3$.

Au chapitre 1, nous avons remarqué que l'état $|GHZ_4\rangle$ se construisait très simplement en faisant agir un circuit de $\langle CNOT\rangle_4$ sur un état complètement factorisé de $\mathcal{H}^{\otimes 4}$ (voir figure 1.6). Nous nous demandons maintenant si ce type de circuit est assez puissant pour créer un état génériquement intriqué. La proposition suivante répond à cette question.

Proposition 5.11. *Un circuit de portes CNOT agissant sur un état complètement factorisé de 4 qubits peut produire de l'intrication générique. L'état*

$$|GE\rangle = X_{[0:1]}X_{[2:0]}X_{[0:3]}X_{[1:0]}(T \otimes P \otimes P \otimes P)H^{\otimes 4}\,|0000\rangle \tag{5.48}$$

est génériquement intriqué. Il est produit par le circuit ci-dessous.



Démonstration. En utilisant la formule (5.34) on obtient $\Delta(|GE\rangle) = -\dfrac{1}{2^{24}} \simeq -5.96 \times 10^{-8}$. □

État intriqué de 4 qubits équivalent à $|W_4\rangle$

Nous examinons maintenant s'il est possible d'obtenir un état équivalent à $|W_4\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$ quand un circuit de portes *CNOT* agit sur un état complètement factorisé. L'orbite SLOCC de $|W_4\rangle$ appartient au cône nilpotent qui est la variété algébrique définie par l'annulation de tous les invariants (*i.e.* $B(|\psi\rangle) = L(|\psi\rangle) = M(|\psi\rangle) = D_{xy}(|\psi\rangle) = 0$, voir section 5.1.3). Le cône nilpotent contient exactement 31 orbites et l'orbite de $|W_4\rangle$ est caractérisée, à l'intérieur du cône nilpotent, par un vecteur de 8 bits résultant de l'évaluation des 8 polynômes covariants $A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F$ et P_L dont la définition est donnée en annexe C.

Soit $V = [P_1, \ldots, P_m]$ un vecteur de polynômes covariants, on rappelle que pour tout état $|\psi\rangle$, la notation $V[|\psi\rangle]$ désigne le vecteur de bits $[[P_1(|\psi\rangle)], \ldots, [P_m(|\psi\rangle)]]$, avec $[P_i(|\psi\rangle)] = 0$ si $P_i(|\psi\rangle) = 0$ et $[P_i(|\psi\rangle)] = 1$ si $P_i(|\psi\rangle) \neq 0$. Le critère suivant est une conséquence directe des résultats de [101, section III].

Lemme 5.12. *Soient* $V_1 = [B, L, M, D_{xy}]$ *et* $V_2 = [A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F, P_L]$. *Un état de 4 qubits* $|\psi\rangle$ *est dans l'orbite SLOCC de* $|W_4\rangle$ *si et seulement si*

$$V_1[|\psi\rangle] = [0,0,0,0] \text{ et } V_2[|\psi\rangle] = [1,1,1,1,0,0,0,0]. \tag{5.49}$$

En utilisant ce lemme, on peut répondre à notre question initiale.

Proposition 5.13. *L'orbite SLOCC de* $|W_4\rangle$ *ne peut pas être atteinte par un circuit de* $\langle CNOT\rangle_4$ *agissant sur un état complètement factorisé.*

Démonstration. Soit un état complètement factorisé de 4 qubits

$$|F(u)\rangle = (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \otimes (c_0|0\rangle + c_1|1\rangle) \otimes (d_0|0\rangle + d_1|1\rangle),$$

avec $u = [a_0, a_1, b_0, b_1, c_0, c_1, d_0, d_1]$ un vecteur de nombres complexes. Pour tout circuit $C \in \langle CNOT\rangle_4$, on montre que l'état $|\psi(u)\rangle = C|F(u)\rangle$ ne peut pas être dans l'orbite de $|W_4\rangle$. L'algorithme est le suivant. Pour chaque C dans $\langle CNOT\rangle_4$ (20 160 cas), on résout le système

$$B(|\psi(u)\rangle) = L(|\psi(u)\rangle) = M(|\psi(u)\rangle) = D_{xy}(|\psi(u)\rangle) = 0.$$

Les solutions sont des vecteurs de $\mathcal{H}^{\otimes 4}$: $|\psi_1(u)\rangle, \ldots, |\psi_m(u)\rangle$. Pour chaque solution $|\psi_i(u)\rangle$, on résout le système

$$P_D^1(|\psi_i(u)\rangle) = P_D^2(|\psi_i(u)\rangle = P_F(|\psi_i(u)\rangle) = P_L(|\psi_i(u)\rangle = 0,$$

et pour chaque solution $|\psi_{ij}(u)\rangle$, on calcule P_C^2 : on vérifie que le polynôme $P_C^2(|\psi_{ij}(u)\rangle)$ est nul pour tout u, C, i, j. On déduit du lemme 5.12 que $|\psi(u)\rangle$ n'est pas SLOCC-équivalent à $|W_4\rangle$. Le script Maple qui implante cet algorithme est disponible à l'adresse [164] et le temps de calcul est de plusieurs heures sur un PC de base. □

5.3 États maximalement intriqués de 4 qubits

5.3.1 Position du problème et résultats précédents

Selon Miyake [143, 141], les états génériquement intriqués sont ceux qui n'annulent pas l'hyperdéterminant et la valeur de $|\Delta_n|$ est une façon de quantifier cette intrication générique. Dans le cas de 4 qubits, l'hyperdéterminant Δ_4 est un énorme polynôme homogène de degré 24 en 16 variables qui comporte 2 894 276 termes et possède une structure géométrique reliée aux triangulations du 4-cube [104]. Malgré sa taille, il est encore maniable par un système de calcul formel. Depuis la formule donnée par Schläfli en 1852 (voir à ce propos [83, section 14.4]), d'autres méthodes ont été développées pour le calculer, notamment une expression de Δ_4 en termes de polynômes SLOCC-invariants de plus petits degrés (5.34) donnée par Luque et Thibon dans [133]. Dans un autre registre, on peut également citer une évaluation de Δ_4 basée sur des réseaux de neurones (Jaffali et Oeding [108]).

En s'inspirant des idées de Miyake, Gour et Wallach considèrent dans [91] qu'un état de 4 qubits ayant la plus grande quantité d'intrication est un état qui rend maximal le module de Δ_4. Bien entendu, il existe d'autres mesures de l'intrication et donc différentes notions d'états maximalement intriqués (voir par exemple [90]). Pour une introduction pédagogique sur ce sujet, nous suggérons la consultation des sections 2.2.3 et 6.1.1 de la

thèse de Jaffali [106]. Dans ce qui suit le terme *état maximalement intriqué* fait référence à un état de 4 qubits qui maximise $|\Delta_4|$.

Dans leur papier [91, section IV], Gour and Wallach conjecturent que l'état $|L\rangle$ (voir figure 5.5) est le seul état maximalement intriqué à une opération locale unitaire près. Un an plus tard, cette conjecture est prouvée par Chen et Djokovic dans [50] qui montrent que la valeur maximale de $|\Delta_4|$ est $\frac{1}{2^8 3^9} = \frac{1}{5\,038\,848} \simeq 1.98 \times 10^{-7}$. Comme Δ_4 est invariant par l'action de $\mathrm{G}'_{\mathrm{SLOCC}}$, ce résultat implique que l'orbite SLOCC de $|L\rangle$ est confondue avec son orbite LU (sur les polynômes LU-invariants, voir par exemple [131]). L'état $|L\rangle$ possède également la propriété d'être l'unique état, à une opération locale unitaire près, qui maximalise l'α-entropie de Tsallis [172] (une autre mesure de l'intrication), pour $\alpha > 2$ [90]. On peut également mentionner deux autres états maximalement intriqués, qui ont la propriété d'avoir des coordonnées réelles (voir figure 5.5) : l'état $|\Phi_5\rangle$ (reporté d'abord par Osterloh et Siewert [151] puis par Alsina dans sa thèse [4] sous le nom d'état $|HD\rangle$) ainsi que l'état $|M_{2222}\rangle$ (découvert par Jaffali [106]).

Figure 5.5 Quelques états de 4-qubits pour lesquels $|\Delta_4|$ est maximal.

$$|L\rangle = \frac{1}{\sqrt{3}}(|u_0\rangle + \omega\,|u_1\rangle + \omega^*\,|u_2\rangle) \tag{5.50}$$

avec : $\omega = \mathrm{e}^{\frac{\mathrm{i}\pi}{3}}$

$|u_0\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle) = |\Phi^+\rangle\,|\Phi^+\rangle$
$|u_1\rangle = \frac{1}{2}(|0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle) = |\Phi^-\rangle\,|\Phi^-\rangle$
$|u_2\rangle = \frac{1}{2}(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle) = |\Psi^+\rangle\,|\Psi^+\rangle$
$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$

$$|\Phi_5\rangle = \frac{1}{\sqrt{6}}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle + \sqrt{2}\,|1111\rangle) \tag{5.51}$$

$$|M_{2222}\rangle = \frac{1}{\sqrt{8}}\,|v_1\rangle + \frac{\sqrt{6}}{4}\,|v_2\rangle + \frac{1}{\sqrt{2}}\,|v_3\rangle \tag{5.52}$$

avec : $|v_1\rangle = \frac{1}{\sqrt{6}}(|0000\rangle + |0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle + |1111\rangle)$
$|v_2\rangle = \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)$
$|v_3\rangle = \frac{1}{\sqrt{8}}(-|0001\rangle + |0010\rangle - |0100\rangle + |0111\rangle + |1000\rangle - |1011\rangle + |1101\rangle - |1110\rangle)$

Bien que les états maximalement intriqués soient considérés comme une ressource physique importante en théorie de l'information quantique (voir à ce propos l'introduction de [50]), nous constatons qu'il n'existe pas, à notre connaissance, de proposition de circuits quantiques destinés à produire les états maximalement intriqués de la figure 5.5.

Pour l'état $|GE\rangle$ (5.48), on a $\Delta_4(|GE\rangle) \simeq -5.96 \times 10^{-8}$, ce qui est une quantité d'intrication non maximale, bien que nettement supérieure à la moyenne qui est d'environ 1.32×10^{-9} (valeur basée sur 10000 états aléatoires, mentionnée dans [4]). Nous nous sommes donc demandés s'il était possible de produire de l'intrication maximale dans les mêmes conditions (un circuit de portes $CNOT$ agissant sur un état factorisé), en choisissant bien l'état factorisé de départ. La réponse s'est avérée affirmative et nous allons décrire dans ce qui suit une famille de circuits de $\langle CNOT\rangle_4$ qui permet d'atteindre un niveau maximal d'intrication.

Ce travail est accompagné d'un module Python [55] qui fait largement appel aux fonctionnalités du module SymPy, un système de calcul formel en Python. Il fournit une

implantation des différents algorithmes, états et portes quantiques utilisés. La preuve de certaines propositions reposant essentiellement sur des calculs basiques d'algèbre linéaire, nous avons choisi dans ce cas de renvoyer le lecteur vers la fonction du module qui effectue les vérifications nécessaires, plutôt que de l'ennuyer avec des calculs de peu d'intérêt.

5.3.2 Quelques identités utiles entre opérateurs unitaires

Si deux vecteurs normalisés $|\psi\rangle$ et $|\psi'\rangle$ de l'espace de Hilbert sont égaux à une phase globale près, alors ils représentent le même état physique du système et nous écrivons dans ce cas $|\psi\rangle \simeq |\psi'\rangle$. Dans le même ordre d'idée, nous écrivons $U \simeq U'$ pour deux opérateurs unitaires U et U' tels que $U' = \mathrm{e}^{\mathrm{i}\varphi}U$ pour une certaine phase φ. En utilisant cette notation, on a les relations suivantes entre les opérateurs unitaires classiques :

$$R_z(\pi) \simeq Z,\ R_z(\pi/2) \simeq P,\ R_z(-\pi/2) \simeq P^\dagger,\ R_z(\pi/4) \simeq T \tag{5.53}$$

$$R_y(\pi) \simeq Y,\ R_y(\pi/2) = HZ = XH,\ R_y(-\pi/2) = ZH = HX \tag{5.54}$$

On rappelle qu'on désigne une permutation de $\mathfrak{S}_n$ et la matrice de permutation correspondante dans $\mathrm{GL}_n(\mathbb{F}_2)$ par le même symbole σ. On rappelle également que, si U désigne un opérateur unitaire agissant sur un qubit (donc un opérateur de $\mathcal{H}$) et si $v = [v_0 \dots v_{n-1}]^{\mathrm{t}}$ est un vecteur de $\mathbb{F}_2^n$, alors U_v désigne le produit $\prod_{i=0}^{n-1} U_i^{v_i}$, où U_i est l'opérateur unitaire de $\mathcal{H}^{\otimes n}$ correspondant à l'action de U sur le qubit i. Dans les développements de cette section, on utilisera à plusieurs reprises le résultat suivant.

Proposition 5.14. *Soit U un opérateur unitaire agissant sur un qubit, soit σ une permutation de $\mathfrak{S}_n$ et soit v un vecteur de $\mathbb{F}_2^n$. On a l'identité suivante :*

$$S_\sigma U_v S_\sigma^{-1} = U_{\sigma v} \tag{5.55}$$

Démonstration. L'identité $S_{(i\ j)}U_iS_{(i\ j)} = U_j$ (1.76) se généralise en $S_\sigma U_i S_{\sigma^{-1}} = U_{\sigma(i)}$. On a donc :

$$S_\sigma U_v S_{\sigma^{-1}} = S_\sigma \prod_{i=0}^{n-1} U_i^{v_i} S_{\sigma^{-1}} = \prod_{i=0}^{n-1} U_{\sigma(i)}^{v_i}.$$

Les facteurs du produit $\prod_{i=0}^{n-1} U_{\sigma(i)}^{v_i}$ commutent entre eux, donc en les réordonnant on a :

$$S_\sigma U_v S_{\sigma^{-1}} = \prod_{i=0}^{n-1} U_i^{v_{\sigma^{-1}(i)}}.$$

Comme $\sigma v = [v_{\sigma^{-1}(0)} \dots v_{\sigma^{-1}(n-1)}]^{\mathrm{t}}$, on en déduit l'identité (5.55). □

5.3.3 Méthodologie utilisée dans l'exploration numérique

Nous abordons ici le problème suivant : est-il possible d'obtenir un état maximalement intriqué en faisant agir un circuit quantique du groupe $\langle CNOT\rangle_4$ sur un état de l'orbite LU de $|0000\rangle$?

Nous utilisons la décomposition classique Z-Y d'un opérateur unitaire agissant sur un qubit (voir chapitre 1, section 1.2).

$$\mathrm{e}^{\mathrm{i}\varphi} R_z(\alpha) R_y(\beta) R_z(\alpha') \tag{5.56}$$

En utilisant cette décomposition, tout opérateur unitaire U de $\mathcal{H}^{\otimes 4}$ complètement factorisé (*i.e.* $U = V_0 \otimes V_1 \otimes V_2 \otimes V_3$) dépend, à une phase près, des 12 paramètres réels de la matrice

$$\mathcal{P} = \begin{bmatrix} \alpha_0 & \beta_0 & \alpha'_0 \\ \alpha_1 & \beta_1 & \alpha'_1 \\ \alpha_2 & \beta_2 & \alpha'_2 \\ \alpha_3 & \beta_3 & \alpha'_3 \end{bmatrix}. \tag{5.57}$$

Définissons l'opérateur unitaire $U(\mathcal{P})$ par :

$$\begin{aligned} U(\mathcal{P}) = R_z(\alpha_0)R_y(\beta_0)R_z(\alpha'_0) \otimes R_z(\alpha_1)R_y(\beta_1)R_z(\alpha'_1) \\ \otimes R_z(\alpha_2)R_y(\beta_2)R_z(\alpha'_2) \otimes R_z(\alpha_3)R_y(\beta_3)R_z(\alpha'_3). \end{aligned} \tag{5.58}$$

Comme une rotation autour de l'axe $\hat{z}$ appliquée à un qubit dans l'état $|0\rangle$ est un simple changement de phase, il est possible d'écrire n'importe quel état de l'orbite LU de $|0000\rangle$ (à une phase globale près) en utilisant seulement deux paramètres réels α et β par qubit. Ainsi, tout état de cette orbite est égal (à une phase globale près) à un état $|\mathcal{P}\rangle$ défini par :

$$|\mathcal{P}\rangle = R_z(\alpha_0)R_y(\beta_0) \otimes R_z(\alpha_1)R_y(\beta_1) \otimes R_z(\alpha_2)R_y(\beta_2) \otimes R_z(\alpha_3)R_y(\beta_3) \,|0000\rangle\,. \tag{5.59}$$

En utilisant les définitions des matrices de rotation autour des axes $\hat{z}$ et $\hat{y}$ (voir table 1.1), on obtient :

$$|\mathcal{P}\rangle = (a_0\,|0\rangle + a_1\,|1\rangle) \otimes (b_0\,|0\rangle + b_1\,|1\rangle) \otimes (c_0\,|0\rangle + c_1\,|1\rangle) \otimes (d_0\,|0\rangle + d_1\,|1\rangle), \tag{5.60}$$

$$\begin{aligned} \text{avec } (a_0, a_1) &= (\mathrm{e}^{-\mathrm{i}\alpha_0/2}\cos\frac{\beta_0}{2}, \mathrm{e}^{\mathrm{i}\alpha_0/2}\sin\frac{\beta_0}{2}), \\ (b_0, b_1) &= (\mathrm{e}^{-\mathrm{i}\alpha_1/2}\cos\frac{\beta_1}{2}, \mathrm{e}^{\mathrm{i}\alpha_1/2}\sin\frac{\beta_1}{2}), \\ (c_0, c_1) &= (\mathrm{e}^{-\mathrm{i}\alpha_2/2}\cos\frac{\beta_2}{2}, \mathrm{e}^{\mathrm{i}\alpha_2/2}\sin\frac{\beta_2}{2}), \\ (d_0, d_1) &= (\mathrm{e}^{-\mathrm{i}\alpha_3/2}\cos\frac{\beta_3}{2}, \mathrm{e}^{\mathrm{i}\alpha_3/2}\sin\frac{\beta_3}{2}). \end{aligned}$$

Tout état résultant de l'action d'un opérateur unitaire de $\langle CNOT\rangle_4$ sur un état de l'orbite LU de $|0000\rangle$ peut donc s'écrire, à une phase globale près, sous la forme

$$|A, \mathcal{P}\rangle = X_A\,|\mathcal{P}\rangle\,, \tag{5.61}$$

avec A une matrice de $\mathrm{GL}_4(\mathbb{F}_2)$ et $\mathcal{P}$ une matrice de paramètres.

Afin de déterminer les états du type $|A, \mathcal{P}\rangle$ capables de maximiser $|\Delta_4|$, on peut se limiter à considérer uniquement les classes à droite suivant le sous-groupe de $\langle CNOT\rangle_4$ engendré par les portes $SWAP$ (groupe $\langle SWAP\rangle_4 \simeq \mathfrak{S}_4$, voir section 2.1.1). En effet, $|\Delta_4|$ est invariant par permutation des qubits, *i.e.* $|\Delta_4(X_A\,|\mathcal{P}\rangle)| = |\Delta_4(S_\sigma X_A\,|\mathcal{P}\rangle)|$ pour toute permutation $\sigma \in \mathfrak{S}_4$. L'ordre du groupe $\langle CNOT\rangle_4$ étant 20 160 (identité (2.31)), le nombre de classes est égal à $20\,160/24 = 840$. Nous calculons pour chaque classe un représentant de longueur optimale en les générateurs $X_{[i:j]}$ (fonction `right_cosets_perm_GL4` du module Python).

Le calcul de Δ_4 pour un état donné est réalisé en utilisant l'algorithme proposé par Luque et Thibon dans [133, section IV] (fonction `hyper_det` du module Python).

Après avoir éliminé toutes les classes pour lesquelles $\Delta_4(|A,\mathcal{P}\rangle)$ s'annule pour toute matrice de paramètres $\mathcal{P}$, nous obtenons une liste de 333 représentants (fonction `non_zero_HD_strings` du module Python). Pour chacun de ces représentants, nous utilisons une marche aléatoire sur l'espace de recherche défini par les 8 paramètres α_i et β_i (pour $i = 0 \ldots 3$) afin de maximiser la valeur de $|\Delta_4(|A,\mathcal{P}\rangle)|$ (fonction `search_max_HD` du module Python). L'algorithme de marche aléatoire est une heuristique d'optimisation numérique qui a déjà été utilisée par Jaffali à propos de l'hyperdéterminant [106, p.156] ou par Amouzou *et al.* [6] dans des recherches sur les états d'hypergraphes de 4 qubits (hypergraph states). Nous le rappelons ci-dessous (algorithme 5.1).

Algorithme 5.1 MARCHE-ALEATOIRE(Δ)

Entrée : Une fonction $\Delta(p)$ à maximiser
Sortie : Un vecteur p de paramètres pouvant éventuellement maximiser Δ

choisir une ampitude minimale $a_{\min}$
choisir une amplitude initiale $a > a_{\min}$
choisir un nombre maximal d'itérations $c_{\max}$
générer aléatoirement un vecteur p de paramètres initiaux.
tant que $a > a_{\min}$ **faire**
    compteur $\leftarrow 0$
    meilleur $\leftarrow$ `False`
    tant que *compteur* $< c_{\max}$ **et** *meilleur* $=$ `False` **faire**
        compteur $\leftarrow$ *compteur* $+ 1$
        générer aléatoirement un vecteur de descente d
        calculer les nouveaux paramètres : $p' \leftarrow p + a * d$
        si $\Delta(p') > \Delta(p)$ **alors**
            $p \leftarrow p'$
            meilleur $\leftarrow$ `True`
        fin si
    fin tant que
    si *meilleur* $=$ `False` **alors**
        $a \leftarrow a/2$
    fin si
fin tant que
retourner p

Nous constatons qu'il est possible d'atteindre la valeur maximale de $\frac{1}{2^8 3^9}$ pour $|\Delta_4|$, avec une précision de 10^{-22}, pour exactement 12 représentants. Ces représentants sont décrits en section 5.3.5. Finalement, à partir des valeurs approchées des paramètres $\mathcal{P}$ calculés par la marche aléatoire, nous devinons des valeurs exactes possibles pour les angles α_i et β_i, puis nous vérifions (calcul exact avec SymPy) que ces valeurs exactes satisfont bien l'égalité $|\Delta_4(|A,\mathcal{P}\rangle)| = \frac{1}{2^8 3^9}$.

5.3.4 Un premier circuit de portes *CNOT* pour maximiser $|\Delta_4|$

Soient i, j, k, ℓ des entiers distincts de $\{0, 1, 2, 3\}$. Nous définissons comme suit l'opérateur unitaire $M_k^{(i,j)}$ de $\langle CNOT \rangle_4$ ainsi que $A_k^{(i,j)}$ sa matrice de bit associée dans

$\mathrm{GL}_4(\mathbb{F}_2)$ par l'isomorphisme Φ (voir théorème 2.8).

$$M_k^{(i,j)} = X_{[i:j]}X_{[j:k]}X_{[k:i]}X_{[i:\ell]}X_{[\ell:j]} \tag{5.62}$$

$$A_k^{(i,j)} = [i:j][j:k][k:i][i:\ell][\ell:j] \tag{5.63}$$

Dans cette section, nous montrons comment atteindre le maximum de $|\Delta_4|$ en utilisant l'opérateur

$$M_2^{(0,1)} = X_{[0:1]}X_{[1:2]}X_{[2:0]}X_{[0:3]}X_{[3:1]}. \tag{5.64}$$

Nous étendrons ces résultats à tout opérateur du type $M_k^{(i,j)}$ dans la section suivante.

Comme

$$A_2^{(0,1)} = [0:1][1:2][2:0][0:3][3:1] = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \tag{5.65}$$

et

$$A_3^{(0,1)} = [0:1][1:3][3:0][0:2][2:1] = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}, \tag{5.66}$$

on remarque que $A_3^{(0,1)} = (0\ 2\ 3)A_2^{(0,1)}$. Ainsi on a

$$M_3^{(0,1)} = S_{(0\ 2\ 3)}M_2^{(0,1)}, \tag{5.67}$$

ce qui implique que $M_3^{(0,1)}$ et $M_2^{(0,1)}$ représentent la même classe. Nous notons cette classe $\widehat{(0,1)}$.

Proposition 5.15. *Soient $\mathcal{P}_{\max}$ et $\mathcal{P}'_{\max}$ les deux matrices de paramètres définies par*

$$\mathcal{P}_{\max} = \begin{bmatrix} \pi/2 & \pi/2 & 0 \\ \pi/2 & \pi/2 & 0 \\ \pi/4 & \cos^{-1}\frac{\sqrt{3}}{3} & 0 \\ \pi/4 & \cos^{-1}\frac{\sqrt{3}}{3} & 0 \end{bmatrix} \quad \textit{et} \quad \mathcal{P}'_{\max} = \begin{bmatrix} \pi/2 & \pi/2 & 0 \\ \pi/2 & \pi/2 & 0 \\ 3\pi/4 & \cos^{-1}\frac{\sqrt{3}}{3} & 0 \\ 3\pi/4 & \cos^{-1}\frac{\sqrt{3}}{3} & 0 \end{bmatrix}. \tag{5.68}$$

Les états

$$|\psi_{\max}\rangle = M_2^{(0,1)}\,|\mathcal{P}_{\max}\rangle \tag{5.69}$$

et

$$|\psi'_{\max}\rangle = M_2^{(0,1)}\,|\mathcal{P}'_{\max}\rangle \tag{5.70}$$

maximisent le module de l'hyperdéterminant de 4 qubits. On a

$$\Delta_4(|\psi_{\max}\rangle) = \Delta_4(|\psi'_{\max}\rangle) = -\frac{1}{2^8 3^9}, \tag{5.71}$$

$$|\psi_{\max}\rangle = \frac{\sqrt{3}}{3}\,|w_1\rangle + \frac{3+\sqrt{3}}{6}\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\,|w_2\rangle + \frac{3-\sqrt{3}}{6}\mathrm{e}^{\mathrm{i}\frac{\pi}{4}}\,|w_3\rangle \tag{5.72}$$

et

$$|\psi'_{\max}\rangle = \frac{\sqrt{3}}{3}\,|w_1\rangle + \frac{3+\sqrt{3}}{6}\mathrm{e}^{-\mathrm{i}\frac{\pi}{4}}\,|w_2\rangle + \frac{3-\sqrt{3}}{6}\mathrm{e}^{\mathrm{i}\frac{3\pi}{4}}\,|w_3\rangle\,, \tag{5.73}$$

avec

$$|w_1\rangle = \frac{1}{\sqrt{8}}(|0001\rangle + \mathrm{i}\,|0011\rangle + |0101\rangle - \mathrm{i}\,|0111\rangle + |1000\rangle + \mathrm{i}\,|1010\rangle + |1100\rangle - \mathrm{i}\,|1110\rangle),$$
$$|w_2\rangle = \frac{1}{2}(-|0000\rangle - \mathrm{i}\,|0110\rangle - \mathrm{i}\,|1011\rangle + |1101\rangle),$$
$$|w_3\rangle = \frac{1}{2}(|0010\rangle + \mathrm{i}\,|0100\rangle - \mathrm{i}\,|1001\rangle + |1111\rangle).$$

Démonstration. Les différentes affirmations peuvent être vérifiées par le calcul en lançant la fonction `check_psi_max_is_MHS` du module Python. □

Dans notre recherche de paramètres $\mathcal{P}$ tels que $M_2^{(0,1)}|\mathcal{P}\rangle$ maximise $|\Delta_4|$, nous constatons que toutes les valeurs de $\mathcal{P}$ calculées par la marche aléatoire sont reliées à $\mathcal{P}_{\max}$ et à $\mathcal{P}'_{\max}$ par des opérations très simples sur ces matrices. Ces opérations sont décrites dans la proposition suivante et son corollaire. Ces résultats numériques suggèrent la possibilité que ces opérations appliquées aux matrices $\mathcal{P}_{\max}$ ou $\mathcal{P}'_{\max}$ soient en fait suffisantes pour décrire toutes les matrices $\mathcal{P}$ telles que $M_2^{(0,1)}|\mathcal{P}\rangle$ soit un état maximalement intriqué (conjecture 5.20).

Soit $\mathcal{P}$ une matrice de paramètres et k un entier de $\{0,1,2,3\}$. On définit les trois opérations suivantes sur $\mathcal{P}$:

- $[-\beta_k]\mathcal{P}$ est la matrice obtenue à partir de $\mathcal{P}$ en remplaçant β_k par son opposé,
- $[\alpha_k + \pi]\mathcal{P}$ est la matrice obtenue à partir de $\mathcal{P}$ en ajoutant π à α_k,
- $[-\alpha_k, -\beta_k + \pi]\mathcal{P}$ est la matrice obtenue à partir de $\mathcal{P}$ en remplaçant α_k par son opposé et β_k par $-\beta_k + \pi$.

Dans ce qui suit, on désignera l'une quelconque de ces 12 opérations par l'expression *opération élémentaire sur les paramètres.*

Proposition 5.16. *Soit $\mathcal{P}$ et $\mathcal{P}'$ deux matrices de paramètres. L'état $|\mathcal{P}'\rangle$ est dans l'orbite de $|\mathcal{P}\rangle$ sous l'action du groupe de Pauli $\mathcal{E}_4$ si et seulement si $\mathcal{P}'$ s'obtient à partir de $\mathcal{P}$ par une suite d'opérations élémentaires sur les paramètres.*

On a les identités suivantes pour tout $k \in \{0,1,2,3\}$:

$$|[-\beta_k]\mathcal{P}\rangle = Z_k\,|\mathcal{P}\rangle\,, \tag{5.74}$$
$$|[\alpha_k + \pi]\mathcal{P}\rangle = -\mathrm{i}Z_k\,|\mathcal{P}\rangle\,, \tag{5.75}$$
$$|[-\alpha_k, -\beta_k + \pi]\mathcal{P}\rangle = X_k\,|\mathcal{P}\rangle\,. \tag{5.76}$$

Démonstration. Nous prouvons seulement l'identité (5.74), les preuves des deux autres identités étant similaires. Sans perte de généralités, on suppose que $k = 0$.
D'une part, on a :

$$X_0\,|\mathcal{P}\rangle = (X(a_0\,|0\rangle + a_1\,|1\rangle)) \otimes (b_0\,|0\rangle + b_1\,|1\rangle) \otimes (c_0\,|0\rangle + c_1\,|1\rangle) \otimes (d_0\,|0\rangle + d_1\,|1\rangle)$$
$$= (a_1\,|0\rangle + a_0\,|1\rangle) \otimes (b_0\,|0\rangle + b_1\,|1\rangle) \otimes (c_0\,|0\rangle + c_1\,|1\rangle) \otimes (d_0\,|0\rangle + d_1\,|1\rangle),$$

avec $(a_0, a_1) = (\mathrm{e}^{-\mathrm{i}\alpha_0/2}\cos\frac{\beta_0}{2}, \mathrm{e}^{\mathrm{i}\alpha_0/2}\sin\frac{\beta_0}{2})$ 5.60.

D'autre part, on a :

$$|[-\alpha_0, -\beta_0+\pi]\mathcal{P}\rangle = (a'_0|0\rangle + a'_1|1\rangle)\otimes(b_0|0\rangle + b_1|1\rangle)\otimes(c_0|0\rangle + c_1|1\rangle)\otimes(d_0|0\rangle + d_1|1\rangle),$$

avec $(a'_0, a'_1) = (\mathrm{e}^{-\mathrm{i}(-\alpha_0/2)}\cos\frac{-\beta_0+\pi}{2}, \mathrm{e}^{-\mathrm{i}\alpha_0/2}\sin\frac{-\beta_0+\pi}{2}) = (a_1, a_0)$.

On en déduit que $X_0|\mathcal{P}\rangle = |[-\alpha_0, -\beta_0+\pi]\mathcal{P}\rangle$.

A partir des identités (5.75), (5.76) et de l'égalité $Y = \mathrm{i}XZ$, on obtient

$$|[-\alpha_k, -\beta_k+\pi][\alpha_k+\pi]^3\mathcal{P}\rangle = Y_k|\mathcal{P}\rangle\,.$$

On voit donc que toutes les opérations de Pauli sur l'état $|\mathcal{P}\rangle$ se traduisent par des opérations élémentaires sur les paramètres. □

Corollaire 5.17. *Soient A une matrice de $\mathrm{GL}_4(\mathbb{F}_2)$ et $\mathcal{P}$ une matrice de paramètres. Si $|\Delta_4|$ est maximal pour l'état $|A,\mathcal{P}\rangle$ alors $|\Delta_4|$ est également maximal pour tout état $|A,\mathcal{P}'\rangle$ où $\mathcal{P}'$ est obtenue à partir de $\mathcal{P}$ par une suite d'opérations élémentaires sur les paramètres.*

Démonstration. Supposons que $|\Delta_4|$ soit maximal pour l'état $|A,\mathcal{P}\rangle = X_A|\mathcal{P}\rangle$. Soit $\mathcal{P}'$ la matrice obtenue en appliquant à $\mathcal{P}$ une suite d'opérations élémentaires sur les paramètres. D'après la proposition 5.16 et la proposition 4.2, il existe deux vecteurs u et v dans $\mathbb{F}_2^4$ tels que $|\mathcal{P}'\rangle \simeq X_uZ_v|\mathcal{P}\rangle$. D'où $X_A|\mathcal{P}'\rangle \simeq X_AX_uZ_v|\mathcal{P}\rangle \simeq X_AX_uZ_vX_A^{-1}X_A|\mathcal{P}\rangle$. En utilisant l'identité (4.12), on obtient alors $|A,\mathcal{P}'\rangle \simeq X_{Au}Z_{(A^{-1})^{\mathrm{t}}v}|A,\mathcal{P}\rangle$. Par conséquent, $|A,\mathcal{P}'\rangle$ est dans l'orbite LU de $|A,\mathcal{P}\rangle$, ce qui implique que $|\Delta_4|$ est maximal pour l'état $|A,\mathcal{P}'\rangle$. □

Remarque 5.18. Nous observons que les matrices $\mathcal{P}_{\max}$ et $\mathcal{P}'_{\max}$ ne sont pas reliées par des opérations élémentaires sur les paramètres. Donc il n'existe pas d'opérateur X_uZ_v du groupe de Pauli $\mathcal{E}_4$ tel que $|\mathcal{P}'_{\max}\rangle \simeq X_uZ_v|\mathcal{P}_{\max}\rangle$. Cela implique que les états $|\psi_{\max}\rangle$ et $|\psi'_{\max}\rangle$ définissent deux orbites distinctes par l'action de $\mathcal{E}_4$.

En fait, d'après les identités (5.68) et (5.53), on voit que $|\mathcal{P}'_{\max}\rangle \simeq P_2P_3|\mathcal{P}_{\max}\rangle$. En utilisant la méthode décrite au début de la section 5.3.6, nous calculons une matrice $\mathcal{P}_{\psi\to\psi'}$ et une phase φ tels que $|\psi'_{\max}\rangle = \mathrm{e}^{\mathrm{i}\varphi}U(\mathcal{P}_{\psi\to\psi'})|\psi_{\max}\rangle$. Nous obtenons $\mathcal{P}_{\psi\to\psi'} = \begin{bmatrix} -\pi/2 & -\pi/2 & -\pi/2 \\ \pi/2 & \pi & \pi \\ 0 & \pi/2 & \pi \\ -\pi/2 & -\pi/2 & -\pi/2 \end{bmatrix}$ et $\varphi = -\frac{\pi}{3}$. Puis, par les identités (5.53) et (5.54), on obtient

$$|\psi'_{\max}\rangle = \mathrm{e}^{-\mathrm{i}\frac{7\pi}{12}}(PHP^\dagger \otimes PX \otimes H \otimes PHP^\dagger)|\psi_{\max}\rangle \tag{5.77}$$

Cette dernière égalité peut être vérifiée en utilisant la fonction `check_psi_to_psi_prime` du module Python.

Remarque 5.19. Comme $M_3^{(0,1)} = S_{(0\,2\,3)}M_2^{(0,1)}$, l'invariance de $|\Delta_4|$ par permutation des qubits montre que l'ensemble des matrices de paramètres $\mathcal{P}$ ayant leur dernière colonne nulle telles que $M_3^{(0,1)}|\mathcal{P}\rangle$ maximise $|\Delta_4|$ est égal à l'ensemble de ces même matrices $\mathcal{P}$ telles que $M_2^{(0,1)}|\mathcal{P}\rangle$ maximise $|\Delta_4|$. Nous notons cet ensemble $\mathrm{PMAX}^{(0,1)}$.

Conjecture 5.20. *Toute matrice dans $\mathrm{PMAX}^{(0,1)}$ peut être obtenue à partir de $\mathcal{P}_{\max}$ ou de $\mathcal{P}'_{\max}$ par une suite d'opérations élémentaires sur les paramètres.*

5.3.5 D'autres circuits de portes *CNOT* maximisant $|\Delta_4|$

Nous généralisons les résultats de la section précédente en décrivant d'autres circuits de portes *CNOT* qui permettent de produire un état maximalement intriqué de 4 qubits en agissant sur un état complètement factorisé. Nous conjecturons que ces circuits sont les seuls circuits de portes *CNOT* ayant cette propriété.

Proposition 5.21. *Soient i, j, k, ℓ des entiers distincts de $\{0, 1, 2, 3\}$, alors les opérateurs unitaires $M_k^{(i,j)}$ et $M_\ell^{(i,j)}$ définissent la même classe à droite suivant le sous groupe $\langle SWAP\rangle_4$ de $\langle CNOT\rangle_4$. Cette classe est notée $\widehat{(i,j)}$:*

$$\widehat{(i,j)} = \langle SWAP\rangle_4 M_k^{(i,j)} = \{S_\sigma X_{[i:j]} X_{[j:k]} X_{[k:i]} X_{[i:\ell]} X_{[\ell:j]}\} \mid \sigma \in \mathfrak{S}_4\}. \tag{5.78}$$

Démonstration. Soit σ la permutation $\begin{pmatrix} 0 & 1 & 2 & 3 \\ i & j & k & \ell \end{pmatrix}$. En utilisant l'identité (2.9), on conjugue chaque membre de l'égalité $M_3^{(0,1)} = S_{(0\,2\,3)} M_2^{(0,1)}$ (5.67) par S_σ et on obtient $M_\ell^{(i,j)} = S_{(i\,k\,\ell)} M_k^{(i,j)}$. □

Proposition 5.22. *Pour toute permutation σ de $\mathfrak{S}_4$ on a : $S_\sigma \widehat{(i,j)} S_\sigma^{-1} = \widehat{(\sigma(i), \sigma(j))}$.*

Démonstration. Par l'identité (2.9), on obtient : $S_\sigma M_k^{(i,j)} S_\sigma^{-1} = M_{\sigma(k)}^{(\sigma(i),\sigma(j))}$. On déduit le résultat annoncé de la proposition 5.21. □

On rappelle que $\overline{\sigma}$ désigne la matrice de permutation associée à la permutation σ dans laquelle les bits on été inversés (voir section 2.4). On a ainsi :

$$\overline{(0\,2\,3)} = (0\,2\,3)\overline{I}_4 = (0\,2\,3) \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

On observe que $A_2^{(0,1)} = \overline{(0\,2\,3)}[1:0]$ (voir (5.65) et proposition 2.6).

Ainsi $\widehat{(0,1)} = \langle SWAP\rangle_4 X_{\overline{I}_4} X_{[1:0]}$ et en conjuguant chaque membre de cette égalité par une permutation des qubits S_σ, on obtient : $\widehat{(\sigma(0), \sigma(1))} = \langle SWAP\rangle_4 X_{\overline{I}_4} X_{[\sigma(1):\sigma(0)]}$ (voir identité (2.50)). Ainsi, pour tout couple (i, j) d'entiers distincts, on a :

$$\widehat{(i,j)} = \langle SWAP\rangle_4 X_{\overline{I}_4} X_{[j:i]}. \tag{5.79}$$

On remarque que l'opérateur $X_{\overline{I}_4} X_{[j:i]}$ n'est pas un représentant de longueur minimale de la classe $\widehat{(i,j)}$. En effet, $\left|X_{\overline{I}_4} X_{[1:0]}\right| = 7$, mais $\left|M_2^{(0,1)}\right| = 5$ (en utilisant la commande `cnot_opt` [54]). Cependant les représentants $X_{\overline{I}_4} X_{[j:i]}$ ont l'avantage de permettre une démonstration courte de la proposition suivante.

Proposition 5.23. *Deux couples différents (i, j) et (k, ℓ) d'entiers de $\{0, 1, 2, 3\}$ définissent deux classes distinctes $\widehat{(i,j)}$ et $\widehat{(k,\ell)}$.*

Démonstration. On raisonne par l'absurde : soient deux couples différents (i, j) et (k, ℓ) tels que $\widehat{(i,j)} = \widehat{(k,\ell)}$. Alors $X_{\overline{I}_4} X_{[j:i]} = S_\sigma X_{\overline{I}_4} X_{[\ell:k]}$ pour une certaine permutation σ. De la proposition 2.20 on déduit que $X_{[j:i]} X_{[\ell:k]} = S_\sigma$. Or le seul cas où le produit de deux transvections est égale à une permutation est le cas où ces transvections sont égales. □

Remarque 5.24. La remarque 5.19 peut se généraliser à n'importe quelle classe $\widehat{(i,j)}$ et nous définissons donc $\mathrm{PMAX}^{(i,j)}$ comme étant l'ensemble des matrices $\mathcal{P}$ ayant leur dernière colonne nulle telles que l'état $M_k^{(i,j)}\left|\mathcal{P}\right\rangle$ (avec $k \notin \{i,j\}$) maximise $|\Delta_4|$.

Pour une matrice de paramètre $\mathcal{P}$, on désigne par σP la matrice obtenue en multipliant $\mathcal{P}$ à gauche par la matrice de permutation σ (*i.e.* la ligne i de $\mathcal{P}$ est remplacée par la ligne $\sigma^{-1}(i)$ de $\mathcal{P}$).

Proposition 5.25. *Soient i,j deux entiers de $\{0,1,2,3\}$ et σ une permutation de $\mathfrak{S}_4$.*

(i) Si $\mathcal{P} \in \mathrm{PMAX}^{(i,j)}$ alors $\sigma\mathcal{P} \in \mathrm{PMAX}^{(\sigma(i),\sigma(j))}$.

(ii) $\mathrm{PMAX}^{(\sigma(i),\sigma(j))} = \sigma\mathrm{PMAX}^{(i,j)}$

Démonstration. Soit $\mathcal{P} \in \mathrm{PMAX}^{(i,j)}$ et $k \notin \{i,j\}$ alors l'état $|\psi\rangle = M_k^{(i,j)}\left|\mathcal{P}\right\rangle$ maximise $|\Delta_4|$. Soit $\sigma \in \mathfrak{S}_4$, alors l'état $S_\sigma\left|\psi\right\rangle$ maximise aussi $|\Delta_4|$. On a : $S_\sigma\left|\psi\right\rangle = S_\sigma M_k^{(i,j)}\left|\mathcal{P}\right\rangle = M_{\sigma(k)}^{(\sigma(i),\sigma(j))} S_\sigma\left|\mathcal{P}\right\rangle$. Or $S_\sigma\left|\mathcal{P}\right\rangle = S_\sigma U(\mathcal{P})\left|0000\right\rangle = S_\sigma U(\mathcal{P}) S_\sigma^{-1}\left|0000\right\rangle$ et, en utilisant l'identité (5.55), il vient $S_\sigma\left|\mathcal{P}\right\rangle = \left|\sigma\mathcal{P}\right\rangle$, d'où $S_\sigma\left|\psi\right\rangle = M_{\sigma(k)}^{(\sigma(i),\sigma(j))}\left|\sigma\mathcal{P}\right\rangle$. Puisque $S_\sigma\left|\psi\right\rangle$ maximise $|\Delta_4|$, alors $\sigma\mathcal{P} \in \mathrm{PMAX}^{(\sigma(i),\sigma(j))}$, ce qui prouve l'affirmation (i). L'égalité (ii) se déduit facilement de (i). □

Les résultats numériques obtenus en utilisant la marche aléatoire suggèrent la conjecture suivante.

Conjecture 5.26. *Tout circuit de portes CNOT capable de maximiser l'hyperdéterminant de 4-qubits à partir d'un état complètement factorisé est, à une permutation des qubits près, un circuit du type $X_{\overline{I}_4} X_{[i:j]}$. Il y a ainsi* $\mathrm{card}(\mathfrak{S}_4) \times 12 = 288$ *éléments du groupe $\langle CNOT\rangle_4$ ayant cette propriété.*

5.3.6 Circuits générant les états $|L\rangle$, $|\Phi_5\rangle$ et $|M_{2222}\rangle$

Soit un état $|\psi\rangle$ de l'ensemble $\{|L\rangle, |\Phi_5\rangle, |M_{2222}\rangle\}$. Selon la conjecture de Gour-Wallach [91] démontrée par Chen et Djokovic [50], il existe une matrice $\mathcal{P}$ de paramètres ainsi qu'une phase φ telle que

$$|\psi\rangle = \mathrm{e}^{\mathrm{i}\varphi} U(\mathcal{P})\left|\psi_{\max}\right\rangle. \tag{5.80}$$

Afin de calculer $\mathcal{P}$ et φ, la première idée peut être de tenter de résoudre un système non linéaire de 16 équations à l'aide d'un logiciel de calcul formel mais sa résolution semble actuellement hors de portée des systèmes de calcul actuels (nous avons essayé Maple et le module Python SymPy).

Néanmoins, nous observons qu'il est possible de transformer la recherche d'une solution de l'équation (5.80) en un problème d'optimisation en exploitant la remarque suivante : $|\psi\rangle = \mathrm{e}^{\mathrm{i}\varphi} U(\mathcal{P})\left|\psi_{\max}\right\rangle$ si et seulement si la somme des modules des 16 coordonnées de $|\psi\rangle - \mathrm{e}^{\mathrm{i}\varphi} U(\mathcal{P})\left|L\right\rangle$ s'annule. Nous utilisons à nouveau l'heuristique de marche aléatoire sur un espace de 13 paramètres réels (les 12 paramètres de $\mathcal{P}$ plus la phase φ) afin de minimiser cette somme et obtenons ainsi une solution approchée du système (fonction `search_LU_from_state1_to_state2` du module Python). A partir de cette valeur approchée, nous devinons une solution exacte probable et vérifions par calcul formel (en utilisant le module SymPy de Python) qu'il s'agit bien d'une solution exacte. Les résultats sont résumés dans la table 5.4. Finalement, en utilisant

Table 5.4 Opérateurs locaux unitaires pour atteindre les états $|L\rangle$, $|\Phi_5\rangle$ et $|M_{2222}\rangle$ à partir de l'état $|\psi_{\max}\rangle$.

$$\boxed{\theta = \cos^{-1}\frac{\sqrt{3}}{3}}$$

$$|L\rangle = \mathrm{e}^{-\mathrm{i}\frac{11\pi}{12}} U(\mathcal{P}_{\psi\to L})\,|\psi_{\max}\rangle \qquad \text{avec } \mathcal{P}_{\psi\to L} = \begin{bmatrix} \pi & \pi/2 & -\pi/2 \\ \pi/2 & -\pi/2 & \pi \\ 0 & \pi & \pi \\ 0 & -\pi/2 & \pi/2 \end{bmatrix}$$

$$|\Phi_5\rangle = \mathrm{e}^{-\mathrm{i}\frac{7\pi}{12}} U(\mathcal{P}_{\psi\to\Phi_5})\,|\psi_{\max}\rangle \qquad \text{avec } \mathcal{P}_{\psi\to\Phi_5} = \begin{bmatrix} -\pi/3 & \theta-\pi & -3\pi/4 \\ \pi/3 & \theta & 3\pi/4 \\ \pi & \theta & 3\pi/4 \\ 2\pi/3 & \pi-\theta & \pi/4 \end{bmatrix}$$

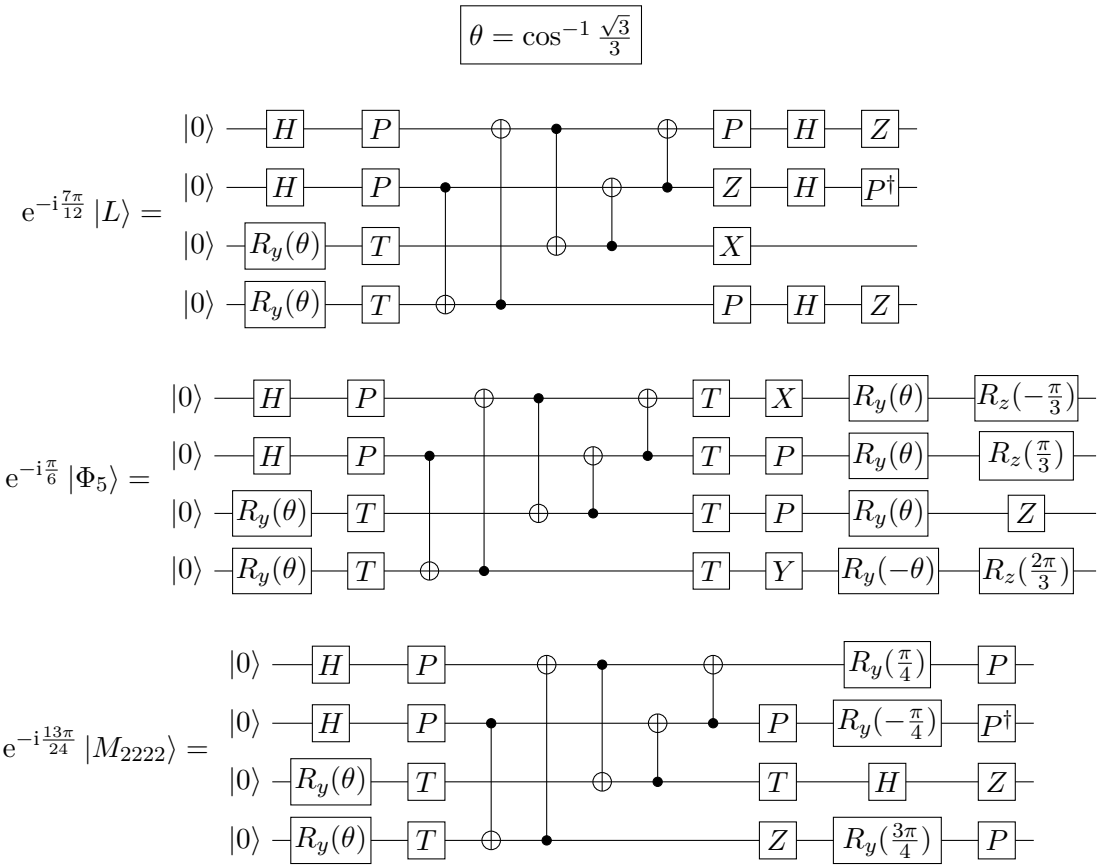
$$|M_{2222}\rangle = \mathrm{e}^{\mathrm{i}\frac{5\pi}{12}} U(\mathcal{P}_{\psi\to M_{2222}})\,|\psi_{\max}\rangle \quad \text{avec } \mathcal{P}_{\psi\to M_{2222}} = \begin{bmatrix} \pi/2 & \pi/4 & 0 \\ -\pi/2 & -\pi/4 & \pi/2 \\ 0 & -\pi/2 & \pi/4 \\ \pi/2 & 3\pi/4 & \pi \end{bmatrix}$$

les identités (5.53) et (5.54), et en combinant les résultats de la table 5.4 avec ceux de la proposition 5.15, il est possible de construire des circuits quantiques assez simples générant les états $|L\rangle$, $|\Phi_5\rangle$ and $|M_{2222}\rangle$. Ces circuits sont décrits figure 5.6 et on peut vérifier qu'ils sont corrects en utilisant la fonction `check_circuits` du module Python.

Nous avons implanté le circuit produisant l'état $|L\rangle$ dans un des ordinateurs d'IBM accessible au public [3]. Nous rappelons que le graphe de connectivité de ces ordinateurs n'est pas complet et que le bruit dans les portes impose d'utiliser le moins de portes possible et particulièrement le moins de portes $CNOT$ possible. Nous avons choisi l'ordinateur de 5 qubits ibmq-quito parce que son graphe de connectivité est $\{\{1,0\},\{1,2\},\{1,3\},\{3,4\}\}$, donc les portes $X_{[0:1]}$, $X_{[1:2]}$ et $X_{[3:1]}$ du sous-circuit qui implante l'opérateur $M_2^{(0,1)} = X_{[0:1]}X_{[1:2]}X_{[2:0]}X_{[0:3]}X_{[3:1]}$ sont des portes natives. Les deux autres portes $X_{[2:0]}$ et $X_{[0:3]}$ doivent être simulées à partir de portes $SWAP$ ou en utilisant la méthode explicitée dans la section 2.1.2 (le lecteur pourra vérifier que les deux méthodes proposées dans cette section aboutissent à un total de 8 portes $CNOT$ pour implanter ces deux portes). Ainsi il est possible d'écrire l'opérateur $M_2^{(0,1)}$ à l'aide de seulement 11 portes $CNOT$ natives :

$$M_2^{(0,1)} = X_{[0:1]}X_{[1:2]}\underbrace{X_{[0:1]}X_{[1:0]}X_{[0:1]}}_{S_{(0\ 1)}}X_{[2:1]}X_{[1:3]}\underbrace{X_{[0:1]}X_{[1:0]}X_{[0:1]}}_{S_{(0\ 1)}}X_{[3:1]}. \tag{5.81}$$

Figure 5.6 Circuits quantiques générant les états $|L\rangle$, $|\Phi_5\rangle$ and $|M_{2222}\rangle$ à une phase globale près. Pour une meilleure lisibilité, on a remplacé certaines rotations par les portes universelles classiques H, P et T en utilisant les identités (5.53).



Après compilation, le circuit quantique implantant l'état $|L\rangle$ utilise 22 portes unaires, 11 portes *CNOT* et a une profondeur de 18 (voir figure 5.7). Malgré cette longueur modérée, nous obtenons de nombreuses mesures qui, en théorie, ne devraient pas apparaître (voir l'histogramme de la figure 5.7). En effet, d'après l'identité (5.50), on a

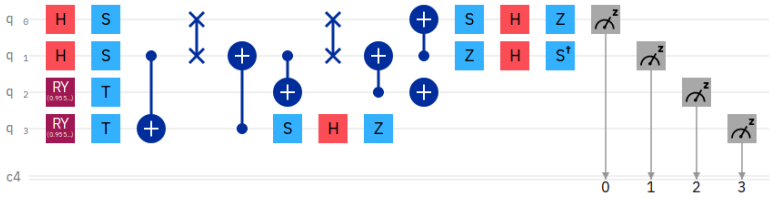
$$|L\rangle = \tfrac{1}{2}e^{i\frac{\pi}{6}}(|0000\rangle + |1111\rangle) + \tfrac{\sqrt{3}}{6}e^{-i\frac{\pi}{3}}(|0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle), \tag{5.82}$$

donc les états de base $|0001\rangle, |0010\rangle, |0100\rangle, |1000\rangle, |0111\rangle |1011\rangle, |1101\rangle$ ou $|1110\rangle$ ne peuvent théoriquement pas apparaître après la mesure.

Les causes de ce problème sont principalement les erreurs de mesures (environ 3% sur cette machine) et les erreurs dans les portes (environ 1,3% d'erreurs sur les portes *CNOT*). Ces résultats expérimentaux suggèrent qu'il y a encore des difficultés techniques importantes à surmonter avant de pouvoir produire l'état $|L\rangle$ par un circuit tel que celui proposé dans les figures 5.6 et 5.7.

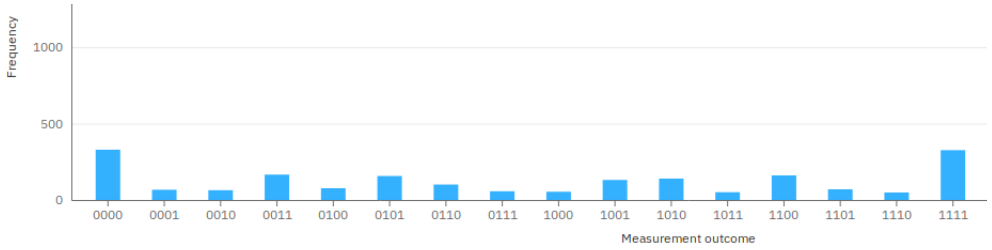
Figure 5.7 Implantation dans l'ordinateur quantique ibmq-quito d'un circuit produisant l'état $|L\rangle$. L'histogramme est basé sur 2000 mesures.

Circuit avant compilation :



Circuit après compilation :

Mesures :



5.4 Conclusion et perspectives

Dans ce chapitre, nous avons montré que les circuits de portes *CZ* et les circuits de portes *CNOT* étaient des outils intéressants pour construire certains états intriqués classiques considérés comme des ressources utiles dans la théorie de l'information quantique. En particulier, les circuits de portes *CNOT* agissant sur des états complètement factorisés sont capables de créer des états génériquement intriqués et maximalement intriqués au sens de Miyake [141] jusqu'à 4 qubits. Nous avons également proposé un circuit quantique générant l'état $|L\rangle$ dont les propriétés ont été décrites par Gour et Wallach [90], [91] et par Chen et Djokovic [50].

Il serait intéressant de savoir si certains résultats peuvent être prolongés pour plus de 4 qubits. Ainsi, on peut se demander si un circuit de portes *CNOT* peut produire des états génériquement intriqués de 5 ou 6 qubits comme c'est le cas pour 4 qubits (proposition 5.11). Une idée pour aborder ce problème pourrait être d'utiliser à nouveau la propriété tirée de [83, p.445] que nous avons déjà mentionnée dans la section 5.1.4 et qui est basée sur le type de solutions du système S_φ (5.40) : $\Delta_n(|\varphi\rangle) \neq 0$ si et seulement si ce système n'a que des solutions triviales.

Une autre question concerne les états maximalement intriqués au delà de 4 qubits : peuvent-ils être encore produits par des circuits de portes *CNOT* ? Dans la section

5.3.5, nous avons établi un lien entre les états maximalement intriqués de 4 qubits et les circuits de portes *CNOT* représentant l'opérateur $X_{\overline{I}_4} X_{[j:i]}$. Est-il possible qu'un lien similaire existe encore dans le cas de 6 qubits entre les opérateurs $X_{\overline{I}_6} X_{[j:i]}$ et les états maximalement intriqués ? Ces questions sont certainement plus difficiles puisqu'on ne sait pas évaluer l'hyperdéterminant pour plus de 4 qubits.

Conclusion générale et perspectives de recherche

Conclusion

La mise au point d'un ordinateur quantique fonctionnel est un défi technologique considérable qui se heurte à des obstacles techniques majeurs. Dans la phase actuelle des recherches, les deux principales difficultés sont la décohérence et les erreurs sur les portes quantiques. Pour tenter de surmonter ces problèmes, on peut utiliser deux approches théoriques complémentaires : les codes correcteurs d'erreurs et l'optimisation des circuits quantiques. Dans ces deux approches, les portes de Clifford jouent un rôle essentiel. D'abord parce qu'elles constituent un sous ensemble des portes universelles et sont à ce titre omniprésentes. Ensuite parce qu'elles sont indispensables au développement du calcul quantique résistant aux erreurs en étant utilisées dans les codes correcteurs. Pour ces deux raisons, inventer des méthodes efficaces de simplification des circuits de Clifford est un objectif important contribuant à améliorer la fiabilité des calculs.

Dans cette thèse, nous avons décrit en détail différents types de circuits quantiques composés de portes de Clifford. Au cours de cette description, nous avons relevé et utilisé une grande diversité de structures algébriques qui se sont avérées utiles pour étudier ces circuits sous plusieurs angles. La plus importante d'entre elles est la structure de groupe. Les groupes concernés sont construits grâce à des opérations usuelles comme le produit direct et semi-direct ou encore le quotient. Les groupes bien connus impliqués dans ces opérations sont le groupe symétrique, le groupe à deux éléments, des groupes classiques comme le groupe linéaire ou le groupe symplectique, et enfin les groupes de Coxeter. Ces derniers ont été décrit en termes de générateurs et de relations.

Les structures de groupes sous-jacentes aux circuits étudiés permettent de bien comprendre les opérations transformant un circuit en un circuit équivalent. Elles sont donc utiles pour proposer des algorithmes de réduction ou d'optimisation du nombre de portes quantiques de ces circuits. Ainsi, dans les algorithmes exposés, nous avons souvent utilisé l'opération de conjugaison d'un élément du groupe par un autre. Dans le même ordre d'idée, en établissant un lien avec certains groupes de Coxeter, nous avons pu exploiter l'existence d'une forme réduite dans ces groupes pour proposer une heuristique de réduction de certains circuits.

Dans certains cas, la connaissance du groupe associé à un type de circuit peut également nous aider à définir une forme générique pour ces circuits. Ces formes sont appelées formes normales ou formes canoniques dans la littérature scientifique. Ainsi la forme normale ZX pour les circuits de portes $CNOT$ et CZ est une conséquence de la structure de produit semi-direct du groupe engendré. Ces formes normales reflètent donc bien la structure algébrique de ces circuits. De plus, elles donnent une borne supérieure

sur le nombre de portes nécessaires pour représenter les opérations encodées par ces circuits. De cette façon, la mise sous forme normale d'un circuit permet dans certains cas de réduire le nombre de portes quantiques dans ce circuit.

Pour classifier les états intriqués obtenus par l'action de certains types de circuits de Clifford, nous avons également fait appel à la notion de groupe et d'action de groupe sur un ensemble au travers des équivalences SLOCC, LU ou LC entre états intriqués. Afin de décrire les orbites ainsi obtenues, les notions de polynômes invariants et covariants jouent un rôle essentiel. Là encore, il s'agit d'outils issus de la théorie des groupes. En effet, un polynôme invariant est un polynôme qui reste invariant lorsque le groupe SLOCC agit sur la fonction d'onde. Pour l'essentiel, notre travail sur l'intrication a consisté à utiliser ces différents outils afin de montrer que les circuits de portes $CNOT$, et dans une moindre mesure les circuits de porte CZ, ont la capacité de créer une grande variété d'états intriqués, au moins pour les petits systèmes de qubits.

Les résultats exposés dans cette thèse contribuent à montrer l'intérêt d'une approche algébrique pour étudier les circuits quantiques du point de vue de deux grandes problématiques très présentes dans l'ère NISQ : d'une part l'optimisation des circuits comme un des moyens de contrer les effets des erreurs dans les portes quantiques, d'autre part la classification de l'intrication et la production d'états intriqués remarquables qui constituent une ressource fondamentale pour le calcul quantique.

Perspectives de recherche

Une première extension naturelle à nos travaux consisterait à appliquer à d'autres types de circuit les techniques de descriptions algébriques développées dans cette thèse. En particulier, il serait intéressant de comprendre ce que peut apporter la description des groupes de portes, ou de leur quotient, en terme de quotients de groupes de Coxeter ou d'autres familles classiques de groupe. A titre d'exemple, étudier les différents sous-groupes obtenus quand on ajoute des portes T aux portes de Clifford pourrait constituer un premier axe de recherche.

L'optimisation des circuits de porte $CNOT$ reste une problématique importante car ces portes sont omniprésentes dans les circuits quantiques. Pour réduire les circuits de portes $CNOT$, l'heuristique basée sur l'élimination gaussienne appliquée à la matrice de $\mathrm{GL}_n(\mathbb{F}_2)$ représentant le circuit à été successivement améliorée par l'algorithme de Patel-Markov-Hayes [154], puis par l'algorithme GreedyGE (Greedy Gaussian Elimination [40]). Cependant, une décomposition d'une matrice de $\mathrm{GL}_n(\mathbb{F}_2)$ donnée par ce dernier algorithme n'est généralement pas optimale. On pourrait donc essayer de la réduire par un nouvel algorithme utilisant les règles de réécriture énoncées dans le théorème 2.17.

Au sujet de l'intrication, notre approche s'est limitée à deux types de circuits très particuliers et nous n'avons pas étudié l'intrication apparaissant dans les circuits de Clifford en général. Dans un premier temps, on pourrait considérer des circuits du groupe $\langle CZ, CNOT\rangle_n$ mis sous la forme ZX qui agissent sur un état complètement factorisé. On chercherait alors à comprendre ce qu'apporte l'ajout de porte CZ à la suite des portes $CNOT$ sur la diversité des types d'intrication apparaissant en fin de circuit. Ensuite, il s'agirait d'étendre cette étude à des circuits de Clifford quelconques mis sous forme genPZX.

Pour quantifier l'intrication, nous avons utilisé une mesure basée sur l'hyperdéterminant. Dans l'état actuel des connaissances, cet outil a une portée limitée car on ne

connaît pas d'expression de cet invariant pour des états de plus de 4 qubits. Néanmoins, il existe un critère, que nous avons mis en oeuvre dans l'annexe D, afin de déterminer si un certain état $|\psi\rangle$ est génériquement intriqué sans passer par le calcul de l'hyperdéterminant. Pour cela, on doit vérifier qu'un certain système d'équations (5.40) n'a que des solutions triviales. Dans la même optique, il serait intéressant de se demander s'il existe un algorithme efficace permettant de déterminer si un état $|\psi\rangle$ donné par ses amplitudes complexes est maximalement intriqué, sans avoir à calculer $\Delta_n(|\psi\rangle)$.

Cependant, il est fort possible qu'il s'agisse d'une question mathématique très difficile. Aussi, on peut proposer d'ouvrir un peu cette problématique en apparence purement mathématique en déplaçant légèrement le champ de recherche vers la physique quantique expérimentale et en posant une question plus générale : trouver des méthodes pour détecter et quantifier l'intrication statistiquement, c'est à dire par une série de mesures. Existe-t-il par exemple des inégalités analogues à celles de Bell qui permettraient de reconnaître statistiquement si un état est génériquement intriqué ? Une première étape serait la recherche de méthodes visant à détecter l'intrication générique des états de quelques qubits. Dans un deuxième temps, on pourrait se poser la question, sans doute plus difficile, de la reconnaissance des états maximalement intriqués.

Annexe A

Rappel des principales notions de théorie des groupes utilisées

On récapitule ici les définitions et propriétés sur les groupes qui sont utilisées tout au long de ce mémoire. Il s'agit de notions classiques qu'on trouve facilement dans la littérature mathématique. Les propriétés sont rappelées sans démonstration. Pour plus de détails et d'exemples, le lecteur pourra se référer à l'ouvrage de Josette Calais [42] ainsi qu'à [163] et [72]. Un livre classique sur les groupes de Coxeter est [60] et nous avons aussi utilisé [27].

A.1 Généralités

A.1.1 Structure de groupe

Définition A.1. Un groupe $(G, *)$ est la donnée d'un ensemble G et d'une loi de composition interne sur G (une opération binaire sur G), notée $*$, qui vérifie les conditions suivantes.

(i) La loi $*$ est associative : $\forall (x, y, z) \in G^3, (x * y) * z = x * (y * z)$

(ii) Il existe un élément neutre, *i.e.* un élément e vérifiant : $\forall x \in G, x * e = e * x = x$

(iii) Tout élément x de G admet un inverse : $\forall x \in G, \exists y \in G, x * y = y * x = e$

Proposition A.2. *Dans un groupe $(G, *)$, l'élément neutre e est unique et tout élément x possède un unique inverse que l'on note x^{-1}.*

Définition A.3. On dit qu'un groupe est commutatif (ou abélien), si deux éléments quelconques commutent, c'est à dire si : $\forall (x, y) \in G^2, x * y = y * x$.

A.1.2 Sous-groupe et partie génératrice

Définition A.4. Soit $(G, *)$ un groupe. Une partie H de G est un sous-groupe de G si elle vérifie les conditions suivantes :

(i) H contient l'élément neutre e,

(ii) $\forall (x, y) \in H^2, x * y \in H$

(iii) $\forall x \in H, x^{-1} \in H$

Définition A.5. Soit S une partie d'un groupe G. Le groupe engendré par S, que l'on note $\langle S \rangle$, est le plus petit sous-groupe de G contenant S. Si $\langle S \rangle = G$, on dit que S est une partie génératrice de G.

Proposition A.6. *Le groupe engendré par S est l'intersection de tous les sous-groupes de G contenant S. C'est aussi l'ensemble des éléments de G pouvant s'écrire sous la forme $x_1^{\varepsilon_1} * \cdots * x_n^{\varepsilon_n}$ avec $n \in \mathbb{N}$, $x_1, \dots x_n$ des éléments de S et $\varepsilon_1, \dots, \varepsilon_n$ éléments de $\{1, -1\}$.*

Définition A.7. Soit $(G, *)$ un groupe fini et S une partie génératrice de G. Le graphe de Cayley droit (resp. gauche) de G relativement à S est le graphe orienté dont les sommets sont les éléments de G et tel qu'il y a un arc de x vers y si et seulement s'il existe un élément s de S tel que $y = x * s$ (resp. $y = s * x$) (voir plus loin exemple A.1).

A.1.3 Morphisme de groupe

Définition A.8. Soient deux groupes $(G, *)$ et $(G', \bullet)$.

(i) Une application f de G dans G' est un morphisme de groupe si : $\forall (x, y) \in G^2, f(x * y) = f(x) \bullet f(y)$.

(ii) Un isomorphisme est un morphisme bijectif. Deux groupes G et G' sont isomorphes s'il existe un isomorphisme de l'un vers l'autre. On écrit alors $G \simeq G'$.

(iii) Un automorphisme d'un groupe de G est un isomorphisme de G dans G.

Proposition A.9. *Soit $f : G \longrightarrow G'$ un morphisme de groupe alors $f(e_G) = e_{G'}$ et pour tout $x \in G$, $(f(x))^{-1} = f(x^{-1})$.*

On rappelle que $\ker(f)$ est l'ensemble des éléments de G dont l'image par f est $e_{G'}$ et que $\mathrm{Im}(f)$ est l'ensemble des images par f des éléments de G.

Proposition A.10. *Soit $f : G \longrightarrow G'$ un morphisme de groupe, alors $\ker(f)$ est un sous-groupe de G et $\mathrm{Im}(f)$ est un sous-groupe de G'.*

A.1.4 Action d'un groupe sur un ensemble

Définition A.11. Soit A un ensemble et $(G, *)$ un groupe et soit une application de $G \times A$ dans A qui, à tout couple (x, a), associe un élément de A noté $x \cdot a$. On dit que cette application est une action du groupe G sur l'ensemble A si la loi externe $\cdot$ vérifie les deux conditions suivantes :

(i) $\forall a \in A, e.a = a$

(ii) $\forall (x, y) \in G^2, \forall a \in A, x \cdot (y \cdot a) = (x * y) \cdot a$

Proposition et définition A.12. *Soit $(G, *)$ un groupe agissant sur un ensemble A et soit $a \in A$. On appelle orbite de a sous l'action de G l'ensemble $\{x \cdot a \mid x \in G\}$. L'ensemble des orbites forme une partition de A.*

Dans la suite, afin d'alléger l'écriture, on écrira généralement xy à la place de $x * y$.

A.2 Groupe quotient

A.2.1 Classes d'équivalence modulo un sous-groupe

Proposition et définition A.13. *Soit G un groupe, H un sous-groupe de G et x, y des éléments de G.*

(i) La relation $x \sim y \iff x^{-1}y \in H$ est une relation d'équivalence sur G. La classe d'équivalence de x est l'ensemble xH, appelé classe à gauche de x (modulo H).

(ii) La relation $x \sim y \iff yx^{-1} \in H$ est une relation d'équivalence sur G. La classe d'équivalence de x est l'ensemble Hx, appelé classe à droite de x (modulo H).

(iii) L'ensemble des classes d'équivalence à gauche a même cardinal que l'ensemble des classes d'équivalence à droite. Quand ce cardinal est fini, on l'appelle l'indice de H dans G et on le note $[G : H]$.

Théorème A.14 (de Lagrange)**.** *Si H est un sous-groupe d'un groupe G fini, alors le cardinal de H divise celui de G et on a : $[G : H] = \frac{|G|}{|H|}$.*

A.2.2 Sous-groupe normal

Définition A.15. Soit G un groupe et x, y deux éléments de G. L'élément yxy^{-1} s'appelle le conjugué de x par y. L'opération qui à tout élément y de G associe son conjugué par x s'appelle la conjugaison par x.

Proposition A.16. *Soit G un groupe.*

(i) Pour tout x de G, la conjugaison par x est un automorphisme de G dont l'inverse est la conjugaison par x^{-1}.

(ii) L'application de G dans le groupe $\mathrm{Aut}(G)$ des automorphismes de G qui, à chaque élément x de G, associe la conjugaison par x est un morphisme de G dans $\mathrm{Aut}(G)$.

Définition A.17. On dit qu'un sous-groupe H d'un groupe G est un groupe normal (ou distingué) si H est stable par conjugaison, c'est à dire si, pour tout élément x de G, on a : $xHx^{-1} = H$.

Proposition et définition A.18. *Si H est un sous-groupe normal de G alors chaque classe à gauche xH est égale à la classe à droite Hx. Soit G/H l'ensemble des classes et soit $\diamond$ la loi de composition interne sur G/H définie par $xH \diamond yH = xyH$. Alors $(G/H, \diamond)$ est un groupe appelé groupe quotient de G par H.*

Proposition A.19. *Soit $f : G \longrightarrow G'$ un morphisme de groupe. Le noyau de f est un sous-groupe normal de G et on a le diagramme commutatif suivant :*

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ \downarrow{\scriptstyle p} & & \uparrow{\scriptstyle i} \\ G/\ker(f) & \xrightarrow{\quad \tilde{f} \quad} & \mathrm{Im}(f) \end{array}$$

où

- *p est la projection canonique de G dans $G/\ker(f)$ qui associe, à chaque élément de G, sa classe d'équivalence modulo $\ker(f)$,*

- *$\tilde{f}$ est l'isomorphisme qui associe à chaque classe l'image par f d'un représentant de cette classe,*
- *i est l'injection canonique de* $\mathrm{Im}(f)$ *dans G'.*

Exemple A.20. Soit $n \in \mathbb{N}^*$ et f le morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{C}^*, \times)$ tel que $f(k) = \mathrm{e}^{\mathrm{i}\frac{2k\pi}{n}}$. Alors $\ker(f) = n\mathbb{Z}$ et $\mathrm{Im}(f)$ est le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité. Le groupe quotient $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{U}_n$.

Définition A.21. Un groupe simple est un groupe non réduit à l'élément neutre dont les seuls sous-groupes normaux sont lui même et $\{e\}$.

A.2.3 Normalisateur

Définition A.22. Soit A une partie d'un groupe G.

(i) On dit qu'un élément x de G normalise A si $xAx^{-1} = A$.

(ii) On dit qu'une partie B de G normalise A si tout élément de B normalise A.

(iii) Le normalisateur de A dans G, noté $N_G(A)$ est l'ensemble des éléments de G qui normalisent A.

Proposition A.23. *Soit A une partie d'un groupe G.*

(i) Le normalisateur de A dans G est un sous-groupe de G.

(ii) Si H est un sous-groupe de G, alors $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal.

(iii) H est un sous-groupe normal de G si et seulement si $N_G(H) = G$.

A.3 Produits directs et semi-directs

A.3.1 Produit direct de groupes

Proposition et définition A.24. *Soient deux groupes $(G, *)$ et $(G', \bullet)$ et la loi de composition interne $\diamond$ sur le produit cartésien $G \times G'$, définie par $(x, x') \diamond (y, y') = (x * y, x' \bullet y')$. Alors $(G \times G', \diamond)$ est un groupe appelé groupe produit (direct) de $(G, *)$ et $(G', \bullet)$.*

A.3.2 Produit semi-direct interne

Définition A.25. Soit H un sous-groupe normal d'un groupe G et F un sous-groupe de G. On dit que G est le produit semi-direct interne de H par F si tout élément de G peut s'écrire de manière unique comme le produit d'un élément de H par un élément de F.

Remarque A.26. Soit x_1 et x_2 deux éléments de G. On pose $x_1 = h_1 f_1$ et $x_2 = h_2 f_2$, avec $(h_1, h_2) \in H^2$ et $(f_1, f_2) \in F^2$. On obtient la décomposition de $x_1 x_2$ comme produit d'un élément de H par un élément de F en écrivant

$$x_1 x_2 = (h_1 f_1)(h_2 f_2) = (h_1 f_1 h_2 f_1^{-1})(f_1 f_2) \tag{A.1}$$

et en posant $h_3 = f_1 h_2 f_1^{-1}$. Comme H est stable par conjugaison, alors $h_3 \in H$ et on obtient ainsi $x_1 x_2 = (h_1 h_3)(f_1 f_2)$.

Soit φ le morphisme de F dans $\mathrm{Aut}(H)$ tel que, pour tout f dans F, $\varphi(f)$ est la conjugaison par f d'un élément de H. L'égalité A.1 s'écrit

$$x_1 x_2 = (h_1 f_1)(h_2 f_2) = (h_1 \varphi(f_1)(h_2))(f_1 f_2). \tag{A.2}$$

A.3.3 Produit semi-direct externe

Définition A.27. Soit H et F deux groupes, soit φ un morphisme de F dans $\mathrm{Aut}(H)$ et soit $G = H \times F$. On définit une loi de composition interne sur G par :

$$(h_1, f_1)(h_2, f_2) = (h_1 \varphi(f_1)(h_2), f_1 f_2) \tag{A.3}$$

Munit de cette loi, G est un groupe appelé produit semi-direct externe de H par F relativement à φ. On écrit alors $G = H \rtimes_\varphi F$.

Remarque A.28. Le produit semi-direct externe est une généralisation du produit direct dans la mesure où ce dernier est un produit semi-direct relativement à un morphisme constant φ qui envoie chaque élément de F sur l'identité de $\mathrm{Aut}(H)$.

Remarque A.29. Le lien entre le produit semi-direct externe de H par F et le produit semi-direct interne de H par F est le suivant. Soit H et F deux sous-groupes de G tels que G soit le produit semi-direct interne de H par F. Soit φ le morphisme de F dans $\mathrm{Aut}(H)$ tel que, pour tout f dans F, $\varphi(f)$ est la conjugaison par f d'un élément de H. Alors le groupe $G' = H \rtimes_\varphi F$ et le groupe G sont des groupes isomorphes, un isomorphisme possible envoyant chaque élément (h, f) de G' sur le produit hf de G.

A.4 Groupe symétrique

A.4.1 Généralités

Définition A.30. Soit $n \in \mathbb{N}^*$, on appelle groupe symétrique de degré n, noté $\mathfrak{S}_n$, l'ensemble des permutations de $\{0, \ldots, n-1\}$, c'est à dire l'ensemble des bijections de $\{0, \ldots, n-1\}$ dans lui même.

Remarque A.31. Dans la définition usuelle du groupe symétrique $\mathfrak{S}_n$, on considère les permutations de $\{1, \ldots, n\}$. Cependant, les n qubits d'un système étant numérotés de 0 à $n-1$ nous avons décidé d'adapter les définitions à cette numérotation, ce qui ne change absolument rien à la théorie.

Exemple A.32. Une première façon de représenter un élément de $\mathfrak{S}_n$ est d'utiliser une matrice $2 \times n$ en écrivant sur la première ligne les n entiers et sur la seconde leurs images. Par exemple : $\gamma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 0 & 3 & 2 & 1 \end{pmatrix}$ est la permutation de $\mathfrak{S}_6$ telle que $\gamma(0) = 4, \ldots, \gamma(5) = 1$.

Définition A.33. Soit $\sigma \in \mathfrak{S}_n$.

(i) On appelle inversion de σ tout couple d'entiers (i, j) tel que $0 \leqslant i < j \leqslant n-1$ et $\sigma(i) > \sigma(j)$.

(ii) On dit qu'une permutation est paire si elle admet un nombre pair d'inversions et on dit qu'elle est impaire dans le cas contraire.

(iii) La signature d'une permutation σ, notée $\varepsilon(\sigma)$, est le nombre égal à 1 si σ est paire et égal à -1 dans le cas contraire.

Proposition et définition A.34. *La signature ε est un morphisme du groupe $\mathfrak{S}_n$ dans le groupe $(\{-1,1\},\times)$. En conséquence, l'ensemble des permutations paires est un sous-groupe normal de $\mathfrak{S}_n$ puisque c'est le noyau de ε. Ce sous-groupe s'appelle le groupe alterné de degré n.*

A.4.2 Permutations cycliques

Définition A.35. Un cycle ou permutation circulaire est une permutation σ de $\mathfrak{S}_n$ pour laquelle il existe un entier $p \geqslant 1$ et des entiers $i_1, \ldots, i_p$ distincts tels que $\sigma(i_k) = i_{k+1}$ pour $k = 1, \ldots, p-1$, $\sigma(i_p) = i_1$ et $\sigma(i) = i$ pour $i \notin \{i_1, \ldots, i_p\}$.

On dit que p est la longueur du cycle (ou que σ est un p-cycle) et on note $\sigma = (i_1 \ldots i_p)$. L'ensemble $\{i_1, \ldots, i_p\}$ s'appelle le support du cycle. Un 2-cycle s'appelle une transposition et les cycles de longueur 1 sont tous égaux à la permutation identité I.

Théorème A.36. *Toute permutation peut se décomposer de façon unique en un produit commutatif de cycles à supports deux à deux disjoints.*

Exemple A.37. On reprend la permutation γ définie dans l'exemple A.32. On observe que $\gamma(0) = 4, \gamma(4) = 2, \gamma(2) = 0$ (premier cycle), que $\gamma(1) = 5, \gamma(5) = 1$ (deuxième cycle) et que $\gamma(3) = 3$ (troisième cycle). La décomposition de cette permutation en cycles est donc : $\gamma = (0\ 4\ 2)(1\ 5)(3)$. En général on omet les cycles de longueur 1 et on écrit par exemple $\gamma = (0\ 4\ 2)(1\ 5)$. Notez bien que, même si la décomposition est unique, l'écriture d'un cycle donné ne l'est pas. Ainsi $(0\ 4\ 2) = (2\ 0\ 4) = (4\ 2\ 0)$ et $(1\ 5) = (5\ 1)$.

Proposition A.38. *Tout p-cycle se décompose en produit de $p-1$ transpositions :*

$$(i_1 \ldots i_p) = \prod_{k=1}^{p-1} (i_k\ i_{k+1}). \tag{A.4}$$

Théorème A.39. *Les transpositions engendrent le groupe symétrique.*

Remarque A.40. La signature d'une transposition étant égale à -1 (une seule inversion), une conséquence du théorème A.39 et de la proposition A.34 est qu'une permutation est paire si et seulement si elle se décompose en un nombre pair de transpositions.

Exemple A.41. Pour obtenir la décomposition d'une permutation en produit de transpositions, on l'écrit d'abord en produit de cycle puis on utilise l'égalité (A.4). Ainsi, en reprenant l'exemple A.32, on obtient $\gamma = (0\ 4)(4\ 2)(1\ 5)$.

A.4.3 Type cyclique d'une permutation

Définition A.42. Une partition d'un entier n non nul est un tuple d'entiers $(a_1, \ldots a_p)$ tel que $n = \sum_{i=1}^{p} a_i$ et $a_1 \geqslant \ldots \geqslant a_p$.

Définition A.43. Soit σ une permutation de $\mathfrak{S}_n$ qui se décompose en un produit de p cycles disjoints de longueurs respectives $\ell_1, \ell_2, \ldots \ell_p$ avec $\ell_1 \geqslant \ell_2 \geqslant \ldots \geqslant \ell_p$ et $\sum_{i=1}^{p} \ell_i = n$. Le type cyclique de σ est la partition $(\ell_1, \ldots, \ell_p)$ de l'entier n.

Exemple A.44. Le type cyclique de la permutation identité de $\mathfrak{S}_6$ est $(1,1,1,1,1,1)$ et le type cyclique de γ (exemple A.32) est $(3,2,1)$.

Définition A.45. On considère sur $\mathfrak{S}_n$ la relation d'équivalence $\mathcal{R}$ définie par $\sigma\mathcal{R}\sigma' \iff \exists\gamma \in \mathfrak{S}_n, \sigma' = \gamma\sigma\gamma^{-1}$. Les classes d'équivalence par cette relation sont appelées classes de conjugaison de $\mathfrak{S}_n$.

Remarque A.46. Les classes de conjugaison sont en fait les différentes orbites quand le groupe symétrique agit sur lui même par conjugaison (*i.e.* $\gamma \cdot \sigma = \gamma\sigma\gamma^{-1}$).

Proposition A.47. *Deux permutations appartiennent à la même classe de conjugaison si et seulement si elles ont le même type cyclique.*

A.4.4 Exemple : le groupe $\mathfrak{S}_3$

On illustre une partie des différentes notions sur les groupes en considérant le cas du groupe symétrique de degré 3.

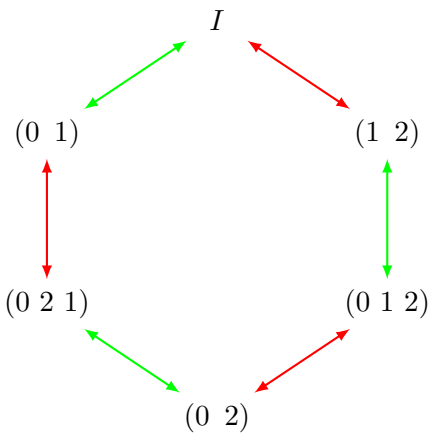
Les transpositions de $\mathfrak{S}_3$ sont (0 1), (1 2) et (0 2). Ces transpositions engendrent $\mathfrak{S}_3$. Cependant on remarque que (0 2) = (0 1)(1 2)(0 1) donc l'ensemble $S = \{(0\ 1), (1\ 2)\}$ est une partie génératrice de $\mathfrak{S}_3$. On a représenté dans la figure A.1 le graphe de Cayley gauche de $\mathfrak{S}_3$ relativement à S.

Il n'y a que trois partitions possibles pour l'entier 3. Chacune de ces partitions est le type cyclique des permutations d'une même classe de conjugaison selon le tableau ci-dessous.

Partition	Classe de conjugaison
$(1,1,1)$	$\{I\}$
$(2,1)$	$\{(0\ 1), (1\ 2), (0\ 2)\}$
(3)	$\{(0\ 1\ 2), (0\ 2\ 1)\}$

Le groupe alterné de degré 3 est le sous-groupe normal formé par les trois permutations paires $\{(0\ 1\ 2), (0\ 2\ 1)\}, I\}$. Ce groupe est engendré par (0 1 2) ou par (0 2 1). Le quotient de $\mathfrak{S}_3$ par le groupe alterné est isomorphe au groupe à deux éléments $(\{-1, 1\}, \times)$ (voir proposition A.34).

Figure A.1 Graphe de Cayley gauche du groupe $\mathfrak{S}_3$ relativement aux générateurs (0 1) (arcs en vert) et (1 2) (arcs en rouge).

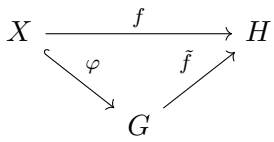


A.5 Groupes libres et présentations de groupes

De manière informelle, une présentation d'un groupe est une façon compacte et parlante de décrire ce groupe en donnant des *générateurs* et des *relations* que doivent suivre ces générateurs. Cette présentation est basée sur la notion de groupe libre sur un ensemble, c'est à dire un groupe engendré par les éléments d'un ensemble avec le moins de contraintes possibles. L'idée générale est qu'en rajoutant des contraintes au groupe libre (les relations de la présentation), on peut définir n'importe quel groupe comme quotient d'un groupe libre.

A.5.1 Groupe libre

Définition A.48. Soit G un groupe, X un ensemble et φ une injection de X dans G. On dit que le groupe G est libre sur X s'il vérifie la propriété suivante, dite *propriété universelle* : pour tout groupe H et tout application f de X dans H, il existe un unique morphisme de groupe $\tilde{f}$ de G dans H qui prolonge f , c'est à dire tel que le diagramme suivant commute (*i.e.* $f = \tilde{f} \circ \varphi$) :



Remarque A.49. D'un point de vue informel, on peut faire le parallèle entre X et une base d'un espace vectoriel : la donnée des images de cette base par un morphisme d'espaces vectoriels (*i.e.* une application linéaire) définit entièrement ce morphisme.

Proposition A.50. *Soit X un ensemble, il existe un unique groupe libre sur X. On le note $\mathcal{F}_X$.*

Construction du groupe libre

Soit X un ensemble, on construit le groupe libre sur X de la façon suivante. Soit X' un ensemble en bijection avec X tel que $X \cap X' = \emptyset$. Pour tout élément x de X, on note x' l'élément correspondant dans X' par cette bijection et on pose $\overline{X} = X \cup X'$. On considère $\overline{X}^*$, l'ensemble des mots sur l'alphabet $\overline{X}$ munit de l'opération de concaténation des mots.

On appelle opération élémentaire sur un mot, la suppression ou l'ajout dans ce mot de xx' ou de $x'x$, avec $x \in X$. On considère la relation d'équivalence $\sim$ sur $\overline{X}^*$ définie de la manière suivante : deux mots w_1 et w_2 sont équivalents si on peut passer de l'un à l'autre par une suite finie d'opérations élémentaires. On note $[w]$ la classe d'un mot w. Sur l'ensemble quotient $\overline{X}^*/\sim$, l'opération de concaténation induit une loi interne $\bullet$ définie par : $[w_1] \bullet [w_2] = [w_1 w_2]$ pour toutes classes $[w_1]$ et $[w_2]$. L'élément neutre de $\bullet$ est la classe du mot vide et l'inverse de $[x_1 \dots x_n]$ (où les x_i sont des lettres de l'alphabet $\overline{X}$) est la classe du mot $y_n \dots y_1$ où les y_i sont définis par : $y_i = x'$ si $x_i = x$ avec $x \in X$ et $y_i = x$ si $x_i = x'$ avec $x' \in X'$. La loi interne $\bullet$ munit donc l'ensemble $\overline{X}^*/\sim$ d'une structure de groupe. On démontre que ce groupe vérifie la propriété universelle, c'est donc le groupe libre sur X.

Exemple A.51. Le groupe libre sur un singleton $\{x\}$ est isomorphe à $\mathbb{Z}$.

A.5.2 Présentation d'un groupe

Définition A.52. Une présentation de groupe est la donnée d'une ensemble X et d'une partie $\mathcal{R}$ de $\mathcal{F}_X$. On dit que X est l'ensemble des générateurs et $\mathcal{R}$ l'ensemble des relations. Cette présentation est notée $\langle X \mid \mathcal{R} \rangle$.

Proposition et définition A.53. *La clôture normale d'une partie S d'un groupe G, notée $\mathrm{cln}_G(S)$ est le plus petit sous-groupe normal de G contenant S. Elle est constituée de l'ensemble des produits des conjugués de puissances d'éléments de S :*

$$\mathrm{cln}_G(S) = \left\{ \prod_{i=1}^{m} g_i s_i^{n_i} g_i^{-1} \mid m \in \mathbb{N}, n_i \in \mathbb{N}, g_i \in G, s_i \in S \right\}. \tag{A.5}$$

Définition A.54. Le groupe défini par la présentation $\langle X \mid \mathcal{R} \rangle$ est le quotient du groupe libre $\mathcal{F}_X$ par la clôture normale de $\mathcal{R}$.

Définition A.55. Une présentation d'un groupe G quelconque est la donnée d'une présentation $\langle X \mid \mathcal{R} \rangle$ et d'un isomorphisme entre G et le groupe défini par cette présentation. On dit alors que $\langle X \mid \mathcal{R} \rangle$ est une présentation de G et on note $G \simeq \langle X \mid \mathcal{R} \rangle$.

Exemple A.56. Voici trois exemples de présentations de groupes.

- Une présentation de $(\mathbb{Z}, +)$ ou du groupe libre sur un singleton est $\langle x \mid \emptyset \rangle$.
- Une présentation de $(\mathbb{Z}_n, +)$ ou du groupe des racines n-ièmes de l'unité est $\langle x \mid x^n \rangle$ (plus généralement, il s'agit de la présentation du groupe monogène à n éléments).
- Une présentation du groupe symétrique $\mathfrak{S}_3$ (voir section A.4.4) est :

  $$\langle x, y \mid x^2, y^2, (xy)^3 \rangle.$$

  Soit w un élément $\mathcal{F}_{\{x,y\}}$ et $[w]$ la classe de w modulo les relations. Un isomorphisme entre $\mathfrak{S}_3$ et le quotient du groupe libre $\mathcal{F}_{\{x,y\}}$ défini par cette présentation associe $[x]$ à la transposition $(0\ \ 1)$ et $[y]$ à la transposition $(1\ \ 2)$. Les 6 éléments du groupe quotient sont $\{[1], [x], [y], [xy], [yx], [xyx]\}$. On a par exemple $[yxy] = [xyx]$ et $[xxy] = [y]$.

A.5.3 Groupes de Coxeter

Définition A.57. Un groupe de Coxeter W est un groupe ayant une présentation du type

$$\langle s_0, \ldots, s_{k-1} \mid (s_i s_j)^{m_{ij}}, 0 \leqslant i, j \leqslant k-1 \rangle \tag{A.6}$$

avec $m_{ij} \in \mathbb{N} \cup \{\infty\}$, $m_{ij} = m_{ji}$, $m_{ii} = 1$, $m_{ij} \geqslant 2$ si $i \neq j$ et $m_{ij} = \infty$ quand on n'impose pas de relation entre s_i et s_j.

Soit S l'ensemble des générateurs, on dit que (W, S) est système de Coxeter.

Remarque A.58. Les relations d'une présentation d'un groupe de Coxeter sont encodées dans la matrice (m_{ij}) appelée matrice de Coxeter du système (W, S). Cette matrice est donc une matrice symétrique dont les éléments sur la diagonale valent 1.

On représente également un système de Coxeter par un diagramme de Coxeter-Dynkin qui est un graphe dont les sommets sont étiquetés par les générateurs s_i et les arêtes $\{i, j\}$ sont étiquetées par les entiers m_{ij}, sauf dans les cas $m_{ij} = 3$ où l'arête n'est pas étiquetée et les cas $m_{ij} = 2$ où l'arête est retirée.

Exemple A.59. Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions élémentaires, c'est à dire celles du type $(i\ \ i+1)$, qu'on note plus simplement s_i. En effet, pour une transposition quelconque $(i\ \ j)$ avec $i < j$ on a :

$$(i\ \ j) = s_i s_{i+1} \dots s_{j-2} s_{j-1} s_{j-2} \dots s_{i+1} s_i.$$

Deux transpositions élémentaires s_i et s_j ayant des supports disjoints commutent donc $(s_i s_j)^2 = I$ et quand elles ne commutent pas, on a $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$, donc $(s_i s_{i+1})^3 = I$. On démontre qu'une présentation de $\mathfrak{S}_n$ est donnée par les générateurs τ_i pour $i = 0 \dots n-2$ et les relations τ_i^2 pour $i = 0 \dots n-2$, $(\tau_i \tau_{i+1})^3$ pour $i = 0 \dots n-3$ et $(\tau_i \tau_j)^2$ pour $i, j = 0 \dots n-2$ et $j > i+1$. Pour $n \geqslant 3$, la matrice du système de Coxeter défini par ces générateurs est :

$$\begin{bmatrix} 1 & 3 & 2 & \cdots & 2 \\ 3 & \ddots & \ddots & \ddots & \vdots \\ 2 & \ddots & \ddots & \ddots & 2 \\ \vdots & \ddots & \ddots & \ddots & 3 \\ 2 & \cdots & 2 & 3 & 1 \end{bmatrix}.$$

Exemple A.60. Le groupe diédral est un autre exemple classique de groupe de Coxeter. Pour $n \geqslant 3$, le groupe diédral D_{2n} est le groupe des isométries laissant invariant un polygone à n côtés. Ses éléments sont les n symétries et les n rotations laissant invariant le polygone et il a donc pour cardinal $2n$. On remarque qu'il est engendré par deux symétries : une symétrie s_1 selon la médiatrice d'un segment et une symétrie s_2 selon un axe joignant le centre du polygone à l'une des extrémités de ce segment. Ainsi $s_1 s_2$ est une rotation d'angle $\frac{2\pi}{n}$ et $(s_1 s_2)^n = I$. On démontre qu'une présentation de D_{2n} est $\langle x, y \mid x^2, y^2, (xy)^n \rangle$.

Annexe B

Preuves des théorèmes donnant une présentation du groupe $\langle CZ, SWAP\rangle_n$

B.1 Preuve du théorème 3.8

Si $n = 2$ le résultat annoncé s'écrit

$$\langle CZ, SWAP\rangle_2 \simeq \langle z_0, s_0 \mid z_0^2, s_0^2, (z_0 s_0)^2\rangle,$$

ce qui vrai car le groupe $\langle CZ, SWAP\rangle_2$ est un groupe commutatif formé des 4 éléments I, $Z_{\{0,1\}}$, $S_{(0\ 1)}$ et $Z_{\{0,1\}}S_{(0\ 1)}$ qui sont tous des involutions. Ce groupe est isomorphe à $\mathbb{Z}_2^2$ et c'est un groupe de Coxeter (penser à deux miroirs perpendiculaires).

Remarquons que, pour $n = 3$, le théorème affirme que

$$\langle CZ, SWAP\rangle_3 \simeq \langle z_0, z_1, s_0, s_1 | z_0^2, z_1^2, s_0^2, s_1^2, (s_0 s_1)^3, (z_0 z_1)^2, (z_0 s_0)^2, (z_1 s_1)^2 \\ (z_0 s_1)^4, (z_1 s_0)^4, s_0 s_1 z_0 s_1 s_0 z_1\rangle,$$

ce qui est la première présentation de $\langle CZ, SWAP\rangle_3$ obtenue dans l'exemple 3.7 (équation (3.24)).

Supposons $n \geqslant 3$ et appliquons la proposition 3.5. On obtient pour $\langle CZ, SWAP\rangle_n$ la présentation $\langle \mathcal{S} \mid \mathcal{R}\rangle$ avec

$$\mathcal{S} = \mathcal{T} \cup \mathcal{Z} \text{ et } \mathcal{R} = \mathcal{RT} \cup \mathcal{RZ} \cup \mathcal{RC},$$

où

$$\mathcal{T} = \{s_i \mid 0 \leqslant i \leqslant n-2\},$$

$$\mathcal{Z} = \{z_{\{i,j\}} \mid 0 \leqslant i < j \leqslant n-1\},$$

$$\begin{aligned} \mathcal{RT} =& \{s_i^2 \mid 0 \leqslant i \leqslant n-2\} \cup \{(s_i s_j)^2 \mid 0 \leqslant i < j-1 \leqslant n-3\} \\ & \cup \{(s_i s_{i+1})^3 \mid 0 \leqslant i \leqslant n-3\}, \end{aligned} \tag{B.1}$$

$$\begin{aligned}\mathcal{RZ} =&\{z_{\{i,j\}}^2 \mid 0 \leqslant i < j \leqslant n-1\}\\ &\cup \{(z_{\{i,j\}}z_{\{p,q\}})^2 \mid 0 \leqslant i < j \leqslant n-1, 0 \leqslant p < q \leqslant n-1\},\end{aligned}$$

$$\mathcal{RC} = \{s_p z_{\{i,j\}} s_p z_{\{\tau_p(i),\tau_p(j)\}} \mid 0 \leqslant i < j \leqslant n-1, 0 \leqslant p \leqslant n-2\},$$

avec τ_p la transposition $(p\ \ p+1)$.

Le sous-groupe $G_T = \langle \mathcal{T} \mid \mathcal{RT}\rangle$ est isomorphe au groupe symétrique $\mathfrak{S}_n$, le sous-groupe $G_Z = \langle \mathcal{Z} \mid \mathcal{RZ}\rangle$ est isomorphe à $\mathbb{Z}_2^{\binom{n}{2}}$ et l'ensemble de relations $\mathcal{R}C$ encode la conjugaison d'un élément de $\mathcal{Z}$ par un élément de G_T. Plus précisément, si σ est une permutation de $\mathfrak{S}_n$ et w_σ est l'image de σ dans G_T, alors les relations de $\mathcal{RT}$, $\mathcal{RZ}$ et $\mathcal{RC}$ impliquent que

$$w_\sigma z_{\{i,j\}} w_\sigma^{-1} = z_{\{\sigma(i),\sigma(j)\}}. \tag{B.2}$$

Pour simplifier les notations, on pose dans la suite de cette démonstration $z_{ij} = z_{\{i,j\}}$ et $z_i = z_{\{i,i+1\}}$. La relation $z_{ij}^2 = 1$ peut se déduire de la relation $z_i^2 = 1$ et des relations de $\mathcal{RT} \cup \mathcal{RC}$. En effet, il suffit de considérer une permutation σ qui envoie $\{i,j\}$ sur $\{i,i+1\}$ et d'écrire $z_{ij}^2 = (w_\sigma^{-1} z_i w_\sigma)^2 = w_\sigma^{-1} z_i^2 w_\sigma = 1$. De la même façon, si σ est une permutation qui envoie $\{i,j\}$ sur $\{i_1, i_1+1\}$ et $\{p,q\}$ sur $\{i_2, i_2+1\}$, avec $0 \leqslant i < j \leqslant n-1$, $0 \leqslant p < q \leqslant n-1$, $i \neq p$, $j \neq q$ et $0 \leqslant i_1, i_2 \leqslant n-2$, on a $(z_{ij}z_{pq})^2 = (w_\sigma^{-1} z_{i_1} w_\sigma w_\sigma^{-1} z_{i_2} w_\sigma)^2 = w_\sigma^{-1}(z_{i_1}z_{i_2})^2 w_\sigma$. Ainsi la relation $(z_{ij}z_{pq})^2 = 1$ peut s'obtenir à partir de $(z_{i_1}z_{i_2})^2 = 1$ et des relations de $\mathcal{RT} \cup \mathcal{RC}$. Si ($i = p$ et $j \neq q$) ou ($i \neq p$ et $j = q$), il n'existe pas de permutation qui envoie $\{i,j\}$ sur $\{i_1, i_1+1\}$ et $\{p,q\}$ sur $\{i_2, i_2+1\}$, avec $0 \leqslant i_1, i_2 \leqslant n-2$. On introduit alors l'ensemble de relations

$$\mathcal{RTZ} = \{(z_i s_j)^4 \mid 0 \leqslant i, j \leqslant n-2, |i-j| = 1\}.$$

Ces relations peuvent se déduire de $\mathcal{R}$ car $(z_i s_{i+1})^4 = (z_i z_{ii+2})^2$ et $(z_i s_{i-1})^4 = (z_i z_{i-1i+1})^2$. Si ($i = p$ et $j \neq q$) ou ($i \neq p$ et $j = q$) alors il existe une permutation σ envoyant $\{i,j\}$ sur $\{i_1, i_1+1\}$ et $\{p,q\}$ sur $\{i_1, i_1+2\}$ avec $0 \leqslant i_1 \leqslant n-3$. On a alors $(z_{ij}z_{pq})^2 = (w_\sigma^{-1} z_{i_1} z_{i_1 i_1+2} w_\sigma)^2 = w_\sigma^{-1}(z_{i_1} z_{i_1 i_1+2})^2 w_\sigma = w_\sigma^{-1}(z_{i_1} s_{i_1+1})^4 w_\sigma$.

En conclusion, on a donc

$$\langle \mathcal{S} \mid \mathcal{R}\rangle = \langle \mathcal{S} \mid \mathcal{R}'\rangle$$

avec

$$\mathcal{R}' = \mathcal{RT} \cup \mathcal{RZ}' \cup \mathcal{RC} \cup \mathcal{RTZ}$$

et

$$\mathcal{RZ}' = \{z_i^2 \mid 0 \leqslant i \leqslant n-2\} \cup \{(z_i z_p)^2 \mid 0 \leqslant i, p \leqslant n-2\}.$$

On va maintenant retirer les relations redondantes de $\mathcal{RC}$ et prouver qu'on peut remplacer cet ensemble par

$$\begin{aligned}\mathcal{RC}' = &\{(s_j z_i)^2 \mid |i-j| \neq 1\} \cup \{s_i s_{i+1} z_i s_{i+1} s_i z_{i+1} \mid 0 \leqslant i \leqslant n-3\}\\ &\cup \{s_{j-1} z_{ij} s_{j-1} z_{ij-1} \mid 0 \leqslant i \leqslant j-2 \leqslant n-3\}\end{aligned}$$

dans la présentation $\langle \mathcal{S} \mid \mathcal{R}'\rangle$. Le premier et le dernier ensemble de $\mathcal{RC}'$ sont inclus dans $\mathcal{RC}$. En outre, dans $\langle \mathcal{S} \mid \mathcal{R}'\rangle$, on a $s_i s_{i+1} z_i s_{i+1} s_i z_{i+1} = s_i z_{ii+2} s_i z_{i+1} \in \mathcal{RC}$. Réciproquement, posons

$$\mathcal{R}'' = \mathcal{RT} \cup \mathcal{RZ}' \cup \mathcal{RC}' \cup \mathcal{RTZ}$$

et montrons que, pour tout $w \in \mathcal{RC}$, on a $w = 1$ dans $\langle S \mid \mathcal{R}'' \rangle$. On a :

$$\begin{aligned}\mathcal{RC} \setminus \mathcal{RC}' \subset &\{s_p z_{ij} s_p z_{ij} \mid p \notin \{i-1, i, j-1, j\}\} \cup \{s_j z_{ij} s_j z_{ij+1} \mid 0 \leqslant i \leqslant j-1 \leqslant n-3\} \\ &\cup \{s_{i-1} z_{ij} s_{i-1} z_{i-1j} \mid 1 \leqslant i < j \leqslant n-1\} \\ &\cup \{s_i z_{ij} s_i z_{i+1j} \mid 0 \leqslant i \leqslant j-2 \leqslant n-3\}.\end{aligned}$$

On distingue donc 4 cas :

(i) Considérons l'élément $s_j z_{ij} s_j z_{ij+1}$ avec $0 \leqslant i \leqslant j-1 \leqslant n-3$. On a $s_j z_{ij} s_j z_{ij+1} = (z_{ij+1} s_j z_{ij} s_j)^{-1} = s_j (s_j z_{ij+1} s_j z_{ij})^{-1} s_j = s_j^2 = 1$ dans $\langle \mathcal{S} \mid \mathcal{R}'' \rangle$.

(ii) Considérons l'élément $s_{i-1} z_{ij} s_{i-1} z_{i-1j}$ avec $1 \leqslant i < j \leqslant n-1$. Si $i = j-1$ alors, en utilisant le second et le troisième ensemble de la définition de $\mathcal{RC}'$, on obtient $s_{i-1} z_{ii+1} s_{i-1} z_{i-1i+1} = s_{i-1} z_i s_{i-1} s_i z_{i-1} s_i = s_{i-1} z_i z_i s_{i-1} = 1$ dans $\langle \mathcal{S} \mid \mathcal{R}'' \rangle$. Si $i < j-1$ alors $s_{i-1} z_{ij} s_{i-1} z_{i-1j} = s_{i-1} s_{j-1} z_{ij-1} s_{j-1} s_{i-1} s_{j-1} z_{i-1j-1} s_{j-1} = s_{j-1} s_{i-1} z_{ij-1} s_{i-1} z_{i-1j-1} s_{j-1}$ et, par induction sur $|i-j|$, on obtient $s_{j-1} s_{i-1} z_{ij-1} s_{i-1} z_{i-1j-1} s_{j-1} = s_{j-1}^2 = 1$ dans $\langle \mathcal{S} \mid \mathcal{R}'' \rangle$.

(iii) Considérons l'élément $s_i z_{ij} s_i z_{i+1j}$ avec $0 \leqslant i < j-2 \leqslant n-3$. On a $s_i z_{ij} s_i z_{i+1j} = s_i (s_i z_{i+1j} s_i z_{ij})^{-1} s_i = 1$ en utilisant le cas précédent.

(iv) Supposons que $p \notin \{i-1, i, j-1, j\}$. On procède par induction sur $|i-j|$. Si $j = i+1$ alors le résultat s'obtient directement en utilisant le premier ensemble de relations de $\mathcal{RC}'$. Si $p = i+1 = j-2$ alors, en utilisant les cas précédents, on obtient :

$$s_{i+1} z_{ii+3} s_{i+1} z_{ii+3} = s_{i+1} s_{i+2} s_{i+1} z_i s_{i+1} s_{i+2} s_{i+1} s_{i+2} s_{i+1} z_i s_{i+1} s_{i+2}.$$

Puis, en utilisant le fait que z_i et s_{i+2} commutent dans $\langle \mathcal{S} \mid \mathcal{R}'' \rangle$ ainsi que les relations de $\mathcal{RT}$, on a :

$$s_{i+1} s_{i+2} s_{i+1} z_i s_{i+1} s_{i+2} s_{i+1} s_{i+2} s_{i+1} z_i s_{i+1} s_{i+2} = s_{i+2} s_{i+1} s_{i+2} z_i s_{i+2} z_i s_{i+1} s_{i+2} = 1.$$

Si $p \neq j-2$ alors, en utilisant l'hypothèse de récurrence :

$$s_p z_{ij} s_p z_{ij} = s_p s_{j-1} z_{ij-1} s_{j-1} s_p s_{j-1} z_{ij-1} s_{j-1} = s_{j-1} s_p z_{ij-1} s_p z_{ij-1} s_{j-1} = 1.$$

Finalement, si $p \neq i+1$ alors, en utilisant l'hypothèse de récurrence :

$$s_p z_{ij} s_p z_{ij} = s_p s_i z_{i+1j} s_i s_p s_i z_{i+1j} s_i = s_i s_p z_{i+1j} s_p z_{i+1j} s_i = 1$$

On a donc prouvé que $\langle S \mid \mathcal{R} \rangle = \langle S \mid \mathcal{R}'' \rangle$. On applique maintenant la proposition 3.6 avec

$$\mathcal{S}_1 = \{z_i \mid 0 \leqslant i \leqslant n-2\} \cup \{s_i \mid 0 \leqslant i \leqslant n-2\}$$

et

$$\mathcal{S}_2 = \{z_{ij} \mid 0 \leqslant i \leqslant j-2 \leqslant n-3\}.$$

On obtient $\mathcal{R}'' = \mathcal{R}_1 \cup \mathcal{R}_2$ avec

$$\mathcal{R}_1 = \mathcal{RT} \cup \mathcal{RZ}' \cup \mathcal{RTZ} \cup \{(z_i s_j)^2 \mid |i-j| \neq 1\} \cup \{s_i s_{i+1} z_i s_{i+1} s_i z_{i+1} \mid 0 \leqslant i \leqslant n-3\}$$

et

$$\mathcal{R}_2 = \{s_{j-1} z_{ij} s_{j-1} z_{ij-1} \mid 0 \leqslant i \leqslant j-2 \leqslant k-3\}.$$

Afin d'obtenir $\mathcal{R}'_2$, on substitue chaque occurrence de z_{ij} dans $\mathcal{R}_2$ par $s_{j-1}s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-2}s_{j-1}$ ce qui nous donne

$$\mathcal{R}'_2 = \{s_{j-1}\cdot s_{j-1}s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-1}\cdot s_{j-1}\cdot s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-2} \\ \mid 0\leqslant i\leqslant j-2\leqslant k-3\}.$$

On remarque alors que chaque élément $s_{j-1}\cdot s_{j-1}s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-1}\cdot s_{j-1}\cdot s_{j-2}\cdots s_{i+1}z_is_{i+1}\cdots s_{j-2}$ de $\mathcal{R}'_2$ se réduit à 1 en utilisant les relations de $\mathcal{RT}$ et de $\mathcal{RZ}'$. Finalement, on en déduit que $\langle \mathcal{S} \mid \mathcal{R}\rangle = \langle \mathcal{S}_1 \mid \mathcal{R}_1\rangle$, comme attendu.

B.2 Preuve du théorème 3.11

On trouve de nombreuses redondances dans la présentation du théorème 3.8. Tout d'abord, on calcule

$$\begin{aligned}(z_is_{i-1})^4 &\overset{(vii),(i)}{=} (s_{i-1}s_iz_{i-1}s_i)^4\\ &\overset{(iii),(v)}{=} (s_{i-1}s_iz_{i-1}s_{i-1}s_iz_{i-1}s_{i-1}s_i)^2\\ &\overset{(iii),(i)}{=} s_is_{i-1}(s_iz_{i-1})^4s_{i-1}s_i.\end{aligned} \tag{B.3}$$

Les nombres en chiffres romains correspondent aux règles du théorème 3.8 utilisées pour obtenir chaque égalité. Ainsi, en supposant que $(z_{i-1}s_i)^4 = 1$, on obtient la relation $(z_is_{i-1})^4 = 1$. Cette dernière relation est donc redondante et peut être retirée de la présentation.

Considérons maintenant les relations $\{(z_iz_j)^2 = 1 \mid 0\leqslant i<j\leqslant n-2\}$ du point (iv) du théorème 3.8.

Si $j = i+1$, on a :

$$\begin{aligned}(z_iz_{i+1})^2 &\overset{(vii),(i)}{=} (z_is_is_{i+1}z_is_{i+1}s_i)^2\\ &\overset{(v)}{=} (s_iz_is_{i+1}z_is_{i+1}s_i)^2\\ &\overset{(i)}{=} s_i(z_is_{i+1})^4s_i.\end{aligned}$$

En supposant que $(z_is_{i+1})^4 = 1$ et en appliquant la règle (i), on a donc $(z_iz_{i+1})^2 = 1$, aussi cette relation peut être enlevée de la présentation.

Si $j = i+2$ alors on a

$$\begin{aligned}(z_iz_{i+2})^2 &\overset{(vii),(i)}{=} (s_{i-1}s_iz_{i-1}s_is_{i-1}z_{i+2})^2\\ &\overset{(v)}{=} (s_{i-1}s_iz_{i-1}z_{i+2}s_is_{i-1})^2\\ &\overset{(i)}{=} s_{i-1}s_i(z_{i-1}z_{i+2})^2s_is_{i-1}\\ &\overset{(vii),(i)}{=} s_{i-1}s_i(z_{i-1}s_{i+1}s_{i+2}z_{i+1}s_{i+2}s_{i+1})^2s_is_{i-1}\\ &\overset{(v)}{=} s_{i-1}s_i(s_{i+1}s_{i+2}z_{i-1}z_{i+1}s_{i+2}s_{i+1})^2s_is_{i-1}\\ &\overset{(i)}{=} s_{i-1}s_is_{i+1}s_{i+2}(z_{i-1}z_{i+1})^2s_{i+2}s_{i+1}s_is_{i-1}.\end{aligned}$$

En supposant que $(z_0z_2)^2 = 1$, on montre par récurrence sur i que $(z_iz_{i+2})^2 = 1$.

Si $j > i+2$, alors on a

$$\begin{array}{rcl}(z_iz_j)^2 & \overset{(vii),(i)}{=} & (z_is_{j-1}s_jz_{j-1}s_js_{j-1})^2\\ & \overset{(v)}{=} & (s_{j-1}s_jz_iz_{j-1}s_js_{j-1})^2\\ & \overset{(i)}{=} & s_{j-1}s_j(z_iz_{j-1})^2s_js_{j-1}.\end{array}$$

En supposant que $(z_iz_{i+2})^2 = 1$, on montre par récurrence sur j que $(z_iz_j)^2 = 1$.

En résumé, nous venons de prouver que, en supposant vraies les règles des points $(vii), (vi), (v), (i)$ du théorème 3.8, toutes les règles du point (iv) (i.e $\{(z_iz_j)^2 = 1 \mid 0 \leqslant i < j \leqslant n-2\}$) sont redondantes, sauf une règle : $(z_0z_2)^2 = 1$. On remarque également que $(z_0z_2)^2 = (z_0s_1s_2s_0s_1z_0s_1s_0s_2s_1)^2 = (z_0s_1s_2s_0s_1)^4$.

On applique maintenant la proposition 3.6 en posant $\mathcal{S}_1 = \{z_0, s_0, \dots, s_{n-2}\}$ et $\mathcal{S}_2 = \{z_1, \dots, z_{n-2}\}$ puisque

$$z_i = (s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}).$$

On a

$$\mathcal{R}_1 = \mathcal{RT} \cup \{z_0^2 = 1, (z_0s_1)^4 = 1, (z_0s_1s_2s_0s_1)^4 = 1\} \cup \{(z_0s_j)^2 = 1 \mid j \neq 1\}$$

et

$$\begin{array}{rcl}\mathcal{R}_2 & = & \{z_i^2 = 1 \mid 1 \leqslant i \leqslant n-2\} \cup \{(z_is_{i+1})^4 = 1 \mid 1 \leqslant i \leqslant n-3\}\\ & & \cup\{(z_is_j)^2 = 1 \mid 1 \leqslant i,j \leqslant n-2, j \notin \{i-1, i+1\}\}\\ & & \cup\{s_is_{i+1}z_is_{i+1}s_iz_{i+1} = 1 \mid 0 \leqslant i \leqslant n-3\}\end{array}$$

avec $\mathcal{RT}$ l'ensemble des relations définissant le groupe symétrique (voir équation B.1). Ainsi $\mathcal{R}_2' = \mathcal{T}_1 \cup \mathcal{T}_2 \cup \mathcal{T}_3 \cup \mathcal{T}_4$ avec

$$\mathcal{T}_1 = \{((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}))^2 = 1 \mid 1 \leqslant i \leqslant n-2\},$$

$$\mathcal{T}_2 = \{((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1})^4 = 1 \mid 1 \leqslant i \leqslant n-3\},$$

$$\mathcal{T}_3 = \{((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_j)^2 = 1 \mid 1 \leqslant i,j \leqslant n-2, j \notin \{i-1, i+1\}\},$$

$$\begin{array}{rl}\mathcal{T}_4 = \{s_is_{i+1}(s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1}s_i & \\ (s_is_{i+1})\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_{i+1}s_i) = 1 \mid 0 \leqslant i \leqslant n-3\}. & \end{array}$$

On remarque que $((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}))^2 \overset{\mathcal{R}_1}{=} 1$, donc on peut retirer de $\mathcal{R}_2'$ les relations de $\mathcal{T}_1$.

Dans les calculs qui suivent, on utilise souvent la relation de tresse

$$s_is_{i-1}s_i = s_{i-1}s_is_{i-1} \tag{B.4}$$

qui se déduit facilement de $\mathcal{RT}$. On pose

$$r_{ij} = (s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_j. \tag{B.5}$$

Les relations de $\mathcal{T}_2$ s'écrivent alors $r_{ii+1}^4 = 1$. Montrons que les relations de $\mathcal{T}_2$ sont redondantes. En utilisant les relations dans le groupe symétrique (les relations de $\mathcal{RT}$) et la relation de tresse (B.4), on obtient

$$(s_1s_0)\cdots(s_is_{i-1})s_{i+1}(s_{i-1}s_i)\cdots(s_0s_1) = s_{i+1}s_i\cdots s_2s_1s_2\cdots s_is_{i+1}. \tag{B.6}$$

On a alors :

$$\begin{aligned}
r_{ii+1}^4 &\overset{(B.5)}{=} ((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1})^4\\
&\overset{(B.6)}{=} (s_{i-1}s_i)\cdots(s_0s_1)(z_0s_{i+1}s_i\cdots s_2s_1s_2\cdots s_is_{i+1})^3z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1}\\
&\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_0s_1)s_{i+1}s_i\cdots s_2(z_0s_1)^3z_0s_2\cdots s_is_{i+1}(s_1s_0)\cdots(s_is_{i-1})s_{i+1}\\
&\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_0s_1)(s_{i+1}s_i\cdots s_2s_1s_2\cdots s_is_{i+1})(s_1s_0)\cdots(s_is_{i-1})s_{i+1}\\
&\overset{(B.6)}{=} s_{i+1}s_{i+1}\\
&\overset{\mathcal{RT}}{=} 1.
\end{aligned}$$

On en déduit qu'on peut éliminer les relations de $\mathcal{T}_2$.

Les relations de l'ensemble $\mathcal{T}_3$ s'écrivent $r_{ij}^2 = 1$. Afin de montrer que ces relations sont redondantes, nous distinguons trois cas.

(i) Si $j > i+1$ alors

$$\begin{aligned}
r_{ij}^2 &\overset{\mathcal{R}_1}{=} ((s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1}))^2s_j^2\\
&\overset{\mathcal{R}_1}{=} 1.
\end{aligned}$$

(ii) Si $j = i$ alors en utilisant la relation de tresse (B.4) on obtient :

$$(s_1s_0)\cdots(s_is_{i-1})s_i = s_0(s_1s_0)\cdots(s_is_{i-1}). \tag{B.7}$$

D'où :

$$\begin{aligned}
r_{ii}^2 &\overset{(B.7)}{=} ((s_{i-1}s_i)\cdots(s_0s_1)z_0s_0(s_1s_0)\cdots(s_is_{i-1}))^2\\
&\overset{\mathcal{R}_1}{=} (s_{i-1}s_i)\cdots(s_0s_1)(z_0s_0)^2(s_1s_0)\cdots(s_is_{i-1})\\
&\overset{\mathcal{R}_1}{=} 1.
\end{aligned}$$

(iii) Si $j < i-1$ alors on a

$$\begin{aligned}
r_{ij}^2 &\overset{\mathcal{RT}}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\
&\quad\cdot(s_1s_0)\cdots(s_js_{j-1})(s_{j+1}s_j)(s_{j+2}s_{j+1})s_j\cdots(s_is_{i-1}))^2\\
&\overset{\mathcal{RT}}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\
&\quad\cdot(s_1s_0)\cdots(s_js_{j-1})(s_{j+1}s_{j+2})(s_js_{j+1}s_j)\cdots(s_is_{i-1}))^2\\
&\overset{(B.4)}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\
&\quad\cdot(s_1s_0)\cdots(s_js_{j-1})(s_{j+1}s_{j+2})(s_{j+1}s_js_{j+1})\cdots(s_is_{i-1}))^2\\
&\overset{(B.4)}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\
&\quad\cdot(s_1s_0)\cdots(s_js_{j-1})(s_{j+2}s_{j+1})(s_{j+2}s_js_{j+1})\cdots(s_is_{i-1}))^2\\
&\overset{\mathcal{RT}}{=} ((s_{i-1}s_i)\cdots(s_js_{j+1})(s_{j-1}s_j)\cdots(s_0s_1)z_0\\
&\quad\cdot(s_1s_0)\cdots(s_js_{j-1})s_{j+2}(s_{j+1}s_j)(s_{j+2}s_{j+1})\cdots(s_is_{i-1}))^2\\
&\overset{\mathcal{RT}}{=} (s_{i-1}s_i)\cdots(s_js_{j+1})((s_{j-1}s_j)\cdots(s_0s_1)z_0\\
&\quad\cdot(s_1s_0)\cdots(s_js_{j-1})s_{j+2})^2(s_{j+1}s_j)(s_{j+2}s_{j+1})\cdots(s_is_{i-1})\\
&\overset{\mathcal{RT}}{=} 1 \text{ (en utilisant le premier cas)}
\end{aligned}$$

On peut donc éliminer de $\mathcal{R}_2'$ toutes les relations de $\mathcal{T}_3$.

Finalement, les relations de $\mathcal{T}_4$

$$s_i s_{i+1}(s_{i-1}s_i)\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_is_{i-1})s_{i+1}s_i \\ (s_is_{i+1})\cdots(s_0s_1)z_0(s_1s_0)\cdots(s_{i+1}s_i)$$

se réduisent facilement à 1 en utilisant seulement $s_i^2 = z_0^2 = 1$. Ces relations sont donc aussi redondantes. Ainsi le groupe $\langle CZ, SWAP\rangle_n$ est isomorphe à $\langle \mathcal{S}_1 \mid \mathcal{R}_1\rangle$ et nous obtenons l'énoncé du théorème 3.11 en envoyant z_0 sur g_0 et chaque s_i sur g_{i+1}.

Annexe C

Polynômes covariants associés à un système de 4 qubits

On explique dans cette annexe comment calculer les polynômes covariants qui sont utilisés dans la section 5.1.3 d'une part, pour déterminer le type d'intrication d'un état de 4 qubits, et dans la section 5.2.3 (lemme 5.12) d'autre part, afin de vérifier si un état est dans l'orbite SLOCC de $|W_4\rangle$.

On donne d'abord la définition de l'opération de transvection de deux formes binaires multilinéaires f et g en les variables $x^{(1)} = (x_0^{(1)}, x_1^{(1)}), \ldots, x^{(p)} = (x_0^{(p)}, x_1^{(p)})$:

$$(f,g)_{i_1,\ldots,i_p} = \operatorname{tr} \Omega^{i_1}_{x^{(1)}} \ldots \Omega^{i_p}_{x^{(p)}} f(x'^{(1)}, \ldots, x'^{(p)}) g(x''^{(1)}, \ldots, x''^{(p)}), \tag{C.1}$$

où Ω_x est l'opérateur de Cayley

$$\Omega_x = \begin{vmatrix} \frac{\partial}{\partial x'_0} & \frac{\partial}{\partial x''_0} \\ \frac{\partial}{\partial x'_1} & \frac{\partial}{\partial x''_1} \end{vmatrix} \tag{C.2}$$

et tr envoie chaque variable x', x'' sur x (*i.e.* efface $'$ et $''$). Dans [101] Holweck, Luque et Thibon ont donné un système complet de générateurs de l'algèbre des polynômes covariants pour 4 qubits. Ces générateurs sont obtenus par une suite d'opérations de transvection à partir de la forme de base

$$A = \sum_{i,j,k,\ell} \alpha_{ijk\ell} x_i y_j z_k t_\ell \tag{C.3}$$

associée à un état donné $\sum_{i,j,k,\ell} \alpha_{ijk\ell} |ijk\ell\rangle$ d'un système de 4 qubits. Ci-dessous nous donnons la définition d'une partie de ces générateurs ; ceux qui sont utilisés dans le chapitre 5 de cette thèse.

Symbole	Transvectant
B_{2200}	$\frac{1}{2}(A,A)^{0011}$
B_{2020}	$\frac{1}{2}(A,A)^{0101}$
B_{2002}	$\frac{1}{2}(A,A)^{0110}$
B_{0220}	$\frac{1}{2}(A,A)^{1001}$
B_{0202}	$\frac{1}{2}(A,A)^{1010}$
B_{0022}	$\frac{1}{2}(A,A)^{1100}$

Symbole	Transvectant
C^1_{1111}	$(A,B_{2200})^{1100}+(A,B_{0022})^{0011}$
C_{3111}	$\frac{1}{3}\left((A,B_{2200})^{0100}+(A,B_{2020})^{0010}+(A,B_{2002})^{0001}\right)$
C_{1311}	$\frac{1}{3}\left((A,B_{2200})^{1000}+(A,B_{0220})^{0010}+(A,B_{0202})^{0001}\right)$
C_{1131}	$\frac{1}{3}\left((A,B_{2020})^{1000}+(A,B_{0220})^{0100}+(A,B_{0022})^{0001}\right)$
C_{1113}	$\frac{1}{3}\left((A,B_{2002})^{1000}+(A,B_{0202})^{0100}+(A,B_{0022})^{0010}\right)$

Symbole	Transvectant
D_{2200}	$(A,C^1_{1111})^{0011}$
D_{2020}	$(A,C^1_{1111})^{0101}$
D_{2002}	$(A,C^1_{1111})^{0110}$
D_{0220}	$(A,C^1_{1111})^{1001}$
D_{0202}	$(A,C^1_{1111})^{1010}$
D_{0022}	$(A,C_{1111})^{1100}$
D_{4000}	$(A,C_{3111})^{0111}$
D_{0400}	$(A,C_{1311})^{1011}$
D_{0040}	$(A,C_{1131})^{1101}$
D_{0004}	$(A,C_{1113})^{1110}$

Symbole	Transvectant
E^1_{3111}	$(A,D_{2200})^{0100}+(A,D_{2020})^{0010}+(A,D_{2002})^{0001}$
E^1_{1311}	$(A,D_{2200})^{1000}+(A,D_{0220})^{0010}+(A,D_{0202})^{0001}$
E^1_{1131}	$(A,D_{2020})^{1000}+(A,D_{0220})^{0100}+(A,D_{0022})^{0001}$
E^1_{1113}	$(A,D_{2002})^{1000}+(A,D_{0202})^{0100}+(A,D_{0022})^{0010}$

Symbole	Transvectant
F_{4200}	$(A,E^1_{3111})^{0011}$
F_{4020}	$(A,E^1_{3111})^{0101}$
F_{4002}	$(A,E^1_{3111})^{0110}$
F_{0420}	$(A,E^1_{1311})^{1001}$
F_{0402}	$(A,E^1_{1311})^{1010}$
F_{0042}	$(A,E^1_{1131})^{1100}$
F_{2400}	$(A,E^1_{1311})^{0011}$
F_{2040}	$(A,E^1_{1131})^{0101}$
F_{2004}	$(A,E^1_{1113})^{0110}$
F_{0240}	$(A,E^1_{1131})^{1001}$
F_{0204}	$(A,E^1_{1113})^{1010}$
F_{0024}	$(A,E^1_{1113})^{1100}$
F^1_{2220}	$(A,E^1_{1311})^{0101}-(A,E^1_{3111})^{1001}+(A,E^1_{1131})^{0011}$
F^1_{2202}	$(A,E^1_{1311})^{0110}-(A,E^1_{3111})^{1010}+(A,E^1_{1113})^{0011}$
F^1_{2022}	$(A,E^1_{3111})^{1100}-(A,E^1_{1131})^{0110}+(A,E^1_{1113})^{0101}$
F^1_{0222}	$(A,E^1_{1311})^{1100}-(A,E^1_{1131})^{1010}+(A,E^1_{1113})^{1001}$

Symbole	Transvectant
G_{5111}	$(A, F_{4002})^{0001} + (A, F_{4020})^{0010} + (A, F_{4200})^{0100}$
G_{1511}	$(A, F_{0402})^{0001} + (A, F_{0420})^{0010} + (A, F_{2400})^{1000}$
G_{1151}	$(A, F_{0042})^{0001} + (A, F_{0240})^{0100} + (A, F_{2040})^{1000}$
G_{1115}	$(A, F_{0204})^{0100} + (A, F_{0024})^{0010} + (A, F_{2004})^{1000}$
G^1_{3111}	$(A, F_{4200})^{1100}$
G^2_{3111}	$(A, F_{4020})^{1010}$
G^1_{1311}	$(A, F_{2400})^{110}$
G^2_{1311}	$(A, F_{0420})^{0110}$
G^1_{1131}	$(A, F_{2040})^{1010}$
G^2_{1131}	$(A, F_{0240})^{0110}$
G^1_{1113}	$(A, F_{2004})^{1001}$
G^2_{1113}	$(A, F_{0204})^{0101}$

Symbole	Transvectant
H_{4200}	$(A, G_{5111})^{1011}$
H_{4020}	$(A, G_{5111})^{1101}$
H_{4002}	$(A, G_{5111})^{1110}$
H_{0420}	$(A, G_{1511})^{1101}$
H_{0402}	$(A, G_{1511})^{1110}$
H_{0042}	$(A, G_{1151})^{1110}$
H_{2400}	$(A, G^1_{1511})^{0111}$
H_{2040}	$(A, G_{1151})^{0111}$
H_{2004}	$(A, G^1_{1115})^{0111}$
H_{0240}	$(A, G_{1151})^{1011}$
H_{0204}	$(A, G_{1115})^{1011}$
H_{0024}	$(A, G^1_{1115})^{1101}$
H^1_{2220}	$(A, G^1_{1311})^{0101} + (A, G^1_{3111})^{1001} + (A, G^1_{1131})^{0011}$
H^2_{2220}	$(A, G^2_{1311})^{0101} + (A, G^2_{3111})^{1001} + (A, G^2_{1131})^{0011}$
H^1_{2202}	$(A, G^1_{1311})^{0110} + (A, G^1_{3111})^{1010} + (A, G^1_{1113})^{0011}$
H^1_{2022}	$(A, G^1_{3111})^{1100} + (A, G^1_{1131})^{0110} + (A, G^1_{1113})^{0101}$
H^1_{0222}	$(A, G^1_{1311})^{1100} + (A, G^1_{1131})^{1010} + (A, G^1_{1113})^{1001}$

Symbole	Transvectant
I^1_{5111}	$(A, H_{4020})^{0010} + (A, H_{4200})^{0100} + (A, H_{4002})^{0001}$
I^1_{1511}	$(A, H_{0420})^{0010} + (A, H_{2400})^{1000} + (A, H_{4002})^{0001}$
I^1_{1151}	$(A, H_{0240})^{0100} + (A, H_{2040})^{1000} + (A, H_{0042})^{0001}$
I^1_{1115}	$(A, H_{0204})^{0100} + (A, H_{2004})^{1000} + (A, H_{0024})^{0010}$

Symbole	Transvectant
J_{4200}	$(A, I^1_{5111})^{1011}$
J_{4020}	$(A, I^1_{5111})^{1101}$
J_{4002}	$(A, I^1_{5111})^{1110}$
J_{0420}	$(A, I^1_{1511})^{1101}$
J_{0402}	$(A, I^1_{1511})^{1110}$
J_{0042}	$(A, I^1_{1151})^{1110}$
J_{2400}	$(A, I^1_{1511})^{0111}$
J_{2040}	$(A, I^1_{1151})^{0111}$
J_{2004}	$(A, I^1_{1115})^{0111}$
J_{0240}	$(A, I^1_{1151})^{1011}$
J_{0204}	$(A, I^1_{1115})^{1011}$
J_{0024}	$(A, I^1_{1115})^{1101}$

Symbole	Transvectant
K_{3311}	$= (A, J_{4200})^{1000} - (A, J_{2400})^{0100}$
K_{3131}	$= (A, J_{4020})^{1000} - (A, J_{2040})^{0010}$
K_{3113}	$= (A, J_{4002})^{1000} - (A, J_{2004})^{0001}$
K_{1331}	$= (A, J_{0420})^{0100} - (A, J_{0240})^{0010}$
K_{1313}	$= (A, J_{0402})^{0100} - (A, J_{0204})^{0001}$
K_{1133}	$= (A, J_{0042})^{0010} - (A, J_{0024})^{0001}$
K_{5111}	$= (A, J_{4200})^{0100} - (A, J_{4020})^{0010} + (A, J_{4002})^{0001}$
K_{1511}	$= (A, J_{2400})^{1000} - (A, J_{0420})^{0010} + (A, J_{0402})^{0001}$
K_{1151}	$= (A, J_{2040})^{1000} - (A, J_{0240})^{0100} + (A, J_{0042})^{0001}$
K_{1115}	$= (A, J_{2004})^{1000} - (A, J_{0204})^{0110} + (A, J_{0024})^{0010}$

Symbole	Transvectant
L_{6000}	$(A, K_{5111})^{0111}$
L_{0600}	$(A, K_{1511})^{1011}$
L_{0060}	$(A, K_{1151})^{1101}$
L_{0006}	$(A, K_{1115})^{1110}$

A partir de ces générateurs, on construit les polynômes covariants qui sont utilisés dans les sections 5.1.3 et 5.2.3.

- Polynômes utilisés pour déterminer le niveau d'intrication d'un système de 4 qubits (voir [102, section V] pour une description complète de l'algorithme) :

$$\mathcal{L} = L_{6000} + L_{0600} + L_{0060} + L_{0006},$$
$$\mathcal{K}_3 = K_{3311} + K_{3131} + K_{3113} + K_{1331} + K_{1313} + K_{1133},$$
$$\mathcal{K}_5 = K_{5111} + K_{1511} + K_{1151} + K_{1115},$$
$$\overline{\mathcal{G}} = G^1_{3111}G^1_{1311}G^1_{1131}G^1_{1113},\ \mathcal{G} = G^2_{3111} + G^2_{1311} + G^2_{1131} + G^2_{1113},$$
$$\mathcal{H} = H^1_{2220} + H^1_{2202} + H^1_{2022} + H^1_{0222},$$
$$\mathcal{D} = D_{4000} + D_{0400} + D_{0040} + D_{0004},$$
$$\mathcal{C} = (A, B_{2200})^{0110} + (A, B_{2002})^{1001}.$$

- Polynômes utilisés pour caractériser l'orbite SLOCC de $|W_4\rangle$ (voir [101, section III]) :

$$P_B = B_{2200} + B_{2020} + B_{2002} + B_{0220} + B_{0202} + B_{0022},$$
$$P^1_C = C_{3111} + C_{1311} + C_{1131} + C_{1113},$$
$$P^2_C = C_{3111}C_{1311}C_{1131}C_{1113},$$
$$P^1_D = \mathcal{D} = D_{4000} + D_{0400} + D_{0040} + D_{0004},$$

$$P_D^2 = D_{2200} + D_{2020} + D_{2002} + D_{0220} + D_{0202} + D_{0022},$$
$$P_F = F^1_{2220} + F^1_{2202} + F^1_{2022} + F^1_{0222},$$
$$P_L = \mathcal{L} = L_{6000} + L_{0600} + L_{0060} + L_{0006}.$$

Annexe D

Intrication de l'état $|GHZ_n\rangle$

Dans cette annexe, nous montrons que l'état $|GHZ_n\rangle$ n'est pas génériquement intriqué dès que $n > 3$. À cette fin, nous utilisons le résultat de Miyake [141] qui affirme qu'un état est génériquement intriqué si et seulement si il n'annule pas l'hyperdéterminant Δ_n. Dans la pratique, on ne peut pas calculer l'hyperdéterminant dès que n dépasse 4 en raison de sa taille. Cependant, il existe une méthode permettant de tester sa nullité en interprétant l'égalité $\Delta_n(|\psi\rangle) = 0$ en terme d'existence de solutions d'un certain système d'équations (voir [83, p. 445]). Nous commençons par rappeler la propriété utilisée.

On considère les n variables binaires $\mathbf{x}^{(i)} = (x_0^{(i)}, x_1^{(i)})$, $i = 0 \dots n-1$. A chaque état $|\psi\rangle = \sum_{0 \leqslant b_0,\dots,b_{n-1} \leqslant 1} \alpha_{b_0 \dots b_{n-1}} |b_0 \cdots b_{n-1}\rangle$, on associe la forme binaire multilinéaire

$$A(|\psi\rangle) = \sum_{0 \leqslant b_0,\dots,b_{n-1} \leqslant 1} \alpha_{b_0 \dots b_{n-1}} x_{b_0}^{(0)} \cdots x_{b_{n-1}}^{(n-1)}. \tag{D.1}$$

L'hyperdéterminant s'annule pour l'état $|\psi\rangle$ si et seulement si le système

$$\{A(|\psi\rangle) = 0\} \cup \{\frac{d}{dx_i^{(j)}} A(|\psi\rangle) = 0 \mid 0 \leqslant i \leqslant 1, 0 \leqslant j \leqslant n-1\} \tag{D.2}$$

a une solution $\hat{\mathbf{x}}^{(0)}, \dots, \hat{\mathbf{x}}^{(n-1)}$ telle que :

$$\hat{\mathbf{x}}^{(j)} \neq (0,0), \text{ pour tout } j = 0 \dots n-1. \tag{D.3}$$

Pour l'état $|GHZ\rangle_n$ ce système s'écrit :

$$\begin{aligned} &x_0^{(0)} \cdots x_0^{(n-1)} + x_1^{(0)} \cdots x_1^{(n-1)} = x_0^{(1)} \cdots x_0^{(n-1)} = x_1^{(1)} \cdots x_1^{(n-1)} = x_0^{(0)} x_0^{(2)} \cdots x_0^{(n-1)} \\ &= x_1^{(0)} x_1^{(2)} \cdots x_1^{(n-1)} = \cdots = x_0^{(0)} \cdots x_0^{(n-2)} = x_1^{(0)} \cdots x_1^{(n-2)} = 0. \end{aligned} \tag{D.4}$$

Pour $n > 3$, on vérifie qu'il suffit de choisir $x_0^{(0)} = x_0^{(1)} = x_1^{(2)} = x_1^{(3)} = 0$ pour satisfaire au système (D.4). Ainsi on peut construire des solutions de (D.4) vérifiant la condition (D.3) et on en déduit que $|GHZ_n\rangle$ n'est pas génériquement intriqué dès que $n > 3$.

Dans les cas où $n = 2, 3$, on remarque qu'une solution de (D.4) ne peut vérifier la condition (D.3) , ainsi $|GHZ_2\rangle = |EPR\rangle$ et $|GHZ_3\rangle$ sont génériquement intriqués. Par exemple pour $n = 3$ le système (D.4) s'écrit :

$$\begin{cases} x_0^{(0)} x_0^{(1)} x_0^{(2)} + x_1^{(0)} x_1^{(1)} x_1^{(2)} = 0 \\ x_0^{(0)} x_0^{(1)} = x_0^{(0)} x_0^{(2)} = x_0^{(1)} x_0^{(2)} = 0 \\ x_1^{(0)} x_1^{(1)} = x_1^{(0)} x_1^{(2)} = x_1^{(1)} x_1^{(2)} = 0 \end{cases}$$

et on ne peut avoir de solution telle que $(x_0^{(0)}, x_1^{(0)}) \neq (0,0)$, $(x_0^{(1)}, x_1^{(1)}) \neq (0,0)$ et $(x_0^{(2)}, x_1^{(2)}) \neq (0,0)$.

Annexe E

Liste des solutions au système d'équations 5.40 de la section 5.1.4

Nous donnons dans cette annexe des solutions non triviales au système $S_{|\varphi_G\rangle}$ (5.40), afin de prouver que $\Delta_5(|\varphi_G\rangle) = 0$ pour tout état

$$|\varphi_G\rangle = Z_G(a_0|0\rangle + a_1|1\rangle)(b_0|0\rangle + b_1|1\rangle)(c_0|0\rangle + c_1|1\rangle)(d_0|0\rangle + d_1|1\rangle)(e_0|0\rangle + e_1|1\rangle).$$

résultant de l'application d'un circuit Z_G de $\langle CZ\rangle_5$ sur un état complètement factorisé de 5 qubits. Les solutions sont données dans les tableaux E.1, E.2 et E.3 avec les notations

$$\begin{aligned}
\triangle_1 &= \sum_{i,j,k} (-1)^{j(i+1)+ik} a_i b_j c_k, \\
\triangle_2 &= \sum_{i,j,k} (-1)^{i(j+k)} a_i b_j c_k, \\
\triangle_3 &= \sum_{i,j,k} (-1)^{k(1+j)+ij} a_i b_j c_k, \\
\triangle_4 &= \sum_{i,j,k} (-1)^{j(i+k)} a_i b_j c_k, \\
\triangle_5 &= \sum_{ijk} (-1)^{k+j(k+i)} a_i b_j c_k, \\
\triangle_6 &= \sum_{ijk} (-1)^{j(i+k)} a_i b_j c_k.
\end{aligned}$$

Table E.1 Solutions non triviales au système S_{φ_G} pour $\text{card}(G) < 5$

Classes	Représentants	Cardinal	Solutions $[x_0, y_0, z_0, t_0, s_0]$
$\{\}$	$\{\}$	1	$[1, -\frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, 1]$
$\{\{i,j\}\}$	$\{\{4,3\}\}$	10	$[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\}\}$	$\{\{4,3\},\{4,2\}\}$	30	$[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{k,\ell\}\}$	$\{\{4,3\},\{2,1\}\}$	15	$[1, 1, 1, -\frac{d_1(c_0-c_1}{d_0(c_0+c_1)}, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\}\}$	$\{\{4,3\},\{4,2\},\{4,1\}\}$	20	$[1, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{j,k\},\{i,k\}\}$	$\{\{4,3\},\{3,2\},\{4,2\}\}$	10	$[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{j,\ell\}\}$	$\{\{4,3\},\{4,2\},\{3,1\}\}$	60	$[1, 1, 1, -\frac{d_1 \triangle_1}{d_0 \triangle_2}, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{\ell,m\}\}$	$\{\{4,3\},\{4,2\},\{1,0\}\}$	30	$[1, 1, 1, -\frac{d_1}{d_0}, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\},\{i,m\}\}$	$\{\{4,3\},\{4,2\},\{4,1\},\{4,0\}\}$	5	$[1, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\},\{j,m\}\}$	$\{\{4,3\},\{4,2\},\{4,1\},\{3,0\}\}$	60	$[1, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{j,k\},\{i,k\},\{i,\ell\}\}$	$\{\{4,3\},\{3,2\},\{4,2\},\{4,1\}\}$	60	$[1, -\frac{(i-1)b_1}{(i+1)b_0}, (i+1)\frac{c_1}{c_0}, 1, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{j,k\},\{k,\ell\},\{i,\ell\}\}$	$\{\{4,3\},\{3,2\},\{2,1\},\{4,1\}\}$	15	$[\frac{a_1}{a_0}, \frac{b_1}{b_0}, -\frac{c_1}{c_0}, \frac{d_1}{d_0}, 1]$
$\{\{i,j\},\{k,\ell\},\{\ell,m\},\{k,m\}\}$	$\{\{4,3\},\{2,1\},\{1,0\},\{2,0\}\}$	10	$[1, 1, 1, -\frac{d_1(c_0-c_1)}{d_1(c_0+c_1)}, -\frac{e_1}{e_0}]$
$\{\{i,j\},\{j,k\},\{k,\ell\},\{\ell,m\}\}$	$\{\{4,3\},\{3,2\},\{2,1\},\{1,0\}\}$	60	$[1, 1, 1, -\frac{d_1 \triangle_3}{d_0 \triangle_4}, \frac{e_1}{e_0}]$

Table E.2 Solutions non triviales au système S_{φ_G} pour $\mathrm{card}(G) = 5$

Classes	Représentants	Cardinal	Solutions $[x_0, y_0, z_0, t_0, s_0]$
$\{\{i,j\},\{j,k\},\{k,\ell\},$ $\{\ell,m\},\{i,m\}\}$	$\{\{4,3\},\{3,2\},\{2,1\},$ $\{1,0\},\{4,0\}\}$	12	$[1,1,1,\frac{-d_1\triangle_5}{d_0\triangle_6},-\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\},$ $\{i,m\},\{j,k\}\}$	$\{\{4,3\},\{4,2\},\{4,1\},$ $\{4,0\},\{3,2\}\}$	30	$[1,-\frac{b_1(i-1)}{b_0(i+1)},(i+1)\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\},$ $\{j,m\},\{j,k\}\}$	$\{\{4,3\},\{4,2\},\{4,1\},$ $\{3,0\},\{3,2\}\}$	60	$[1,-\frac{b_1(i-1)}{b_0(i+1)},(i+1)\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\},$ $\{j,k\},\{k,\ell\}\}$	$\{\{4,3\},\{4,2\},\{4,1\},$ $\{3,2\},\{2,1\}\}$	30	$[-i\frac{a_1}{a_0},i\frac{b_1(i-1)}{b_0(i+1)},\frac{c_1}{c_0},\frac{d_1}{d_0},1]$
$\{\{i,j\},\{j,k\},\{k,\ell\},$ $\{i,\ell\},\{j,m\}\}$	$\{\{4,3\},\{3,2\},\{2,1\},$ $\{4,1\},\{3,0\}\}$	60	$[\frac{a_1(i-1)(b_0-b_1)}{a_0(i+1)(b_0+b_1)},1,\frac{c_1}{c_0}i,1,1]$
$\{\{i,j\},\{j,k\},\{i,k\},$ $\{i,\ell\},\{\ell,m\}\}$	$\{\{4,3\},\{3,2\},\{4,2\},$ $\{4,1\},\{1,0\}\}$	60	$[1,-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$

Table E.3 Solutions non triviales au système S_{φ_G} pour $\mathrm{card}(G) > 5$

Classes $\{\{i,j\} \mid 0 \leqslant i < j \leqslant 4\} \setminus E'$ avec $E' =$	Représentants $E' =$	Cardinal	Solutions $[x_0, y_0, z_0, t_0, s_0]$
$\{\}$	$\{\}$	1	$[\frac{a_1}{a_0},-\frac{b_1}{b_0},-\frac{c_1}{c_0},\frac{d_1}{d_0},1]$
$\{\{i,j\}\}$	$\{\{4,3\}\}$	10	$[\frac{a_1}{a_0},-\frac{b_1}{b_0},-\frac{c_1}{c_0},\frac{d_1}{d_0},1]$
$\{\{i,j\},\{i,k\}\}$	$\{\{4,3\},\{4,2\}\}$	30	$[1,-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$
$\{\{i,j\},\{k,\ell\}\}$	$\{\{4,3\},\{2,1\}\}$	15	$[\frac{a_1}{a_0},-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\}\}$	$\{\{4,3\},\{4,2\},\{4,1\}\}$	20	$[-\frac{a_1}{a_0},-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,1]$
$\{\{i,j\},\{j,k\},\{i,k\}\}$	$\{\{4,3\},\{3,2\},\{4,2\}\}$	10	$[1,\frac{b_1}{b_0},-\frac{c_0}{c_1},1,-\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{j,\ell\}\}$	$\{\{4,3\},\{4,2\},\{3,1\}\}$	60	$[\frac{a_1}{a_0},1,-\frac{b_1(c_0-c_1)}{b_0(c_0+c_1)},1,1,-\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{\ell,m\}\}$	$\{\{4,3\},\{4,2\},\{1,0\}\}$	30	$[1,-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,-\frac{e_1}{e_0}]$
$\{\{i,j\},\{i,k\},\{i,\ell\},$ $\{i,m\}\}$	$\{\{4,3\},\{4,2\},\{4,1\},$ $\{4,0\}\}$	5	$[-\frac{a_1}{a_0},-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,1]$
$\{\{i,j\},\{i,k\},\{i,\ell\},$ $\{j,m\}\}$	$\{\{4,3\},\{4,2\},\{4,1\},$ $\{3,0\}\}$	60	$[-\frac{a_1}{a_0},-\frac{b_1(i-1)}{b_0(i+1)},i\frac{c_1}{c_0},1,1]$
$\{\{i,j\},\{j,k\},\{i,k\},$ $\{i,\ell\}\}$	$\{\{4,3\},\{3,2\},\{4,2\},$ $\{4,1\}\}$	60	$[-\frac{a_1}{a_0},\frac{b_1}{b_0},-\frac{c_1}{c_0},1,1]$
$\{\{i,j\},\{j,k\},\{k,\ell\},$ $\{i,\ell\}\}$	$\{\{4,3\},\{3,2\},\{2,1\},$ $\{4,1\}\}$	15	$[-\frac{a_1(c_0-c_1)}{a_0(c_0+c_1)},1,1,-\frac{d_1(b_0-b_1)}{d_0(b_0+b_1)},1]$
$\{\{i,j\},\{k,\ell\},\{\ell,m\},$ $\{k,m\}\}$	$\{\{4,3\},\{2,1\},\{1,0\},$ $\{2,0\}\}$	10	$[\frac{a_1}{a_0},-\frac{b_1}{b_0},-\frac{c_1}{c_0},\frac{d_1}{d_1},1]$
$\{\{i,j\},\{j,k\},\{k,\ell\},$ $\{\ell,m\}\}$	$\{\{4,3\},\{3,2\},\{2,1\},$ $\{1,0\}\}$	60	$[\frac{a_0(c_0-c_1)}{a_1(c_0+c_1)},-\frac{b_1}{b_0},1,1,-\frac{e_1}{e_0}]$

Index

Bibliographie

[1] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5), November 2004.

[2] Georgii Adelson-Velskii and Evgenii Landis. An algorithm for the organization of information. *Soviet Mathematics, Doklady*, 3(5) :1259–1263, 1962.

[3] `https://quantum-computing.ibm.com/`.

[4] Daniel Alsina. *Multipartite entanglement and quantum algorithms*. PhD thesis, Universitat de Barcelona, 2017. arXiv :1706.08318.

[5] Steven C. Althoen and Renate Mclaughlin. Gauss-jordan reduction : A brief history. *The American Mathematical Monthly*, 94(2) :130–142, 1987.

[6] Grâce Amouzou, Jeoffrey Boffelli, Hamza Jaffali, Kossi Atchonouglo, and Frédéric Holweck. Entanglement and non-locality of four-qubit connected hypergraph states. *International Journal of Quantum Information*, 20(3), 2022.

[7] 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, October 2014.

[8] Matthew Amy and Michele Mosca. T-count optimization and reed–muller codes. *IEEE Transactions on Information Theory*, 65(8) :4771–4784, August 2019.

[9] Pablo Arrighi, Vincent Nesme, and Reinhard Werner. One-dimensional quantum cellular automata over finite, unbounded configurations. In Carlos Martín-Vide, Friedrich Otto, and Henning Fernau, editors, *Language and Automata Theory and Applications*, pages 64–75, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[10] Alain Aspect. Proposed experiment to test the nonseparability of quantum mechanics. *Phys. Rev. D*, 14(8) :1944–1951, October 1976.

[11] Alain Aspect. Bell's theorem : The naive view of an experimentalist, 2004.

[12] Jon Aytac and Ammar Husain. Some coxeter groups in reversible and quantum computation. arXiv :quant-ph/1810.08865.

[13] Roger Bach, Damian Pope, Sy-Hwang Liou, and Herman Batelaan. Controlled double-slit electron diffraction. *New Journal of Physics*, 15(3) :033018, March 2013.

[14] 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.

[15] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and John M. Martinis. Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature*, 508 :500–503, April 2014.

[16] Marc Bataille. Reduced quantum circuits for stabilizer states and graph states, 2021. `https://arxiv.org/abs/2107.00885`.

[17] Marc Bataille. Quantum circuits generating four-qubit maximally entangled states. *Mathematical Structures in Computer Science*, 32(3) :257–270, 2022.

[18] Marc Bataille. Quantum circuits of CNOT gates : optimization and entanglement. *Quantum Information Processing*, 21(7) :269, 2022.

[19] Marc Bataille and Jean-Gabriel Luque. Quantum circuits of CZ and SWAP gates : optimization and entanglement. *Journal of Physics A : Mathematical and Theoretical*, 52(32) :325302, July 2019.

[20] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame. Experimental demonstration of graph-state quantum secret sharing. *Nature Communications*, 5(1), November 2014.

[21] John.S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3) :195–200, 1964.

[22] Paul Benioff. The computer as a physical system : A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22 :563–591, May 1980.

[23] Charles H. Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *Theoretical Computer Science*, 560 :7–11, December 2014.

[24] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13) :1895–1899, March 1993.

[25] Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal. Exact and asymptotic measures of multipartite pure-state entanglement. *Physical Review A*, 63(1), December 2000.

[26] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69(20) :2881–2884, November 1992.

[27] Anders Björner and Francesco Brenti. *Combinatorics of Coxeter Groups*. Springer-Verlag Berlin, 2005.

[28] Arnaud Bodin. *Quantum, Un peu de mathématiques pour l'informatique quantique.* Exo7, 2021.

[29] David Bohm. *Quantum theory.* Prentice-Hall, New York, 1951.

[30] N. Bohr. Can quantum-mechanical description of physical reality be considered complete ? *Phys. Rev.*, 48(8) :696–702, October 1935.

[31] Georges Boole. Exposition of a general theory of linear transformation. *Camb. Math. J.*, 3 :1–20, 1841.

[32] Robert I. Booth and Damian Markham. Flow conditions for continuous variable measurement-based quantum computing, 2021.

[33] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 80(6) :1121–1125, February 1998.

[34] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660) :575–579, December 1997.

[35] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing, 1999.

[36] Sergey Bravyi and Dmitri Maslov. Hadamard-free circuits expose the structure of the Clifford group, 2020. arXiv :2003.09412.

[37] Emmanuel Briand, Jean-Gabriel Luque, and Jean-Yves Thibon. A complete set of covariants of the four qubit system. *Journal of Physics A : Mathematical and General*, 36(38) :9915–9927, September 2003.

[38] Emmanuel Briand, Jean-Gabriel Luque, Jean-Yves Thibon, and Frank Verstraete. The moduli space of three-qutrit states. *Journal of Mathematical Physics*, 45(12) :4855–4867, December 2004.

[39] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1) :19–26, January 2009.

[40] Timothée Goubault De Brugière, Marc Baboulin, Benoît Valiron, Simon Martiel, and Cyril Allouche. Gaussian elimination versus greedy methods for the synthesis of linear reversible circuits. *ACM Transactions on Quantum Computing*, 2(3) :1–26, September 2021.

[41] A. V. Burlakov, L. A. Krivitskii, S. P. Kulik, G. A. Maslennikov, and M. V. Chekhova. Measurement of qutrits. *Optics and Spectroscopy*, 94(5) :684–690, May 2003.

[42] J. Calais. *Théorie des groupes.* Dunod, 1981.

[43] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Transactions on Information Theory*, 44(4) :1369–1387, 1998.

[44] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Physical Review Letters*, 78(3) :405–408, January 1997.

[45] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2) :1098–1105, August 1996.

[46] AR Calderbank, PJ Cameron, WM Kantor, and JJ Seidel. Z4-Kerdock codes, orthogonal spreads, and extremal euclidean line-sets. *Proceedings of the London Mathematical Society*, 75(2) :436–480, 1997.

[47] Arthur Cayley. On the theory of linear transformations. *Cambridge Math. J.*, 4, 1845.

[48] Arthur Cayley. Mémoire sur les hyperdéterminants. *Journal für die reine und angewandte Mathematik*, 30 :1–37, 1846.

[49] Arthur Cayley. *The Collected Mathematical Papers*, volume 1 of *Cambridge Library Collection - Mathematics*. Cambridge University Press, 2009.

[50] Lin Chen and Dragomir Z. Djokovic. Proof of the Gour-Wallach conjecture. *Physical Review A*, 88(4), October 2013.

[51] Oleg Chterental and Dragomir Z. Djokovic. Normal forms and tensor ranks of pure states of four qubits, 2006.

[52] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74(20) :4091–4094, May 1995.

[53] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden variable theories. *Physical Review Letters*, 23 :880–884, 1969.

[54] `https://github.com/marcbataille/cnot-circuits/blob/AVL-Tree/optimization/cnot_opt.c`.

[55] `https://github.com/marcbataille/maximum-hyperdeterminant-states`.

[56] `https://github.com/marcbataille/stabilizer-circuits-normal-forms/tree/graph_states`.

[57] Bob Coecke and Ross Duncan. Interacting quantum observables : categorical algebra and diagrammatics. *New Journal of Physics*, 13(4) :043016, April 2011.

[58] Macauley Coggins. *Quantum Computing with Qiskit*. Scarborough Quantum Computing Ltd, 2021.

[59] Claude Cohen-Tannoudji, Bernard Diu, and Frank Laloë. *Mécanique quantique*. Hermann, 1998.

[60] H. S. M. Coxeter and W. O. J. Moser. *Generators and Relations for Discrete Groups*. Springer Berlin, Heidelberg, 1980.

[61] Andrew Cross. The IBM Q experience and QISKit open-source quantum computing software. In *APS March Meeting Abstracts*, volume 2018 of *APS Meeting Abstracts*, page L58.003, January 2018.

[62] Henri De Boutray. *Computational studies of entanglement and quantum contextuality properties towards their formal vérification*. PhD thesis, Université de Bourgogne Franche-Comté, 2021. Thèse de doctorat dirigée par Giorgetti, Alain-Holweck, Frédéric et Masson, Pierre-Alain.

[63] Jeroen Dehaene, Maarten Van den Nest, Bart De Moor, and Franck Verstraete. Local permutations of products of Bell states and entanglement distillation. *Physical Review A*, 67(2), February 2003.

[64] Jeroen Dehaene and Bart De Moor. Clifford group, stabilizer states, and linear and quadratic operations over GF(2). *Physical Review A*, 68(4), October 2003.

[65] `https://www.cnrs.fr/fr/cnrsinfo/le-pepr-quantique-demarre`.

[66] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Series A*, 400(1818) :97–117, July 1985.

[67] David Deutsch. Vidéos de david deutsch. https ://www.daviddeutsch.org.uk/videos/.

[68] David Deutsch and Jozsa ; Richard. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London A : Mathematical, Physical and Engineering Sciences*, 439(1907) :553–558, 1992.

[69] Ellie D'Hondt and Prakash Panangaden. The computational power of the W and GHZ states, 2004. arXiv :quant-ph/0412177.

[70] David P. DiVincenzo. Quantum computation. *Science*, 270(5234) :255–261, 1995.

[71] David P. DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A*, 51(2) :1015–1022, February 1995.

[72] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Wiley, 3 edition, 2004.

[73] Ross Duncan, Aleks Kissinger, Simon Perdrix, and John van de Wetering. Graph-theoretic simplification of quantum circuits with the zx-calculus. *Quantum*, 4 :279, June 2020.

[74] Wolfgang Dür, Guifre Vidal, and Cirac J. Ignacio. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62 :062314, 2000.

[75] W. Dür, H. Aschauer, and H.-J. Briegel. Multiparticle entanglement purification for graph states. *Physical Review Letters*, 91(10), September 2003.

[76] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete ? *Physical Review, Vol. 47*, 1935.

[77] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6) :661–663, August 1991.

[78] Richard P. Feynman. Simulating Physics with Computers. *International Journal of Theoretical Physics*, 21 :467–488, June 1982.

[79] Michael H. Freedman, Kitaev Alexei, Michael J. Larsen, and Zhenghan Wang. Topological quantum computation. *Bulletin of American Mathematical Society*, 40 :31–38, 2004.

[80] Li-Bin Fu, Jing-Ling Chen, and Xian-Geng Zhao. Maximal violation of the clauser-horne-shimony-holt inequality for two qutrits. *Physical Review A*, 68(2), August 2003.

[81] Vincenzo Galgano and Frédéric Holweck. Graph states and the variety of principal minors, 2021.

[82] A. Garsia and Université du Québec à Montréal. Laboratoire de combinatoire et d'informatique mathématique. *The Saga of Reduced Factorizations of Elements of the Symmetric Group*. Publications du Laboratoire de Combinatoire et d'Informatique Mathématique. Université du Québec, 2002.

[83] Israel M Gelfand, Mikhail M. Kapranov, and Zelevisnky Andrei V. *Discriminants, Resultants and Multidimensional Determinant*. Birkhäuser, 1992.

[84] Neil A. Gershenfeld and Isaac L. Chuang. Bulk spin-resonance quantum computation. *Science*, 275(5298) :350–356, 1997.

[85] Daniel Gottesman. Class of quantum error-correcting codes saturating the quantum hamming bound. *Phys. Rev. A*, 54(3) :1862–1868, September 1996.

[86] Daniel Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, Pasadena, CA, 1997.

[87] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61(4) :042311, March 2000.

[88] Daniel Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation, 2009. arXiv :0904.2557.

[89] Timothée Goubault de Brugière, Marc Baboulin, Benoît Valiron, Simon Martiel, and Cyril Allouche. Quantum cnot circuits synthesis for nisq architectures using the syndrome decoding problem. In Ivan Lanese and Mariusz Rawski, editors, *Reversible Computation*, pages 189–205, Cham, 2020. Springer International Publishing.

[90] Gilad Gour and Nolan R. Wallach. All maximally entangled four-qubit states. *Journal of Mathematical Physics*, 51(11) :112201, November 2010.

[91] Gilad Gour and Nolan R. Wallach. On symmetric SL-invariant polynomials in four qubits, 2012. arXiv :1211.5586.

[92] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58(12) :1131, 1990.

[93] 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. ACM.

[94] Otfried Gühne, Géza Tóth, Philipp Hyllus, and Hans J. Briegel. Bell inequalities for graph states. *Phys. Rev. Lett.*, 95(12) :120405, September 2005.

[95] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel. Entanglement in Graph States and its Applications. *arXiv e-prints*, pages quant–ph/0602096, February 2006.

[96] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(6), June 2004.

[97] Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, Maarten Van den Nest, and Briegel Hans J. Entanglement in graph states and its applications. In *Volume 162 : Quantum Computers, Algorithms and Chaos*, Proceedings of the International School of Physics "Enrico Fermi", pages 115 – 218, Amsterdam, The Netherlands, 2006. IOS Press Ebooks.

[98] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3) :1829–1834, March 1999.

[99] Frédéric Holweck. Testing quantum contextuality of binary symplectic polar spaces on a noisy intermediate scale quantum computer. *Quantum Information Processing*, 20(7) :247, July 2021.

[100] Frédéric Holweck, Jean-Gabriel Luque, and Thibon Jean-Yves. Geometric descriptions of entangled states by auxiliary varieties. *Journal of Mathematical Physics*, 53(10) :102203, 2012.

[101] Frédéric Holweck, Jean-Gabriel Luque, and Thibon Jean-Yves. Entanglement of four qubit systems : A geometric atlas with polynomial compass I (the finite world). *Journal of Mathematical Physics*, 55(1) :012202, 2014.

[102] Frédéric Holweck, Jean-Gabriel Luque, and Thibon Jean-Yves. Entanglement of four-qubit systems : a geometric atlas with polynomial compass II (the tame world). *Journal of Mathematical Physics*, 58(2) :022201, 2017.

[103] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2) :865–942, June 2009.

[104] Peter Huggins, Bernd Sturmfels, Josephine Yu, and Debbie S. Yuster. The hyperdeterminant and triangulations of the 4-cube. *Mathematics of Computation*, 77(263) :1653–1679, September 2008.

[105] INRIA. Théorie des codes correcteurs d'erreur : des résultats fondamentaux pour aller vers l'ordinateur quantique. https://www.inria.fr/fr/theorie-codes-correcteurs.

[106] Hamza Jaffali. *Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés*. PhD thesis, Université Bourgogne Franche-Comté, 2020.

[107] Hamza Jaffali and Frédéric Holweck. Quantum entanglement involved in grover's and shor's algorithms : the four-qubit case. *Quantum Information Processing*, 18(5), March 2019.

[108] Hamza Jaffali and Luke Oeding. Learning algebraic models of quantum entanglement. *Quantum Information Processing*, 19(9), August 2020.

[109] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. New protocols and lower bounds for quantum secret sharing with graph states. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 1–12. Springer Berlin Heidelberg, 2013.

[110] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics, 2017.

[111] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics, 2018.

[112] D.L. Johnson. *Presentation of groups, London Math. Soc. Lecture Note series 22.* Cambridge University Press, 1976.

[113] Aleks Kissinger and Arianne Meijer van de Griend. Cnot circuit extraction for topologically-constrained quantum memories. arXiv :1904.00633, 2019.

[114] Aleks Kissinger and John van de Wetering. Reducing the number of non-Clifford gates in quantum circuits. *Physical Review A*, 102(2), August 2020.

[115] Etienne Klein. Comment la physique quantique est-elle née ? `https://www.youtube.com/watch?v=2EQaU7sl-_c`.

[116] Alexander Klyachko. Coherent states, entanglement, and geometric invariant theory. arXiv :quant-ph/0206012v1.

[117] Donald E. Knuth. *The Art of Computer Programming, Volume 3 : Sorting and Searching, Reading.* Mass. : Addison-Wesley, 1973.

[118] Pieter Kok, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1) :135–174, January 2007.

[119] B. Kraus. Local unitary equivalence of multipartite pure states. *Physical Review Letters*, 104(2), January 2010.

[120] Samuel A. Kutin, David Petrie Moulton, and Lawren M. Smithline. Computation at a distance, 2007.

[121] Constantin Le Paige. Sur la théorie des formes binaires à plusieurs séries de variables. *Bull. Acad. Roy. Sci. Belgique*, 3(T. 2) :40 – 53, 1881.

[122] Constantin Le Paige. Sur les formes trilinéaires. *C. R. Acad. Sci. Paris*, 92 :1103–1105, 1881.

[123] Anthony Leverrier and Gilles Zémor. Efficient decoding up to a constant fraction of the code length for asymptotically good quantum codes, 2022.

[124] Anthony Leverrier and Gilles Zémor. Quantum tanner codes, 2022.

[125] N. Linden, S. Popescu, and S. Popescu. On multi-particle entanglement. *Fortschritte der Physik*, 46(4-5) :567–578, June 1998.

[126] Daniel Loss and David P. DiVincenzo. Quantum computation with quantum dots. *Physical Review A*, 57(1) :120–126, January 1998.

[127] David Louapre. La plus belle expérience de la physique. https://www.youtube.com/watch?v=zPolTp0ddRg.

[128] David Louapre. L'(autre) expérience fondatrice de la mécanique quantique. https://www.youtube.com/watch?v=Br7tE3OtbQo.

[129] David Louapre. L'intrication quantique et les inégalités de Bell. https://www.youtube.com/watch?v=0eZ_63iKPho.

[130] David Louapre. Science étonnante. https://www.youtube.com/@ScienceEtonnante.

[131] J. Luque, J. Thibon, and F. Toumazet. Unitary invariants of qubit systems. *Mathematical Structures in Computer Science*, 17 :1133 – 1151, 2007.

[132] Jean-Gabriel Luque. *Invariants des hypermatrices.* Habilitation à diriger des recherches, Université de Marne la Vallée, December 2008.

[133] Jean-Gabriel Luque and Jean-Yves Thibon. The polynomial invariants of four qubits. *Phys. Rev. A*, 67 :042303, 2003.

[134] Jean-Gabriel Luque and Jean-Yves Thibon. Algebraic invariants of five qubits. *Journal of Physics A : Mathematical and General*, 39(2) :371–377, December 2005.

[135] Igor Geront'evich Lysënok. Some algorithmic properties of hyperbolic groups. *Izv. Akad. Nauk SSSR Ser. Mat*, 53(4) :814–832, 1989.

[136] Yuri Ivanovitch Manin. *Computable and Noncomputable (in Russian).* Sovetskoye Radio, Moscow, 1980.

[137] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78(4), October 2008.

[138] Dmitri Maslov. Linear depth stabilizer and quantum fourier transformation circuits with no auxiliary qubits in finite-neighbor quantum architectures. *Physical Review A*, 76(5), November 2007.

[139] Dmitri Maslov and Martin Roetteler. Shorter stabilizer circuits via bruhat decomposition and quantum circuit transformations. *IEEE Transactions on Information Theory*, 64(7) :4729–4738, July 2018.

[140] Mehdi Mhalla, Mio Murao, Simon Perdrix, Masato Someya, and Peter S. Turner. Which graph states are useful for quantum information processing ? In *Theory of Quantum Computation, Communication, and Cryptography*, pages 174–187. Springer Berlin Heidelberg, 2014.

[141] Akimasa Miyake. Classification of multipartite entangled states by multidimensional determinant. *Phys. Rev. A*, 67 :012108, 2003.

[142] Akimasa Miyake. Multipartite entanglement under stochastic local operations and classical communication, 2004.

[143] Akimasa Miyake and Miki Wadati. Multipartite entanglement and hyperdeterminants. *Quantum Information and Computation*, 2(7) :540–555, 2002.

[144] Y. Nakamura, Yu. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-cooper-pair box. *Nature*, 398(6730) :786–788, April 1999.

[145] 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), May 2018.

[146] Beatrice Nash, Vlad Gheorghiu, and Michele Mosca. Quantum circuit optimizations for nisq architectures. *Quantum Science and Technology*, 5(2) :025010, March 2020.

[147] Fabrice Nicot and Corentin Paillassard. Quantique, la révolution du xxi^{e} siècle. *Sciences et Avenir- La Recherche*, pages 34–47, April 2022.

[148] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information : 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[149] Akito Noiri, Kenta Takeda, Takashi Nakajima, Takashi Kobayashi, Amir Sammak, Giordano Scappucci, and Seigo Tarucha. Fast universal quantum gate above the fault-tolerance threshold in silicon. *Nature*, 601 :338–342, January 2022.

[150] Peter Olver. *Classical Invariant Theory*. Cambridge University Press, Cambridge UK, 1999.

[151] Andreas Osterloh and Jens Siewert. Entanglement monotones and maximally entangled states in multipartite qubit systems. *International Journal of Quantum Information*, 04(03) :531–540, June 2006.

[152] `https://atos.net/en/insights-and-innovation/quantum-computing`.

[153] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical ldpc codes, 2021.

[154] Ketan Patel, Igor Markov, and John Hayes. Optimal synthesis of linear reversible circuits. *Quantum Information and Computation*, 8, May 2004.

[155] Frédéric Paulin. Introduction aux groupes de lie pour la physique. `https://www.imo.universite-paris-saclay.fr/~frederic.paulin/notescours/cours_centrale.pdf`.

[156] Simon Perdrix. *Modèles formels du calcul quantique : ressources, machines abstraites et calcul par mesure*. Thèses, INPG, December 2006. Prix de thèse INP Grenoble 2008.

[157] Adrián Pérez-Salinas, Diego García-Martín, Carlos Bravo-Prieto, and José Latorre. Measuring the tangle of three-qubit states. *Entropy*, 22(4) :436, April 2020.

[158] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2 :79, 2018.

[159] William H. Press, Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery. *Numerical Recipes : The Art of Scientific Computing, Third Edition*. Cambridge University Press, 2007.

[160] https://iontrap.duke.edu/.

[161] Narayanan Rengaswamy, Robert Calderbank, Henry D. Pfister, and Swanand Kadhe. Synthesis of logical Clifford operators via symplectic geometry. In *2018 IEEE International Symposium on Information Theory (ISIT)*. IEEE, June 2018.

[162] Joël Riou. Les groupes de coxeter. https://xavier.caruso.ovh/popularization/mathpark/coxeter.pdf.

[163] J. Rothman. *An Introduction to the Theory of Groups*. World Scientific, 2 edition, 2012.

[164] https://github.com/marcbataille/cnot-circuits/blob/master/entanglement/findW4.mpl.

[165] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4) :R2493–R2496, October 1995.

[166] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5) :1484–1509, October 1997.

[167] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77(5) :793–797, July 1996.

[168] M. Steffen, D. P. DiVincenzo, J. M. Chow, T. N. Theis, and M. B. Ketchen. Quantum computing : An IBM perspective. *IBM Journal of Research and Development*, 55(5) :13 :1–13 :11, 2011.

[169] Robert Steinberg. *Lectures on Chevalley Groups*. University Lecture Series 66. American Mathematical Society, 2016.

[170] Yao Tang. Efficient CNOT synthesis for NISQ devices. arXiv :2011.06760, 2020.

[171] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.8)*, 2023. https://www.sagemath.org.

[172] Constantino Tsallis. Possible generalization of boltzmann-gibbs statistics. *Journal of Statistical Physics*, 52(1) :479–487, 1988.

[173] Lev Vaidman. Teleportation of quantum states. *Physical Review A*, 49 :1473–1476, February 1994.

[174] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. Graphical description of the action of local Clifford transformations on graph states. *Physical Review A*, 69(2), February 2004.

[175] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3) :1619–1633, March 1998.

[176] Frank Verstraete, Jeronen Dehaene, Bart De Moor, and Henri Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, 65 :052112, 2002.

[177] Tzu-Chieh Wei. Measurement-based quantum computation, March 2021.

[178] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Physical Review Letters*, 81(23) :5039–5043, December 1998.

[179] Robert Wilson. *The Finite Simple Groups*. Springer London Ltd, 2009.

[180] K. Wright, K. M. Beck, S. Debnath, J. M. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. C. Pisenti, M. Chmielewski, C. Collins, and et al. Benchmarking an 11-qubit quantum computer. *Nature Communications*, 10(1), November 2019.

[181] Xiao Xue, Maximilian Russ, Nodar Samkharadze, Brennan Undseth, Amir Sammak, Giordano Scappucci, and Lieven M. K. Vandersypen. Quantum logic with spin qubits crossing the surface code threshold. *Nature*, 601 :343–347, January 2022.

[182] Bo Yang, Rudy Raymond, Hiroshi Imai, Hyungseok Chang, and Hidefumi Hiraishi. Testing scalable Bell inequalities for quantum graph states on IBM quantum devices, 2021.

[183] D. M. Zajac, T. M. Hazard, X. Mi, E. Nielsen, and J. R. Petta. Scalable gate architecture for a one-dimensional array of semiconductor spin qubits. *Phys. Rev. Applied*, 6(5) :054013, November 2016.

[184] Fang Zhang and Jianxin Chen. Optimizing T gates in Clifford+T circuit as pi/4 rotations around Paulis, 2019.

Titre : Aspects algébriques des circuits quantiques de portes de Clifford. Application à l'optimisation des circuits et à l'intrication

Mots-clés : circuits quantiques, portes de Clifford, optimisation, formes normales, intrication quantique, hyperdéterminant

Résumé : Nous étudions sous l'angle de l'algèbre différents types de circuits quantiques composés de portes quantiques bien connues appelées portes de Clifford. Les outils algébriques utilisés sont principalement issus de la théorie des groupes, de la théorie des invariants et de la géométrie algébrique. Cette étude est reliée à deux problématiques importantes dans la phase actuelle du développement de l'informatique quantique : l'optimisation des circuits quantiques afin de limiter les effets indésirables du bruit dans ces circuits et la production d'états intriqués considérés comme des ressources fondamentales dans divers protocoles de communication.
Nous nous intéressons d'abord aux structures de groupe sous-jacentes à ces circuits. Dans certains cas, cette étude nous permet de développer des algorithmes de réduction de circuits, généralement des heuristiques. Ainsi, nous montrons que le groupe engendré par les portes CZ et $SWAP$ est le quotient d'un groupe de Coxeter et nous en déduisons une heuristique de réduction de circuit utilisant l'algorithme de Dehn. Nous donnons également une écriture des états de graphes en $O(n^2/\ln n)$ portes quantiques agissant sur deux qubits. Enfin, nous construisons une nouvelle forme pseudo-normale pour les circuits de Clifford, reliée à une décomposition originale des matrices du groupe symplectique $\mathrm{Sp}_{2n}(\mathbb{F}_2)$.
Dans un second temps, nous étudions l'apparition de l'intrication dans les circuits de portes CZ d'une part, et de portes $CNOT$ d'autre part. Dans le cas d'un petit nombre de qubits, nous montrons que ces circuits sont capables de produire des états intriqués utiles que nous classifions en orbites sous l'action du groupe SLOCC. Nous nous intéressons également à la possibilité de créer des états génériquement intriqués, c'est à dire des états qui n'annulent pas l'hyperdéterminant de Cayley. En particulier, nous proposons une construction d'un état de 4 qubits qui rend maximal le module de l'hyperdéterminant en utilisant des portes $CNOT$ agissant sur un état factorisé.

Title : Algebraic aspects of Clifford gate quantum circuits. Application to circuit optimization and entanglement

Keywords : quantum circuits, Clifford gates, optimisation, normal forms, quantum entanglement, hyperdeterminant

Abstract : We are exploring different types of quantum circuits composed of well-known quantum gates called Clifford gates from an algebraic perspective. The algebraic tools used are mainly derived from group theory, invariant theory, and algebraic geometry. This study is related to two significant issues in current quantum computing development : circuit optimization to reduce the impact of noise, and producing entangled states, which are essential resources for various communication protocols.
We first focus on the group structures underlying these circuits. In some cases, this study allows us to develop circuit reduction algorithms, typically heuristics. Thus, we show that the group generated by the CZ and $SWAP$ gates is the quotient of a Coxeter group and we use the Dehn algorithm to derive a heuristic for reducing those circuits. We also provide a way to write graph states using $O(n^2/\ln n)$ quantum gates acting on two qubits. Finally, we construct a new pseudo-normal form for Clifford circuits, related to an original decomposition of matrices from the symplectic group $\mathrm{Sp}_{2n}(\mathbb{F}_2)$.
Secondly, we study the occurrence of entanglement in circuits made up of CZ gates and $CNOT$ gates. For a small number of qubits, we show that these circuits can produce useful entangled states, which we classify into orbits under the action of the SLOCC group. We also investigate the possibility of creating generically entangled states, that is, states that do not cancel the Cayley hyperdeterminant. In particular, we propose a construction of a 4-qubit state that maximizes the modulus of the hyperdeterminant using $CNOT$ gates acting on a factorized state.