Marches quantiques généralisées pour l'algorithmique quantique

Olga Lopez Acevedo

Ecole doctorale science et ingenierie
Université de Cergy-Pontoise

Thèse

présentée pour obtenir

le grade de Docteur en Sciences de l'Université de Cergy-Pontoise
Spécialité Physique Théorique

par

Olga Lopez Acevedo

Marches quantiques généralisées pour l'algorithmique quantique

le 19 Décembre 2005
devant le jury composé de :

M. Vladimir Georgescu	Président du Jury
M. Rémy Mosseri	Rapporteur
Mme Nilanjana Datta	Rapporteur
M. François Dunlop	Co-directeur de thèse
M. Thierry Gobron	Co-directeur de thèse
M. Bertrand Georgeot	Examinateur

"-Hay multitud de caminos. Hay uno que va para Contla ; otro que viene de allá. Otro más que enfila derecho a la sierra. Ése que se mira desde aquí, que no sé para dónde irá -y me señaló con sus dedos el hueco del tejado, allí donde el techo estaba roto-."

Juan Rulfo, *Pedro Paramo*

Short abstract/Résumé

English version

We have studied quantum algorithms with the purpose of facing the problem of the calculation of a matrix permanent when the calculation to solve this problem is performed on a quantum machine instead of on a classical one. After constructing some algorithms, we started to study the quantum equivalent of a random walk. These walks are models of a quantum particle evolving at discrete time over a graph, and they have been introduced hoping to build new quantum algorithms from them. We started by generalizing the existing model of quantum walk in order to construct new classes of quantum walks, and we tried to classify all the possible models of these walks. To achieve this, we related the conditions for the existence of the quantum walks to the structure of the graph. For Cayley graphs of groups, we transformed these relations into equations involving generators of the group and started a classification of the walks defined on Cayley graphs of the simplest groups. Then, with the purpose of identifying relevant parameters for the classification of these walks we studied quantum walks over two kinds of graphs: the hypercube and simple lattices in one and two dimensions. For these graphs we obtained an analytical expression for the wave function, in order to explore numerically quantities such as the hitting time and the variance of the walk. Finally, we also extended two existing theorems. The first about the existence of quantum scalar walks and the second related to the weak limit of the walk. These results enable us to consider the classification of more complex graphs with an aim of obtaining structural information on the quantum sub-algorithms that can be constructed within this approach.

Version française

Nous avons étudié les algorithmes quantiques dans le but d'aborder de cette manière le problème du calcul du permanent d'une matrice, lorsque le calcul est réalisé sur une machine quantique et non classique. Après avoir construit quelques algorithmes, nous nous sommes interessés aux marches quantiques, qui sont les équivalents quantiques des marches aléatoires classiques. Ces marches simulent l'évolution à temps discret d'une particule quantique sur un graphe. Un regain d'intérêt pour ces modèles est apparu car ils peuvent être à la base de nouveaux algorithmes quantiques.
Dans ce domaine, nous avons commencé par généraliser le modèle existant de marche quantique, ce qui nous a permis de construire de nouvelles classes de modèles. Nous avons entrepris de classifier les modèles possibles. Nous avons donc relié des conditions d'existence de ses marches à la structure du graphe et pour les graphes de

Cayley des groupes nous avons réécrit ces conditions en termes des relations de groupe. Nous avons ensuite commencé une classification des marches associées aux groupes les plus simples.
Dans la recherche des paramètres importants pour leur classification nous avons étudié des marches sur deux types de graphes : l'hypercube et le réseau simple à une et deux directions. Pour ces graphes nous avons calculé analytiquement la fonction d'onde et exploré numériquement des quantités comme le temps d'arrivée et la variance.
Nous avons de plus élargi deux théorèmes existants, le premier concernant l'existence des marches scalaires et le deuxième la limite en temps infini des moments de la marche. Ces résultats nous permettent d'envisager de compléter la classification des marches pour des graphes plus complexes dans le but d'obtenir des informations structurales sur les sous-algorithmes quantiques possibles par cette approche.

Présentation

La théorie de la complexité quantique cherche à comprendre comment la difficulté à résoudre des problèmes peut changer si le système avec lequel on réalise le calcul est quantique et non classique. Ce type de question n'est pas nouveau dans la théorie de l'information. En fait, changer le modèle initialement construit, la machine de Turing, pour une machine de Turing "non déterministe" et savoir si ces deux machines sont équivalentes est une des questions ouvertes les plus importantes, plus connu comme le problème "$P \neq NP$". On a donc d'une part des machines bien définies et des problèmes à résoudre de l'autre. Chaque machine peut résoudre une partie des problèmes et leur assigne une difficulté suivant les ressources qu'elle utilise. Elle permet de séparer les problèmes qu'elle peut résoudre dans des classes de complexité. La question à résoudre est quelle est la relation entre ces classes de complexité. Dans le premier chapitre on expose les définitions de base de la théorie de la complexité classique ainsi que celles de l'algorithmique quantique. On présente donc ce que la machine quantique peut changer à la théorie établie du point de vue de la complexité .
Pour établir la complexité d'un problème il faut déterminer des limites, minimales en temps par exemple, qu'un algorithme résolvant le problème utilisera dans la machine. Il n'est pas nécessaire de construire l'algorithme pour déterminer ces limites. Des question ponctuelles comme savoir si deux classes sont différentes peuvent être résolues par l'étude d'un seul problème. Dans la partie initiale de la thèse on s'est proposé d'étudier le problème du permanent avec une machine quantique. Nous avons cherché à savoir si des algorithmes quantiques pouvaient résoudre ce problème en un temps polynomial mais nous n'avons pas pu construire de tels algorithmes. Dans le chapitre deux, on présente quelques algorithmes qu'on a construis pendant cette recherche.
A la base du succès des algorithmes polynomiaux sur une machine quantique se trouve la Transformée de Fourier Quantique qui est plutôt un sous-algorithme qui réalise sa tache plus rapidement que son équivalent classique [40]. Une recherche d'autres sous-algorithmes est donc utile. Pour cette raison nous avons entrepris d'étudier les marches quantiques, des sous-algorithmes quantiques potentiels, en cherchant en particulier des aspects se différenciant de façon importante de leurs équivalents classiques. Trouver de telles différences devrait permettre de construire des algorithmes quantiques les utilisant pour résoudre des problèmes en relation avec des graphes, justement ceux qui sont considérés parmi les plus difficiles et dont le permanent est un exemple. Nous nous sommes donc proposé de classifier les marches quantiques en essayant de les séparer par un critère montrant une différence importante avec les marches classiques. Nous avons commencé par élargir la définition

existante [5] utilisant un modèle plus proche des automates cellulaires quantiques. Nous avons ensuite démontré que de tels modèles peuvent être unitaires et entrepris la classification de telles marches sur des graphes de Cayley. Ces résultats sont présentés aussi dans le preprint [4]. Nous avons d'autre part modifié des résultats existants, le théorème "No-go" [29] et la limite faible de la probabilité [28] et [20] pour prendre en compte les nouveaux modèles ici définis. Ces résultats sont présentés dans le chapitre 3.
Finalement dans le chapitre 4 nous avons commencé à explorer quelques aspects des marches à partir desquels on pourrait construire une idée intuitive de leur fonctionnement. Pour ceci nous avons d'abord calculé analytiquement la fonction d'onde dans quelques cas, l'hypercube et la marche sur un réseau simple de dimension 1 et 2. A partir de ces résultats, nous avons calculé numériquement des grandeurs comme le temps de traversée et la variance des marches pour ensuite les comparer aux résultats connus. Dans la dernière section nous avons calculé pour ces derniers réseaux les opérateurs d'évolution de marches vérifiant les conditions de symétrie du graphe. Ce chapitre ouvre des directions de recherches futures que nous discuterons dans la conclusion.

O. Lopez Acevedo, T. Gobron, Quantum Walks on Cayley graphs,*J. Phys A : Math.Gen. 39 (2006)*. LANL preprint quant-ph/0503078.

Remerciements

Cette thèse a été principalement effectue au laboratoire LPTM de l'université de Cergy. Je voudrais remercier son directeur Hung The Diep pour toute l'aide et la confiance qu'il m'a porte pendant ses trois années. Je tiens à exprimer ma reconnaissance à Vladimir Georgescu pour avoir accepté de présider le jury de ma soutenance, à Rémy Mosseri et Nilanjana Datta pour avoir accepte la tache de rapporteurs et à Bertrand Georgeot pour faire partie comme examinateur. Je remercie à tous les membres du jury leur lecture attentive du manuscrit, leurs suggestions importantes et leurs questions intéressantes ce qui est un grand encouragement pour moi. Ce travail a été suivi par Thierry Gobron et Francois Dunlop, je dois leur remercier l'indépendance avec laquelle nous avons travaillé pendant ma thèse et qui a contribue a ma formation. Au laboratoire LPTM ce travail a profité des discussions avec Zoltan Nagy et Marco Mancini à qui je remercie aussi son amitié et son soutien. Dans différentes étapes du travail ainsi que dans la tache d'apprendre a enseigner j'ai profité de l'expérience de Guy Trambly et Jean Philippe Kownacki à qui je remercie de me l'avoir partage. Ce manuscrit a été mis en forme avec l'aide précieuse de Sylvain Reynal. Je dois remercier également à Sylvie Villemin pour son aide toujours efficace et à Yann Costes pour ses compétences en informatique dont j'ai profite au début de cette thèse. Je remercie aussi aux autres membres du laboratoire leur aide a différents moments de cette thèse et les moment partages autour du café. La partie finale de cette thèse et sa rédaction a été effectue pendant un stage de cinq mois a l'Institut de Mathématiques de l'Université de Greifswald en Allemagne. Je tiens à remercier Michael Schurmann et Uwe Franz pour leur invitation. J'ai suis reconnaissante de leur effort pour suivre en cours de route le développement de cette thèse et de m'orienter avec leurs discussions et conseils. Cette thèse a été enrichie de leur façon de travailler ainsi que des discussions avec les autres membres du groupe Rolf Gohm, Santanu Dey, Nicolas Weatherall, Melanie Hintz et Lingaraj Sahu. Je garde de cette expérience les meilleurs souvenirs de ces trois ans, tant pour le travail dans l'institut comme pour les excursions a travers l'Allemagne. Pour terminer un merci a Caroline, Andrés, Nicolás, Javier et Lorena pour leur amitié et pour l'hébergement pendant les fous derniers jours de cette thèse. Je dois pour terminer exprimer les plus importants mercis à Jaime et à ma famille ce n'est que par leur soutien inconditionel et par leur bonne humeur que j'ai eu le nécessaire pour arriver au bout de cette thèse.

Table des matières

Table des figures

Introduction

Dans la Théorie de l'information le processus de calcul est modélisé par l'action d'une machine, la machine de Turing, formulée dans les années 30 par Alan M. Turing [41]. La thèse fondamentale, appelé thèse de Church-Turing associe les fonctions calculables par un algorithme aux fonctions calculables par ces machines. La machine quantique comme définie dans la suite n'est pas en contradiction avec cette thèse car une machine classique peut simuler ces algorithmes, de façon non efficace bien sûr. Pour prendre en compte l'efficacité de la machine une autre thèse a été développée, la thèse de Church "forte" laquelle suppose qu'il y a une machine qui doit pouvoir simuler toute autre machine réalisable avec un temps polynomial, ce modèle étant justement la machine de Turing probabiliste.
En voulant remplacer la thèse de Churg-Turing par une thèse qui contiendrait explicitement le caractère physique de la machine et donc du processus de calcul, Deutsch [17] a proposé une machine quantique qui devrait être capable de simuler n'importe quel système quantique. Comme la nouvelle machine quantique est physiquement réalisable elle pourrait contredire la thèse de Church-Turing forte.
Le but de la première section est de présenter les définitions ainsi que les références qui précisent ce que peut apporter l'algorithmique quantique à la théorie de la complexité.
Quelques algorithmes quantiques importants pour le deuxième chapitre de cette thèse sont présentés dans la deuxième section et dans la dernière section on peut trouver quelques résultats sur les marches quantiques, sujet sur lequel porte la partie principale de cette thèse.

0.1 Bases de l'algorithmique quantique

Les bases de l'algorithmique quantique sont maintenant bien établies et nous suivrons principalement pour la partie classique le livre de Papadimitriou [36] et pour la partie quantique le livre de Nielsen et Chuang [35] ainsi que l'article de Keyl [25].
Nous allons commencer par définir le modèle de calcul classique appelé machine de Turing ainsi que le modèle de circuits, modèle équivalent à la machine de Turing, et certaines classes de complexité associées. Ensuite, après avoir défini le modèle de calcul quantique nous résumons les relations existantes entre les différentes classes.

0.1.1 Modèles de calcul classique

Machine de Turing [36]

La machine de Turing est une machine qui devrait calculer tout algorithme possible, cette affirmation est une hypothèse qui n'a pas été contredite en presque un siècle de développement de la Théorie de l'Information. Elle est connue comme la thèse de Church-Turing : **Thèse de Church-Turing** : *La classe de fonctions calculables par une machine de Turing correspond exactement à la classe des fonctions qu'on pourrait naturellement voir comme étant calculables par un algorithme.*
De façon générale, une machine de Turing accepte une chaîne de caractères comme entrée, la modifie suivant une fonction appelé programme et s'arrête quand un état spécifique est obtenu au cours de l'itération. Elle est équipée d'un pointeur, qui peut être déplacé suivant les instructions du programme et qui signale un élément de la chaîne de caractères qui doit être "lu" par la machine et éventuellement modifié dans l'étape suivante.
Une **machine de Turing** M est un quadruplet $M = (\Sigma, K, \delta, s)$. Σ est un ensemble fini appelé alphabet, il contient les éléments particuliers appelés blanc ($\sqcup$) et départ ($\triangleright$). La chaîne de caractères utilisée par M est une séquence ordonnée d'éléments de Σ. K est un ensemble fini, dont les éléments sont appelés des états de la machine. L'état initial sera toujours noté s. On a que K et Σ sont disjoints. δ est une fonction appelée programme et définie par

$$\delta : K \times \Sigma \to (K \cup \{oui, non, arret\}) \times \Sigma \times \{\leftarrow, \rightarrow, \_\}$$

Les éléments de l'ensemble $\{\leftarrow, \rightarrow, \_\}$, des instructions qui indiquent le sens de déplacement du pointeur que la machine doit réaliser, et les éléments de l'ensemble $\{oui, non, arret\}$, des instructions qui commandent l'arrêt de la machine, ne sont pas dans $K \cup \Sigma$.
Dans une itération quelconque la machine lit un élément de la chaîne indiqué par le curseur et un autre élément appelé état. Ensuite ces états sont modifiés suivant le programme δ et le curseur est déplacé. La machine s'arrêtera quand un des états suivants (qui ne sont pas dans K) seront atteints : *oui, non, arrêt.*
Un état global, à un temps donné de la machine, peut être représenté par un couple $(q, \underline{x_0}x_1 \dots x_n)$ où q est un élément de K, $x_0x_1 \dots x_n$ est une chaîne de caractères et le symbole $\_$ indique la position du curseur et l'élément de la chaîne qui va a être lu. Ainsi par exemple si la machine se trouve dans l'état $(s, \underline{x})$, avec $s \in K$ et $x \in \Sigma$, a partir de (s, x) la fonction δ détermine quel est le nouvel état qui va remplacer s , le nouveau symbole qui va remplacer x et la direction, gauche, droite ou aucune $(\leftarrow, \rightarrow, \_)$, dans laquelle le pointeur va être déplacé. Dans l'étape suivante un nouvel état, un nouveau symbole seront lus, modifiés par le programme et le pointeur déplacé. L'itération se fait jusqu'à atteindre un nouvel état d'arrêt. Il existe quelques règles en plus, l'une évite que le pointeur "tombe" vers la gauche : $\delta(q, \triangleright) = (q', x, s)$ implique $(q', x, s) = (q', \triangleright, \rightarrow)$ et une autre permet d'augmenter la taille de la chaîne en insérant un symbole blanc en bout de chaîne si le pointeur indique le dernier élément et le curseur doit être déplace vers la droite.
Au moment de l'arrêt la machine M aura en plus de l'état d'arrêt une chaîne de caractères finale qui dépend de la chaîne de caractères initiale. On peut donc dire

que la machine M calcule une fonction qui associe une chaîne initiale x a une chaîne finale notée $M(x)$.
Comme le modèle de calcul quantique a été construit en analogie avec un autre modèle appelé modèle de circuits on utilisera ce modèle pour définir les autres machines et les classes de complexité du reste de la section.

Modèle de circuits [25]

Un **calcul classique déterministe** consiste en l'évaluation d'une transformation $f : \mathbb{B}^n \to \mathbb{B}^m$, où $\mathbb{B} = \{0, 1\}$.
Si $m = 1$ alors f est une n-fonction booléenne. Par exemple les opérations logiques $\wedge$ "et" et $\vee$ "ou" sont des 2-fonctions booléennes, $\neg$ "non" est une 1-fonction booléenne.
Une **expression booléenne** prend l'une des formes suivantes :
a) x_i une variable booléenne, variable à deux valeurs possibles 0 ou 1.
b) $\neg\phi_1$, avec ϕ_1 une expression booléenne.
c) $\phi_1 \vee \phi_2$, avec ϕ_1 et ϕ_2 des expressions booléennes.
d) $\phi_1 \wedge \phi_2$, avec ϕ_1 et ϕ_2 des expressions booléennes.

Proposition 0.1 *[36] Toute n-fonction booléenne peut être exprimée comme une expression booléenne ϕ_f contenant n variables $x_1, x_2, \ldots, x_n$.*

Une façon possible est la forme appelé disjonctive. Cette forme s'obtienne en construisant une expression booléenne ϕ_x pour chaque élément x de $\mathbb{B}^n$ tel que $f(x) = 1$; le résultat de cette expression ϕ_x n'est 1 que si la variable est exactement x. Finalement on forme une expression contenant toutes les ϕ_x connectés par des 2-fonctions $\vee$.
Un **circuit** est un graphe acyclique orienté. Les vertex du graphe sont des variables booléennes ou des "portes", les portes sont les fonctions booléennes $\wedge, \vee, \neg$. Les vertex associes aux variables booléennes n'ont qu'un lien sortant (ils représentent l'entrée du circuit), les vertex associes aux n-fonctions ont n liens incidents et il y a dans le graphe un vertex qui n'a pas de lien sortant et représente la sortie. Une entrée valable est un élément de $\mathbb{B}^n$ tel qu'il est possible associer une valeur $\{0, 1\}$ à tous les autres vertex du graphe.
Prenons comme exemple la fonction 3-fonction booléenne définie par

$$f(x) = \begin{cases} 1 & x = (0, 0, 1) \\ 1 & x = (1, 0, 1) \\ 0 & \text{autrement} \end{cases} \tag{1}$$

l'expression booléenne ϕ_f forme disjonctive de f et le circuit la décrivant sont

$$\phi_f = (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \tag{2}$$

En combinant ces définitions et la proposition on obtient que

Proposition 0.2 *Un calcul classique déterministe est l'application d'un circuit à une entrée valable*

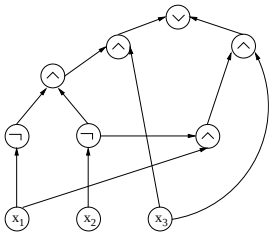


FIG. 1 – Circuit décrivant l'expression ϕ_f

Le **temps d'un circuit** est le nombre d'étapes nécessaires pour exécuter le circuit, en permettant l'action simultanée de portes, la **taille d'un circuit** est le nombre de portes formant le circuit.
Un **problème de décision** est décrit par une famille de fonction booléennes $\{f_n\}$, la taille de l'entrée de f_n est n.
Un choix de la théorie est d'étudier uniquement ce type de calcul, les problèmes plus généraux devant être transformés en un problème de décision.
Une **famille uniforme de circuits polynomiaux** $C = \{C_n\}$ est une famille de circuits tels que C_n a une entrée de n variables, la taille du circuit est bornée par un polynôme fixe $p(n)$, et est uniforme dans le sens qu'une machine de Turing classique peut construire le circuit à partir d'une entrée de taille n avec espace borné (logarithmiquement).
Un **algorithme aléatoire** T est un circuit avec portes "probabilistes", c'est à dire que T associe à un élément $x \in \mathbb{B}^n$ une distribution de probabilité $T_{x.}$ sur $\mathbb{B}^m$. De façon générale ceci est équivalent à dire que si on répète plusieurs fois l'algorithme avec comme entrée x on obtient la sortie y, où y est un élément de $\mathbb{B}^m$, avec probabilité T_{xy}.
Thèse de Church forte *: Tout modèle de calcul peut être simulé par une machine de Turing probabiliste (algorithme aléatoire) avec au plus une augmentation polynomiale du nombre de portes élémentaires utilisées.*

0.1.2 Classes de complexité

Les classes de complexité permettent de séparer les problèmes suivant la façon dont la taille du circuit varie avec le nombre de variables de l'entrée. Une liste détaillé des classes de complexité classiques et quantiques connues se trouve dans [1].
Un problème de décision est en **P** si et seulement si le problème a une famille uniforme de circuits polynomiaux.
Un problème de décision (famille de fonctions booléennes $\{f_n\}$)est en **NP** s'il existe une famille de fonctions booléennes $\{g_n\}$ en classe P telle que si $f_m(x) = 1$ alors il existe un y tel que $g_n(x, y) = 1$, y est appelé alors un témoin, et si $f_m(x) = 0$ alors pour tous les y qui prétendent être un témoin $g_n(x, y) = 0$.
Tout problème en P est aussi en NP, le sens contraire est une question ouverte appelé le problème $P \neq NP$.
BPP est la classe de problèmes de décision admettant un algorithme aléatoire avec temps polynomial et avec une probabilité d'erreur plus petite que $\frac{1}{2} - \epsilon$ pour un ϵ

fixe.

0.1.3 Notation et calcul du temps

Pour calculer le temps d'un algorithme sont nécessaires les résultats suivants [27]. Supposons deux entiers inférieurs à $n = 2^m$ donc décrits avec m bits

- Leur somme requiert un nombre d'opérations binaires maximal m
- Leur multiplication requiert un nombre maximal de m^2 opérations binaires

Une opération binaire est réalisée dans un temps unité dans le modèle de circuits. On a aussi la notation suivante pour préciser le temps d'un algorithme. Si f, g sont des fonctions de $\mathbb{N} \to \mathbb{N}$ alors

- $f(n)$ est $O(g(n))$ s'il existent des constantes n_0, c telles que pour tout $n \geq n_0$ alors $f(n) \leq cg(n)$.
- $f(n)$ est $\Omega(g(n))$ s'il existent des constantes n_0, c telles que pour tout $n \geq n_0$ alors $cg(n) \leq f(n)$.
- $f(n)$ est $\Theta(g(n))$ si $f(n)$ est $O(g(n))$ et $f(n)$ est $\Omega(g(n))$.

Dans le premier cas, $f(n)$ est $O(g(n))$, on dit que f croît moins vite que g, dans le deuxième cas, $f(n)$ est $\Omega(g(n))$, f croît plus vite que g et dans le troisième $f(n)$ est $\Theta(g(n))$, f et g croissent de la même façon.

0.1.4 Modèle de calcul quantique

La construction du modèle de calcul quantique s'est faite essentiellement du milieu des années 80 au milieu des années 90. Après la définition de la machine de Turing quantique [17], le modèle de circuits a été mis en place, par exemple [18] [43], il n'est cependant pas le seul modèle possible. Les relations entre les classes de complexité qu'on exposera par la suite ont été démontrés quelques années après par [10].

Un **registre quantique**, formé de N qubits, est un espace de Hilbert $\mathcal{H}^{\otimes N}$ avec $\mathcal{H} = \mathbb{C}^2$. On utilise une base orthonormale $\{|0\rangle, |1\rangle\}$ de $\mathcal{H}$ de telle sorte que chaque élément $x \in \mathbb{B}^N$ peut être décrit en termes de la base du système complet $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$. Un **circuit quantique** est un graphe G représentant une composition d'opérateurs unitaires éléments d'un ensemble appelé ensemble universel. Tout opérateur unitaire sur un registre quantique de longueur arbitraire peut être représenté comme une composition d'éléments de G. Par exemple l'ensemble formé par toutes les opérations unitaires sur $\mathcal{H}$ et l'opération C_{not}, definie par la suite, sur $\mathcal{H} \otimes \mathcal{H}$ permettent de former un ensemble universel. Nous décrirons une façon possible de représenter les circuits quantiques dans la section suivante.
On peut donc définir, de façon analogue un calcul quantique :
Un **calcul quantique** *est un circuit quantique appliqué à un état d'entrée $|\psi\rangle$ d'un registre quantique.*
Étapes du calcul du problème représenté par la fonction booléenne f.
1. Préparation de l'état approprié comme entrée, par exemple $|\psi_0\rangle = |x\rangle \in \mathcal{H}^{\otimes N}$.
2. Application du circuit C, dont U_C est l'opérateur unitaire correspondant. On obtient $|\psi\rangle = U_C|\psi_0\rangle$.
3. Mesure sur la base initialement décrite, on obtient un élément y de $\mathbb{B}^N$ avec prob-

abilité $P(y) = |\langle y|\psi\rangle|^2$.
4. Eventuellement, on réalise un calcul classique $g(y)$ tel que $f(x) = g(y)$.
BQP est la classe de problèmes de décision qui peuvent être résolus en temps polynomial avec un algorithme quantique avec probabilité d'erreur inférieure à $\frac{1}{4}$. La conjecture $BPP \neq BQP$ entraînerait, si elle était prouvée, l'invalidité de la thèse forte de Church.

0.1.5 Portes élémentaires et universalité

L'ensemble de portes le plus utilisé pour construire des algorithmes contient quatre matrices unitaires appelées Hadamard avec opérateur noté H, Phase avec S, controlled-not avec C_{not} et $\frac{\pi}{8}$ avec P. La démonstration qu' un tel ensemble est universel se trouve en détail dans le texte de Nielsen et Chuang [35] page 188.
Ces matrices agissent sur un qubit, ou sur deux dans le cas de C_{not} et sont définies d'abord sur un des espaces $\mathcal{H}$ et étendues sur tout l'espace $\mathcal{H}^{\otimes n}$ par produit tensoriel avec $n-1$ matrices identité sur tous les autres $n-1$ espaces. Si des matrices agissent de façon non triviale uniquement sur un sous espace de dimension 2 engendré par deux vecteurs de la base choisie, ces matrices sont appelées matrices à deux niveaux. Ces définitions permettent de décrire le schéma de la démonstration d'universalité consiste en trois étapes. Dans la première on établit qu'une matrice unitaire quelconque U de dimension d peut être exprimée comme produit de matrices à deux niveaux. Dans la deuxième étape on démontre que toute matrice unitaire à deux niveaux peut être représentée exactement comme produit de matrices sur un qubit et la matrice C_{not}. Finalement dans la troisième étape on démontre que toute matrice sur un qubit peut être obtenue avec exactitude arbitraire en utilisant les matrices "Hadamard", "Phase", "controlled-not" et "$\frac{\pi}{8}$".
Pour représenter un algorithme quantique (un circuit quantique) il suffit de représenter la suite d'opérateurs élémentaires qui composent l'opérateur complet. De plus, pour décrire les portes élémentaires il est suffisant, étant donné qu'il s'agit des matrices sur un et deux qubits, d'indiquer uniquement sur quel qubit ils agissent de façon non triviale. Par définition, pour reconstruire la matrice totale il suffit de multiplier tensoriellement par des matrices identité agissant sur les autres qubits. Une façon possible de décrire un circuit quantique est donc de représenter chaque qubit avec une suite de liens, les vertex représentant des matrices sur un et sur deux qubits. Sur la figure suivante on a représenté un circuit sur un registre de 4 qubits. L'opérateur que le circuit décrit est le produit de la matrice sur un qubit U agissant de façon non triviale sur le deuxième qubit et la matrice sur deux qubits V agissant de façon non triviale sur les deux derniers qubits. Sur un vecteur de la base standard de l'espace

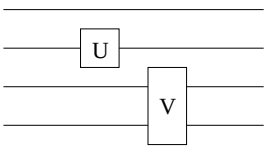


FIG. 2 – Circuit décrivant la composition de l'opérateur sur un qubit U et de l'opérateur sur deux qubits V

$\mathcal{H}^2$ "controlled-not" agit comme

$$C_{not}|x_0, x_1\rangle = |x_0, x_0 \oplus x_1\rangle \tag{3}$$

Ainsi sur la figure suivante on représente un registre formé de deux qubits. L'opérateur controlled-not modifiera le qubit inferieur, indexé par un, dépendant du qubit supérieur, indexé par zéro.

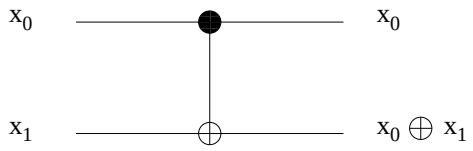


FIG. 3 – Circuit décrivant la porte C_{not}

avec $\oplus$ dénotant la somme modulo 2. Plus généralement sur un espace de dimension supérieure

$$C_{not\,i,j}\,|x_0, x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n\rangle = |x_0, x_1, \ldots, x_i, \ldots, x_i \oplus x_j, \ldots, x_n\rangle \tag{4}$$

Une matrice unitaire 2×2 est déterminée par quatre paramètre réels (modulo 2π) :

$$U(\delta, \alpha, \beta, \theta) = e^{i\delta} \begin{pmatrix} e^{\frac{i}{2}(\alpha+\beta)} \cos\frac{\theta}{2} & e^{\frac{i}{2}(\alpha-\beta)} \sin\frac{\theta}{2} \\ -e^{-\frac{i}{2}(\alpha-\beta)} \sin\frac{\theta}{2} & e^{-\frac{i}{2}(\alpha+\beta)} \cos\frac{\theta}{2} \end{pmatrix} \tag{5}$$

Il est utile de définir maintenant une porte semblable à la porte classique réversible appelée Toffoli. Cette porte ne fait pas partie de l'ensemble universel qu'on utilise ici, pourtant comme elle sera largement utilisé dans les algorithmes du prochain chapitre nous représenterons par T la composition des 40 opérateurs élémentaires décrits dans la figure 4, il faut prendre en compte que $P^\dagger = P^7$. Sur la base standard elle est définie par

$$T|x_0, x_1, x_2\rangle = |x_0, x_1, x_0 x_1 \oplus x_2\rangle \tag{6}$$

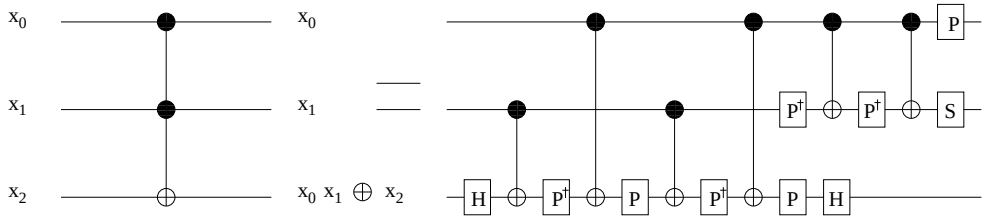


FIG. 4 – Circuit quantique décrivant la porte T

De la même façon que pour C_{not} on peut indexer T pour indiquer le sous espace sur lequel il agit de façon non triviale. Ce produit d'opérateurs vu comme un circuit a un temps égal a 37 [35] page 182. La différence entre C_{not} et T est que le premier agit dépendant de l'état d'un qubit tandis que le deuxième agit dépendant de deux. On peut généraliser ce type d'action avec

$$\Lambda_m(\sigma_x)|x_0, x_1, \ldots, x_m, x_{m+1}\rangle = |x_0, x_1, \ldots, x_m, x_0 x_1 \ldots x_m \oplus x_{m+1}\rangle \tag{7}$$

On peut construire une telle porte avec de l'ordre de m portes T et en effectuant de l'ordre de m additions de qubits. $\Lambda_m(\sigma_x)$ est une porte telle que si $(x_0, \ldots, x_m) = (1, \ldots, 1)$, où en associant les coefficients à la décomposition binaire de x et i si $x = 2^m - 1$ alors le dernier qubit est modifié par l'action de la matrice σ_x. Supposons qu'on a un registre formé de $m+1$ qubits, on peut donc définir $C_{i,not}$ une porte telle que $C_{2^m-1,not} = \Lambda_m(\sigma_x)$ et pour un autre entier agit de la même façon sur le dernier qubit si les premiers forment la décomposition binaire de l'entier i. Cette porte s'obtient en modifiant la porte $\Lambda_m(\sigma_x)$, en ajoutant des matrices σ_x agissant sur les qubits dont le coefficient est 0. Un exemple se trouve dans la figure suivante 0.1.5. En plus du temps de $\Lambda_m(\sigma_x)$ il faut ajouter au maximum $2m$ matrices σ_x. On a donc que cette porte a un temps $O(m)$. La matrice σ_x sur un qubit est définie par $\sigma_x|x\rangle = |1 \oplus x\rangle$ et s'obtient en termes de l'ensemble universel par $\sigma_x = HS^2H$.

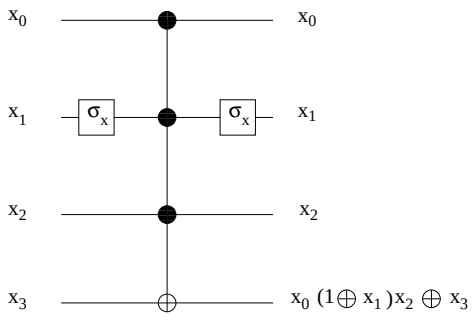


FIG. 5 – Circuit décrivant la porte $C_{2,not}$ sur un registre de 4 qubits

0.2 Algorithmes quantiques

Depuis le milieu des années 90 jusqu'à présent l'effort principal a été porté à trouver des algorithmes quantiques avec une performance meilleure que celle des algorithmes classiques. L'algorithme quantique le plus important est l'algorithme de Shor [39]. L'importance de cet algorithme est qu'il indique que la machine quantique peut être plus fondamentale que la machine classique. Cet algorithme permet de résoudre en un temps polynomial un problème que la machine classique n'a encore pu résoudre que avec un temps exponentiel. D'autres raisons qui ont contribué à faire de cet algorithme un algorithme très connu est d'une part que le problème mathématique est simple à comprendre, le problème de factorisation, et d'autre part que la solution de ce problème a des implications importantes dans d'autres domaines comme la cryptographie. On peut trouver une description de cet algorihtme dans [35].
Un autre algorithme important est celui de Grover, ou algorithme de tri, à la base d'un algorithme qu'on utilisera par la suite. Pour cette raison nous allons présenter cet algorithme plus en détail dans cette introduction. L'algorithme classique pour le même problème cependant n'est que quadratiquement supérieur en temps que l'algorithme de Grover. Les applications de cet algorithme, comme par exemple l'algorithme d'estimation d'amplitude auront le même type de gain en temps par

rapport a l'algorithme classique équivalent. Finalement, dans les dernières années quelques algorithmes utilisant comme base les marches quantiques ont été construits [38] [7].

0.2.1 Algorithme de tri (Grover)

En termes généraux le problème à résoudre est de trouver dans un ensemble un élément qui a une certaine propriété décrite par une fonction n-booléenne f. Si on choisit f telle que

$$f(x) = \begin{cases} 1 & x = x_0 \\ 0 & \text{autrement} \end{cases} \tag{8}$$

alors le problème est de déterminer x_0. On considère un espace de Hilbert de dimension $N = 2^n$, la base de cet espace est $\{|i\rangle\}_{i=0,N-1}$.

Étape 1 : On applique une matrice Hadamard sur chacun des n qubits. L'opérateur complet est $U_1 = H^{\otimes n}$

$$|\psi_0\rangle = U_1|0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle \tag{9}$$

Étape 2 : Soit un opérateur défini comme

$$I_{|\psi\rangle} = \begin{cases} -|x\rangle & x = \psi \\ |x\rangle & \text{autrement} \end{cases} \tag{10}$$

avec lequel on construit $Q = -HI_{|0\rangle}HI_{|x_0\rangle}$ alors

$$|\psi_1\rangle = Q^k|\psi_0\rangle \tag{11}$$

avec $k = Int[\sqrt{N}\frac{\pi}{4} + \frac{1}{2}]$.

Étape 3 : Mesure du système par rapport à la base standard. On obtient l'état $|x_0\rangle$ avec probabilité $P \geq 1 - \frac{1}{N}$

Le temps de l'algorithme est donc pour la première étape $O(n)$ pour la deuxième $O(\sqrt{N}(2n + T(I_{|0\rangle}) + T(I_{|x_0\rangle})$ et pour la troisième 1. On a que $T(M)$ est le temps associé à l'opérateur M. Il est possible de construire $I_{|0\rangle}$ avec un opérateur $\Lambda_n(\sigma_x)$ agissant sur un qubit supplémentaire. Le temps associé est donc $O(n)$. Maintenant, le temps sera déterminé par la deuxième étape et si on suppose que l'opérateur $I_{|x_0\rangle}$ a un temps unité l'algorithme complet aura un temps $O(\sqrt{N})$. On ne peut pas déterminer à l'avance la forme de $I_{|x_0\rangle}$ puisqu'il dépend du problème particulier à résoudre, le temps de l'algorithme complet dependra donc de la possibilité de construire l'operateur $I_{|x_0\rangle}$ dans le temps supposé. On appelle ce type d'algorithme un algorithme avec oracle, où l'opérateur spécifique au problème est supposé avoir un temps unité. Dans le deuxième chapitre nous construirons l'opérateur qui joue le rôle de l'oracle pour le problème du permanent dans un temps tel que il nous permet d'utiliser l'algorithme estimation d'amplitude qui sera décrit dans la section suivante et gagner le facteur .

0.2.2 Algorithme d'estimation d'amplitude

L'algorithme est décrit dans [12]. On présentera ici une version simplifiée, la version dont on se servira par la suite. Supposons que f est une fonction $f : \mathbb{Z}_N \to \{0, 1\}$. On définit les ensembles X_1 et X_0 avec $X_i = \{x \in X | f(x) = i\}$. Le problème est donc de déterminer $|X_1|$, le nombre d'éléments dans l'ensemble X_1. On suppose pour simplifier $N = 2^n$ pour un n entier positif et $M = 2^m$ pour un m entier positif. L'espace de Hilbert complet est le produit tensoriel de deux espaces $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ où le premier est un produit de m espaces élémentaires de dimension deux et le deuxième de n de façon que $\dim \mathcal{H} = MN$. La base est $\{|i\rangle \otimes |j\rangle\}_{i=0,\ldots,M-1, j=0,\ldots,N-1}$ .L'état initial $|\psi_0\rangle = |0\rangle \otimes |0\rangle$. L'opérateur $S_\chi : \mathcal{H}_2 \to \mathcal{H}_2$ est l'oracle, supposé de temps unité et défini par

$$S_\chi : |x\rangle \to (-1)^{f(x)}|x\rangle \tag{12}$$

L'opérateur $\mathcal{A} : \mathcal{H}_2 \to \mathcal{H}_2$ agit sur le vecteur $|0\rangle$ par

$$\mathcal{A}|0\rangle = |\psi_1\rangle + |\psi_0\rangle = \sum_{x \in X_O} |x\rangle + \sum_{y \in X_1} |y\rangle \tag{13}$$

Étape 1 : On crée une superposition de tous les états de la base de $\mathcal{H}_2$ avec l'opérateur $\mathcal{A}$

$$|\psi_1\rangle = (\mathbb{1} \otimes \mathcal{A})|\psi_0\rangle = \frac{-i}{2}|0\rangle \otimes (e^{i\theta_a}|\psi_+\rangle - |e^{-i\theta_a}|\psi_-\rangle) \tag{14}$$

Étape 2 : Avec la transformée de Fourier F_M on crée une superposition de tous les états de la base de $\mathcal{H}_1$

$$|\psi_2\rangle = (F_M \otimes \mathbb{1})|\psi_1\rangle = \frac{1}{\sqrt{2M}} \sum_{j=0}^{M-1} |j\rangle \otimes (e^{i\theta_a}|\psi_+\rangle - e^{-i\theta_a}|\psi_-\rangle) \tag{15}$$

Étape 3 : On modifie la partie du vecteur appartenant à l'espace $\mathcal{H}_1$ dépendant de la partie appartenant à l'espace $\mathcal{H}_2$, plus précisément si le vecteur du premier espace est $|j\rangle$ l'action sur le deuxième est la puissance j de l'opérateur Q qui contient l'oracle S_χ

$$|\psi_3\rangle = \Lambda_M(Q)|\psi_2\rangle = \frac{e^{i\theta_a}}{\sqrt{2}}|S_M(\frac{\theta_a}{\pi})\rangle|\psi_+\rangle - e^{-i\theta_a}|S_M(1 - \frac{\theta_a}{\pi}\rangle \otimes |\psi_-\rangle \tag{16}$$

avec $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_\chi$ et $\Lambda_M(Q) = \sum_{j=0}^{M-1} Q^j \otimes |j\rangle\langle j|$

Étape 4 : On réalise la transformée de Fourier inverse

$$|\psi_4\rangle = F_M^{-1} \otimes \mathbb{1}|\psi_3\rangle = \frac{e^{i\theta_a}}{\sqrt{2}}|M\frac{\theta_a}{\pi}\rangle|\psi_+\rangle - \frac{e^{-i\theta_a}}{\sqrt{2}}|M - M\frac{\theta_a}{\pi}\rangle|\psi_-\rangle \tag{17}$$

Étape 5 : Mesure du premier sous espace. On obtient l'état x avec une probabilité $P \geq \frac{8}{\pi^2}$, on calcule classiquement $\tilde{\theta}_a = \frac{\pi x}{M}$ et $\tilde{a} = \sin^2 \tilde{\theta}_a$. L'erreur dans le calcul, entre la valeur exacte $a = \frac{|X_1|}{N}$ et la mesure $\tilde{a}$ est $|a - \tilde{a}| \leq 2\sqrt{a(1-a)}\frac{\pi}{M} + (\frac{\pi}{M})^2$.

Maintenant on appelle **Count(f,M)** l'algorithme utilisant l'algorithme précédant pour estimer $t = |X_1|$ en fixant M. A partir de $\tilde{a}$ il calcule classiquement $\tilde{t} = N\tilde{a}$. La sortie de Count(f,M) est donc $\tilde{t}$. On demontre que la valeur obtenue est proche de la solution t telle que $|\tilde{t} - t| \leq \frac{2\pi}{M}\sqrt{t(N-t)} + N(\frac{\pi}{M})^2$ et avec probabilité $P \geq \frac{8}{\pi^2}$.

0.2.3 Algorithmes pour les problèmes de la classe NP

Dans la classe NP se trouvent un bon nombre de problèmes importants, comme par exemple le TSP, problème du voyageur du commerce, $\#SAT$ compter le nombre de solutions d'un problème SAT. Une liste de tels problèmes peut être trouvée en [1]. Le problème $P \neq NP$ est tellement important pour la théorie de l'information et les mathématiques qu'il fait partie des sept problèmes du millénium choisis par le Clay Mathematics Institute [2]. Il est donc naturel que beaucoup d'efforts ont été portés sur la classification des problèmes NP par une machine quantique. Un problème de classe NP, le problème de factorisation a été démontré être soluble par une machine quantique en un temps polynomial donc appartenant aussi à la classe BQP. Ce problème n'a pas été demontré être dehors la classe de complexité P.
Il existe aussi une classe qui contient les problèmes avec la propriét é suivante : la solution d'un suel de ces problèmes permettrait de résoudre tout les autres problèmes de la classe NP ; cette classe est appelée $NP-$complète. Jusqu'à présent il n'a pas été construit d'algorithme quantique avec le modèle de circuits résolvant de façon polynomiale de tels problèmes. Par contre, il a été prouvé qu'en supposant une évolution non linéaire d'un système quantique on pourrait construire une machine permettant de les résoudre [3].
Dans le texte de base de Nielsen [35] page 263 on peut trouver un algorithme pour résoudre un problème NP en utilisant l'algorithme Estimation d'amplitude [12]. Même si le temps de l'algorithme quantique est toujours exponentiel, le temps classique devient quadratiquement plus grand. Par contre avec un modèle appelé "Quantum adiabatic quantum computer" plusieurs algorithmes ont été proposés résolvant ces problèmes [19] [32] et [31], des cas nécessitant un temps exponentiel subsistent. Des simulations de ces algorithmes avec des ordinateurs classiques se trouvent dans [9]. Récemment ce modèle et le modèle de circuits ont été démontrés être équivalents [6].

0.3 Marches quantiques

Les marches quantiques ont été introduites en [5] dans le but d'être la base de nouveaux algorithmes quantiques. Un modèle proche avait déjà été étudié auparavant, les automates quantiques cellulaires. Nous allons présenter les deux modèles ainsi que les principaux résultats liés à chacun.

0.3.1 Automates scalaires cellulaires

Soit L un réseau généré par d vecteurs indépendants de $\mathbb{R}^d$. On denote par E l'ensemble de ces d vecteurs. ϕ est une fonction : $\mathbb{N} \times L \rightarrow S$ où $S = \{z \in \mathbb{C} | \, |z| \leq 1\}$

et w une fonction : $L \to \mathbb{C}$. L'évolution est localement définie par :

$$\phi_{t+1}(x) = \sum_{e \in E} w(x+e)\phi_t(x+e) \tag{18}$$

L'évolution est unitaire et dans ce cas le théorème suivant est valable

Theorème 1 *Théorème "No-go" [29] : Le seul automate scalaire unitaire, en n'importe quelle dimension d, évolue par une translation constante et un facteur de phase arbitraire.*

0.3.2 Marches quantiques

Soit G un graphe k-régulier où l'ensemble des liens incidents pour chaque vertex ont été ordonnés et appelés par un entier de 1 à k. L'état d'une particule est décrit par un vecteur d'un espace de Hilbert $\mathcal{H} = \mathcal{H}_I \otimes \mathcal{H}_G$ où $\mathcal{H}_G$ décrit la position de la particule et $\mathcal{H}_I$ des degrés de liberté internes. L'opérateur évolution est unitaire et se décompose en un opérateur C qui mélange les états internes et un opérateur translation S.

$$|\psi_t\rangle = U^t|\psi_0\rangle \tag{19}$$
$$U = S(C \otimes \mathbb{1}) \tag{20}$$
$$S = \sum_{i=1}^{k} |i\rangle\langle i| \otimes T_i \tag{21}$$
$$T_i|x\rangle = |y\rangle \tag{22}$$

où y est le vertex qui forme avec x le lien marqué avec l'entier i dans la liste des liens incidents sur x. Dans [5] ce modèle a été étudié d'une façon générale, les auteurs ont calculé des limites minimales sur des quantités pertinentes pour définir les marches. Ces quantités sont entre autres un temps de mélange (équivalent au "sampling time" classique) et un temps de traversée. En utilisant ces définitions ils obtiennent que on peut espérer augmenter ces quantités au plus de façon polynomiale, par rapport aux marches classiques. D'autres articles présentent des résultats sur des graphes particuliers, un des premiers comportements signalés comme différents est la dépendance de la variance dans le temps. La variance classique augmente linéairement tandis que la variance quantique quadratiquement pour une marche unidimensionnelle avec espace interne de dimension deux [8] [34]. Depuis, ce comportement a été étudié dans la limite du continu en espace et temps [26] et dans la limite de temps infini [28].
Aux résultats de Konno sur la limite faible de la marche unidimensionnelle ont suivi des essais de généralisation à des dimensions supérieures [20].
Pour tester l'influence du choix de l'opérateur interne on peut varier de façon aléatoire l'opérateur appelé "coin operator". Dans [37] les auteurs ont trouvé numériquement qu'avec ce comportement la variance devient linéaire. Pour savoir si l'enchevêtrement de l'état initial a une influence sur la marche, dans [14] les auteurs ont considéré numériquement plusieurs cas qui suggèrent qu'il y a en effet une telle relation.
Mais de tous le seul résultat indiquant une différence importante avec la marche

classique est le temps de traversée de la marche sur l'hypercube [23]. Si le graphe est l'hypercube de dimension n pour un opérateur particulier et une condition initiale symétrique il a été démontré dans cet article que la particule traverse l'hypercube en un temps polynomial en n, c'est à dire que la probabilité de se trouver dans le vertex de distance de Hamming maximal par rapport au point initial est proche de un. Si l'operateur évolution de la marche est W, l'état initial ϕ_0 et $|x\rangle$ est l'état d'arrivée, alors on dit que la marche a un (t, p) temps d'arrivée si

$$|\langle x|W^t|\phi_0\rangle|^2 \geq p \tag{23}$$

Dans [23] il a été demontré que pour un p donnée comme une fonciton de la dimension de l'hypercube, une fonction qui s'approche de 1 à mesure que la dimension de l'hypercube augmente, il existe un temps d'arrivée qui est une fonction linaire dans la dimension de l'hypercube. Pourtant ce résultat n'est pas utilisable pour se déplacer à un autre point du graphe, en fait pour un point se trouvant à la moitié de la distance maximale ce temps est exponentiel.

0.3.3 Graphes de Cayley

On explicitera maintenant la construction d'un graphe de Cayley à partir d'un groupe et sa présentation car une partie importante des marches quantiques étudiées dans cette thèse est définie sur ce type de graphes. Nous allons suivre dans les sections suivantes les définitions utilisées dans le livre de White page 19 [42].

La présentation d'un groupe

Soit Γ un groupe avec $\{g_1, g_2, g_3, \ldots\}$ un sous ensemble de Γ.
Un **mot** dans $g_1, g_2, g_3, \ldots$ est un produit fini $f_1 f_2 \ldots f_n$ où chaque f_i est dans l'ensemble $\{g_1, g_2, g_3, \ldots, g_1^{-1}, g_2^{-1}, g_3^{-1}, \ldots\}$. Une **relation** est une égalité entre deux mots.
Si chaque élément de Γ peut être exprimé comme un mot dans $g_1, g_2, g_3, \ldots$ alors ont dit que $g_1, g_2, g_3, \ldots$ sont **générateurs** de Γ.
Si Γ est généré par $g_1, g_2, g_3, \ldots$ et si toute relation dans Γ peut être déduite à partir des relations $P = P', Q = Q', R = R', \ldots$ alors on écrit

$$\Gamma = \langle g_1, g_2, g_3, \ldots \mid P = P', Q = Q', R = R' \ldots \rangle \tag{24}$$

et le terme de droite est appelé une **présentation** de Γ.
Un élément d'un ensemble générateur d'un groupe Γ est appelé **élément redondant** si il peut être écrit comme un mot dans dans les autres générateurs. Un ensemble générateur d'un groupe Γ est appelé **ensemble générateur minimal** si il ne contient pas d'éléments redondants.
Un graphe dirigé D est dit **fortement connecté** si, pour toute paire u, v de vertex différents, il y a un chemin dirigé de u à v. On dit que D est **faiblement connecté** si le (non dirigé) pseudo graphe sous jacent à D est connecté.

Le graphe de Cayley colorié associé à la présentation d'un groupe

Soit P la présentation d'un groupe Γ et on dénote par $C_P(\Gamma)$, ou par convention par $C_\Delta(\Gamma)$ où Δ est l'ensemble générateur dans P, le graphe de Cayley colorié de P pour Γ.
A chaque présentation du groupe est associe un graphe : chaque vertex correspond à un élément du groupe et les liens sont déterminés et coloriés à partir des générateurs. Si les vertex v_1 et v_2 correspondent aux éléments g_1 et g_2 alors il y a un lien direct (auquel on associe la couleur h) de v_1 vers v_2 si et seulement si $g_1 h = g_2$.
On a donc que $C_\Delta(\Gamma)$ est un graphe dirigé et colorié avec ensemble de vertex $X(C_\Delta(\Gamma))$ et ensemble de liens $E(C_\Delta(\Gamma))$

$$X(C_\Delta(\Gamma)) = \Gamma \tag{25}$$

$$E(C_\Delta(\Gamma)) = \{(g, g\delta)_\delta \,|\, g \in \Gamma, \delta \in \Delta\} \tag{26}$$

Le graphe $C_\Delta(\Gamma)$ dépend non seulement du groupe mais de l'ensemble générateur choisi pour un même groupe. L'effet d'un élément minimal ou redondant dans l'ensemble générateur est différent dans la construction du graphe comme le précise le théorème suivant

Theorème 2 *[42] Soit Γ un group fini (infini). Un générateur h est redondant si et seulement si le résultat d'enlever tous les liens colorés avec h dans $C_\Delta(\Gamma)$ est un graphe directe fortement (faiblement) connecté.*

Le graphe de Cayley (non colorié et non orienté)

Soit Δ un ensemble générateur du groupe Γ avec les conditions suivantes
i) $e \notin \Delta$, e l'élément identité du groupe
ii) $\delta \in \Delta$, $\delta^2 \neq e$, $\delta^{-1} \notin \Delta$
iii) $\delta \in \Delta$, $\delta^2 = e$, chaque paire $(g, g\delta)$ et $(g\delta, g)$ de liens dirigés est remplacé par un seul lien non dirigé $\{g, g\delta\}$
alors le pseudo graphe obtenu du graphe de Cayley colorié $C_\Delta(\Gamma)$ supprimant toutes les directions et toutes les couleurs est un graphe (sans boucles et sans liens multiples). Ce graphes est appelé un graphe de Cayley et est dénoté $G_\Delta(\Gamma)$.
Dans la suite de la thèse on définira des marches quantiques sur des graphes de Cayley coloriés. On utilisera le terme graphe de Cayley au lieu de graphe de Cayley colorié sans pour autant voulant signifier qu'on supprime la direction et la couleur des liens.

Exemples

Pour illustrer comment varie le graphe obtenu d'un même groupe en variant la présentation nous fixerons comme groupe $\Gamma = (\mathbb{Z}^2, +)$ et on notera les generateurs $(1, 0)$ et $(0, 1)$ par δ_x et δ_y respectivement. Nous construirons les trois graphes de Cayley coloriés résultants de choisir un des ensembles générateurs parmi

$$\Delta_1 = \{\delta_x, \delta_y\} \text{ ensemble générateur minimal} \tag{27}$$

$$\Delta_2 = \{\delta_x, \delta_y\, \delta'_x, \delta'_y\} \tag{28}$$

$$\Delta_3 = \{\delta_x, \delta_y, \delta_z\} \tag{29}$$

et les présentations

$$< \Delta_1 | \delta_x \delta_y = \delta_y \delta_x > \tag{30}$$
$$< \Delta_2 | \delta_x \delta'_x = e, \delta_y \delta'_y = e, \delta_x \delta_y = \delta_y \delta_x > \tag{31}$$
$$< \Delta_3 | \delta_z = \delta_x \delta_y, \delta_x \delta_y = \delta_y \delta_x > \tag{32}$$

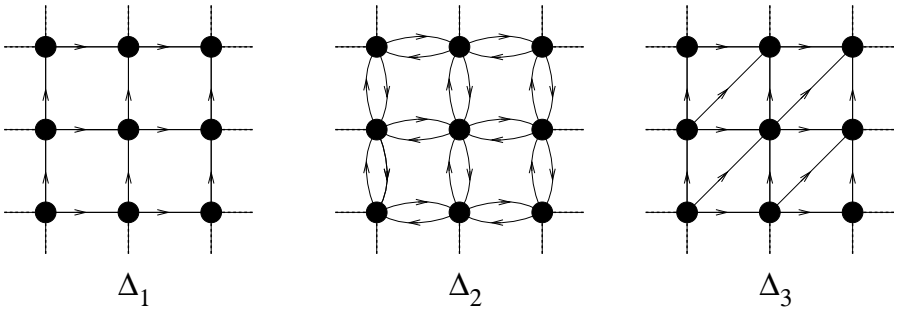


FIG. 6 – Graphes de Cayley colorés du groupe $\mathbb{Z}^2$ avec différentes présentations

Chapitre 1

Le problème du permanent

1.1 Introduction

Le calcul du permanent d'une matrice est un problème réputé difficile. Après le succès de l'algorithme de Shor [39], des tentatives pour réduire le temps de ce type de problèmes en utilisant des algorithmes quantiques ont été faites. L'idée centrale est que l'utilisation de la superposition des états quantiques devrait permettre de diminuer le temps de calcul de certains problèmes, comme le permanent, en analogie avec le calcul en parallèle. Il est possible de transformer directement un algorithme classique existant en un quantique, il suffit de le transformer en un algorithme classique réversible. Les deux premiers algorithmes présentés "somme" et "multiplication" sont justement deux exemples. Convertir un algorithme classique en un quantique n'entraîne pas directement une diminution du temps de calcul par le seul fait d'être un algorithme quantique. Pour le calcul de permanent, nous avons montré qu'une façon naturelle d'essayer de le résoudre, en utilisant le "calcul en parallèle quantique", nécessiterait une porte non unitaire. Nous avons construit aussi un algorithme quantique de temps exponentiel en utilisant un autre algorithme existant l'algorithme d' "Estimation d'amplitude".

1.2 Algorithme de somme

L'algorithme classique qui additionne deux entiers est une boucle dont chaque étape calcule le i-ème coefficient du résultat (l'entier étant décrit par sa décomposition binaire).
Supposons donc deux entiers a et b et leurs décompositions binaires $(a_0, a_1, \ldots, a_{n-1})$ et $(b_0, b_1, \ldots, b_{n-1})$. L'idée est d'additionner les deux coefficients a_i et b_i en s'aidant des deux registres c_{in} et c_{out}. Le calcul suit la formule

$$(a_i, b_i, c_{in}) \rightarrow (a_i, r_i, c_{out}) \tag{1.1}$$

$$r_i = c_{in} \oplus a_i \oplus b_i \tag{1.2}$$

$$c_{out} = a_i b_i \oplus c_{in} a_i \oplus c_{in} b_i \tag{1.3}$$

où $\oplus$ dénote la somme modulo deux.
Dans le tableau suivant nous pouvons vérifier que r_i est le i-ème coefficient de $a + b$

et que c_{out} contient l'information nécessaire pour calculer le coefficient supérieur, c'est à dire $i+1$

a_i	b_i	c_{in}	$\rightarrow$	a_i	r_i	c_{out}
0	0	0		0	0	0
0	1	0		0	1	0
1	0	0		1	1	0
1	1	0		1	0	1
0	0	1		0	1	0
0	1	1		0	0	1
1	0	1		1	0	1
1	1	1		1	1	1

(1.4)

L'algorithme quantique accepte donc comme entrée

$$|\psi_0\rangle = |a, b\rangle \otimes |0, \ldots, 0\rangle \tag{1.5}$$

et obtient la sortie correcte après application de U

$$U|\psi_0\rangle = |a, a+b \mod 2^n\rangle \otimes |0, \ldots, 0\rangle \tag{1.6}$$

Pour simplifier la forme des opérateurs nous réarrangeons la position des coefficients comme suit

$$|\psi_0\rangle = |0, a_0, b_0, 0, a_1, b_1, \ldots, 0, a_{n-1}, b_{n-1}, 0\rangle \tag{1.7}$$

L'opérateur de base S_j, de 3 niveaux effectue la transformation

$$S_j : |c_{in}, a_j, b_j, 0\rangle \rightarrow |c_{in}, a_j, r_j, c_{out}\rangle \tag{1.8}$$

tandis que S'_j remet le coefficient c_{out} à zéro

$$S'_j : |c_{in}, a_j, r_j, c_{out}\rangle \rightarrow |c_{in}, a_j, r_j, 0\rangle \tag{1.9}$$

L'algorithme total sera donc $U = S'_{n-1} \ldots S'_0 S_{n-1} \ldots S_0$. Pour calculer le temps il faut décrire S et S' en terme des portes de la base universelle. Rappelons rapidement l'effet des portes T et C_{not}

$$C_{not\,i,j}|x_i, x_j\rangle = |x_i, x_i \oplus x_j\rangle \tag{1.10}$$

$$T_{i,j,k}|x_i, x_j, x_k\rangle = |x_i, x_j, x_i x_j \oplus x_k\rangle \tag{1.11}$$

ou chaque $x_i \in \{0, 1\}$. On a donc que $S = C_{not\,1,3}\, T_{1,3,4}\, C_{not\,2,3}\, T_{2,3,4}$ et la figure 1.1(a) représente le circuit correspondant. Vérifions l'effet de S sur l'état $|\Phi_0\rangle = |x_1, x_2, x_3, 0\rangle$

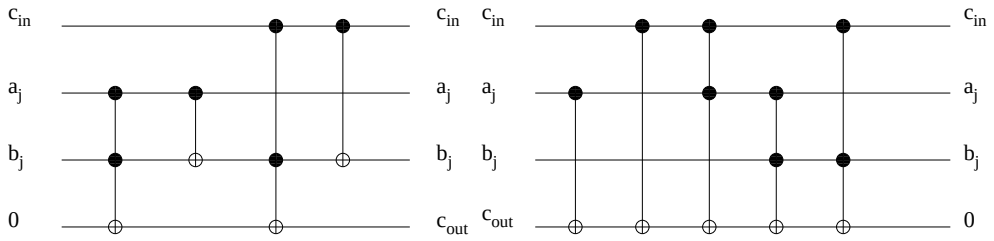
$$|\Phi_1\rangle = T_{2,3,4}|\Phi_0\rangle \quad = |x_1, x_2, x_3, x_2 x_3\rangle \tag{1.12}$$

$$|\Phi_2\rangle = C_{not\,2,3}|\Phi_1\rangle \quad = |x_1, x_2, x_2 \oplus x_3, x_2 x_3\rangle \tag{1.13}$$

$$|\Phi_3\rangle = T_{1,3,4}|\Phi_2\rangle \quad = |x_1, x_2, x_2 \oplus x_3, x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3\rangle \tag{1.14}$$

$$|\Phi_4\rangle = C_{not\,1,3}|\Phi_3\rangle \quad = |x_1, x_2, x_1 \oplus x_2 \oplus x_3, x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3\rangle \tag{1.15}$$

Le temps associé à l'opérateur S est 76. L'opérateur S' de la même façon agit non trivialement sur un sous espace de dimension huit. Le circuit correspondant S' se



(a) Circuit décrivant l'opérateur S (b) Circuit décrivant l'opérateur S'

FIG. 1.1 – Portes de base de l'algorithme Somme

trouve dans la figure 1.1(b) et peut s'écrire $S' = T_{1,3,4}\, T_{2,3,4}\, T_{1,2,4}\, C_{not\,1,4}\, C_{not\,2,4}$. Le temps associé est 113.
L'algorithme consiste d'abord dans la préparation de l'état initial contenant l'information sur les deux entiers, puis dans l'application de n fois l'opérateur S et n fois l'opérateur S', la mesure du système qui donne le résultat en base deux. Le circuit complet se trouve décrit dans la figure 1.2. L'algorithme a un temps polynomial, le détail par étape est

- Préparation de $|\Phi_0\rangle$: On utilise $2n$ matrices σ_x
- Opérateur U : On utilise n opérateurs S et S'
- Mesure : Dans le modèle on a défini cette étape étant de temps $t = 1$

Comme le résultat de l'algorithme est la décomposition binaire de l'entier somme, éventuellement on peut ajouter une partie classique servant à convertir cette décomposition dans une autre, décimale par exemple. Chaque étape requiert un temps proportionnel à n donc l'algorithme a un temps $O(n)$

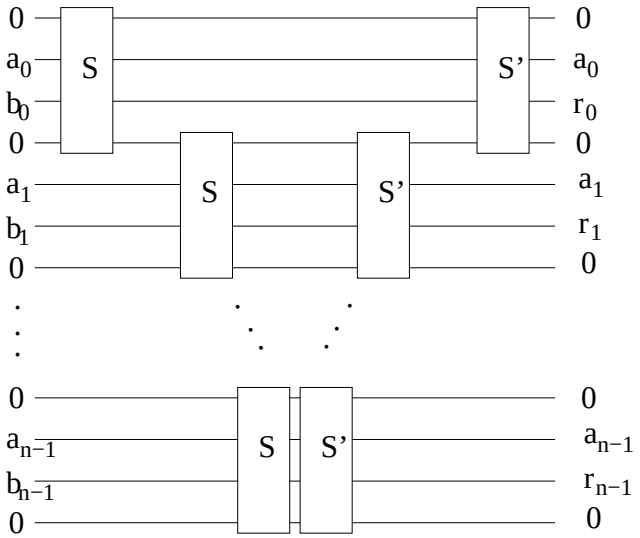


FIG. 1.2 – Circuit décrivant l'algorithme Somme

1.3 Algorithme de multiplication

Une multiplication peut être mise sous la forme d'une somme de n termes, où n est le nombre de bits utilisés.

$$a\,b = (a_0 2^0 + \cdots + a_{n-1}2^{n-1})(b_0 2^0 + \cdots + b_{n-1}2^{n-1}) \tag{1.16}$$

$$= \sum_{i=0}^{n-1}(\sum_{j=0}^{n-1} a_j b_i 2^{j+i}) = \sum_{i=0}^{n-1}(S_i) \tag{1.17}$$

L'algorithme consiste d'abord à transformer

$$|a, b, 0, \ldots, 0\rangle \rightarrow |a, b, S_0, \ldots, S_{n-1}, 0, \ldots, 0\rangle \tag{1.18}$$

pour ensuite utiliser l'algorithme de somme

$$|a, b, S_0, \ldots, S_{n-1}, 0, \ldots, 0\rangle \rightarrow |a, b, S_0, \ldots, S_{n-1}, \sum_i S_i\rangle \tag{1.19}$$

et finalement (partie réversible)

$$|a, b, S_0, \ldots, S_{n-1}, \sum_i S_i\rangle \rightarrow |a, b, 0, \ldots, 0, \sum_i S_i\rangle \tag{1.20}$$

La première porte étape s'obtient en utilisant de l'ordre de n^2 fois une porte T , la deuxième en utilisant n fois l'algorithme de somme déjà décrit et la troisième en utilisant de nouveau n^2 fois la porte T puisque $T^2 = \mathbb{1}$. Le temps de l'algorithme est donc $O(n^2)$. Nous ne décrirons pas de façon plus détaillée l'algorithme.

1.4 Algorithme pour calculer le permanent d'une matrice {0,1}

Si on suppose A une matrice avec éléments $a_{i,j} \in \{0, 1\}$ le permanent de A est défini par

$$perm(A) = \sum_{\sigma \in S_n} \prod_i a_{i,\sigma(i)} \tag{1.21}$$

où S_n est l'ensemble des permutations de n éléments. Comme il y a un nombre $n!$ de termes dans la somme, le temps associé à l'algorithme "définition" consistant dans le calcul littéral de l'expression (1.21) est supérieur à $n!$, c'est à dire $\Omega(n!)$. Le meilleur algorithme exact, connu comme la formule de Ryser

$$perm(A) = (-1)^n \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|} \prod_{i=1}^{n} (\sum_{j \in S} a_{i,j}) \tag{1.22}$$

a un temps $O(n^2 2^n)$.
Une idée simple pour utiliser le parallélisme est de créer une superposition d'états chacun associé à un terme de la somme dans l'équation (1.21) et construire un

opérateur qui les mélange de façon à obtenir le permanent. Supposant qu'on a un espace de Hilbert de dimension $\dim(\mathcal{H}) = 2n^n + 1$ et une base $\{|i_1, i_2, \ldots, i_n\rangle \otimes |j\rangle\}$ avec $1 \leq i_k \leq n$ et $0 \leq j \leq n^n$. Les étapes successives devraient donner les vecteurs suivants

$$|\psi_0\rangle = |0, \ldots, 0\rangle \tag{1.23}$$

$$|\psi_1\rangle = \sum_{i_1,\ldots,i_n=1}^{n} |i_1, i_2, \ldots, i_n\rangle \otimes |0\rangle \tag{1.24}$$

$$|\psi_2\rangle = \sum_{i_1,\ldots,i_n=1}^{n} |i_1, i_2, \ldots, i_n\rangle \otimes |f(i_1, \ldots, i_n)\rangle \tag{1.25}$$

$$|\psi_3\rangle = \sum_{i_1,\ldots,i_n=1}^{n} |i_1, i_2, \ldots, i_n\rangle \otimes |\sum_{i_1,\ldots,i_n=1}^{n} f(i_1, \ldots, i_n)\rangle \tag{1.26}$$

Avec la définition

$$f(i_1, \ldots, i_n) = \begin{cases} a_{1,i_1} \ldots a_{n,i_n} & \text{si} \{i_1, \ldots, i_n\} = \{1, 2, \ldots, n\} \\ 0 & \text{autrement} \end{cases} \tag{1.27}$$

on obtient que $perm(A) = \sum_{i_1=1}^{n} \sum_{i_n=1}^{n} f(i_1, \ldots, i_n)$. Cette dernière étape pourtant n'est pas unitaire et la démonstration est similaire a celle du théorème "No-cloning" [35] page 532. Supposons deux matrices A et A' telles que $perm(A) \neq perm(A')$ et $|\psi_2\rangle$ et $|\psi_2'\rangle$ les vecteurs obtenus dans l'étape numéro 2 de l'algorithme. Supposons que U est l'opérateur unitaire qui réalise la dernière étape et qui ne dépend pas de A et A'. On a donc $\langle\psi_3'|\psi_3\rangle = \langle\psi_2'|\psi_2\rangle$ or le terme de gauche est zéro tandis que le terme de droite, sauf cas particulier, est différent de zéro. L'opération n'est donc pas unitaire.

1.4.1 Algorithme quantique utilisant "Count(f,M)"

Le problème du calcul du permanent peut se mettre sous la forme du calcul du nombre d'éléments appartenant à l'ensemble X_1 défini comme

$$X_1 = \{(x_1, \ldots, x_n) \in \mathbb{N}^n | \{x_1, \ldots, x_n\} \in S_n \,,\, a_{1,x_1} \ldots a_{n,x_n} = 1\} \tag{1.28}$$

Sous cette forme le problème du permanent peut être résolu en utilisant un algorithme quantique existant. Count(f,M) est un algorithme quantique décrit dans [12]. Supposons qu'on a une fonction $f : X \to \mathbb{B}$ telle que $f(x) = 1$ si $x \in X_1$ et $f(x) = 0$ si $x \in X_0$, on a que X_1 et X_0 sont disjoints et $X = X_0 \cup X_1$. On choisit une espace de Hilbert et une base telle que chaque vecteur de la base correspond à un élément de X. L'algorithme "Count(f,M)" estime avec une précision dépendant de M le nombre t d'éléments dans l'ensemble X_1. Les trois caractéristiques principales de l'algorithme sont

1. L'algorithme accepte comme entrée un vecteur d'un espace de Hilbert de dimension N, et a comme sortie un entier $\tilde{t}$ tel que

$$|\tilde{t} - t| \leq \frac{2\pi}{M}\sqrt{t(N-t)} + N(\frac{\pi}{M})^2 \tag{1.29}$$

avec probabilité $P \geq \frac{8}{\pi^2}$.

2. L'algorithme utilise deux opérateurs $\mathcal{A}$ et $\mathcal{S}_\chi$. Le dernier joue le rôle de l'oracle donc associé à la fonction f. Sur la base choisie

$$\mathcal{A}|0,\ldots,0\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{n-1}|i\rangle \tag{1.30}$$

$$= \sum_{x\in X_0}\frac{1}{\sqrt{N}}|x\rangle + \sum_{y\in X_1}\frac{1}{\sqrt{N}}|y\rangle \tag{1.31}$$

$$= |\psi_0\rangle + |\psi_1\rangle \tag{1.32}$$

$$\mathcal{S}_\chi|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle \text{ si } x \in X - X_1 \\ -|x\rangle \text{ si } x \in X_1 \end{cases} \tag{1.33}$$

3. Le temps de l'algorithme est

$$T = T(\mathcal{A}) + (\log_2 M)^2 + M\log_2 N + MT(\mathcal{S}_\chi) + T(\mathcal{A}) \tag{1.34}$$

Nous allons décrire en détail quelle est la forme des opérateurs. $\mathcal{H}_k$ a une base $\{|i\rangle \otimes |j\rangle\}$ où $0 \leq i \leq n-1$ et $0 \leq j \leq 1$, la dimension de l'espace total est donc $(n+2)^n$. L'opérateur $\mathcal{A}$ est un produit de n opérateurs $\mathcal{A} = \mathcal{A}_1 \ldots \mathcal{A}_n$ où chaque $\mathcal{A}_i$ agit de façon non triviale uniquement sur $\mathcal{H}_i$. Il doit effectuer la transformation suivante

$$\mathcal{A}_i|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{n}}\sum_{j=1}^{n}|j-1\rangle \otimes |a_{1,j}\rangle \tag{1.35}$$

Cet opérateur s'obtient en deux étapes, la première est simplement un produit de matrices Hadamard H qui génèrent la superposition $|0\rangle \rightarrow \sum_{j=1}^{n}|j-1\rangle$. Dans la deuxième étape on utilise des opérateurs de la forme $C_{i,not}$ appliqués uniquement si $a_{j,i}$ est différent de zéro. Le temps utilisé est donc $O(n^2)$.
L'opérateur $S_\chi = G^\dagger EG$ est le produit de trois opérateurs où le premier à être appliqué G compare toutes les paires, pour chaque paire (k,k') ou $k = 1,\ldots,n$ et $k' = 1,k$ il agit contrôlé par les vecteurs $|i_k\rangle$ et $|i_{k'}\rangle$ appartenant à l'espace $\mathcal{H}_k$ et $\mathcal{H}_{k'}$ respectivement. Le deuxième E multiplie le vecteur par la phase correspondante (1.33) et (1.28), et le troisième remet les vecteurs utilisés pour les calculs intermédiaires dans leur état initial. Chaque opérateur se décompose de la façon suivante

- G est le produit de n^2 opérateurs $G = \prod_{k=1}^{n-1}\prod_{l=k+1,n} g_{l,k}$. Pour chaque paire (k,l) l'opérateur $g_{k,l}$ compare les coefficients i_k, i_l du vecteur et marque un vecteur extra avec cette information. A la fin, le vecteur contenant l'information "toutes les paires sont différentes" sera une permutation et il pourra être distingué des autres. A son tour $g_{k,l}$ se décompose en $\log_2 n$ opérateurs qui comparent bit à bit les deux entiers i_k et i_l, donc pour le coefficient numéro j

$$g_{k,l,j}|(i_k)_j,(i_l)_j,0\rangle = |(i_k)_j,(i_l)_j,(i_k)_j \oplus (i_l)_j\rangle \tag{1.36}$$

  l'opérateur $g_{k,l,j}$ est composé de trois opérateurs élémentaires C_{not}. Le temps de l'opérateur G est donc $T(g) = 3n^2\log_2 n$ ou $O(n^3)$

- E est un opérateur de la forme $C_{j,not}$ avec j entier. Il faut que E, dépendant de tous les coefficients calculés précédemment modifie la phase du vecteur. Ceci se fait a l'aide d'un extra qubit qui est initialement mis dans l'état $H|0\rangle$. Si on réorganise les qubits comme suit

$$|i_0,\ldots,i_{n-1}\rangle \otimes |a_{0,i_1},\ldots,a_{n,i_n}\rangle \\ \otimes |(i_0)_0 \oplus (i_1)_0,\ldots,(i_{n-2})_{n-1} \oplus (i_{n-1})_{n-1}\rangle \otimes H|0\rangle \quad (1.37)$$

  L'opérateur E doit agir sur le dernier qubit si

$$|a_{0,i_1},\ldots,a_{n,i_n}\rangle \otimes |(i_0)_0 \oplus (i_1)_0,\ldots,(i_{n-2})_{n-1} \oplus (i_{n-1})_{n-1}\rangle \\ = |1,\ldots,1\rangle|0,\ldots,0\rangle = |2^n-1\rangle \quad (1.38)$$

  où l'entier 2^n-1 est écrit dans sa décomposition binaire sur $n+n\frac{n(n+1)}{2}$ bits . On a donc que l'opérateur E est égal à $C_{2^n-1,not}$ sur un registre de $n+n\frac{n(n+1)}{2}$ qubits. Le temps pour ce type d'opérateur, proportionnel au nombre de qubits utilisés pour le contrôle est donc $O(n)$.

L'opérateur total a donc un temps polynomial en n, $O(n^4)$. Finalement en remplaçant le temps de chaque opérateur on trouve que l'algorithme "Count(f,M)" modifié pour qu'il calcule le permanent d'une matrice de dimension $n \times n$ utilise un temps dont le terme principal croît comme $O(Mn^4)$.

1.4.2 Algorithme quantique utilisant "ExactCount"

Pour un calcul exact on peut utiliser cet algorithme dont les étapes sont

1. Appeller deux fois l'algorithme Count(f,M) avec $M = \sqrt{n^n}$. On obtient les entiers

$$t'_1 = Count(f, 14\Pi\sqrt{n^n}) \quad (1.39)$$
$$t'_2 = Count(f, 14\Pi\sqrt{n^n}) \quad (1.40)$$

   Boucle : l'entier M est augmenté sans dépasser n^n
2. $M_i = 30\sqrt{(t'_i+1)(n^n-t'_i+2)}\, i = 1,2$
3. $M = \min\{M_1, M_2\}$
4. $t' = \text{Count(f,M)}$
5. La sortie est $\tilde{t}$ avec $|\tilde{t}-t'| \leq \frac{2}{3}$

Le temps est déterminé par l'étape pas numéro quatre de sorte que la valeur moyenne $\langle M\rangle$ est de l'ordre de $\sqrt{(perm+1)(n^n-perm+1)}$. Le temps est donc supérieur à ce facteur et donc exponentiel en n. Il est important de noter que dans les deux cas, en utilisant "Count(f,M)" ou "ExactCount", les algorithmes ont un temps supérieur au temps de l'algorithme de Ryser.

Chapitre 2

Marches quantiques

2.1 Introduction

On dit qu'un algorithme aléatoire est un FPRAS où "fully polynomial randomized aproximated scheme" si on peut approximer avec cet algorithme la solution d'un problème (où l'erreur depend d'une constante ϵ) avec un temps polynomial non seulement dans la taille de l'entrée du problème mais aussi dans $\frac{1}{\epsilon}$. C'est 'a dire que si $\tilde{Z}$ est la sortie de l'algorithme et Z la valeur qu'on veut calculer on doit obtenir $P\left((1-\epsilon)\tilde{Z} \leq Z \leq (1+\epsilon)\tilde{Z}\right) \geq \frac{3}{4}$
En 2001 il a été demontré que la solution du problème du permanent peut s'approximer avec un FPRAS dont l'étape principale est une marche aléatoire sur l'espace des graphes ayant la propriété d'être un "Matching graph" [22].
La marche aléatoire est un algorithme réalisant (simulant) l'évolution à temps discret d'une chaîne de Markov sur l'espace choisi Ω et qui converge vers une distribution π reliée à la solution du problème. La propriété de la chaîne qui détermine la vitesse de l'algorithme est appelée le temps de mixage, le temps minimal nécessaire pour que la chaîne converge vers la distribution attendue.
En parallèle avec l'utilisation des marches aléatoires dans l'algorithmique classique, on a défini des modèles de marches quantiques pouvant être utilisés pour réaliser les mêmes tâches que les marches classiques [5]. Dans cette optique, les auteurs ont défini plusieurs grandeurs importantes pour préciser l'utilité, pour l'algorithmique, des nouvelles marches dont le temps de mixage est un exemple. Bien que les marches quantiques ne permettent de réaliser que des gains de temps polynomiaux par rapport aux algorithmes déjà utilisant une marche classique, elles sont considérées comme de bons candidats pour construire de nouveaux algorithmes quantiques [24]. A l'appui de cette affirmation se trouvent maintenant les algorithmes "Element distinctness" [7] et "Search algorithm" [38].
Dans ce domaine, le but de notre travail a été de classifier les marches quantiques possibles en cherchant des propriétés se différenciant des marches classiques. Identifier des telles différences permettrait de construire des algorithmes quantiques les utilisant comme élément clé pour réduire la complexité des problèmes. Nous avons donc entrepris d'élargir la définition initiale et de commencer une classification des marches possibles (sections 3.2 à 3.4). Finalement avec ces nouveaux modèles nous avons élargi quelques théorèmes connus (section 3.5) qui indiquent des directions de

recherche futures.

2.2 Modèle et unitarité

Il existe deux modèles de marches quantiques, l'un avec un temps discret et l'autre avec un temps continu. La différence essentielle entre les deux semble être la nécessité pour la première d'un espace interne additionnel pour que l'évolution de la particule soit unitaire. Il est donc intéressant d'étudier quel est l'effet de cet espace interne. Dans le chapitre suivant nous avons mis ensemble quelques résultats qui suggèrent qu'il est raisonnable de chercher à classifier les marches suivant la dimension de l' espace interne et les symétries possibles. Nous commençons par élargir la définition des marches quantiques de façon à pouvoir varier la dimension de l'espace interne additionnel. Ce modèle est similaire aux modèle des automates cellulaires, la différence principale est que nous sommes intéressés par d'autres types de graphes, non seulement les réseaux.
Soit G un graphe orienté, où il est possible d'avoir deux liens de sens contraire entre deux points, et E l'ensemble de liens du graphe tels que $G = (X, E)$. Soit $\mathcal{H}$ un espace de Hilbert complexe défini comme le produit $\mathcal{H} = \mathcal{H}_I \otimes \mathcal{H}_G$. L'espace $\mathcal{H}_G = \ell^2(X)$ décrit la position de la particule sur le graphe et l'espace $\mathcal{H}_I = \mathbb{C}^d$ décrit des degrés de liberté interne. Soit $\{|x\rangle\}_{x\in X}$ une base de $\mathcal{H}_G$ et $\{|1\rangle, \ldots, |d\rangle\}$ une base de $\mathcal{H}_I$. L'équation d'évolution est

$$|\psi_{t+1}\rangle = W|\psi_t\rangle \tag{2.1}$$

où W est un opérateur unitaire d'évolution à temps discret défini par

$$W = \sum_{x\in X} \sum_{z\in E_x} M_{x,z} \otimes T_{x\to z} \tag{2.2}$$

E_x dénote l'ensemble des vertex atteints à partir de x et $T_{x\to z}$ est l'opérateur qui déplace la particule du point x au point z. Plus précisément $T_{x\to z}$ s'écrit

$$\langle x'|T_{x\to z}|\psi\rangle = \langle x'|z\rangle\langle x|\psi\rangle \tag{2.3}$$

L'opérateur $M_{x,z} : H_I \to H_I$ est une application modifiant les états internes de la particule. Cet opérateur sur l'espace interne, multiplié tensoriellement par l'opérateur déplacement du vertex x au vertex z, dans l'espace position, forme un des termes de l'opérateur évolution (2.2) dans l'espace total. Pour illustrer le sens d'une telle application supposons un état initial $|\psi_t\rangle = |i\rangle \otimes |z\rangle$. Alors après un pas de temps, la probabilité de trouver la particule sur un vertex y voisin de x va dépendre de l'état interne précédent

$$P(y) = \sum_{j=1}^{d} |\langle j|M_{z,y}|i\rangle|^2 \tag{2.4}$$

Si le vertex y n'est pas voisin de x la probabilité est simplement zéro. Par cette dépendance l'image habituelle est celle d'une évolution aléatoire, dont la probabilité de passer d'un point à son voisin est déterminée par un tirage à pile ou face, c'est à

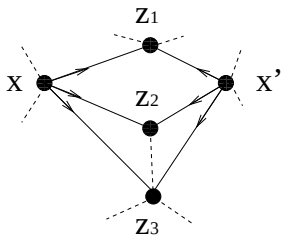


FIG. 2.1 – Une paire de deuxièmes voisins

dire par le tirage d'une pièce qui peut être maintenant différente pour chaque état interne. Dans le modèle défini par Kempe, on associe une pièce à un vecteur de la base standard de l'espace interne et pour cette raison l'espace interne a une dimension fixe et égale à k le nombre de voisins par vertex dans un graphe k-régulier.
L'unitarité de W est satisfaite si et seulement si $W^\dagger W = \mathbb{1}$ et $WW^\dagger = \mathbb{1}$. En considérant coefficient par coefficient on obtient $2(dim\mathcal{H})^2$ équations. Comme les opérateurs de translation ont une forme simple il est plus convenable de réarranger les équations dans des équations matricielles concernant seulement des matrices de l'espace interne et dont les termes dépendent de la structure du graphe. On obtient alors

$$\sum_{z \in E_x \cap E_{x'}} M^\dagger_{x,z} M_{x',z} = \delta_{x,x'} \mathbb{1} \tag{2.5}$$

$$\sum_{z \in E_x \cap E_{x'}} M_{z,x} M^\dagger_{z,x'} = \delta_{x,x'} \mathbb{1} \tag{2.6}$$

$\forall x, x'$ éléments de X. Quand $x \neq x'$ les équations non triviales correspondent à celles où les deux vertex sont second voisins. Le nombre de termes dans la somme est en relation avec le nombre de chemins fermés de longueur 4 avec orientation alternée entre contenant x et x'.
Dans l'exemple de la figure 2.1 une équation du type (2.5) est associée à la paire de seconds voisins x et x'

$$M^\dagger_{x,z_1} M_{x',z_1} + M^\dagger_{x,z_2} M_{x',z_2} + M^\dagger_{x,z_3} M_{x',z_3} = 0 \tag{2.7}$$

une équation du type (2.6) est associée à la paire de seconds voisins z_1 et z_2

$$M_{x,z_1} M^\dagger_{x,z_2} + M_{x',z_1} M^\dagger_{x',z_2} = 0 \tag{2.8}$$

et deux autres équations du même type s'obtiennent en remplaçant la paire z_1, z_2 par z_1, z_3 et par z_2, z_3.

2.3 Marches quantiques sur des graphes de Cayley colorés

Dans le but de simplifier et diminuer le nombre d'équations nous allons nous restreindre à l'étude des graphes de Cayley.

Rappelons brièvement que si Γ est un groupe et P une présentation du groupe avec relations R et ensemble générateur Δ alors le graphe de Cayley coloré $C_\Delta(\Gamma)$ est défini avec

$$X \equiv X(C_\Delta(\Gamma)) = \Gamma \tag{2.9}$$
$$E \equiv E(C_\Delta(\Gamma)) = \{(x, x\delta)_\delta | x \in \Gamma, \delta \in \Delta\} \tag{2.10}$$

On omettra le terme coloré dans la suite. Par la propriété de transitivité des vertex, telle que touts les vertex sont équivalents, on peut supposer que les opérateurs internes dépendent uniquement du générateur. Ainsi, pour un lien quelconque (x, y) l'opérateur interne dépendra du générateur $\delta = x^{-1}y$ et non des vertex x et y

$$M_{x,y} = M_{x^{-1}y} \text{ pour tout } (x, y) \in E \tag{2.11}$$

Avec cette supposition, la forme de l'opérateur évolution est maintenant

$$W = \sum_{\delta \in \Delta} M_\delta \otimes T_\delta \tag{2.12}$$

où T_δ est l'opérateur déplacement associé à l'élément δ, il est donc une permutation de l'ensemble de vertex défini par l'opération dans le groupe

$$T_\delta = \sum_{x \in X} T_{x \to x\delta} \tag{2.13}$$

Les équations (2.5) et (2.6) deviennent

$$\sum_{\delta_1 \delta_2^{-1} = u} M_{\delta_1}^\dagger M_{\delta_2} = \delta_{\{u=e\}} \mathbb{1} \tag{2.14}$$
$$\sum_{\delta_1 \delta_2^{-1} = u} M_{\delta_1} M_{\delta_2}^\dagger = \delta_{\{u=e\}} \mathbb{1} \tag{2.15}$$

où δ_1, δ_2 sont deux éléments de Δ et u est un élément de l'ensemble

$$\Delta_2 = \{\delta\delta'^{-1}; \delta, \delta' \in \Delta\} \tag{2.16}$$

et e est l'élément identité dans le groupe. Le nombre d'équations est le double de la cardinalité de Δ_2. Le nombre de termes dans la somme de chaque équation dépend maintenant du nombre de paires de liens alternés entre seconds voisins, où d'une manière équivalente du nombre de chemins fermés alternés de longueur quatre, ce qui se traduit en une relation entre générateurs du type

$$\delta_1 \delta_2^{-1} \delta_4 \delta_3^{-1} = e \tag{2.17}$$

Comme la présentation choisie du groupe met en évidence les relations entre générateurs, elle est utile pour classifier les différents modèles possibles.

2.3.1 Graphes de Cayley de groupes libres

Un groupe libre est un groupe dont les générateurs ne vérifient que les relations déterminées par les axiomes de groupe. On s'intéressera aux présentations du groupe de la forme

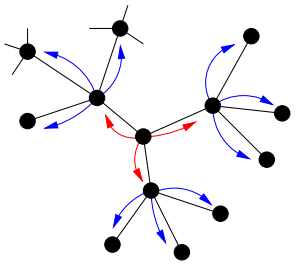
$$\Gamma = \langle\ \Delta | - \rangle \tag{2.18}$$

ou avec éventuellement des relations du type

$$\delta_i \delta_j = e \tag{2.19}$$

$$\delta_k = e \tag{2.20}$$

pour des $\delta_i, \delta_j, \delta_k \in \Delta$, ce qui en termes du graphe revient à permettre des liens doubles et des boucles respectivement.
Pour simplifier la lecture, quand ces types de relations seront présentés on renommera la matrice M_{δ_j} associée au générateur δ_j tel que $\delta_i \delta_j = e$ par $M_{\delta_i^{-1}}$. De même on renommera M_e la matrice associé a δ_k tel que $\delta_k = e$ est une relation dans la présentation.
Dans cette première partie, nous supposons que l'ensemble de relations ne peut être que du premier type (2.19), les graphes avec des boucles seront considérés par la suite. Il n'y a donc pas de relations vérifiant (2.17) et les équations (2.14) et (2.15)



sont simplement

$$M_{\delta_1}^\dagger M_{\delta_2} = M_{\delta_1} M_{\delta_2}^\dagger = 0 \qquad \text{pour tout } \delta_1 \neq \delta_2 \tag{2.21}$$

$$\sum_{\delta \in \Delta} M_\delta M_\delta^\dagger = \sum_{\delta \in \Delta} M_\delta^\dagger M_\delta = \mathbb{1} \tag{2.22}$$

Theorème 3 *Une marche quantique définie sur le groupe libre* (2.18) *avec opérateur évolution* (2.2) *est unitaire si et seulement si les opérateurs de l'espace interne sont de la forme*

$$M_\delta = U\, P_\delta \tag{2.23}$$

où U est une matrice unitaire de dimension $dim(\mathcal{H}_I)$ et $\{P_\delta\}_{\delta \in \Delta}$ est une famille complète de projecteurs orthogonaux

$$\sum_{\delta \in \Delta} P_\delta = \mathbb{1} \tag{2.24}$$

La dimension de l'espace interne est supérieure ou égale à $|\Delta|$.

Preuve : D'abord (2.23) implique (2.21)-(2.22) ce qui se vérifie par remplacement. L'implication dans l'autre sens est moins directe. Supposons (2.21)-(2.22), ces équations impliquent les relations suivantes, la première entre les espaces images des opérateurs internes et la seconde entre les espaces images des opérateurs internes conjugués.

$$\mathcal{H}_I = \oplus_{\delta\in\Delta}\mathcal{I}m(M_\delta) \tag{2.25}$$

$$\mathcal{H}_I = \oplus_{\delta\in\Delta}\mathcal{I}m(M_\delta^\dagger) \tag{2.26}$$

Par (2.21), pour toute paire δ_1 et δ_2 d'éléments différents dans Δ, tout vecteur appartenant à l'espace image de M_{δ_2} sera orthogonal à tout vecteur appartenant au domaine de $M_{\delta_1}^\dagger$ ce qui est équivalent à que tous les espaces $\mathcal{I}m(M_\delta)$ sont orthogonaux entre eux. Par (2.22) on a que si un vecteur en $\mathcal{H}$ n'appartient pas à l'union de tous les domaines de $\mathcal{M}_\delta^\dagger$ alors ce vecteur est le vecteur nul. On obtient de ces deux conditions (2.25). De façon similaire on obtient (2.26) en commençant avec la deuxième équation de (2.21). Définissons la matrice $U \equiv \sum_\delta M_\delta$, unitaire par les relations (2.21)-(2.22), et P_δ le projecteur sur $\mathcal{I}m(M_\delta^\dagger)$ tel que $\{P_\delta\}_{\delta\in\Delta}$ est une famille complète de projecteurs orthogonaux. L'équation (2.23) est donc vérifiée. □
L'ordre de la matrice U et de l'opérateur P_δ peut être modifié dans la solution (2.23), dans ce cas P_δ est le projecteur sur $\mathcal{I}m(M_\delta)$. Quand la dimension de l'espace $\mathcal{I}m(M_\delta)$ est fixée a un, la dimension de l'espace interne $\mathcal{H}_I$ prend sa valeur minimale $dim(\mathcal{H}_I) = |\Delta|$. En plus si une présentation symétrique est choisie, avec des relations du type (**??**) de tel façon que le graphe de Cayley contient un lien double entre deux voisins, on obtient la forme des marches quantiques standard ("coin" solutions). Les autres possibilités dans le cas des groupes libres sont de définir des matrices M_δ de rangs différents variant avec le générateur δ mais ceci introduit une différentiation des générateurs qui briserait les symétries du groupe. Ce point sera discuté plus en détail dans le chapitre suivant. Si Δ contient l'élément identité des relations du type (2.17) peuvent exister et correspondent à la relation de commutation de e avec tout élément du groupe. Pour chaque générateur il faut en plus que le générateur et son inverse soient des éléments de Δ et si ceci est vérifié

$$M_\delta^\dagger\ M_e + M_e^\dagger M_{\delta^{-1}} = 0 \tag{2.27}$$

$$M_e M_\delta^\dagger + M_{\delta^{-1}} M_e^\dagger = 0 \tag{2.28}$$

pour tout $\delta \neq e$. En additionnant toutes les équations de (2.27) on obtient $M_e^\dagger S = -S^\dagger M_e$ où $S = \sum_\delta M_\delta$. En additionnant les équations (2.27) pour un δ et son inverse δ^{-1} on obtient

$$(M_e^\dagger S)(P_\delta + P_{\delta^{-1}}) = (P_\delta + P_{\delta^{-1}})(M_e^\dagger S) \tag{2.29}$$

pour tout $\delta \neq e$. On a donc que la matrice $M_e^\dagger S$ est diagonale par blocs dans la base ou les projecteurs P_δ sont diagonaux . Le problème est donc réduit à un problème unidimensionnel dont la solution est décrite dans la section suivante.

Marches unidimensionnelles

L'exemple le plus simple est la marche quantique sur $\mathbb{Z}$. La présentation du groupe associé est $\Gamma = \langle\delta|-\rangle$, on s'intéressera aussi à la présentation $\Gamma = \langle\delta, \delta'|\delta\delta' =$

$e\rangle$. La dimension minimale de l'espace interne est 2 par l'équation (2.23). Par la forme des opérateurs internes l'opérateur évolution (2.2) peut s'écrire

$$W = (U \otimes Id)(P_\delta \otimes T_\delta + P_{\delta^{-1}} \otimes T_{\delta^{-1}}) \tag{2.30}$$

où U est une matrice unitaire 2×2.
Si l'identité apparaît dans la présentation du groupe, c'est a dire si on choisit la présentation $\Gamma = \langle \delta, \delta', \delta'' | \delta\delta' = e, \delta'' = e \rangle$, alors deux types de solutions sont possibles. Si on considère que chaque terme apparaissant dans la somme des équations (2.27) et (2.28) est nul on obtient le même ensemble d'équations que le groupe libre avec trois générateurs. La solution est de la forme (2.23)

$$W = (U \otimes Id)(P_\delta \otimes T_\delta + P_{\delta^{-1}} \otimes T_{\delta^{-1}} + P_e \otimes Id) \tag{2.31}$$

avec U une matrice unitaire de dimension 3×3. L'autre solution a un espace interne de dimension 2

$$W = (U \otimes Id)\big(\cos(\theta)(P_\delta \otimes T_\delta + P_{\delta^{-1}} \otimes T_{\delta^{-1}}) + i \sin(\theta)\sigma_x \otimes Id\big) \tag{2.32}$$

où U est une matrice unitaire 2×2 et σ_x comme défini précédemment. Ce type de solution a été déjà présenté en [30].
En conclusion, ajouter des relations entre opérateurs change les équations que les opérateurs internes doivent vérifier mais ceci de façon telle qu' une solution des groupes libres est aussi solution des nouvelles équations. De telles solutions existent donc pour tous les groupes en particulier pour les produits libres de groupes libres

$$\Gamma = \langle \delta_1, \cdots, \delta_l | \delta_1^{q_1} = \cdots \delta_l^{q_l} = e \rangle$$

et pour les groupes libres abéliens

$$\Gamma = \langle \delta_1, \cdots, \delta_l | \delta_i\, \delta_j\, \delta_i^{-1} \delta_j^{-1} = e\ \forall i, j \in \{1, \cdots, l\} \rangle$$

2.3.2 Graphes de Cayley de groupes libres abéliens

La relation (2.17) a la forme de la condition d'abélianité quand $\delta_4 = \delta_1^{-1}$ et $\delta_3 = \delta_2^{-1}$. Cette relation implique un terme de plus dans les équations associées à la paire (δ_1, δ_2) si le groupe est abélien et la présentation choisie est symétrique. Autrement les équations seront les mêmes que pour les groupes libres non abéliens. Pour cette raison on considère dans la suite de la section le cas des présentations symétriques des groupes libres abéliens. Comme précédemment on suppose que Δ a des relations uniquement du type (2.19) et non du type (2.20). Dans ce cas la présentation du groupe est

$$\Gamma = \langle \delta_1, \ldots, \delta_n, \delta'_1, \ldots \delta'_n | \delta_i \delta'_i = e\, 1 \leq i \leq n,\ \delta_i \delta_j = \delta_j \delta_i\ \forall \delta_i, \delta_j \in \Delta \rangle \tag{2.33}$$

On peut vérifier dans la figure 0.3.3 que avec une présentation minimale, figure de gauche, le graphe de Cayley n'aura pas de chemins fermés alternés entre deuxièmes voisins tandis qu' avec une présentation symétrique, figure du centre, entre deux deuxièmes voisins quelconques il y aura toujours un chemin fermé alterné de longueur

quatre (correspondant à la relation d'abélianité). Chacun de ces chemins fermés qu'on peut voir dans la figure du centre est associé à un nouveau terme dans les équations (2.14)-(2.15). Ces équations deviennent

$$M_{\delta_i}^\dagger M_{\delta_j} + M_{\delta_j^{-1}}^\dagger M_{\delta_i^{-1}} = 0 \qquad \text{pour tout } \delta_i \neq \delta_j \tag{2.34}$$

$$M_{\delta_i} M_{\delta_j}^\dagger + M_{\delta_j^{-1}} M_{\delta_i^{-1}}^\dagger = 0 \qquad \text{pour tout } \delta_i \neq \delta_j \tag{2.35}$$

$$\sum_{\delta\in\Delta} M_\delta M_\delta^\dagger = \sum_{\delta\in\Delta} M_\delta^\dagger M_\delta = \mathbb{1} \tag{2.36}$$

Quand $\delta_j = \delta_i^{-1}$, les équations (2.34)-(2.35) n'ont qu'un seul terme

$$M_{\delta_i}^\dagger M_{\delta_i^{-1}} = M_{\delta_i^{-1}} M_{\delta_i}^\dagger \;\; = \;\; 0 \tag{2.37}$$

Par ces dernières équations ayant un seul terme nul dans le membre de gauche, on a encore des conditions d'orthogonalité sur les espaces images des opérateurs internes. Pourtant cette condition s'applique uniquement entre les matrices associées à un générateur et à son inverse. L'espace total ne se sépare donc pas en une somme directe comme dans le cas des groupes libres. La proposition suivante est valable pour toute paire de générateurs

Proposition 1 *Soit G un graphe de Cayley d'un groupe abélien libre avec n générateurs* (2.33)*. Si un opérateur évolution* (2.2) *défini sur G est unitaire alors les espaces images des opérateurs M_{δ_i} et M_{δ_j} pour toute paire $\{\delta_i, \delta_j\}$ vérifient*

$$\big(\mathcal{I}m(M_{\delta_i}) \cap \mathcal{I}m(M_{\delta_j}) = \{0\}\big) \Rightarrow \mathcal{I}m(M_{\delta_i}) \perp \mathcal{I}m(M_{\delta_j}) \tag{2.38}$$

La même implication est vraie pour les espaces images des opérateurs conjugués

$$\big(\mathcal{I}m(M_{\delta_i}^\dagger) \cap \mathcal{I}m(M_{\delta_j}^\dagger) = \{0\}\big) \Rightarrow \mathcal{I}m(M_{\delta_i}^\dagger) \perp \mathcal{I}m(M_{\delta_j}^\dagger) \tag{2.39}$$

Preuve : En utilisant (2.35) pour une paire (δ_i,δ_j^{-1}) on obtient

$$\mathcal{I}m(M_{\delta_i} M_{\delta_j^{-1}}^\dagger) = \mathcal{I}m(M_{\delta_j} M_{\delta_i^{-1}}^\dagger) \tag{2.40}$$

et donc

$$\mathcal{I}m(M_{\delta_i} M_{\delta_j^{-1}}^\dagger) \subset \big(\mathcal{I}m(M_{\delta_i}) \cap \mathcal{I}m(M_{\delta_j})\big) \tag{2.41}$$

Supposons maintenant que $\mathcal{I}m(M_{\delta_i})$ et $\mathcal{I}m(M_{\delta_j})$ n'ont pas de sous espace commun. Alors $M_{\delta_i} M_{\delta_j^{-1}}^\dagger = 0$, ce qui peut être écrit

$$\mathcal{I}m(M_{\delta_i}^\dagger) \perp \mathcal{I}m(M_{\delta_j^{-1}}^\dagger) \tag{2.42}$$

et plus particulièrement

$$\mathcal{I}m(M_{\delta_i}^\dagger M_{\delta_j}) \perp \mathcal{I}m(M_{\delta_j^{-1}}^\dagger M_{\delta_i^{-1}}) \tag{2.43}$$

Comme les deux sous espaces sont égaux (par (2.37)) et orthogonaux, ils sont identiques au sous espace nul et on a donc de nouveau $M_{\delta_i}^{\dagger} M_{\delta_j} = 0$. Finalement

$$\mathcal{I}m(M_{\delta_i}) \perp \mathcal{I}m(M_{\delta_j}) \tag{2.44}$$

L' implication (2.38) est alors démontrée. La preuve de (2.39) est équivalente, en commençant avec l' équation (2.34) au lieu de (2.35). □
On peut utiliser la proposition précédente pour trouver des solutions avec un espace interne de dimension inférieure au nombre de générateurs. Supposons d'abord que les espaces images des opérateurs internes n'ont aucun sous espace en commun, par (2.38) ils sont donc orthogonaux entre eux et $dim(\mathcal{H}_I) \geq |\Delta|$. Une condition nécessaire pour l'existence de marches quantiques avec dimension d'espace interne inférieur à $|\Delta|$ est que l'intersection de certains de ces espaces images soit non nulle. Nous allons présenter quelques exemples où ce type de raisonnement nous mène à définir des marches quantiques avec évolution unitaire et dimension d'espace interne différent de $|\Delta|$.

2.4 Exemples

2.4.1 Groupes abéliens libres

Une marche quantique sur $\mathbb{Z}^2$ avec espace interne de dimension deux

On considère une présentation symétrique (2.33) avec $n = 2$. L'opérateur évolution (2.12) est

$$W = M_{\delta_1} \otimes T_{\delta_1} + M_{\delta_1^{-1}} \otimes T_{\delta_1^{-1}} + M_{\delta_2} \otimes T_{\delta_2} + M_{\delta_2^{-1}} \otimes T_{\delta_2^{-1}} \tag{2.45}$$

Il n'est pas possible d'obtenir une solution avec $\dim(\mathcal{H}_I) = 1$, par le théorème No-go. On fixe $\dim(\mathcal{H}_I) = 2$ et on essaye de résoudre les équations qui impliquent l'unitarité de l'opérateur d' évolution. Comme on l'a déjà discuté, choisir des opérateurs internes avec des espaces images disjoints entraîne que la dimension est supérieure ou égale à $|\Delta|$ ici quatre. On fixe le rang de M_δ égal à un pour tout δ. La forme de Jordan canonique des matrices est donc

$$M_\delta = \lambda_\delta |u_\delta\rangle\langle v_\delta| \tag{2.46}$$

En introduisant ces matrices dans les équations (2.34) et (2.35) on obtient une série d'équations vectorielles avec deux types de solutions. Avec la première on peut écrire que

$$M_{\delta_1} = UP_1VP_1 \qquad M_{\delta_1^{-1}} = UP_2VP_2 \tag{2.47}$$

$$M_{\delta_2} = UP_1VP_2 \qquad M_{\delta_2^{-1}} = UP_2VP_1 \tag{2.48}$$

pour deux matrices unitaires quelconques U et V et P_1 P_2 sont deux projecteurs orthogonaux de rang 1. La deuxième se déduit de la première en échangeant δ_1 et

δ_1^{-1}. L'opérateur d'évolution peut se factoriser sous la forme de deux opérateurs de marche à une dimension sur $\frac{1}{\sqrt{2}}\mathbb{Z}$

$$W = (U \otimes 1)(P_1 \otimes (T_{\delta_1} T_{\delta_2})^{\frac{1}{2}} + P_2 \otimes (T_{\delta_1^{-1}} T_{\delta_2^{-1}})^{\frac{1}{2}}) \\ (V \otimes 1)(P_1 \otimes (T_{\delta_1} T_{\delta_2^{-1}})^{\frac{1}{2}} + P_2 \otimes (T_{\delta_1^{-1}} T_{\delta_2})^{\frac{1}{2}}) \quad (2.49)$$

Cette solution peut se généraliser à une dimension arbitraire

Proposition 2 *Soit G le graphe de Cayley d'un groupe libre abélien avec n générateurs et une présentation symétrique* (2.33)*, $|\Delta| = 2n$. Il existe un opérateur évolution unitaire* (2.2) *d'une marche sur G telle que la dimension de l'espace interne est $\frac{|\Delta|}{2}$ pour n pair et $\frac{|\Delta|}{2} + 1$ pour n impair.*

Preuve : L'idée générale est diviser la marche totale en une série de marches bidimensionnelles. Supposons d'abord n pair. L'espace interne est de dimension n et on sépare l'espace total en $\frac{n}{2}$ sous espaces orthogonaux de dimension 2. On sépare aussi les directions possibles (générateurs δ) en paires et on associe une paire et un des sous espaces, le deux éléments de la paire ne doivent pas être en relation avec (2.19). Les espaces image et domaine des opérateurs internes seront des sous espaces des espaces associés. Ainsi pour une paire (δ_i, δ_j) les opérateurs $M_{\delta_i}, M_{\delta_j}, M_{\delta_i^{-1}}, M_{\delta_j^{-1}}$ auront la forme des opérateurs de la marche bidimensionnelle et les projecteurs P_1 et P_2 seront des projecteurs orthogonaux dans le sous espace associé. Supposons maintenant n impair. On répète la construction précédente avec $n-1$ générateurs et un espace de dimension $n-1$, et on additionne un espace de dimension deux où les opérateurs internes du dernier générateur auront la forme des opérateurs d'une marche unidimensionnelle. Tous les opérateurs vérifieront ainsi les équations (2.34)-(2.36). □

Marche sur $\mathbb{Z}^2$ avec espace interne de dimension quatre

La marche quantique standard [5] utilise des opérateurs projection de rang un donc les matrices de l'espace interne sont aussi de rang un. On peut se demander si la définition proposée permet d'obtenir des marches différentes. Si on suppose que les matrices internes sont de rang deux par exemple le modèle suivant est une autre marche avec opérateur évolution unitaire

$$M_{\delta_1} = \frac{1}{\sqrt{2}}(\,|u_1\rangle\langle v_1| + |u_2\rangle\langle v_3|\,) \quad (2.50)$$

$$M_{\delta_1^{-1}} = \frac{1}{\sqrt{2}}(\,-|u_3\rangle\langle v_4| + |u_4\rangle\langle v_2|\,) \quad (2.51)$$

$$M_{\delta_2} = \frac{1}{\sqrt{2}}(\,|u_1\rangle\langle v_2| + |u_3\rangle\langle v_3|\,) \quad (2.52)$$

$$M_{\delta_2^{-1}} = \frac{1}{\sqrt{2}}(\,-|u_4\rangle\langle v_1| + |u_2\rangle\langle v_4|\,) \quad (2.53)$$

ou $\{|u_i\rangle\}_{i=1,\cdot,4}$ et $\{|v_i\rangle\}_{i=1,\cdot,4}$ sont deux bases orthonormales de $\mathcal{H}_I$.

Marche sur $\mathbb{Z}^3$ avec espace interne de dimension quatre

Il a été montré [11] qu'il n'existe pas de marche quantique tridimensionnelle avec espace interne de dimension deux. Nous allons présenter maintenant des solutions sur $\mathbb{Z}^3$ avec un espace interne de dimension quatre. Nous fixons à nouveau le rang des matrices égal à deux. Soit Γ une présentation du groupe symétrique (2.33) et $\{|u_i\rangle\}_{i=1,\cdot,4}$ et $\{|v_i\rangle\}_{i=1,\cdot,4}$ deux bases orthonormales de $\mathcal{H}_I$. Les opérateurs internes sont de la forme

$$M_{\delta_1} = \alpha_1|u_1\rangle\langle v_2| + \beta_1|u_2\rangle\langle v_1| \tag{2.54}$$
$$M_{\delta_1^{-1}} = \gamma_1|u_3\rangle\langle v_4| + \delta_1|u_4\rangle\langle v_3| \tag{2.55}$$
$$M_{\delta_2} = \alpha_2|u_1\rangle\langle v_3| + \gamma_2|u_3\rangle\langle v_1| \tag{2.56}$$
$$M_{\delta_2^{-1}} = \beta_2|u_2\rangle\langle v_4| + \delta_2|u_4\rangle\langle v_2| \tag{2.57}$$
$$M_{\delta_3} = \alpha_3|u_1\rangle\langle v_4| + \delta_3|u_4\rangle\langle v_1| \tag{2.58}$$
$$M_{\delta_3^{-1}} = \beta_3|u_2\rangle\langle v_3| + \gamma_3|u_3\rangle\langle v_2| \tag{2.59}$$

Les constantes vérifient

$$\alpha_2 = \lambda\alpha_1 \qquad \alpha_3 = \mu\alpha_1 \tag{2.60}$$
$$\beta_2 = \bar{\lambda}\nu\beta_1 \qquad \beta_3 = -\bar{\mu}\nu\beta_1 \tag{2.61}$$
$$\gamma_2 = -\lambda\bar{\nu}\gamma_1 \qquad \gamma_3 = -\bar{\mu}\gamma_1 \tag{2.62}$$
$$\delta_2 = -\bar{\lambda}\delta_1 \qquad \delta_3 = \mu\bar{\nu}\delta_1 \tag{2.63}$$

où $|\nu|^2 = 1$, $\lambda, \mu \in \mathbb{C}$ et

$$|\alpha_1| = |\beta_1| = |\gamma_1| = |\delta_1| = \frac{1}{\sqrt{1 + |\lambda|^2 + |\mu|^2}} \tag{2.64}$$

2.4.2 Graphes de Cayley avec multiples connections entre seconds voisins

Un exemple de dimension un

Dans la figure du centre de l'exemple bidimensionnel 0.3.3 on peut voir des chemin fermés entre deux voisins qui modifient les équations d'unitarité en ajoutant un terme. La relation associée à ces chemins fermés est la relation d'abelianité dans le groupe. Quelques deuxièmes voisins pourtant ne sont pas connectés de la même façon et ceci implique l'impossibilité d'une solution scalaire. En connectant ces deuxièmes voisins, par exemple en ajoutant une relation dans la présentation, on modifie le groupe et donc le graphe de façon à rendre possible une marche quantique scalaire. On considère alors le groupe

$$\langle \delta_1, \delta_2, \delta_1', \delta_2' | \delta_1\delta_1' = e, \delta_2\delta_2' = e, \delta_1^2 = \delta_2^2, \delta_1\,\delta_2 =, \delta_2\delta_1 \rangle \tag{2.65}$$

Les quatre matrices M_δ doivent être solution des équations

$$M_{\delta_1}^\dagger M_{\delta_1^{-1}} + M_{\delta_2}^\dagger M_{\delta_2^{-1}} = M_{\delta_1^{-1}} M_{\delta_1}^\dagger + M_{\delta_2^{-1}} M_{\delta_2}^\dagger = 0 \tag{2.66}$$

$$M_{\delta_1}^\dagger M_{\delta_2^{-1}} + M_{\delta_2}^\dagger M_{\delta_1^{-1}} = M_{\delta_2^{-1}} M_{\delta_1}^\dagger + M_{\delta_1^{-1}} M_{\delta_2}^\dagger = 0 \tag{2.67}$$

$$M_{\delta_1}^\dagger M_{\delta_2} + M_{\delta_2}^\dagger M_{\delta_1} + M_{\delta_1^{-1}}^\dagger M_{\delta_2^{-1}} + M_{\delta_2^{-1}}^\dagger M_{\delta_1^{-1}} = 0 \tag{2.68}$$

$$M_{\delta_2} M_{\delta_1}^\dagger + M_{\delta_1} M_{\delta_2}^\dagger + M_{\delta_2^{-1}} M_{\delta_1^{-1}}^\dagger + M_{\delta_1^{-1}} M_{\delta_2^{-1}}^\dagger = 0 \tag{2.69}$$

$$\sum_\delta M_\delta^\dagger M_\delta = \sum_\delta M_\delta M_\delta^\dagger = \mathbb{1} \tag{2.70}$$

Ces équations peuvent être vérifiées en fixant la dimension de l'espace interne à un. L'opérateur évolution est dans ce cas

$$W = \frac{1}{2}\big(e^{i\theta}(\tau_1 \pm \tau_2) + e^{i\varphi}(\tau_1^{-1} \mp \tau_2^{-1})\big) \tag{2.71}$$

où τ_1 et τ_2 sont les opérateurs translation associés à δ_1 et δ_2. Cette marche scalaire est équivalente à une marche sur $\mathbb{Z}$ avec un espace interne de dimension deux en regroupant deux à deux les paires de deuxièmes voisins.

L' hypercube

Considérons le groupe $(\mathbb{Z}_2)^n$

$$\Gamma = \langle \delta_1, \cdots \delta_n | \delta_i^2 = e \,\forall i;\ \delta_i \delta_j \delta_i^{-1} \delta_j^{-1} = e \,\forall i \neq j \rangle \tag{2.72}$$

Le graphe de Cayley de ce groupe est l'hypercube de dimension n. Les équations d'unitarité deviennent

$$M_{\delta_i}^\dagger M_{\delta_j} + M_{\delta_j}^\dagger M_{\delta_i} = 0 \tag{2.73}$$

$$M_{\delta_i} M_{\delta_j}^\dagger + M_{\delta_j} M_{\delta_i}^\dagger = 0 \tag{2.74}$$

$$\sum_\delta M_\delta^\dagger M_\delta = \mathbb{1} \tag{2.75}$$

Proposition 3 *Il existe une marche quantique avec opérateur évolution* (2.2) *sur le graphe de Cayley du groupe* (2.72) *tel que les opérateurs internes sont de la forme* $M_{\delta_i} = \frac{1}{\sqrt{n}}\sigma_i U$ *où* U *est une matrice unitaire de dimension* $dim(\mathcal{H}_I)$ *et* $\{\sigma_1 \dots \sigma_n\}$ *est un ensemble de matrices anticommutantes.*

Preuve : Si l'on requiert que les matrices M_δ soient hermitiennes (ou antihermitiennes) alors le premier ensemble d'équations (2.73)-(2.74) prend la forme d'une relation d'anticommutation pour chaque paires de matrices. Comme les matrices hermitiennes anticommutantes génèrent une algèbre de Clifford, il est naturel de trouver une solution parmi les représentations de cette algèbre. Soit $\{\sigma_1 \dots \sigma_n\}$ un tel ensemble de n matrices et U une matrice unitaire. Un choix possible pour ces matrices M_δ est alors $M_{\delta_i} = \frac{1}{\sqrt{n}}\sigma_i U$. □

2.5 Extensions

La définition que nous avons proposé correspond à un automate cellulaire quand le graphe de Cayley est le graphe du groupe $\mathbb{Z}^d$ et aux marches algorithmiques quand on restreint les opérateurs internes à la forme (2.23) de la marche sur les groupes libres. Nous nous proposons de revoir quelques résultats intéressants qui peuvent maintenant être généralisés. Le premier résultat appelé théorème "No-Go" détermine qu'il n'y à pas d'automate cellulaire scalaire, c'est à dire avec espace interne de dimension un. Nous allons reformuler ce théorème pour déterminer une condition nécessaire sur le graphe pour que des tels modèles de marches puissent exister. On retrouve bien évidement que pour le groupe $\mathbb{Z}^d$ cette condition n'est pas vérifiée. Le deuxième résultat est, pour un graphe isomorphe à $\mathbb{Z}^d$ et un opérateur évolution de la forme d'une marche algorithmique, une limite faible de la probabilité de la particule de se trouver à un temps donné sur un vertex du graphe. Nous calculons la même limite pour les mêmes graphes mais pour un opérateur plus général calculer.

2.5.1 Théorème "No-go" reformulé

Theorème 4 *Soit un graphe de Cayley du groupe G avec présentation $\Gamma =< \Delta | R >$ et une marche quantique* (2.2) *définie sur ce graphe. Une condition nécessaire pour l'existence d'une marche scalaire est que pour toute paire (δ_i, δ_j) d'éléments de Δ il existe au moins une autre paire différente de la première (δ_k, δ_l) telles que*

$$\delta_i \delta_j^{-1} = \delta_k \delta_l^{-1} \tag{2.76}$$

Preuve : Supposons qu'il existe au moins une paire (δ_i, δ_j) ne vérifiant pas (2.76) alors les opérateurs internes associés doivent vérifier l'équation

$$M_{\delta_i} M_{\delta_j}^{\dagger} = 0 \tag{2.77}$$

Si on suppose la dimension de l'espace interne égal à 1 cette équation n'est vérifiée que si l'un des deux scalaires $M_{\delta_i}, M_{\delta_j}^{\dagger}$ est égal à zéro. Identifier un des opérateurs à zéro est équivalent à supprimer un générateur de l'ensemble Δ et donc à modifier le graphe ce qui implique donc par définition qu'il n'y a pas marche quantique sur le graphe. □

Comme on avait déjà remarqué, l'existence d'une marche sur un graphe de Cayley donné dépend de façon importante de la présentation. Cependant pour les automates cellulaires ce théorème implique qu'il n'y a pas de marche scalaire et ceci pour toute présentation du groupe. La preuve est comme suit.

Pour une marche sur le graphe de Cayley du groupe Z^d, pour chaque générateur δ_i il y a trois possibilités : soit lui même ou son inverse sont seuls dans Δ soit les deux sont présents à la fois. Dans les deux premiers cas, la paire formée avec (δ_i, δ_k) (ou δ_i^{-1}) et n'importe quel autre élément δ_k de Δ ne vérifie pas la condition du théorème (2.76). Dans le dernier cas, la paire formé par $(\delta_i, \delta_i^{-1})$ ne vérifie pas la condition du théorème ce qui démontre le corollaire.

Une conséquence directe de (2.23) est que quand le graphe est un graphe de Cayley d'un groupe libre avec d générateurs il est possible de construire une marche avec espace interne de dimension un uniquement si le nombre de générateurs est un.

2.5.2 Limite en temps infini des moments de la marche sur $\mathbb{Z}^d$

Plusieurs auteurs se sont intéressés à la limite à temps infini de la probabilité de la particule sur le graphe. Dans [28] l'auteur a étudié le cas unidimensionnel ($d = 1$) tandis que [20] est une généralisation de ces résultats à des dimensions arbitraires. La démonstration nécessite de supposer le non croisement des valeurs propres de l'opérateur évolution. En modifiant la définition initiale il est possible de suivre exactement les mêmes étapes de leur démonstration. Nous allons maintenant brièvement indiquer ces étapes en précisant comment la modifier pour que cette limite soit aussi valable pour les marches définies dans cette thèse. L'importance de ce résultat est qu'il suggère qu'il n'y a pas non plus de comportement radicalement différent entre les moments de la marche quantique et la marche aléatoire classique sur ce type de graphe.

Quelques définitions

On a un espace de Hilbert défini comme le produit $H = H_C \otimes H_p$ avec $H_C = \mathbb{C}^d$ et $H_P = \ell^2(\mathbb{Z}^d)$.
La base de H_C est la base standard et la base de H_P est donnée par les vecteurs propres $|v_x\rangle$ des opérateurs position $\hat{X}_i$ associés à chaque direction

$$\hat{X}_i|v_x\rangle = x_i|v_x\rangle \tag{2.78}$$

avec $x \in \mathbb{Z}^d$. L'évolution est discrète

$$|\psi_n\rangle = W^n|\psi_0\rangle \tag{2.79}$$

où W est l'opérateur unitaire d'évolution. On définit la transformée de Fourier $F : \ell^2(\mathbb{Z}^d) \to L^2(\mathbb{K}^d)$ où $\mathbb{K} = [0, 2\pi)$ par

$$F : (\psi_{\vec{x}})_J \to \psi(\vec{k})_J = \sum_{\vec{x}\in\mathbb{Z}^d} e^{i\vec{k}.\vec{x}}\psi_{\vec{x}\,J} \tag{2.80}$$

Ainsi $\tilde{W} = (\mathbb{1} \otimes F)W(\mathbb{1} \otimes F^{-1})$ est l'opérateur évolution correspondant sur $\mathbb{C}^d \otimes L^2(\mathbb{K}^d)$ et on note $\lambda_J(\vec{k})$ ses valeurs propres. On note la valeur moyenne

$$E[(\hat{X}_{i,n})^r] = \langle\psi_n|\hat{X}_i^r|\psi_n\rangle \tag{2.81}$$

Le théorème principal est

Theorème 5 *[20]*

$$\lim_{n\to\infty} E[(\sum_{j=1}^{d} c_j \frac{\hat{X}_{j,n}}{n})^r] = \int_\Omega (\sum_{i=1}^{d} c_j h_i(k, J))^r \, d\mu \tag{2.82}$$

où le terme de droite dépend des valeurs propres $\lambda_J(\vec{k})$, les vecteurs propres associés et du vecteur initial $\psi_0(\vec{k}) = F|\psi_0\rangle$. On a aussi que

$$h_i(\vec{k}, J) = \lambda_J(\vec{k})^{-1}(-i\frac{\mathrm{d}}{\mathrm{d}k_i})\lambda_J(\vec{k}) \tag{2.83}$$

où μ est la mesure de probabilité sur $\Omega = \mathbb{K}^d \times \{1, \ldots, J\}$ donnée par

$$\mathrm{d}\mu = |\langle v_J(k), \psi_0(\vec{k})\rangle|^2 \frac{\mathrm{d}\vec{k}}{(2\pi)^2} \tag{2.84}$$

On obtient en particulier avec ce théorème une limite sur les valeurs moyennes et la variance de la marche. Dans l'article les auteurs déduisent à partir de ce résultat la limite en temps infini des fonctions sur le vecteurs position à d-composantes. Nous nous intéresserons au résultat sous la forme (2.82) car la quantité qui semble la plus adéquate pour comparer les marches classiques et quantiques est justement la matrice variance où

$$\sigma^2_{i,j}(n) = E[(\hat{X}_{i,n} - E[\hat{X}_{i,n}])(\hat{X}_{j,n} - E[\hat{X}_{j,n}])] \tag{2.85}$$

Première étape :Transformée de Fourier

A partir de la définition de l'opérateur évolution

$$W = (\sum_{i=1}^{d} P_i \otimes T_i)C \otimes \mathbb{1}$$

où P_i est un projecteur sur un sous espace de dimension un, T_i est l'opérateur déplacement dans la direction i et C est une matrice unitaire $2d \times 2d$ les auteurs calculent la transformée de Fourier de W, notée $\tilde{W}$. On a que

$$\tilde{W}\psi = \psi' \tag{2.86}$$

$$\psi'(\vec{k}) = W(\vec{k})\psi'(\vec{k}) \tag{2.87}$$

$$\tilde{W}(\vec{k}) = \mathcal{D}(\vec{k})C \tag{2.88}$$

où $\mathcal{D}(\vec{k})$ est une matrice diagonale et $\mathcal{D}(\vec{k})_{j,j} = e^{i\vec{\epsilon}_j.\vec{k}}$. $\vec{\epsilon}_1, \ldots, \vec{\epsilon}_{2d}$ dénotent les $2d$ vecteurs de déplacement unité $\pm\vec{e}_i \in \mathbb{Z}^d$ pour $i = 1, \ldots, d$. Maintenant si on part de la définition élargie pour l'opérateur W, c'est a dire $W' = \sum_{i=1}^{2d} M_i \otimes T_i$ on obtient après transformation de Fourier

$$\tilde{W}'(\vec{k}) = \sum_{j=1}^{2d} e^{i\vec{\epsilon}_j.\vec{k}} M_j \tag{2.89}$$

Seconde étape : Calcul de la probabilité

On diagonalise $\tilde{W}(\vec{k})$, et on applique t fois cet opérateur au vecteur initial $\psi_0(\vec{k})$. Mais au lieu de calculer la probabilité pour chaque vertex on calcule la valeur moyenne $E[(\sum_{j=1}^{d} c_j \frac{\hat{X}_{j,n}}{n})^r]$ où tous les termes ont des puissances de t négatives et un seul une puissance nulle, ce qui donne la limite décrite. Dans le calcul de la probabilité la condition utilisée est que $\mathcal{D}(k)$ est une matrice dont les composantes sont des fonctions des composantes de $\vec{k}$ infiniment dérivables. En supposant qu'il n'y a pas de points de croisement les valeurs propres et vecteurs propres sont des fonctions qui vérifient aussi cette condition. Comme la matrice $\tilde{W}'(\vec{k})$ a comme composantes

des fonctions des composantes de $\vec{k}$ infiniment dérivables, avec la même supposition sur les valeurs propres et vecteurs propres on obtient le même théorème.

Donc pour les marches généralisées les moments auront la même dépendance temporelle dans la limite à temps infini si les valeurs propres de la transformée de Fourier de l'opérateur évolution sont non dégénéré es. En plus cette dépendance ne sera que quadratiquement supérieure aux mêmes quantités calculées sur des marches classiques. Récemment, [21] on a commencé à s'intéresser aux effets de ces croisements sur les marches unidimensionnelles. Il a été démontré que la dégénérescence des valeurs propres est en relation avec des effets peu étudiés comme la localisation de la particule sur le vertex initial, c'est a dire que la limite de temps infini de la probabilité de la particule de rester au point initial est non nulle.

Chapitre 3

Différents aspects des marches

3.1 Introduction

Nous avons commencé par étudier le cas le plus important à savoir le temps de traversée de l'hypercube. Ce temps défini avec l' équation (23), dans des conditions similaires varie avec la dimension de façon exponentielle pour une marche classique tandis qu'il est polynomiale dans le cas quantique, la variable étant la dimension de l'hypercube. Nous avons commencé par modifier les paramètres possibles, c'est à dire modifier l'opérateur déplacement et la matrice interne toujours en préservant la symétrie du graphe. Nous avons calculé ensuite l'évolution à temps t de quelques marches définies dans le chapitre précédent. En particulier, nous avons calculé numériquement leur variance pour les comparer. Finalement dans la dernière section, nous avons calculé la forme des opérateurs évolution qu'on obtient après avoir imposé des conditions de symétrie pour des marches sur un réseau simple de dimension un et deux.

3.2 Le temps de traversée de la marche sur l'hypercube

3.2.1 Le modèle

On va utiliser pour décrire l'hypercube le graphe de Cayley avec présentation

$$\Gamma = \langle \delta_1, \ldots, \delta_n | \delta_i \delta_j \delta_j^{-1} \delta_i^{-1} = e, \delta_i^2 = e \rangle \tag{3.1}$$

Le graphe a 2^n vertex éléments dont l'ensemble s'identifie à $\mathbb{B}^n$, l'ensemble des n-uples $(x_0, \ldots, x_{n-1})$ avec $x_i \in \{0, 1\}$. On utilise l'espace de Hilbert $\mathcal{H}_G = \otimes_n \mathcal{H}$ où chaque élément de la base standard $\{|x_0, \ldots, x_{n-1}\rangle\}$ peut être associé à un élément de X de façon évidente. Nous allons introduire la distance de Hamming qui sera utile pour décrire le voisinage d'un point. Pour chaque paire de vertex (x, y) on définit $H(x) = \sum_{i=0}^{n-1} |x_i - y_i|$, ainsi deux vertex x et y sont voisins si et seulement si $H(x, y) = 1$. On peut aussi définir $h(x) = H(x, 0)$ la distance du vertex x au vertex choisi comme origine $(0, \ldots, 0)$. Avec la base choisie la matrice de Pauli σ_x sur un

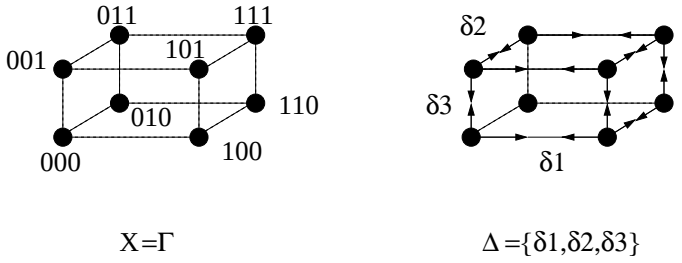


FIG. 3.1 – Construction de l'hypercube de dimension 3 comme un Graphe de Cayley $C_\Delta(\Gamma)$

qubit est la matrice translation d'un vecteur a son voisin. Si on utilise pour l'espace interne la solution des groupes libres on a

$$W = \sum_{j=1,n} P_j U \otimes T_j \tag{3.2}$$

où U est une matrice unitaire $n \times n$ et T est un opérateur translation. On voudrait que T dépende d'un paramètre ϵ qui interpole entre le cas $(\epsilon = 0)$ $T_j : |x_0, \ldots, x_j, \ldots, x_n\rangle \rightarrow |x_0, \ldots, (1-x_j), \ldots, x_n\rangle$ au cas $(\epsilon = 1)$ $T_j = \mathbb{1}$. Nous prenons donc comme opérateur translation $T(\alpha, \beta)_j = \alpha\mathbb{1} + \beta(\sigma_x)_j$, ou comme précédemment les matrices d'un qubit agissent non trivialement uniquement sur le qubit avec index j. Quant à la matrice U un choix qui laisse invariant par permutations de deux indices i, j est

$$U_{i,j} = b + \delta_{i,j} \tag{3.3}$$

avec $b = -(\frac{1+e^{i\phi}}{n})$.
L'unitarité de W est équivalente à

$$M_i M_j^\dagger + M_j M_i^\dagger = 0 \qquad 1 \leq i < j \leq n \tag{3.4}$$

$$\alpha^* \beta M_i M_0^\dagger + \alpha \beta^* M_0 M_i^\dagger = 0 \qquad 1 \leq i \leq n \tag{3.5}$$

$$|\alpha|^2 M_0 M_0^\dagger + |\beta|^2 \sum_i M_i M_i^\dagger = \mathbb{1} \tag{3.6}$$

òu $M_0 = \sum_{i=1}^n M_i$. Ces conditions sont vérifiées avec les matrices internes de la forme de la solution des groupes libres et les constantes paramètres α et β tels que

$$M_i = P_i U \qquad |\alpha|^2 + |\beta|^2 = 1 \tag{3.7}$$

$$M_0 = (\sum_j P_j U) \qquad \alpha\beta^* + \beta\alpha^* = 0 \tag{3.8}$$

On choisit donc $\alpha = -i \sin\epsilon$ et $\beta = \cos\epsilon$. Le cas $\phi = 0$, $\epsilon = 0$ correspond au modèle étudié par Kempe et Moore. Comme l'opérateur déplacement est maintenant $T(\epsilon)_j = (-i \sin\epsilon \mathbb{1} + \cos\epsilon\sigma_x)_j$ on peut associer ϵ à la probabilité de rester sur place. Pour donner un sens à ϕ il faut observer qu' après un pas de temps, on obtient une superposition d'états où chaque vecteur de base a été multiplié soit par a ou par b en fonction de l'état de l'espace interne. Si a et b ont tous les deux la même phase

pour tous temps tous les vecteurs auront la même phase et une modification de la phase relative entre a et b modifiera la phase relative entre vecteurs. Supposons $a = r_a e^{i\theta_a}$ et $b = r_b e^{i\theta_b}$, alors $\tan\theta_a = \frac{\sin\phi}{n-1+\cos\phi}$ et $\tan\theta_b = -\frac{\sin\phi}{1+\cos\phi}$. La variation de ϕ entraîne donc une variation de la différence de phase entre a et b, même dans la limite n infini, ce qui entraîne une variation de la phase relative des états au cours de l'évolution de la marche.

3.2.2 Calcul de la fonction d'onde

Nous allons calculer la probabilité au temps t de trouver la particule dans le site x étant donne une condition initiale "symétrique" $|\psi_0\rangle = \frac{1}{\sqrt{n}}(\sum_{i=1}^{n}|i\rangle) \otimes |0\rangle$. Les deux premières étapes suivent la procédure indiquée par Moore et Russel dans [33].

Diagonalisation de l'opérateur translation

On a l'opérateur

$$W = \sum_{i=1}^{n} P_i U \otimes (-i\sin\epsilon\mathbb{1} + \cos\epsilon\sigma_x)_i \tag{3.9}$$

Les valeurs propres sont $\mu_0 = e^{-i\epsilon}$ et $\mu_1 = -e^{i\epsilon}$ et les vecteurs propres associés $v_0 = \frac{1}{\sqrt{2}}(1,1)$ et $v_1 = \frac{1}{2}(1,-1)$. Dans la base initiale la matrice de passage est la portes d'Hadamard. Si on note F le produit tensoriel de n opérateurs H dans $\mathcal{H}_G$ fois l'identité dans $\mathcal{H}_I$ on a

$$F = \mathbb{1} \otimes (H \otimes \cdots \otimes H) \tag{3.10}$$

$$F^{-1}WF = \sum_i P_i U \otimes (\mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes \underbrace{\begin{bmatrix} \mu_0 & 0 \\ 0 & \mu_1 \end{bmatrix}}_{i} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}) \tag{3.11}$$

$$= \sum_i P_i U \otimes \begin{bmatrix} \mu_0 & 0 \\ 0 & \mu_1 \end{bmatrix}_i \tag{3.12}$$

On va écrire $W' = F^{-1}WF$ comme une somme d'opérateurs

$$W' = \sum_x U_x \otimes |x\rangle\langle x| \tag{3.13}$$

où $(U_x)_{i,j} = a\mu_{x_i}\delta_{i,j} + b\mu_{x_i}(1-\delta_{i,j})$. U_x est donc de la forme

$$U_x = \begin{bmatrix} a\mu_{x_1} & b\mu_{x_1} & \dots & b\mu_{x_1} \\ b\mu_{x_2} & a\mu_{x_2} & \dots & b\mu_{x_2} \\ \vdots & \vdots & \ddots & \vdots \\ b\mu_{x_n} & b\mu_{x_n} & \dots & a\mu_{x_n} \end{bmatrix} \tag{3.14}$$

Diagonalisation de l'opérateur évolution transformé W'

On diagonalise maintenant W' avec matrice de passage $\tau = \sum_y \tau_y \otimes |y\rangle\langle y|$ où τ_y est formé avec les vecteurs propres de U_y.
Les vecteurs et valeurs propres ne dépendent que de $h(y)$ la distance de Hamming du vertex y et l'origine. D'abord pour les cas extrêmes $h(y) = 0$ et $h(y) = n$ il y a une seule valeur propre n fois dégénérée

$$\lambda_0 = -e^{-i(\epsilon-\phi)} \tag{3.15}$$

$$\lambda_n = e^{i(\epsilon+\phi)} \tag{3.16}$$

Pour les autres cas, en posant $k = h(x)$ on a deux valeurs propres solutions du polynôme

$$|U_x - \lambda \mathbb{1}| = \lambda^2 + 2\cos\theta(w_k, \phi, \epsilon)e^{i\frac{\phi}{2}}\lambda + e^{i\phi} \tag{3.17}$$

Ces deux valeurs propres sont de la forme

$$\lambda_k^{\pm} = -e^{i\frac{\phi}{2}}e^{\mp i\theta_k} \tag{3.18}$$

$$\theta_k = \theta_k(\phi, \epsilon) \tag{3.19}$$

$$\cos\theta_k = (1 - 2\frac{k}{n})\cos\frac{\phi}{2}\cos\epsilon + \sin\epsilon \tag{3.20}$$

et dépendent de ϵ, ϕ et k à travers θ_k. Les vecteurs propres associés $v_k^{\pm}$ ont seulement deux types de composantes : la composante dans la direction i dépend de la composante x_i du vertex x associé a k.

$$(v_k^{\pm})_i = (\mu_{1-x_i}(a-b) - \lambda_k^{\pm})\frac{\mu_{x_i}}{n_k^{\pm}} \tag{3.21}$$

où n_k^+ et n_k^- sont des constantes de normalisation $|v_k^{\pm}|^2 = 1$. Le vecteur initial peut s'exprimer en termes des vecteurs v_k^+ et v_k^- comme suit

$$\frac{1}{\sqrt{n}}(1, \ldots, 1) = m_k^+ v_k^+ + m_k^- v_k^- \tag{3.22}$$

$$m_k^+ = \frac{\lambda_k^- n_k^+}{\sqrt{n}(\lambda_k^- - \lambda_k^+)\mu_0\mu_1(a-b)} \tag{3.23}$$

$$m_k^- = \frac{-\lambda_k^+ n_k^-}{\sqrt{n}(\lambda_k^- - \lambda_k^+)\mu_0\mu_1(a-b)} \tag{3.24}$$

Pour le cas $k = 0$ et $k = n$ le vecteur initial est le vecteur propre associé à λ_0 et λ_n.

Calcul de la probabilité

La probabilité de trouver la particule au vertex x à l'instant t est

$$p_{\phi,\epsilon}(x,t) = \sum_i \left| \langle x, i | F(F^{-1}WF)^t F^{-1} | \psi_0 \rangle \right|^2 \tag{3.25}$$

avec $|\psi_0\rangle = \frac{1}{\sqrt{n}}\sum_i |i\rangle \otimes |0\dots0\rangle$. On va calculer le vecteur résultant de l'opération successive de F^{-1} puis de $(F^{-1}WF)^t$ pour finalement projeter sur $\langle x,i|F$ et calculer sa norme.

$$F^{-1}|\psi_0\rangle = \Big(\frac{1}{\sqrt{n}}\sum_i |i\rangle\Big) \otimes \Big(\frac{1}{\sqrt{2^n}}\sum_{y\in\mathbb{B}^n} |y\rangle\Big) \tag{3.26}$$

$$\begin{aligned} =&\frac{1}{\sqrt{2^n}}\Bigg(\Big(\sum_{y\in B^n}\big(m^+_{h(y)}|v^+_{h(y)}\rangle + m^-_{h(y)}|v^-_{h(y)}\rangle\big)\Big)\otimes|y\rangle\Bigg) \\ &+ |v_0\rangle\otimes|0,\dots,0\rangle + |v_n\rangle\otimes|1,\dots,1\rangle\Bigg) \end{aligned} \tag{3.27}$$

Où on définit l'ensemble B^n par $B^n = \mathbb{B}^n\backslash\{(0,\dots,0),(1,\dots,1)\}$. Après l'application de t fois l'opérateur évolution on obtient

$$\begin{aligned} \big(F^{-1}WF\big)^t F^{-1}|\psi_0\rangle = \\ \frac{1}{\sqrt{2^n}}\Bigg(\sum_{y\in B^n}\big(m^+_{h(y)}{\lambda^+_{h(y)}}^t|v^+_{h(y)}\rangle + m^-_{h(y)}{\lambda^-_{h(y)}}^t|v^-_{h(y)}\rangle\big)\otimes|y\rangle \\ + \lambda_0^t|v_0\rangle)\otimes|0,\dots,0\rangle + \lambda_n^t|v_n\rangle\otimes|1,\dots,1\rangle\Bigg) \end{aligned} \tag{3.28}$$

Pour réaliser la dernière opération il est utile de remarquer que

$$\big(\langle u_i|\otimes\langle x|\big)F\big(|u_j\rangle\otimes|y\rangle\big) = \langle u_i|u_j\rangle\frac{1}{\sqrt{2^n}}(-1)^{x.y} \tag{3.29}$$

$$(-1)^{x.y} = \begin{cases} 1 & \text{si } y = (0,\dots,0) \\ (-1)^{h(x)} & \text{si } y = (1,\dots,1) \end{cases} \tag{3.30}$$

Dans l'expression de $p_{\phi,\epsilon}(x,t)$

$$\begin{aligned} p_{\phi,\epsilon}(x,t) =& \sum_i\Big|\frac{1}{\sqrt{2^n}}\sum_{y\in B^n}\big(m^+_{h(y)}{\lambda^+_k}^t\langle i|v^+_{h(y)}\rangle + m^-_{h(y)}{\lambda^-_{h(y)}}^t\langle i|v^-_{h(y)}\rangle\big)\frac{(-1)^{x.y}}{\sqrt{2^n}} \\ &+ \frac{\lambda_0^t}{\sqrt{2^n}}\langle i|v_0\rangle + \frac{\lambda_n^t}{\sqrt{2^n}}(-1)^{h(x)}\langle i|v_n\rangle\Big|^2 \end{aligned} \tag{3.31}$$

$$\begin{aligned} =&\frac{1}{\sqrt{4^n n}}\sum_i\Big|\sum_{y\in B^n}\big(m^+_{h(y)}{\lambda^+_{h(y)}}^t\langle i|v^+_{h(y)}\rangle + m^-_{h(y)}{\lambda^-_{h(y)}}^t\langle i|v^-_{h(y)}\rangle\big)(-1)^{x.y} \\ &+ \lambda_0^t + \lambda_n^t(-1)^{h(x)}\Big|^2 \end{aligned} \tag{3.32}$$

Si $x_i = 0$ se simplifie le premier terme

$$\begin{aligned} m_k^+{\lambda_k^+}^t\langle i|v_k^+\rangle + m_k^-{\lambda_k^-}^t\langle i|v_k^-\rangle = \\ (\lambda_k^-\lambda_k^+)\frac{\lambda_k^{+t-1}-\lambda^{t-1}}{\lambda_k^- - \lambda_k^+} - \frac{1}{\mu_1(a-b)}(\lambda_k^-\lambda_k^+)\frac{\lambda_k^{+t}-\lambda_k^{-t}}{\lambda_k^- - \lambda_k^+} \end{aligned} \tag{3.33}$$

et si $x_i = 1$ on obtient la même expression en changeant μ_1 en μ_0. On définit la fonction pour $0 \leq c \leq 1$

$$f(k,c) = (\lambda_k^- \lambda_k^+) \frac{\lambda_k^{+t-1} - \lambda^{t-1}}{\lambda_k^- - \lambda_k^+} - \frac{1}{\mu_(1-c)(a-b)} (\lambda_k^- \lambda_k^+) \frac{\lambda_k^{+t} - \lambda_k^{-t}}{\lambda_k^- - \lambda_k^+} \tag{3.34}$$

On démontre que

$$\sum_{y \in B^n} f(h(y),c)\,(-1)^{x.y} = \sum_{s=1}^{n-1} (\sum_{q=0}^{h(x)} \left(\begin{array}{c} h(x) \\ q \end{array} \right) \left(\begin{array}{c} n-h(x) \\ s-q \end{array} \right) (-1)^q f(s,c) \tag{3.35}$$

Le terme de gauche a $2^n - 2$ termes dans la somme tandis que le terme de droite en contient n^2. La preuve se fait par récurrence. En terme des paramètres ϵ, ϕ

$$f(k,1) = (-1)^{t-1} e^{i\frac{\phi}{2}t} \frac{\sin\theta_k(t-1)}{\sin\theta_k} - (-1)^{t-1} e^{i\epsilon} e^{i\frac{\phi}{2}t} e^{i\frac{\phi}{2}} \frac{\sin\theta_k t}{\sin\theta_k} \tag{3.36}$$

$$f(k,0) = (-1)^{t-1} e^{i\frac{\phi}{2}t} \frac{\sin\theta_k(t-1)}{\sin\theta_k} + (-1)^{t-1} e^{-i\epsilon} e^{i\frac{\phi}{2}t} e^{i\frac{\phi}{2}} \frac{\sin\theta_k t}{\sin\theta_k} \tag{3.37}$$

D'autre part il y a $\left(\begin{array}{c} n \\ h \end{array} \right)$ vertex à une même distance h de l'origine. Finalement on obtient que l'expression de la probabilité de trouver la particule à distance h de l'origine est

$$\begin{aligned} p_{\phi,\epsilon}(h,t) = \left(\begin{array}{c} n \\ h \end{array} \right) \frac{1}{4^n} \Big\{ & \frac{h}{n} \Big| \sum_{k=1}^{n-1} (-1)^{t-1} e^{i\frac{\phi}{2}t} \Big((\frac{\sin\theta_k(t-1)}{\sin\theta_k} - e^{-i(\epsilon-\frac{\phi}{2})} \frac{\sin\theta_k t}{\sin\theta_k}) \\ & c(k,h-1) - (\frac{\sin\theta_k(t-1)}{\sin\theta_k} + e^{i(\epsilon+\frac{\phi}{2})} \frac{\sin\theta_k t}{\sin\theta_k}) c(k-1,h-1) \Big) \\ & + (-1)^t e^{-i(\epsilon-\phi)t} + e^{i(\epsilon+\phi)t} (-1)^h \Big|^2 \\ & + (1-\frac{h}{n}) \Big| \sum_{k=1}^{n-1} (-1)^{t-1} e^{i\frac{\phi}{2}t} \Big((\frac{\sin\theta_k(t-1)}{\sin\theta_k} - e^{-i(\epsilon-\frac{\phi}{2})} \frac{\sin\theta_k t}{\sin\theta_k}) \\ & c(k,h) + (\frac{\sin\theta_k(t-1)}{\sin\theta_k} + e^{i(\epsilon+\frac{\phi}{2})} \frac{\sin\theta_k t}{\sin\theta_k}) c(k-1,h) \Big) \\ & + (-1)^t e^{-i(\epsilon-\phi)t} + e^{i(\epsilon+\phi)t} (-1)^h \Big|^2 \Big\} \end{aligned}$$

avec $c(k,n) = \sum_{q=0}^{h} \left(\begin{array}{c} h \\ q \end{array} \right) \left(\begin{array}{c} n-1-h \\ k-q \end{array} \right) (-1)^q$.

3.2.3 Le temps de traversée et la probabilité maximale

Nous avons utilisé ces expressions pour étudier le temps de traversée de l'hypercube étudié par Kempe et Moore. Nous avons numériquement fait varier touts les paramètres : ϕ, ϵ, n les résultats sont présentés dans les figures suivantes. Le temps de traversée (23) a été calculé ici avec un p constant et égal à 0.5 et le temps t est

choisi comme le temps minimal pour vérifier la définition. L'état initial et état final sont respectivement

$$|\phi_0\rangle = \sum_i |i\rangle \otimes |0, \ldots, 0\rangle \tag{3.38}$$

$$|x\rangle = \sum_i |i\rangle \otimes |1, \ldots, 1\rangle \tag{3.39}$$

La probabilité qu'on a calculée $\sum_i |\langle i| \otimes \langle 1, \ldots, 1|\psi_n\rangle$ est égale a la probabilité (23) calculée avec l'état final (3.39). Ceci s'obtient du fait que pour tout état de base interne $|i\rangle$ la quantité $\langle i| \otimes \langle 1, \ldots, 1$ est la même.
On s'attendait a voir disparaître le comportement linéaire en variant ϕ la phase entre les chemins. Comme la variation des paramètres n'altère pas la symétrie de l'opérateur, par rapport a toute permutation de deux directions internes, ceci semble suggérer que la symétrie de l'opérateur joue un rôle encore plus important que prévu. Pourtant on a trouvé que en variant les paramètres la valeur de la probabilité maximale était différente. Ainsi pour les valeurs $\epsilon = 0.5$ et $\phi = 0.4$ la probabilité varie entre 0.6 et 1. Comme la probabilité maximale dépend de ϵ et ϕ un choix de la probabilité minimale qui est satisfaisant pour tous les cas étudiés est $p = 0.5$.
Pour les valeurs $\epsilon = 0.0$ et $\phi = 0.0$ cette probabilité maximale tend vers 1 quand la dimension de l'hypercube augmente. On trouve ici qu'elle dépend de ces deux paramètres. Une direction possible à suivre est l'étude systématique du temps de traversée et de la probabilité maximale, en fonction de ϵ et ϕ dans le but d'établir et classifier les différentes phases possibles. Ceci nécessiterait des algorithmes beaucoup plus performants que ceux qu'on a utilisés pour établir ces résultats.

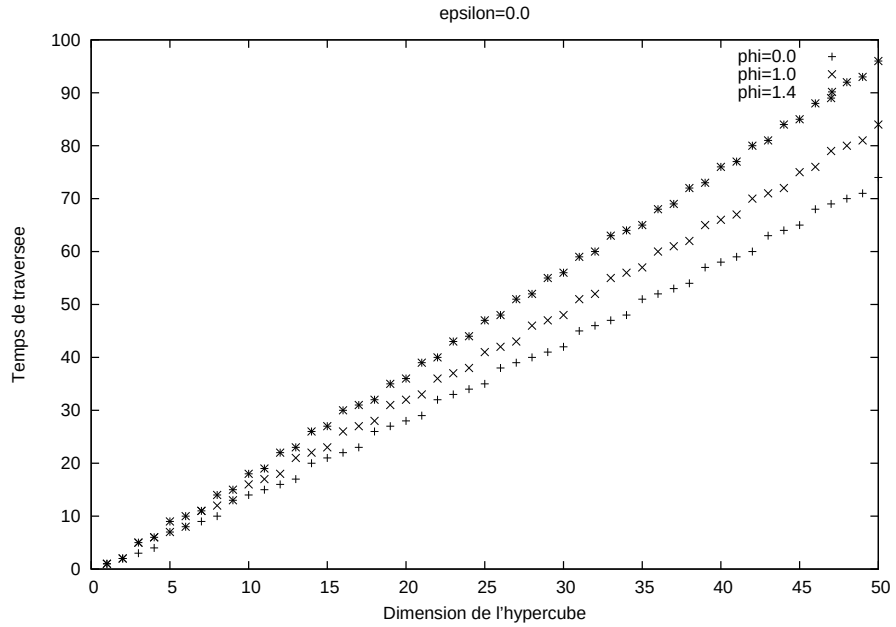


FIG. 3.2 – Temps de traversée de la marche quantique sur l'hypercube de dimension n, en fonction de n. Paramètre $\epsilon = 0.0$, $\phi = 0.0, 1.0, 1.4$

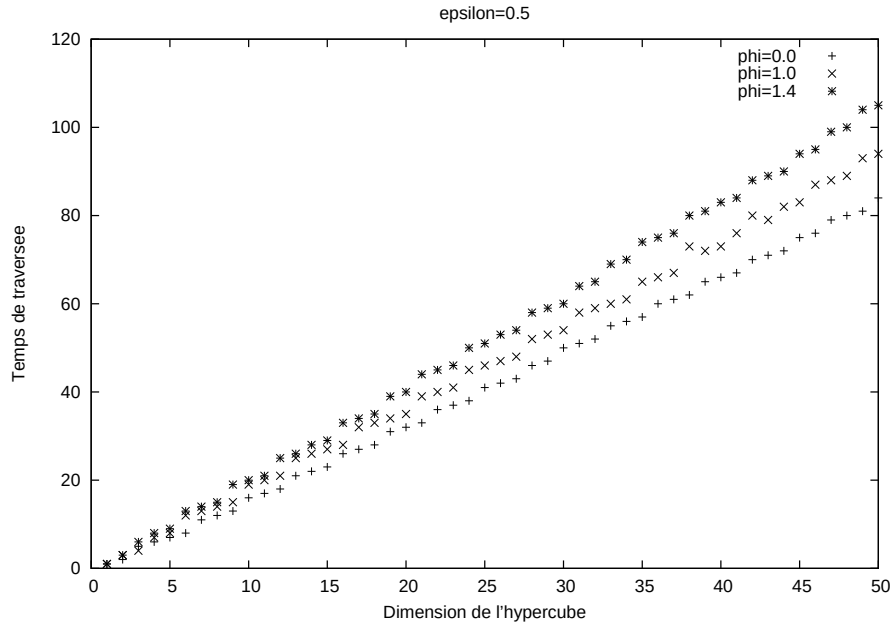


FIG. 3.3 – Temps de traversée de la marche quantique sur l'hypercube de dimension n, , en fonction de n. Paramètre $\epsilon = 0.5$, $\phi = 0.0, 1.0, 1.4$

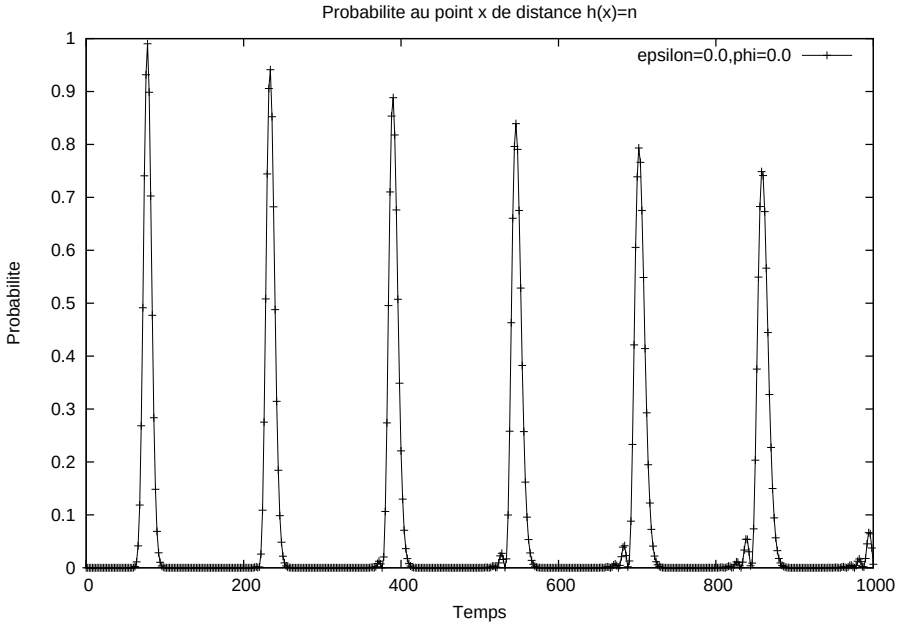


FIG. 3.4 – Probabilité au point de distance de Hamming maximale, par rapport à l'origine, en fonction du temps. Dimension de l'hypercube $n = 50$, paramètres $\epsilon = 0.0\, \phi = 0.0$. Seuls les temps paires sont représentés.

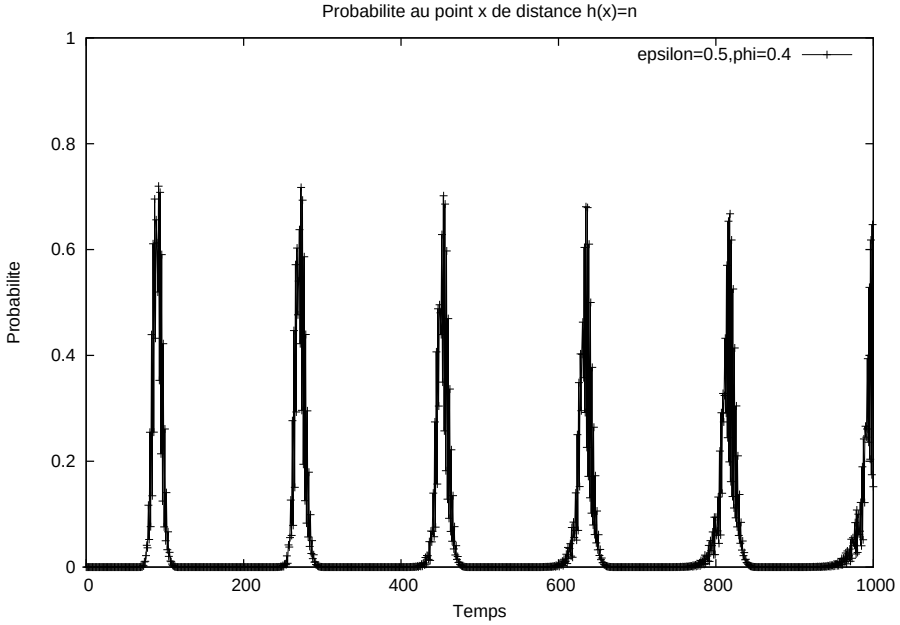


FIG. 3.5 – Probabilité au point de distance de Hamming maximale, par rapport à l'origine, en fonction du temps. Dimension de l'hypercube $n = 50$, paramètres $\epsilon = 0.5$, $\phi = 0.4$.

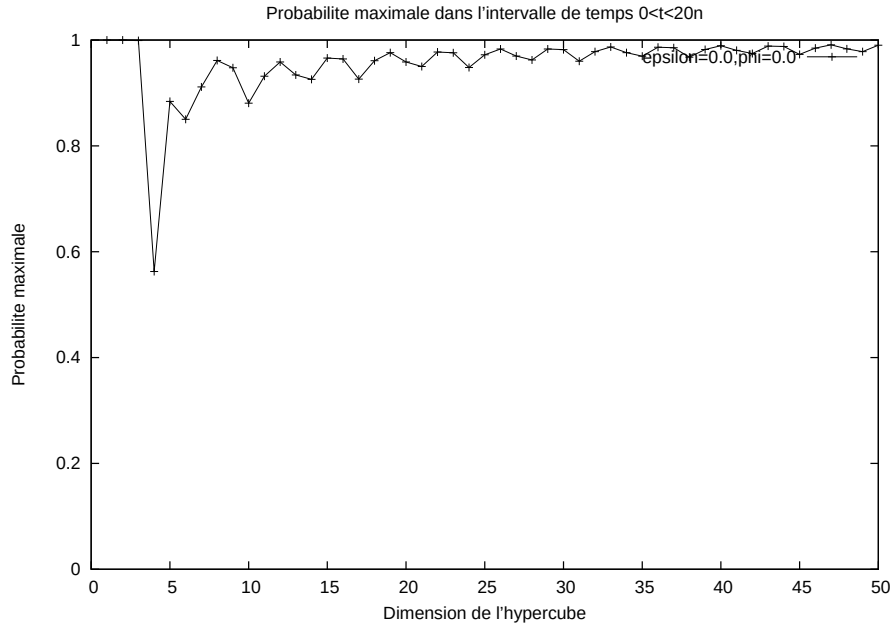


FIG. 3.6 – Probabilité maximale en fonction de la dimension de l'hypercube n, au point de distance de Hamming n sur l'intervalle de temps $0 < t < 20n$. Paramètres $\epsilon = 0.0$, $\phi = 0.0$

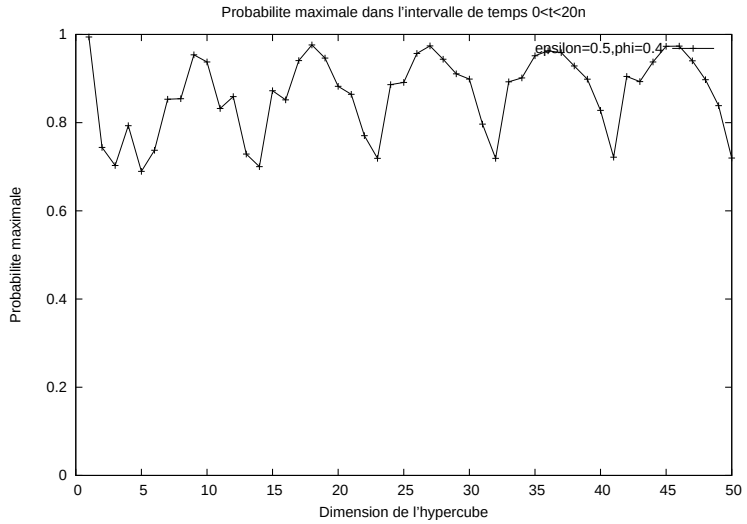


FIG. 3.7 – Probabilité maximale en fonction de la dimension de l'hypercube n, au point de distance de Hamming n sur l'intervalle de temps $0 < t < 20n$. Paramètres $\epsilon = 0.5$, $\phi = 0.4$

3.3 La variance des marches sur des réseaux simples

3.3.1 Marches quantiques et classiques unidimensionnelles

Le modèle le plus étudié est la marche sur $\mathbb{Z}$, nous allons comparer la variance de plusieurs marches différant par la dimension de l'espace interne.

Marche quantique avec espace interne de dimension 2

Le modèle
On suit les définitions décrites dans le chapitre 2. Explicitement la forme des matrices internes M_+ et M_- sera

$$W = M_+ \otimes T_+ + M_- \otimes T_- \tag{3.40}$$

$$M_+ = P_1 U = \begin{pmatrix} e^{\frac{i}{2}(\alpha+\beta)} \cos\frac{\theta}{2} & e^{\frac{i}{2}(\alpha-\beta)} \sin\frac{\theta}{2} \\ 0 & 0 \end{pmatrix} \tag{3.41}$$

$$M_- = P_2 U = \begin{pmatrix} 0 & 0 \\ -e^{\frac{-i}{2}(\alpha-\beta)} \sin\frac{\theta}{2} & e^{\frac{-i}{2}(\alpha+\beta)} \cos\frac{\theta}{2} \end{pmatrix} \tag{3.42}$$

Calcul de la fonction d'onde. On transforme l'évolution

$$\psi_x(t) = \begin{pmatrix} c_{1,x}(t) \\ c_{2,x}(t) \end{pmatrix} \qquad p(x,t) = \sum_{i=1,2} |c_{i,x}(t)|^2 \tag{3.43}$$

La nouvelle équation d'évolution $\psi_x(t) = \tilde{W}\psi_x(t-1)$

$$\tilde{W} = \begin{pmatrix} e^{\frac{i}{2}(\alpha+\beta)} \cos\frac{\theta}{2}\tau^{-1} & e^{\frac{i}{2}(\alpha-\beta)} \sin\frac{\theta}{2}\tau^{-1} \\ -e^{\frac{-i}{2}(\alpha-\beta)} \sin\frac{\theta}{2}\tau & e^{\frac{-i}{2}(\alpha+\beta)} \cos\frac{\theta}{2}\tau \end{pmatrix} \tag{3.44}$$

où $\tau c_{i,x} = c_{i,x+1}$. Par le théorème de Cayley Hamilton $\tilde{W}$ vérifie l'équation

$$W^2 - FW - \lambda \mathbb{1} = 0 \tag{3.45}$$

où $F = e^{\frac{i}{2}(\alpha+\beta)} \cos\frac{\theta}{2}\tau^{-1} + e^{\frac{-i}{2}(\alpha+\beta)} \cos\frac{\theta}{2}\tau$ et $\lambda = -1$. Ceci implique

$$\psi_x(t) = F\psi_x(t-1) + \lambda\psi_x(t-2) \tag{3.46}$$

On définit $\phi_x(t)$ la solution de l'équation précédente avec conditions $\phi_x(-1) = 0$ et $\phi_x(0) = \delta_x$.On a donc que $\phi_x(1) = F\delta_x$. En termes de la fonction $\phi_x(t)$ la solution de (3.46) avec condition initiale

$$\psi_x(0) = c_1 \begin{pmatrix} \delta_x \\ 0 \end{pmatrix} + c_2 \begin{pmatrix} 0 \\ \delta_x \end{pmatrix} \tag{3.47}$$

est

$$\psi_x(t) = c_1 \begin{pmatrix} \phi_x(t) - \tilde{W}_{2,2}\phi_x(t-1) \\ \tilde{W}_{2,1}\phi_x(t-1) \end{pmatrix} + c_2 \begin{pmatrix} \tilde{W}_{1,2}\phi_x(t-1) \\ \phi_x(t) - \tilde{W}_{1,1}\phi_x(t-1) \end{pmatrix} \tag{3.48}$$

On démontre par récurrence que

$$\phi_x(t) = \sum_{l=0}^{\lfloor \frac{t}{2} \rfloor} \lambda^l \begin{pmatrix} t-l \\ l \end{pmatrix} F^{t-2l}\phi_x(0) = \sum_{l=0}^{\lfloor \frac{t}{2} \rfloor} \lambda^l \begin{pmatrix} t-l \\ l \end{pmatrix} \tilde{\phi}_x(t-2l) \tag{3.49}$$

Où

$$\tilde{\phi}_x(q) = F^q\phi_x(0) = \begin{cases} \begin{pmatrix} q \\ \frac{x+q}{2} \end{pmatrix} e^{\frac{i}{2}(\alpha+\beta)x} \cos^q \frac{\theta}{2} & \text{si } x+q \text{ est pair} \\ 0 & \text{autrement} \end{cases} \tag{3.50}$$

En utilisant les résultats précédents on obtient

$$\psi_x(t) = c_1 \begin{pmatrix} \phi_x(t) - e^{\frac{-i}{2}(c_{1,0}(0)+\beta)} \cos\frac{\theta}{2}\phi_{x+1}(t-1) \\ -e^{\frac{-i}{2}(\alpha-\beta)} \sin\frac{\theta}{2}\phi_{x+1}(t-1) \end{pmatrix} + c_2 \begin{pmatrix} e^{\frac{i}{2}(\alpha-\beta)} \sin\frac{\theta}{2}\phi_{x-1}(t-1) \\ \phi_x(t) - e^{\frac{i}{2}(\alpha+\beta)} \cos\frac{\theta}{2}\phi_{x-1}(t-1) \end{pmatrix} \tag{3.51}$$

Si bien cette probabilité avait déjà été obtenue auparavant la méthode de calcul est différente des autres méthodes. Cette méthode peut être utilisé pour d'autres marches dont l'espace interne est de dimension deux. Par la suite on l' utilisera pour calculer la probabilité d'une marche sur un réseau bidimensionnel.
Numériquement on a calculé la variance de la marche pour quelques valeurs des paramètres α, β, θ. Pour les valeurs étudiées la variance est quadratique, voir figures 3.8 et 3.9, en accord donc aux résultats connus.

Marche quantique d'espace interne de dimension égale au temps

La variance linéaire peut être aussi une caractéristique d'une marche quantique. Le cas présenté par la suite est un cas extrême car il suppose que l'espace interne est d'une dimension au moins aussi grande que le nombre de pas réalisés. Cette marche a été étudiée dans [13]

Supposons que l'espace interne est le produit de M espaces élémentaires de dimension 2, l'espace total est un produit $\mathcal{H}_I \otimes \mathcal{H}_G$ avec $\mathcal{H}_I = \otimes_{i=1}^{M}\mathcal{H}$. L'opérateur évolution a la forme standard décrite précédemment (marche unidimensionnelle) c'est à dire le produit d'un opérateur déplacement S et une matrice unitaire dans l'espace interne C.

$$W = S(C \otimes \mathbb{1}) \tag{3.52}$$

A chaque pas de temps, l'opérateur interne ("coin") agit non trivialement uniquement sur un des $\mathcal{H}$ de l'espace interne. Pendant les d premiers pas de temps de la marche l'opérateur agit sur le premier des espaces internes puis change d'espace interne et agit pendant d pas de temps et ainsi M fois. Le temps total de cette marche

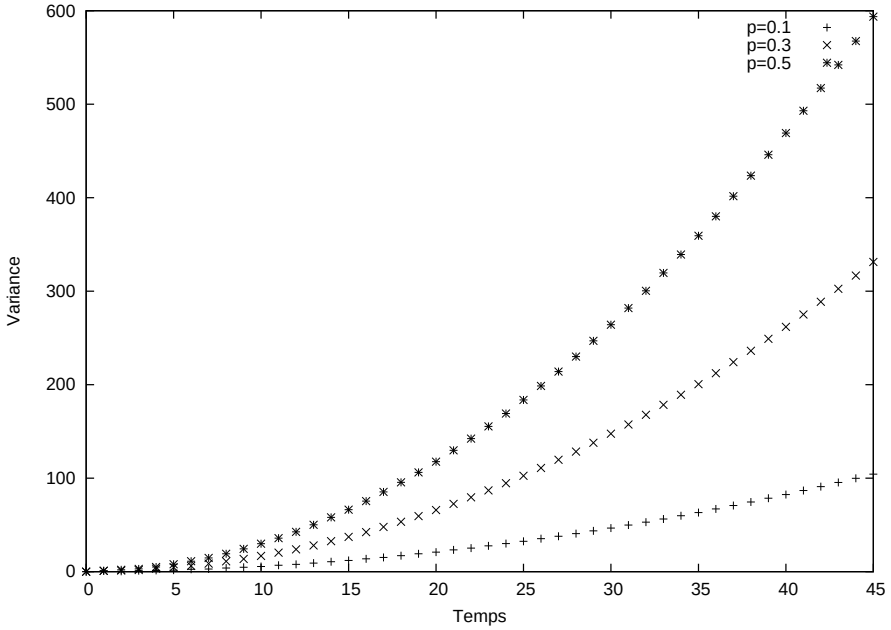


FIG. 3.8 – Variance en fonction du temps de la marche quantique sur $\mathbb{Z}$ avec espace interne de dimension 2. Paramètres $\alpha = \frac{\pi}{2}$, $\beta = -\frac{\pi}{2}$, $\cos^2\theta = p$

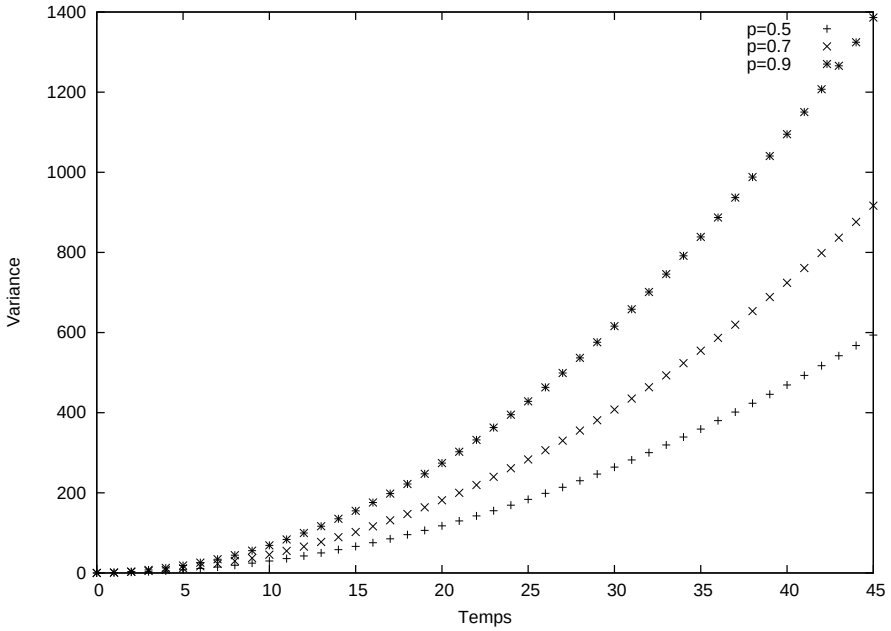


FIG. 3.9 – Variance en fonction du temps de la marche quantique sur $\mathbb{Z}$ avec espace interne de dimension 2. Paramètres $\alpha = \frac{\pi}{2}$, $\beta = -\frac{\pi}{2}$, $\cos^2\theta = p$

est donc $t = dM$.

$$W = \prod_{i=1}^{M} W_i^d \tag{3.53}$$

$$W_i = (M_+)_i \otimes T_+ + (M_-)_i \otimes T_- \tag{3.54}$$

$$M_\pm = P_\pm C \otimes \mathbb{1} \tag{3.55}$$

$$(M_+)_i = \mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes \underbrace{M_+}_{i} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \tag{3.56}$$

où $P_\pm$ sont deux projecteurs orthogonaux dans $\mathcal{H}$

On suppose la matrice interne C sur un qubit de la forme d'une matrice d'Hadamard et comme état initial le produit du vecteur associe au projecteur P_- et la position associée à l'origine. Par une méthode semblable à celle utilisé par [20] les auteurs obtiennent

$$\langle x \rangle_t = C_1 t \tag{3.57}$$

$$\langle x^2 \rangle_t = C_2 t^2 + O(t) \tag{3.58}$$

et suivant la valeur de d

$$d = 1 \qquad C_1 = 0 \qquad C_2 = 0 \tag{3.59}$$

$$d = 2 \qquad C_1 = 0 \qquad C_2 = \frac{1}{8} \tag{3.60}$$

$$d = 3 \qquad C_1 = -\frac{1}{6} \qquad C_2 = \frac{7}{72} \tag{3.61}$$

$$\tag{3.62}$$

Dans la limite extrême d'un nouvel espace interne par pas de temps ($d = 1, t = M$) la marche a une variance semblable a celle de la marche classique. C'est effet est perdu dès qu'on utilise deux fois le même espace interne ($d = 2, t = 2M$) et ($d = 3, t = 3M$).
La dimension de l'espace interne joue un rôle dans le comportement de la variance. Dans ce cas particulier, les auteurs associent l'espace interne et la mémoire de la marche. On peut se demander quel est l'effet sur la variance d'une marche classique avec espace interne. Ce modèle, appelé marche classique corrélée est présentée maintenant.

Marche classique avec espace interne de dimension deux

Classiquement les marches corrélées ont permis d'étudier des systèmes biologiques évoluant avec une mémoire finie. la plupart des grandeurs ont été calculées [16] [15]. Soit e_j ($1 \leq j \leq d$) un vecteur unitaire de $\mathbb{Z}^d$ et $E = \{e_{\pm j}\,;\, 1 \leq j \leq d\}$ ou $e_{-j} = -e_j$. On a une chaîne de Markov avec valeurs dans E $\{\psi_n; n \geq 1\}$ avec matrice de transition $P = \{p_{i,j}; -d \leq i, j \leq d\}$ et distribution initiale $p^{(1)} = \{p_j; -d \leq j \leq d\}$.
On définit la marche aléatoire corrélée CRW comme le processus discret aléatoire

$\{X_n; n \geq 0\}$ sur $\mathbb{Z}^d$ tel que

$$i) \exists S_0 \in \mathbb{Z}^d \text{tel que} \Pr X_0 = S_0 = 1 \tag{3.63}$$

$$ii) X_n = \sum_{k=1}^{n} \psi_k \; (\forall n \geq 1) \tag{3.64}$$

En particulier une marche corrélée symétrique unidimensionnelle a comme vecteur initial $p^{(1)} = [\frac{1}{2}, \frac{1}{2}]$ et $P = \begin{pmatrix} p & q \\ q & p \end{pmatrix}$ où $p + q = 1$. Les premiers moments sont

$$\mu_t = \langle x \rangle_t = 0 \tag{3.65}$$

$$\sigma_t^2 = \langle x^2 \rangle_t = \begin{cases} t\frac{p}{q} + \frac{p-q}{2q^2}[(p-q)^t - 1] & p \neq 1 \\ t^2 & p = 1 \end{cases} \tag{3.66}$$

Le terme de droite tends rapidement vers zéro, cars $|p - q| < 1$ dans le premier cas. Le terme dominant est donc le terme de gauche qui donne à la variance un comportement linéaire. On peut conclure que l'introduction d'une mémoire est lié a une modification de la variance pourtant le nouveau comportement n'est pas quadratique.

3.3.2 Marche quantique bidimensionnelle

L'espace interne est de dimension deux. L'opérateur évolution est

$$W = M_x \otimes T_x + M_{-x} \otimes T_{-x} + M_y \otimes T_y + M_{-y} \otimes T_{-y} \tag{3.67}$$

et les matrices internes ont la forme

$$M_x = \begin{pmatrix} \cos v \cos u & 0 \\ i \cos v \sin u & 0 \end{pmatrix} \qquad M_{-x} = \begin{pmatrix} 0 & i \cos v \sin u \\ 0 & \cos v \cos u \end{pmatrix} \tag{3.68}$$

$$M_y = \begin{pmatrix} 0 & i \sin v \cos u \\ 0 & -\sin v \sin u \end{pmatrix} \qquad M_{-y} = \begin{pmatrix} -\sin v \sin u & 0 \\ i \sin v \cos u & 0 \end{pmatrix} \tag{3.69}$$

Suivant la même méthode que dans la section précédente on peut calculer la fonction d'onde. Avec la même équation de récurrence (3.46) mais avec $\psi_{x,y}(t)$ au lieu de $\psi_x(t)$ et

$$F = \cos v \cos u(\tau_x + \tau_x^{-1}) - \sin v \sin u(\tau_y + \tau_y^{-1}) \tag{3.70}$$

$$\lambda = -1 \tag{3.71}$$

on obtient donc la même solution (3.48) toujours en remplaçant x par x, y. On a que $\phi_{x,y}(t)$ et $\tilde{\phi}_{x,y}$ sont en relation aussi par (3.49) et le dernier est maintenant de la forme si $x + r$ et $y + t - r$ sont paires :

$$\tilde{\psi}_{x,y}(t) \qquad = \qquad \sum_{r=0}^{t} (\cos v \cos u)^r (-\sin v \sin u)^{t-r} \begin{pmatrix} r \\ \frac{x+r}{2} \end{pmatrix} \begin{pmatrix} t-r \\ \frac{y+t-r}{2} \end{pmatrix} \tag{3.72}$$

et $\tilde{\psi}_{x,y}(t) = 0$ autrement La variance est aussi quadratique, voir figures 3.10 et 3.11. Une étape importante à faire est de vérifier si le théorème de la limite faible s'applique dans ce cas confirmant ces résultats.

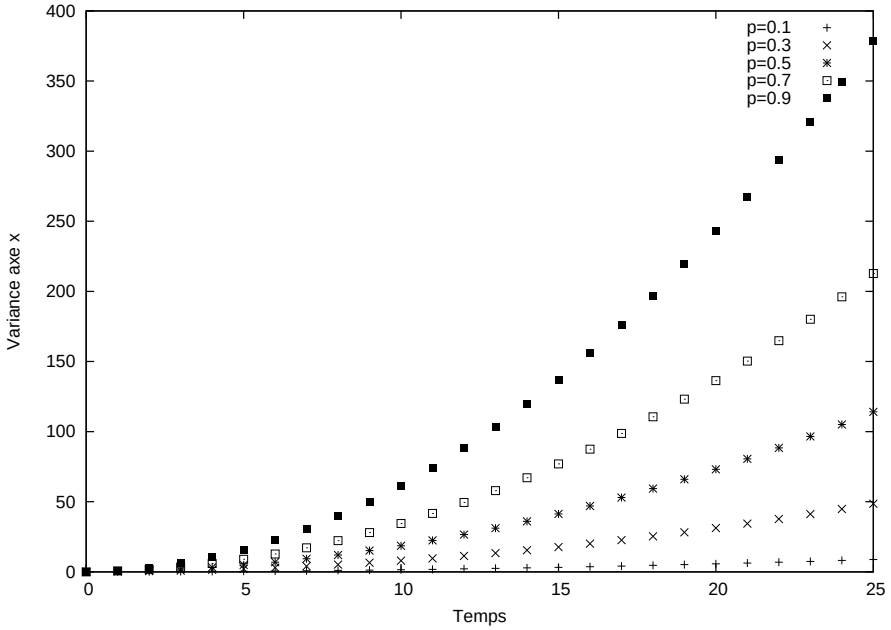


FIG. 3.10 – Variance σ^2_{xx} en fonction du temps de la marche quantique sur $\mathbb{Z}^2$ avec espace interne de dimension 2, sur l'axe x ($\sigma^2_{xx} = \langle X^2 \rangle - \langle X \rangle^2$). Paramètre $p = \cos u = \cos v$

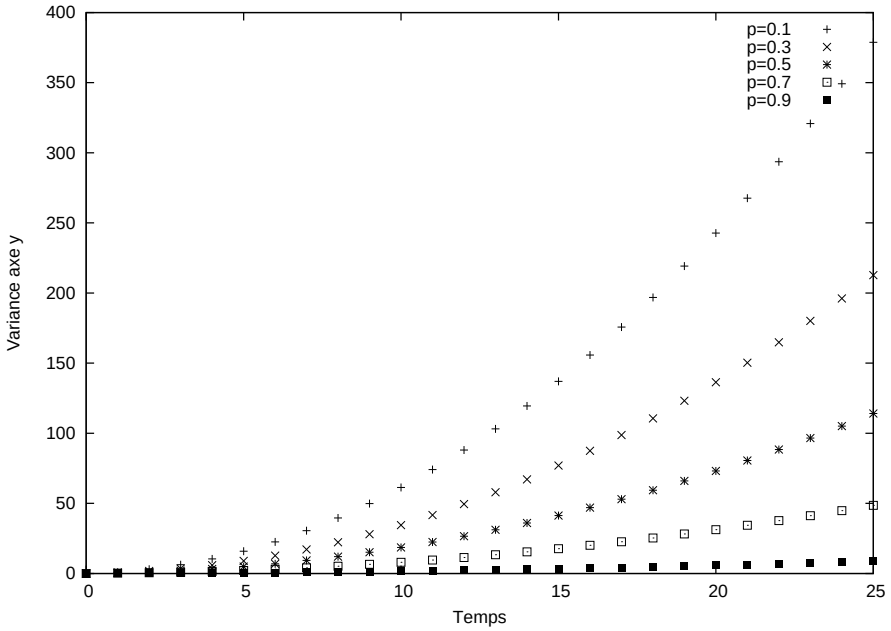


FIG. 3.11 – Variance σ^2_{yy} en fonction du temps de la marche quantique sur $\mathbb{Z}^2$ avec espace interne de dimension 2, sur l'axe y ($\sigma^2_{yy} = \langle Y^2 \rangle - \langle Y \rangle^2$). Paramètre $p = \cos u = \cos v$

3.4 La symétrie

Une marche (ou opérateur évolution W) est symétrique par rapport a une transformation R si

$$W = R^{-1}WR \tag{3.73}$$

Supposons un état initial et son état final après t pas de temps, la condition de symétrie est équivalente à considérer qu'une modification avec R de l'état initial donne un état final qui est obtenu du précédent par la même modification

$$|\psi_t\rangle = W^t|\psi_0\rangle = R^{-1}W^tR|\psi_0\rangle \tag{3.74}$$

Dans le cas des graphes de Cayley les symétries auxquelles nous nous intéresserons seront celles qui correspondent à des permutations des générateurs. Supposons alors que S est l'opérateur sur l'espace décrivant le graphe et qui fait une permutation des vertex suivant la symétrie cherchée. L'opérateur complet sera donc de la forme

$$R = A \otimes S \tag{3.75}$$

où A est une matrice quelconque de l'espace interne. Si S est unitaire, comme l'opérateur complet R est unitaire on aura que A est une matrice unitaire aussi. Supposons que l'opérateur déplacement suivant le générateur δ se transforme en $T_{S(\delta)} = S^{-1}T_\delta S$ alors l'équation (3.73) devient un ensemble d'équations entre matrices de l'espace interne $\mathcal{H}_I$

$$M_{S(\delta)} = A^{-1}M_\delta A \quad \forall\delta \in \Delta \tag{3.76}$$

3.4.1 Marche quantique unidimensionnelle

Supposons S_x l'opérateur de réflexion tel que

$$S_x|x\rangle = |-x\rangle \tag{3.77}$$

alors nous avons

$$S_x^{-1}T_{\pm x}S_x = T_{\mp x} \tag{3.78}$$

et les équations (3.76) sont

$$A^{-1}M_+A = M_- \tag{3.79}$$
$$A^{-1}M_-A = M_+ \tag{3.80}$$

Si on suppose la solution de la forme des groupes libres, a savoir $M_\pm = UP_\pm$ avec U une matrice unitaire 2×2 et P_+ et P_- deux projecteurs orthogonaux on obtient

$$UP_+A = AUP_- \tag{3.81}$$
$$UP_-A = AUP_+ \tag{3.82}$$

Pour simplicité on va d'abord résoudre ces équations dans une base ou les projecteurs sont diagonaux. Ceci est équivalent a supposer qu'on obtient ces projecteurs par une transformation unitaire sur les projecteurs P_1 et P_2 diagonaux sur la base standard

$$P_+ = VP_1V^\dagger \tag{3.83}$$
$$P_- = VP_2V^\dagger \tag{3.84}$$

avec V une matrice unitaire 2×2. Si on définit $\tilde{U} = VUV^\dagger$ et $\tilde{A} = VAV^\dagger$ les équations (3.81)-(3.82) deviennent

$$\tilde{U}P_1\tilde{A} = \tilde{A}\tilde{U}P_2 \tag{3.85}$$
$$\tilde{U}P_2\tilde{A} = \tilde{A}\tilde{U}P_1 \tag{3.86}$$

qui ont comme solution

$$\tilde{U} = \begin{pmatrix} \cos\frac{\theta}{2} & e^{i\alpha}\sin\frac{\theta}{2} \\ -e^{-i\alpha}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \quad \tilde{A} = \begin{pmatrix} 0 & -e^{i2\alpha} \\ 1 & 0 \end{pmatrix} \tag{3.87}$$

En combinant tous les résultats on obtient que la solution générale de (3.73) avec les matrices internes de la forme de la solution des groupes libres et V défini par (3.83)-(3.84) est $A = V\tilde{A}V^\dagger$ et $U = V\tilde{U}V^\dagger$ où $\tilde{A}$ et $\tilde{U}$ sont donnés par l' équation (3.87).

3.4.2 Marche quantique bidimensionnelle

On va suivre exactement le même raisonnement que pour la marche unidimensionnelle. On a choisi ici deux types de symétries qui peuvent générer les autres symétries de $\mathbb{Z}^2$ par combinaison, l'une est S_1 la réflexion sur un des axes (on choisit ici x) et l'autre S_2 est la rotation d'un angle $\frac{\pi}{2}$. Plus précisément sur un vecteur quelconque de la base

$$S_1|x,y\rangle = |-x,y\rangle \tag{3.88}$$
$$S_2|x,y\rangle = |y,-x\rangle \tag{3.89}$$

On obtient donc que les opérateurs déplacement se transforment

$$S_1^{-1}T_{\pm x}S_1 = T_{\mp x} \qquad S_1^{-1}T_{\pm y}S_1 = T_{\pm y} \tag{3.90}$$
$$S_2^{-1}T_{\pm x}S_2 = T_{\pm y} \qquad S_2^{-1}T_{\pm y}S_2 = T_{\pm x} \tag{3.91}$$

ce qui donne une série d'équations équivalentes à (3.76)

$$A_1^{-1}M_{\pm x}A_1 = M_{\mp x} \qquad A_1^{-1}M_{\pm y}A_1 = M_{\mp y} \tag{3.92}$$
$$A_2^{-1}M_{\pm x}A_2 = M_{\mp y} \qquad A_2^{-1}M_{\pm y}A_2 = M_{\mp x} \tag{3.93}$$

Espace interne de dimension 2

On obtient qu'il n'y a pas de matrices internes $M_{\pm x}$ et $M_{\pm y}$ vérifiant ces deux symétries.

Espace interne de dimension 4

On a aussi que si on suppose les matrices internes de la forme de la solution des groupes libres avec $\dim(\mathcal{H}_I) = 4$

$$M_{\pm x} = P_{\pm x}U \quad M_{\pm y} = P_{\pm y}U \tag{3.94}$$

avec U une matrice unitaire 4×4 et $\{P_{+x}, P_{-x}, P_{+y}, P_{-y}\}$ une famille de projecteurs orthogonaux

$$P_{+x} = VP_1V^\dagger \qquad P_{+x} = VP_2V^\dagger \tag{3.95}$$
$$P_{+y} = VP_3V^\dagger \qquad P_{-y} = VP_4V^\dagger \tag{3.96}$$

où $\{P_i\}$ est une famille de projecteurs orthogonaux sur les sous espaces engendrés par chacun des vecteurs de la base de $\mathcal{H}_I$ on obtient comme solution aux équations de symétrie

$$A_i = V\tilde{A}_iV^\dagger \qquad U = V\tilde{U}V^\dagger \tag{3.97}$$

avec

$$\tilde{A}_1 = \phi_3 \begin{pmatrix} 0 & \lambda^{\frac{1}{2}} & 0 & 0 \\ \lambda^{-\frac{-1}{2}} & 0 & 0 & 0 \\ 0 & 0 & 10 & \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \tilde{A}_2 = \begin{pmatrix} 0 & 0 & \varphi_1 & 0 \\ 0 & 0 & 0 & \varphi_2 \\ 0 & \varphi_3 & 0 & 0 \\ \varphi_4 & 0 & 0 & 0 \end{pmatrix} \tag{3.98}$$

où $\phi_3, \varphi_1, \ldots, \varphi_4 \in \mathbb{C}$ de norme 1 et $\lambda = \frac{\varphi_1\varphi_3}{\varphi_2\varphi_4}$, avec

$$\tilde{U} = D_1XD_2 \qquad X = \begin{pmatrix} d & e & x & x \\ e & d & x & x \\ x & x & d & e \\ x & x & e & d \end{pmatrix} \tag{3.99}$$

où D_1 et D_2 sont des matrices diagonales dont les éléments de la diagonale sont

$$(D_1)_{1,1} = \varphi_1\varphi_3 \qquad (D_1)_{2,2} = (\varphi_1\varphi_3\varphi_2\varphi_4)^{\frac{1}{2}}$$
$$(D_1)_{3,3} = \varphi_3(\varphi_1\varphi_2\varphi_3\varphi_4)^{\frac{1}{4}} \qquad (D_1)_{4,4} = \varphi_2^{\frac{-1}{2}}(\varphi_1\varphi_3\varphi_4)^{\frac{1}{2}}(\varphi_1\varphi_2\varphi_3\varphi_4)^{\frac{1}{4}}$$

$$(D_2)_{1,1} = (\varphi_1\varphi_3)^{\frac{-1}{2}}(\varphi_2\varphi_4)^{\frac{1}{2}}(\varphi_1\varphi_2\varphi_3\varphi_4)^{\frac{-1}{4}} \qquad (D_2)_{2,2} = (\varphi_1\varphi_2\varphi_3\varphi_4)^{\frac{-1}{4}}$$
$$(D_2)_{3,3} = \varphi_3^{-1} \qquad (D_2)_{4,4} = (\varphi_1\varphi_3\varphi_2\varphi_4)^{\frac{-1}{2}}\varphi_2^{\frac{1}{2}}$$

et les variables sont de la forme

$$d = (\varphi_1\varphi_2\varphi_3\varphi_4)^{\frac{-1}{4}}(e^{i\theta_u} + r_ve^{i\theta_v}) \tag{3.100}$$
$$e = r_ve^{i\theta_v} \tag{3.101}$$
$$x = i\sqrt{-\cos(-r_v\theta_u + \theta_v) - r_v^2}\left(\frac{e^{i\theta_u} + 2r_ve^{i\theta_v}}{e^{-i\theta_u} + 2r_ve^{-i\theta_v}}\right)^{\frac{1}{2}} \tag{3.102}$$

ou $0 \leq r_v \leq 1$ et $\theta_u, \theta_v \in \mathbb{R}$. On a donc que la matrice unitaire X dépend de 9 paramètres réels, ce qui réduit le nombre de paramètres possibles pour une matrice unitaire de dimension 4×4.

Conclusion

L'apport général de cette thèse peut se résumer comme une contribution à l'-effort de comprendre les caractéristiques propres aux systèmes quantiques avec des applications algorithmiques en commençant la classification des marches quantiques à temps discret et avec dimension d'espace interne variable.
Avant de commencer l'étude des marches quantiques, nous sommes proposés de résoudre un problème particulier avec un algorithme quantique. Le problème, considéré difficile, est le problème du calcul du permanent d'une matrice. Le premier résultat de cette étape a été de démontrer que une façon naturelle d'essayer de construire l'algorithme fait appel à un opérateur non unitaire. Le deuxième résultat a été de construire un algorithme pour résoudre le problème du permanent en utilisant un algorithme existant appelé "estimation d'amplitude". Pourtant l'algorithme résultant a un temps qui n'est pas intéressant du point de vue algorithmique. Cette procédure se trouvait indiquée dans le livre de Nielsen, notre apport a été de construire explicitement l'opérateur "oracle" correspondants à l'algorithme qui calcule le permanent d'une matrice.
Dans un deuxième temps nous avons décidé donc d'étudier les marches quantiques dans le but de les classifier et de trouver des effets différents des marches classiques qui pourraient être utilisés pour construire des algorithmes performants. La nécessité d'un espace interne est une caractéristique importante des marches à temps discret, la marche à temps continu en opposition peut être définie sans espace interne. La dimension de cet espace a été démontré avoir des conséquences sur la performance de l'algorithme de recherche, basé sur une marche quantique discrète. Dans ce domaine nous avons commencé par élargir la définition existante en la rapprochant de la définition des automates cellulaires quantiques ou en particulier la forme de l'opérateur interne n'est pas fixe et la dimension de l'espace correspondant est variable. Nous avons étudié sous quelles conditions ces modèles existent et dans le cas particulier des graphes de Cayley nous avons récrit ces conditions en utilisant les relations entre éléments du groupe. Grâce à ce type de relation il a été possible de commencer une classification de telles marches pour les groupes les plus simples à savoir les groupes libres et les groupes libres abéliens. Dans le premier cas nous avons démontré que la solution générale correspond à la forme des marches standard si on considère le cas avec espace interne de dimension minimale. Dans le second cas, les groupes libres abéliens, nous avons trouvé des marches avec un espace interne plus petit que ce que est permis avec la solution standard. Quelques exemples intéressants ont été aussi indiques, une marche scalaire et une marche sur l'hypercube où les matrices de l'espace interne sont en lien avec des générateurs de l'algèbre de Clifford.
Deux théorèmes ont pu être élargis pour inclure les marches ici définies. Le théorème

sur les marches scalaires sur réseaux simples (Théorème "No-go") a été reformulé pour un graphe de Cayley. De même nous avons indiqué comment la limite faible des marches sur réseaux simples avec un opérateur de la forme des marches standard peut se modifier pour contenir les marches, sur les mêmes réseaux mais avec un opérateur évolution plus général. Ce résultat indique que les nouvelles marches ne devraient pas avoir des moments exponentiellement différents que si les valeurs propres de l'opérateur évolution sont dégénérées.
Finalement nous avons étudié quelques propriétés des marches, le temps d'arrivée de l'hypercube, la variance et la symétrie des marches sur un réseau simple de dimension un et deux. Nous avons calculé leur fonction d'onde et utilisé ces résultats pour calculer numériquement les grandeurs auxquelles nous nous sommes intéressés. Les résultats indiquent que ces paramètres sont de bonnes quantités qui permettraient classifier des marches dans une définition plus générale comme celle qu'on a proposé dans cette thèse.
Le travail de classification peut donc se continuer utilisant comme paramètres les moments, les symétries de la marche et la dégénérescence des valeurs propres de l'opérateur évolution. Cette dernière semble une ligne de travail importante car des effets comme la localisation de la marche ont déjà été signales comme conséquences de cette dégénérescence. Il est aussi important de continuer à généraliser les résultats déjà existants pour les marches standard comme celui du temps de mixage des graphes réguliers. Il est important de signaler aussi que la plupart des résultats des marches standard correspondent a des graphes de Cayley des groupes abéliens, comme par exemple le théorème de limite faible. Il nous parait donc important de continuer aussi dans la recherche des propriétés de graphes correspondants a des groupes non abéliens.

Bibliographie

[1] http ://www.complexityzoo.com.

[2] http ://claymath.org/millenium/$P_v s_N P$.

[3] D. S. Abrams and S. Lloyd. Nonlinear quantum mechanics implies polynomial time solution for $np-$complete and $\#p$ problems. *Phys. Rev. Lett.*, 81 :3992–3995, 1998. quant-ph/9801041.

[4] O. Lopez Acevedo and T. Gobron. Quantum walks on cayley graphs. *J. Phys. A : Math. Gen*, 39, 2006. quant-ph/0503078.

[5] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. In *Proc. 33th STOC*, New York, NY, 2001. ACM. quant-ph/0012090.

[6] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. LANL preprint. quant-ph/0405098.

[7] A. Ambainis. Quantum walk algorithm for element distinctness. In *Proc. FOCS*, 2004.

[8] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous. One-dimensional quantum walks. In *Proc. Conf. Ann. Symp. Theo. Comp.*, pages 37–49. ACM, 2001.

[9] M. C. Banuls, R. Orus, J. I. Latorre, A. Perez, and P. Ruiz-Femenia. Simulation of many qubit quantum computation with matrix product states. LANL preprint. quant-ph/0503174.

[10] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.*, 26(5) :1411–1473, 1997.

[11] I. Bialynicki-Birula. Weyl dirac and maxwell on a lattice as unitary cellular automata. *Phys. Rev. D*, 49(12) :6920, 1994.

[12] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. LANL preprint. quant-ph/0005055.

[13] T. A. Brun, H. A. Cartet, and A. Ambainis. Quantum walks driven by many coins. *Physical Review A*, 67 :052317, 2003. quant-ph/0210161.

[14] I. Carneiro, M. Loo, X. Xu, M. Girard, V. Kendon, and P. L. Kinght. Entanglement in coined quantum walks on regular graphs. *New J. Phys.*, 7 :156, 2005.

[15] A. Chen and E. Renshaw. The general correlated random walk. *J. Appl. Prob.*, 31 :869–884, 1994.

[16] A. Y. Chen and E. Renshaw. The gillis-domb-fisher correlated random walk. *J. Appl. Prob.*, 29 :792–813, 1992.

[17] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. R. Soc Lond. A*, 400 :97, 1985.

[18] D. Deutsch. Quantum computational networks. *Proc. R. Soc. Lond. A*, 425 :97, 1989.

[19] E. Fahri, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda. A quantum adiabatic evolution algorithm applied to random instances of an np-complete problem. LANL preprint. quant-ph/0104129.

[20] G. Grimmet, S. Janson, and P. F. Scudo. Weak limits for quantum random walks. *Phys. Rev. E*, 69 :0261119, 2004.

[21] N. Inui, N. Konno, and E. Segawa. One-dimensional three-state quantum walk. LANL preprint. quant-ph/0507207.

[22] M. Jerrum, A. Sinclair, and E. Vigoda. A polynomial time approximation algorithm for the permanent of a matrix with non-negative entries. In *Proc. 33th STOC*, New York, NY, 2001. ACM.

[23] J. Kempe. Discrete quantum walk hit exponentially faster. In *Random-Approx 2003 series Lecture notes in Computer Science*, pages 354–369, Heidelberg, 2003. Springer. quant-ph/0205083.

[24] J. Kempe. Quantum random walks - an introductory overview. *Cont. Phys.*, 44(4) :302–307, 2003. quant-ph/0303081.

[25] M. Keyl. Fundamentals of quantum information theory. *Phys. Rep.*, 369(Issue 5), 2002. quant-ph/0202122.

[26] P. L. Knight, E. Roldan, and J. E. Sipe. Propagating quantum walks : the origin of interference structures. LANL preprint. quant-ph/0312133.

[27] N. Koblitz. *A course in number theory and cryptography.* Springer, 1994.

[28] N. Konno. A new type of limit theorems for the one-dimensional quantum random walk. LANL preprint. quant-ph/0206103.

[29] D. A. Meyer. On the absence of homogeneous scalar unitary cellular automata. *Phys. Lett. A*, 223 :5–5261, 1996.

[30] D. A. Meyer. Quantum mechanics of lattice gas automata : One particle plane waves and potentials. *Phys. Rev. E*, 55(5) :5261, 1997.

[31] D. R. Mitchell. Geometric phase based quantum computation applied to an np-complete problem. LANL preprint. quant-ph/0508177.

[32] D. R. Mitchell, C. Adami, W. Lue, and C. P. Williams. A random matrix model of adiabatic quantum computing. LANL preprint. quant-ph/0409088.

[33] C. Moore and A. Russell. Quantum walks on the hypercube. In *Proc. Random*, 2001.

[34] A. Nayak and A. Vishwanath. Quantum walk on the line (extended abstract). LANL preprint. quant-ph/0010117.

[35] M. A. Nielsen and I.L Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2004.

[36] Christos H. Papadimitriou. *Computational complexity*. Addison Wesley, 1994.

[37] P. Ribeiro, P. Milman, and R. Mosseri. Aperiodic quantum random walks. *Phys. Rev. Lett.*, 93(19) :190503, 2004.

[38] N. Shenvi, J. Kempe, and K. BirgittaWhaley. Quantum random walk search algorithm. *Phys. Rev. A*, 67 :052307, 2003.

[39] P. W. Shor. Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, pages 1484–1509, 1997.

[40] P. W. Shor. Progress in quantum algorithms. *Quantum Information Processing*, 3, 2004. http ://www-math.mit.edu/ shor/elecpubs.html.

[41] A. M. Turing. On computable numbers with an application to the entscheidungsproblem. *Proc. Lond. Math. Soc.2*, 442, 1936.

[42] A.T. White. *Graphs of groups on surfaces*. Elsevier, 2001.

[43] A. C. Yao. Quantum circuit complexity. *Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Scicence*, pages 352–361, 1993.

Annexe A

Quantum walks on Cayley graphs

Quantum walks on Cayley graphs

O Lopez Acevedo†‡and T Gobron†

†Laboratoire de Physique Théorique et Modélisation, Université de Cergy-Pontoise, 2 Avenue Adolphe Chauvin 95302 Cergy Pontoise Cedex, France
‡Institut für Mathematik und Informatik, Ernst-Moritz-Arndt-Universität, Friedrich-Ludwig-Jahn Str. 15a, 17487 Greifswald, Germany

E-mail: `lopez@ptm.u-cergy.fr`

Abstract. We address the problem of the construction of quantum walks on Cayley graphs. Our main motivation is the relationship between quantum algorithms and quantum walks. In particular, we discuss the choice of the dimension of the local Hilbert space and consider various classes of graphs on which the structure of quantum walks may differ. We completely characterise quantum walks on free groups and present partial results on more general cases. Some examples are given including a family of quantum walks on the hypercube involving a Clifford Algebra.

PACS number: 03.67.Lx

1. Introduction

Recently many effort has been devoted to the construction of new quantum algorithms. In particular a question which has arisen is whether the known algorithms fully exploit the possibilities of quantum mechanics, or if there could exist more efficient ones. A search for new ideas in this direction has been at the origin of a renewed study of quantum walks models [1], and a few results have already been obtained, showing that these are definitely relevant in this context.

The first general characterisation of walks over graphs was presented in [2]. A possible construction for a walk operator is given, based on its classical equivalent, and some quantities relevant in the context of quantum algorithms are defined and computed. One of the principal results states that for bounded degree graphs the mixing time (defined also in the same work) is at most quadratically faster than the mixing time of the simple classical random walk on the same graph. Even if this general result is not so encouraging, some particular graphs have been shown to have properties intrinsically different from their classical equivalents. In particular, a symmetric quantum walk may get across an hypercube in a time linear with the dimension, while its classical counterpart would take an exponentially larger time.

In algorithmic applications, quantum walks have also shown interesting properties. The first important achievement has been the setting of the quantum search algorithm in the form of a quantum walk over an hypercube [3]. Some other similar quantum search algorithms were constructed after this. In one of them [4], the choice of the coin operator was revealed to be of crucial importance, since different operators may achieve different speed-ups (or no speed-up at all) without obvious reasons. A natural question which arises from this problem is whether there exist quantum walks different to than those defined in [2] and if so, to what extent they could be the source of interesting new properties and algorithmic applications. Another problem lies in the dimension of the internal space: it is always possible to enlarge it, and in [5], it was shown that in an extremal case, the variance of the one dimensional walk recovers the classical behaviour. In a similar direction in [6] and [7] the authors have considered the evolution of a quantum particle governed by a quantum multi-baker map which can be settled as a quantum walk on a line with a multidimensional internal space, the classical limit is also recovereded enlarging the dimension of the internal space. At the opposite, an interesting and still open question is whether there exist quantum walks with local spaces of dimension smaller than that taken in the standard definition. In the context of quantum cellular automata, it is shown in [8] that for the simple lattice in d dimensions there is no nontrivial walk with an internal space of dimension one, also known as the No-go theorem.

In this article we make a step in the direction of determining all possible quantum walks for general graphs and characterising their structures. Starting from a general definition of a quantum walk we deduce necessary and sufficient conditions on the coin operators for the evolution to be unitary (section 2). The next section contains a discussion on

1. Introduction

Recently many effort has been devoted to the construction of new quantum algorithms. In particular a question which has arisen is whether the known algorithms fully exploit the possibilities of quantum mechanics, or if there could exist more efficient ones. A search for new ideas in this direction has been at the origin of a renewed study of quantum walks models [1], and a few results have already been obtained, showing that these are definitely relevant in this context.

The first general characterisation of walks over graphs was presented in [2]. A possible construction for a walk operator is given, based on its classical equivalent, and some quantities relevant in the context of quantum algorithms are defined and computed. One of the principal results states that for bounded degree graphs the mixing time (defined also in the same work) is at most quadratically faster than the mixing time of the simple classical random walk on the same graph. Even if this general result is not so encouraging, some particular graphs have been shown to have properties intrinsically different from their classical equivalents. In particular, a symmetric quantum walk may get across an hypercube in a time linear with the dimension, while its classical counterpart would take an exponentially larger time.

In algorithmic applications, quantum walks have also shown interesting properties. The first important achievement has been the setting of the quantum search algorithm in the form of a quantum walk over an hypercube [3]. Some other similar quantum search algorithms were constructed after this. In one of them [4], the choice of the coin operator was revealed to be of crucial importance, since different operators may achieve different speed-ups (or no speed-up at all) without obvious reasons. A natural question which arises from this problem is whether there exist quantum walks different to than those defined in [2] and if so, to what extent they could be the source of interesting new properties and algorithmic applications. Another problem lies in the dimension of the internal space: it is always possible to enlarge it, and in [5], it was shown that in an extremal case, the variance of the one dimensional walk recovers the classical behaviour. In a similar direction in [6] and [7] the authors have considered the evolution of a quantum particle governed by a quantum multi-baker map which can be settled as a quantum walk on a line with a multidimensional internal space, the classical limit is also recovereded enlarging the dimension of the internal space. At the opposite, an interesting and still open question is whether there exist quantum walks with local spaces of dimension smaller than that taken in the standard definition. In the context of quantum cellular automata, it is shown in [8] that for the simple lattice in d dimensions there is no nontrivial walk with an internal space of dimension one, also known as the No-go theorem.

In this article we make a step in the direction of determining all possible quantum walks for general graphs and characterising their structures. Starting from a general definition of a quantum walk we deduce necessary and sufficient conditions on the coin operators for the evolution to be unitary (section 2). The next section contains a discussion on

the solutions of these equations (section 3). In particular, we characterise all possible walks on the Cayley graph of a free group. In the case of abelian groups, the situation is somewhat more complicated, and after a general discussion we present particular solutions. We construct quantum walks over the two dimensional and three dimensional simple lattice with an internal space of dimension smaller than what was previously known and a generalisation to arbitrary dimensions. We also consider the hypercube as a Cayley graph on which we construct a quantum walk where the coin operators are related to elements of the Clifford algebra. Finally, we propose a possible generalisation of a quantum walk where we depart from the image of a particle moving on a lattice and which could be of interest in the context of quantum algorithms (section 4).

2. Model and unitary relations

A quantum algorithm is a sequence of transformations on a state of a quantum system. The quantum system is described by a tensor product of two dimensional complex Hilbert spaces. There is a preferred basis of the elementary space where vectors are labelled with the integers zero and one in correspondence to classical bits. Then a basis vector of the entire system is $|x_0\rangle \otimes \ldots \otimes |x_n\rangle$ where $x_i \in \{0, 1\}$ and in this way it is possible to associate to each base vector an integer whose binary decomposition coincides with the n-tuple $(x_0, \ldots, x_n)$. The total operator is the product of elementary operators. A presentation of possible sets as well as a demonstration of the universality of these sets may be found in [9].
A quantum walk is a model for the evolution of a particle over a graph. Many of the choices made in building the model may be explained by the aim of studying them as quantum algorithms. Let G be a directed graph with vertex set X and edge set E such that $G = (X, E)$. Let $\mathcal{H}$ be the Hilbert space defined by $\mathcal{H} = \mathcal{H}_I \otimes \mathcal{H}_G$. The space $\mathcal{H}_G = \ell^2(X)$ describes the position of the particle over the graph and the space $\mathcal{H}_I = \mathbb{C}^d$ describes some internal degrees of the particle.Let $\{|x\rangle\}_{x\in X}$ be a base of H_G and $\{|1\rangle, \ldots, |d\rangle\}$ a base of $\mathcal{H}_I$.
The evolution equation is:

$$|\psi_{t+1}\rangle = W|\psi_t\rangle \tag{1}$$

where W is a discrete time evolution operator defined as

$$W = \sum_{x\in X} \sum_{z\in E_x} M_{x,z} \otimes T_{x\to z} \tag{2}$$

where E_x denotes the set of neighbouring sites of x and $T_{x\to z}$ translates the particle from x to z. $T_{x\to z}$ is defined by

$$\langle x'|T_{x\to z}|\psi\rangle = \langle x'|z\rangle\langle x|\psi\rangle \tag{3}$$

$M_{x,z} : H_I \to H_I$ are maps modifying the internal space at the same time as the translation from vertex x to vertex z is applied. Suppose $|\psi_t\rangle = |i\rangle \otimes |z\rangle$. Then after

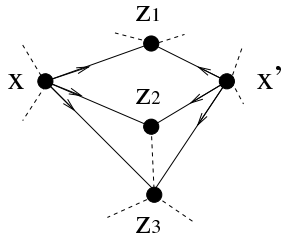


Figure 1. A pair of second neighbours and all paths of length two between them

one time step the probability of finding the particle in at vertex y, a neighbour of z, will depend on the previous internal state:

$$P(y) = \sum_{j=1}^{d} |\langle j|M_{z,y}|i\rangle|^2 \tag{4}$$

One image commonly used to describe the local evolution is that of a coin attached to each vertex and flipped to decide which neighbour the particle will jump to (see for instance [2]) and accordingly the local map $M_{x,y}$ is termed the "coin operator". Here we follow this usage though our model is more general than the image: in fact, it is important to note that originally the internal state was identified to the set of possible outcomes of the coin flip, or equivalently to the set of neighbours, so that the dimension of the internal space at a given vertex was necessarily equal to the number of outgoing edges. Here we have not considered this identification.
Unitarity of W is satisfied if and only if:

$$W^\dagger W = \mathbb{1} \Leftrightarrow \sum_{z \in E_x \cap E_{x'}} M^\dagger_{x,z} M_{x',z} = \delta_{x,x'} \mathbb{1}_{H_I} \tag{5}$$

$$WW^\dagger = \mathbb{1} \Leftrightarrow \sum_{z \in E_x \cap E_{x'}} M_{z,x} M^\dagger_{z,x'} = \delta_{x,x'} \mathbb{1}_{H_I} \tag{6}$$

$\forall x, x'$. When $x \neq x'$, in order to have a non trivial equation, x and x' must be second neighbours and the number of terms in the sum is related to the number of closed paths of length 4 with alternating orientation.
In the example on the figure 1, one condition equation of the form (5) with three terms is associated with the pair of second neighbours x and x' :

$$M^\dagger_{x,z_1} M_{x',z_1} + M^\dagger_{x,z_2} M_{x',z_2} + M^\dagger_{x,z_3} M_{x',z_3} = 0 \tag{7}$$

3. Quantum walks on Cayley Graphs

We will restrict our study from now on to quantum walks on Cayley graphs. We first recall their definitions and main properties. We follow the presentation given in [10]. Given a group Γ one considers a set Δ of elements in Γ such that Δ is a generating set for Γ. The Cayley graph $C_\Delta(\Gamma) = (X, E)$ is defined as the oriented graph with

$$X \equiv X(C_\Delta(\Gamma)) = \Gamma \tag{8}$$

$$E \equiv E(C_\Delta(\Gamma)) = \{(x, x\delta)_\delta | x \in \Gamma, \delta \in \Delta\} \tag{9}$$

When associating a colour to each element of the generating family, the definition of $C_\Delta(\Gamma)$ makes it a coloured directed graph. In addition a Cayley colour graph is vertex transitive, so that each site is equivalent. Thus we consider internal operators which depend only on the edge colour and direction of the edge (x, y) (i.e. only on the generator $\delta = x^{-1}y$) and not on the starting vertex x:

$$M_{x,y} = M_{x^{-1}y} \text{ for all } (x, y) \in E \tag{10}$$

Thus the evolution operator W on $\mathcal{H}$ is

$$W = \sum_{\delta \in \Delta} M_\delta \otimes T_\delta \tag{11}$$

where T_δ is the shift in the direction δ and is defined for all vertices by the group operation

$$T_\delta = \sum_{x \in X} T_{x \to x\delta} \tag{12}$$

The problem is thus reduced to a local one on $\mathcal{H}_I$ and the unitarity conditions (5) and (6) now read:

$$\sum_{\delta_1 \delta_2^{-1} = u} M_{\delta_1}^\dagger M_{\delta_2} = \delta_{\{u=e\}} \mathbb{1} \tag{13}$$

$$\sum_{\delta_1 \delta_2^{-1} = u} M_{\delta_1} M_{\delta_2}^\dagger = \delta_{\{u=e\}} \mathbb{1} \tag{14}$$

where both sums run over all pairs of elements in Δ, u is any element in the set

$$\Delta_2 = \{\delta \delta'^{-1}; \delta, \delta' \in \Delta\} \tag{15}$$

and e is the neutral element in Γ. The number of equations is twice the cardinality of $|\Delta_2|$ and the number of terms in at least some of these equations will be larger than one as soon as there exists closed paths of length 4 on the graph with an alternating orientation, which in terms of the generators is

$$\delta_1 \delta_2^{-1} \delta_4 \delta_3^{-1} = e \tag{16}$$

Because of this relation it will be sometimes useful to define the group Γ itself in terms of the "free presentation"

$$\Gamma = \langle \Delta' | R \rangle \tag{17}$$

where Δ' is a set of generators of a free group and R is the set (which may also be empty) of relations between the elements of Δ' and their inverses which defines the structure of the group. To define the Cayley graph (8) and (9) in the following we will use the generating set Δ defined by

$$\Delta = \{\gamma : \gamma \in \Delta' \vee \gamma^{-1} \in \Delta'\} \tag{18}$$

where Δ' is the generating set used in the free presentation of the group. In particular Δ may contain at the same time a generator and its inverse.
We now list some generic cases of Cayley groups.

3.1. Cayley graphs of free groups

As its name suggests, a free group is a group generated with a (finite) number of generators with no relations between them

$$\Gamma = \langle \Delta' | - \rangle \tag{19}$$

Lets consider the Cayley graph $C_\Delta(\Gamma)$ of the precedent group defined by (8), (9) and (18). The two sets of equations (13) and (14) can be written as:

$$M_{\delta_1}^\dagger M_{\delta_2} \quad = M_{\delta_1} M_{\delta_2}^\dagger = 0 \text{ for all } \delta_1 \neq \delta_2 \tag{20}$$

$$\sum_{\delta\in\Delta} M_\delta M_\delta^\dagger = \sum_{\delta\in\Delta} M_\delta^\dagger M_\delta = \mathbb{1} \tag{21}$$

Theorem 1 *On the Cayley graph of the free group (19), defined by (8), (9) and (18), the quantum walk evolution operator (2) is unitary if and only if the internal operators are of the form,*

$$M_\delta = U\, P_\delta \tag{22}$$

where U is a unitary matrix of dimension $dim(\mathcal{H}_I)$ and $\{P_\delta\}_{\delta\in\Delta}$ is a complete family of orthogonal projectors,

$$\sum_{\delta\in\Delta} P_\delta = \mathbb{1} \tag{23}$$

The internal space is of dimension larger or equal to $|\Delta|$.

Proof: First, it is easy to see that (22) is a solution for (20)-(21). Now suppose (20)-(21), these equations imply the following relation between the images of the maps

$$\mathcal{H}_I = \oplus_{\delta\in\Delta} \mathcal{I}m(M_\delta) \tag{24}$$

$$\mathcal{H}_I = \oplus_{\delta\in\Delta} \mathcal{I}m(M_\delta^\dagger) \tag{25}$$

The fact that a direct sum appears in the right hand sides of (24)-(25) is just a consequence of equations (20) which make all subspaces pairwise orthogonal. The equality (rather than an inclusion) is due to (21). Define $U \equiv \sum_\delta M_\delta$, an unitary matrix by (20)-(21), and P_δ as the orthogonal projector on $\mathcal{I}m(M_\delta^\dagger)$, (22) follows by considering the elements of a vector basis compatible with the decomposition (25) . The claim that (22) is the general solution is thus proven. □

One should note however that the right hand side of (22) could be written in many other ways, for instance with its factors written in the opposite order (which makes P_δ the projector on $Im(M_\delta)$). When the rank of all matrices M_δ is fixed to 1, the dimension on the local Hilbert space takes its minimal value $dim(\mathcal{H}_I) = |\Delta|$, and if a symmetric presentation for the group is chosen (i.e: $\delta \in \Delta$ implies $\delta^{-1} \in \Delta$), the standard definition of quantum "coin" solution [2] is recovered. Besides these solutions, the only other possibility in the case of free groups consists in taking matrices M_δ of rank different from one and possibly varying with δ.

The case when the generating set that defines the Cayley graph contains the group

identity e and at the same time some generators and their inverses is slightly more involved because the group identity e commutes with all the elements in the group. If both a generator δ and his inverse δ^{-1} are in Δ in addition to equations (20) one has

$$M_\delta^\dagger M_e + M_e^\dagger M_{\delta^{-1}} = 0 \tag{26}$$
$$M_e M_\delta^\dagger + M_{\delta^{-1}} M_e^\dagger = 0 \tag{27}$$

for all $\delta \neq e$. Summing all equations in (26), one gets $M_e^\dagger S = -S^\dagger M_e$ where $S = \sum_\delta M_\delta$. Adding again two instances of equations (26) for both a given δ and its inverse δ^{-1} gives

$$(M_e^\dagger S)(P_\delta + P_{\delta^{-1}}) = (P_\delta + P_{\delta^{-1}})(M_e^\dagger S) \tag{28}$$

for all $\delta \neq e$. Thus $M_e^\dagger S$ is block diagonal in the representation where all the orthogonal projectors P_δ's are simultaneously diagonal. The problem can essentially be reduced to the one dimensional case which we explore below. This is the first instance of a solution to equations (26) and (27) different to the solution (22), in the case when there is more than one non-zero term.

3.1.1. One dimensional walks The simplest example is a quantum walk in one dimension. Lets consider the group generated by one element $\Gamma =< \delta | - >$ and the Cayley graph obtained (8)-(9) using Γ and the set $\Delta = \{\delta, \delta^{-1}\}$. The minimal dimension of the internal space is 2 by the preceeding theorem and the form of the solution follows equation (22). The evolution operator defined in (11) reads in this case

$$W = (U \otimes Id)(P_\delta \otimes T_\delta + P_{\delta^{-1}} \otimes T_{\delta^{-1}}) \tag{29}$$

where U is a 2×2 unitary matrix. Two quantum walk evolution operators W and W' differing by an unitary transformation V would be equivalent, since this amounts to a change of basis for the initial and final state. We will suppose V of the form of a tensor product $A \otimes \mathbb{1}$. Thus equation (29) defines a family of inequivalent quantum walks indexed by 4 real parameters: the 4 parameters associated with the unitary matrix U while the projectors $P_\delta, P_{\delta^{-1}}$ become the projectors over the spaces spanned by each one of the basis vectors.

A quantum walk can also be left-right symmetric if it is invariant, up to an unitary transformation $S \otimes \mathbb{1}$, under the transformation $T_\delta \leftrightarrow T_{\delta^{-1}}$. The family of inequivalent and left-right symmetric quantum walks are of the reduced form described before with U

$$U = e^{i\delta} \begin{pmatrix} \cos\frac{\theta}{2} & e^{i\alpha}\sin\frac{\theta}{2} \\ -e^{-i\alpha}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{30}$$

This defines then a 3 parameter family of inequivalent left-right symmetric quantum walks. The unitary S depends also on the 3 parameters. When the identity appears in Δ, two kinds of solutions can be devised depending on whether the two terms appearing in (26)-(27) are separately zero or not. In the first case, one needs to add (at least) one state associated to the identity and the evolution operator becomes

$$W = (U \otimes Id)(P_\delta \otimes T_\delta + P_{\delta^{-1}} \otimes T_{\delta^{-1}} + P_e \otimes Id) \tag{31}$$

where U is a 3×3 unitary matrix, and appears just as a simple extension of the previous example. However, solutions exist with a two dimensional local Hilbert space, and in such cases the evolution operator is

$$W = (U \otimes Id)(\cos(\theta)(P_\delta \otimes T_\delta + P_{\delta^{-1}} \otimes T_{\delta^{-1}}) + \sin(\theta) R_{\frac{\pi}{2}} \otimes Id) \tag{32}$$

where U is a 2×2 unitary matrix, and $R_{\frac{\pi}{2}} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Equivalent solutions with a two dimensional local Hilbert space were presented first in [11]. In conclusion, we also note that solution (22) remains valid when adding relations between generators. Thus such solutions exist for all groups, in particular for free products of cyclic groups,

$$\Gamma = \langle \delta_1, \cdots, \delta_l | \delta_1^{q_1} = \cdots \delta_l^{q_l} = e \rangle$$

and for free Abelian groups,

$$\Gamma = \langle \delta_1, \cdots, \delta_l | \delta_i \, \delta_j \, \delta_i^{-1} \delta_j^{-1} = e \; \forall i, j \in \{1, \cdots, l\} \rangle$$

which we consider in the next section.

3.2. Cayley graphs of free Abelian groups

One should note that the commutation relations between elements from the set of generators and their inverses, for instance

$$\delta_1 \delta_2^{-1} = \delta_2^{-1} \delta_1 \tag{33}$$

do not necessarily imply the existence of a closed path on the graph with alternate orientation of the edges (16), except in the case when the inverses of the elements of Δ are themselves in Δ. The group is defined by:

$$\Gamma = \langle \delta_1, \ldots, \delta_n | \delta_i \delta_j \delta_i^{-1} \delta_j^{-1} = e \forall i, j \in \{1, \ldots, n\} \rangle \tag{34}$$

and the set used to construct the Cayley graph is

$$\Delta = \{\delta_1, \ldots, \delta_n, \delta_1^{-1}, \ldots, \delta_n^{-1}\} \tag{35}$$

In such a case, equations (13)-(14) read

$$M_{\delta_i}^\dagger M_{\delta_j} + M_{\delta_j^{-1}}^\dagger M_{\delta_i^{-1}} \quad = 0 \text{ for all } \delta_i \neq \delta_j \tag{36}$$

$$M_{\delta_i} M_{\delta_j}^\dagger + M_{\delta_j^{-1}} M_{\delta_i^{-1}}^\dagger \quad = 0 \text{ for all } \delta_i \neq \delta_j \tag{37}$$

$$\sum_{\delta \in \Delta} M_\delta M_\delta^\dagger = \sum_{\delta \in \Delta} M_\delta^\dagger M_\delta = \mathbb{1} \tag{38}$$

When $\delta_j = \delta_i^{-1}$, equations (36)-(37) contain a single term and read

$$M_{\delta_i}^\dagger M_{\delta_i^{-1}} = M_{\delta_i^{-1}} M_{\delta_i}^\dagger = 0 \tag{39}$$

These are much less restrictive conditions than (20)-(21), and we lack here the decomposition of $\mathcal{H}_I$ into orthogonal subspaces which allowed us to give a general answer

in the case of free groups. We only notice that equations (36)-(37) are equivalent to the following

$$(\sum_{\delta\in A}\lambda_\delta M_\delta^\dagger))(\sum_{\delta\in A}\lambda_\delta M_\delta^{-1})) = (\sum_{\delta\in A}\lambda_\delta M_\delta^{-1}))(\sum_{\delta\in A}\lambda_\delta M_\delta^\dagger)) = 0 \tag{40}$$

for all subset $A \in \Delta$ such that $\delta \in A \Rightarrow \delta^{-1} \notin A$ and for all families of real parameters $\{\lambda_\delta\}_{\delta\in A}$.
Equations (36)-(37) imply the following proposition which will help us classify the solutions.

Proposition 1 *Let $C_\Delta(\Gamma)$ be the Cayley graph of the free abelian group with n generators ((34)-(35)) . If a quantum walk operator (2) defined on G is unitary then the image subspaces of any two internal operators M_{δ_i} and M_{δ_j} are either orthogonal or contain a common vector subspace. The same implication is valid for the image subspace of their conjugates $M_{\delta_i}^\dagger$ and $M_{\delta_j}^\dagger$:*

$$(\mathcal{I}m(M_{\delta_i}) \cap \mathcal{I}m(M_{\delta_j}) = \{0\}) \Rightarrow \mathcal{I}m(M_{\delta_i}) \perp \mathcal{I}m(M_{\delta_j}) \tag{41}$$

$$(\mathcal{I}m(M_{\delta_i}^\dagger) \cap \mathcal{I}m(M_{\delta_j}^\dagger) = \{0\}) \Rightarrow \mathcal{I}m(M_{\delta_i}^\dagger) \perp \mathcal{I}m(M_{\delta_j}^\dagger) \tag{42}$$

Proof: Using (37) for a pair δ_i, δ_j^{-1}, one has

$$\mathcal{I}m(M_{\delta_i} M_{\delta_j^{-1}}^\dagger) = \mathcal{I}m(M_{\delta_j} M_{\delta_i^{-1}}^\dagger) \tag{43}$$

and thus

$$\mathcal{I}m(M_{\delta_i} M_{\delta_j^{-1}}^\dagger) \subset (\mathcal{I}m(M_{\delta_i}) \cap \mathcal{I}m(M_{\delta_j})) \tag{44}$$

Suppose now that $\mathcal{I}m(M_{\delta_i})$ and $\mathcal{I}m(M_{\delta_j})$ have no common vector subspace. Thus $M_{\delta_i} M_{\delta_j^{-1}}^\dagger = 0$, which can be written

$$\mathcal{I}m(M_{\delta_i}^\dagger) \perp \mathcal{I}m(M_{\delta_j^{-1}}^\dagger) \tag{45}$$

and more particularly

$$\mathcal{I}m(M_{\delta_i}^\dagger M_{\delta_j}) \perp \mathcal{I}m(M_{\delta_j^{-1}}^\dagger M_{\delta_i^{-1}}) \tag{46}$$

Since the two subspaces are equal (by (39)) and orthogonal, they are equal to the null vector space and hence we have again $M_{\delta_i}^\dagger M_{\delta_j} = 0$, and finally

$$\mathcal{I}m(M_{\delta_i}) \perp \mathcal{I}m(M_{\delta_j}) \tag{47}$$

The implication (41) is thus proven. The proof of (42) is equivalent, beginning with equation (36) instead of (37). □
We can use Proposition (1) to find solutions with an internal space dimension smaller than the number of generators in the following way. First we can write

$$\dim(\mathcal{H}_I) \geq \sup_{\delta_i,\delta_j}\{\sum_{\epsilon_1,\epsilon_2=\pm 1} \dim(\mathcal{I}m(M_{\delta_i^{\epsilon_1}}) \cap \mathcal{I}m(M_{\delta_j^{\epsilon_2}}))\} \tag{48}$$

where the sup runs over all pairs δ_i, δ_j such that both $\delta_i \neq \delta_j$ and $\delta_i \neq \delta_j^{-1}$. This inequality is true since the four sets appearing in the right hand side are pairwise

orthogonal by (39). A similar equation could be written involving the $M^\dagger$'s. Suppose now that the supremum on the right hand side of (48) is zero, hence giving no direct condition on the dimension of $dim(\mathcal{H}_I)$. In such a case, all vector subspaces are orthogonal by (41), which imply $dim(\mathcal{H}_I) \geq |\Delta|$. Hence, a necessary condition for the existence of quantum walks with a smaller internal space is that some of the intersections in the sum (48) are non empty. In the following we give some examples.

3.2.1. A two dimensional walk with a two dimensional internal space. We consider here the group $\Gamma = \langle \delta_1, \delta_2 | \delta_1 \delta_2 \delta_1^{-1} \delta_2^{-1} = e \rangle$, a symmetric set $\Delta = \{\delta_1, \delta_1^{-1}, \delta_2, \delta_2^{-1}\}$ and define a quantum walk over the associated Cayley graph through the evolution operator (11) which reads here

$$W = M_{\delta_1} \otimes T_{\delta_1} + M_{\delta_1^{-1}} \otimes T_{\delta_1^{-1}} + M_{\delta_2} \otimes T_{\delta_2} + M_{\delta_2^{-1}} \otimes T_{\delta_2^{-1}} \tag{49}$$

We suppose that the rank of each matrix M_{δ_i} is one. In order to impose $dim(\mathcal{H}_I) = 2$, we require that at least two terms in the right hand side of (48) are zero for each possible pair of generators δ_i, δ_j. We obtain two solutions which transform one derived from the other by changing δ_1 and δ_1^{-1}. Up to an unitary transformation, the solution is

$$M_{\delta_1} = UP_1VP_1 \quad M_{\delta_1^{-1}} = UP_2VP_2 \quad M_{\delta_2} = UP_1VP_2 \quad M_{\delta_2^{-1}} = UP_2VP_1$$

where U and V are two unitary matrices and P_1,P_2 two orthogonal projectors. The evolution operator factorises into a product of two one-dimensional operators

$$W = (U \otimes 1)(P_1 \otimes (T_{\delta_1} T_{\delta_2})^{\frac{1}{2}} + P_2 \otimes (T_{\delta_1^{-1}} T_{\delta_2^{-1}})^{\frac{1}{2}})$$
$$(V \otimes 1)(P_1 \otimes (T_{\delta_1} T_{\delta_2^{-1}})^{\frac{1}{2}} + P_2 \otimes (T_{\delta_1^{-1}} T_{\delta_2})^{\frac{1}{2}})$$

However a quantum walk with a two dimensional internal space which is symmetric by inversion of only one of the axes or by a rotation of angle $\frac{\pi}{2}$ does not exist.
This solution generalises in higher dimensions:

Proposition 2 *Let $C_\Delta(\Gamma)$ be the Cayley graph of the free abelian group with n generators and symmetric presentation (34) and (35). Then there exists a unitary quantum walk operator (2) on G such that the dimension of the internal space is n if n is even and $n+1$ if n is odd.*

Proof: Suppose n even. We consider an internal space of dimension n and decompose it as a direct sum of two dimensional subspaces. We associate to each of these subspaces one different pair of generators. For such a pair (δ_i, δ_j), the four operators $M_{\delta_i}, M_{\delta_j}, M_{\delta_i^{-1}}, M_{\delta_j^{-1}}$ act non trivially only on the associated two-dimensional subspace and can be constructed in the same way as the internal operators of the previous example of two dimensional walk. The dimension of the internal space for such a quantum walk is then half the dimension of the free form solution. Suppose now n odd. We can repeat the previous construction for $n-1$ generators, and add a two dimensional space where the internal operators associated to the last generator will have the form of the internal operators of a one dimensional walk. All the internal operators then verify the

condition equations (36)-(38). □

3.2.2. Two dimensional walks with a four dimensional internal space. The impossibility of having a fully symmetric quantum walk does not hold when taking a four dimensional internal space. One possibility is to suppose that all the intersections involved in (48) are of dimension zero, in this case $dim(\mathcal{H}_I) \geq |\Delta| = 4$ and the minimal choice of the dimension leads to an evolution operator $W = \sum_\delta P_\delta U \otimes T_\delta$ where U is a four dimensional unitary matrix. The other possibility is to suppose that all the intersections involved in (48) are of dimension one. In this case the minimal dimension of the internal space is also four. A simple choice of matrices of rank two verifying all the conditions (36)-(38) is:

$$M_{\delta_1} = \frac{1}{\sqrt{2}}(|u_1\rangle\langle v_1| + |u_2\rangle\langle v_3|) \tag{50}$$

$$M_{\delta_1^{-1}} = \frac{1}{\sqrt{2}}(-|u_3\rangle\langle v_4| + |u_4\rangle\langle v_2|) \tag{51}$$

$$M_{\delta_2} = \frac{1}{\sqrt{2}}(|u_1\rangle\langle v_2| + |u_3\rangle\langle v_3|) \tag{52}$$

$$M_{\delta_2^{-1}} = \frac{1}{\sqrt{2}}(-|u_4\rangle\langle v_1| + |u_2\rangle\langle v_4|) \tag{53}$$

where $\{|u_i\rangle\}_{i=1,\cdot,4}$ and $\{|v_i\rangle\}_{i=1,\cdot,4}$ are two orthonormal bases of $\mathcal{H}_I$. In the following we give the explicit form of the evolution operator supposing that the rank of the matrices M_δ is one and that the walk is symmetric. A permutation of the vertex set Π is associated with a spatial transformation. As in the one dimensional case, the walk is symmetric under this transformation if there exists an unitary S such that $(S\otimes\Pi)^\dagger W(S\otimes\Pi) = W$. In other words, if the initial condition is modified by the transformation $S\otimes\Pi$, the wave function at any time can be deduced from the unmodified wave function by application of the same transformation. We impose invariance under the symmetries of the square lattice by considering the two transformations, $S_i \otimes \Pi_i$ and $S_r \otimes \Pi_r$, being respectively the representation of the inversion along the x axis and the rotation by $\frac{\pi}{2}$. The symmetry condition makes U reduce to a product $U = D^{-1}U_0D$ where D is a diagonal unitary matrix depending on four real parameters and U_0 takes the form:

$$U_0 = \begin{pmatrix} a & b & c & c \\ b & a & c & c \\ c & c & a & b \\ c & c & b & a \end{pmatrix}$$

The matrix U_0 depends on 3 parameters by the unitarity condition. The matrices S_1 and S_2 depend on the same parameters as the matrix D. Then choosing these four parameters equal to one reduces the walk operator to $W = \sum_i P_i U_0 \otimes Ti$ and the matrices S_1 and S_2 are just the inverse permutation of the generators associated to the spatial transformation.

3.2.3. A three dimensional walk with a four dimensional internal space. It has been shown that no nontrivial solution exists in three dimensions with a two dimensional internal space[12]. In the following we give solutions on $\mathbb{Z}^3$ with a four dimensional internal space. The starting point is again equation (48). Taking matrices of rank two would not break this condition for $dim(\mathcal{H}_I)$ provided that each term on the left hand side of (48) is one. Here we thus give the general solution for rank two matrices. Let $\Delta = \{\delta_1, \delta_2, \delta_3, \delta_1^{-1}, \delta_2^{-1}, \delta_3^{-1}\}$. Defines two orthonormal bases $\{|u_i\rangle\}_{i=1,\cdot,4}$ and $\{|v_i\rangle\}_{i=1,\cdot,4}$. Now construct six matrices of rank 2 indexed by the elements of Δ in the form

$$M_{\delta_1} = \alpha_1|u_1\rangle\langle v_2| + \beta_1|u_2\rangle\langle v_1| \quad (54)$$
$$M_{\delta_1^{-1}} = \gamma_1|u_3\rangle\langle v_4| + \delta_1|u_4\rangle\langle v_3| \quad (55)$$
$$M_{\delta_2} = \alpha_2|u_1\rangle\langle v_3| + \gamma_2|u_3\rangle\langle v_1| \quad (56)$$
$$M_{\delta_2^{-1}} = \beta_2|u_2\rangle\langle v_4| + \delta_2|u_4\rangle\langle v_2| \quad (57)$$
$$M_{\delta_3} = \alpha_3|u_1\rangle\langle v_4| + \delta_3|u_4\rangle\langle v_1| \quad (58)$$
$$M_{\delta_3^{-1}} = \beta_3|u_2\rangle\langle v_3| + \gamma_3|u_3\rangle\langle v_2| \quad (59)$$

It is clear that such a choice solves equations (39). The other equations are solved by taking

$$\alpha_2 = \lambda\alpha_1 \quad ; \quad \alpha_3 = \mu\alpha_1 \quad (60)$$
$$\beta_2 = \bar{\lambda}\nu\beta_1 \quad ; \quad \beta_3 = -\bar{\mu}\nu\beta_1 \quad (61)$$
$$\gamma_2 = -\lambda\bar{\nu}\gamma_1 \quad ; \quad \gamma_3 = -\bar{\mu}\gamma_1 \quad (62)$$
$$\delta_2 = -\bar{\lambda}\delta_1 \quad ; \quad \delta_3 = \mu\bar{\nu}\delta_1 \quad (63)$$

where $|\nu|^2 = 1$, $\lambda, \mu \in \mathbb{C}$ and

$$|\alpha_1| = |\beta_1| = |\gamma_1| = |\delta_1| = \frac{1}{\sqrt{1 + |\lambda|^2 + |\mu|^2}} \quad (64)$$

3.3. Cayley graphs with multiply connected second neighbours

In this section we consider Cayley graphs in which any second neighbour is connected by at least two alternating paths. They might be of interest since the condition equations contain at least two terms. Here, we only consider two examples in which each second neighbour is connected by at least two alternate paths. Both are interesting in their own right: the first one admits a scalar solution, while the other admits solutions in terms of a Clifford algebra.

3.3.1. A simple one dimensional example Let us consider the commutative group with two generators (34) with one more relation $\delta_1^2 = \delta_2^2$ in the presentation and as defining set for the Cayley graph $\Delta = \{\delta_1, \delta_2, \delta_1^{-1}, \delta_2^{-1}\}$.
The four matrices M_δ have to be taken as solutions of the four equations:

$$M_{\delta_1}^\dagger M_{\delta_1^{-1}} + M_{\delta_2}^\dagger M_{\delta_2^{-1}} = M_{\delta_1^{-1}} M_{\delta_1}^\dagger + M_{\delta_2^{-1}} M_{\delta_2}^\dagger = 0 \quad (65)$$

$$M_{\delta_1}^\dagger M_{\delta_2^{-1}} + M_{\delta_2}^\dagger M_{\delta_1^{-1}} = M_{\delta_2^{-1}} M_{\delta_1}^\dagger + M_{\delta_1^{-1}} M_{\delta_2}^\dagger = 0 \tag{66}$$

$$M_{\delta_1}^\dagger M_{\delta_2} + M_{\delta_2}^\dagger M_{\delta_1} + M_{\delta_1^{-1}}^\dagger M_{\delta_2^{-1}} + M_{\delta_2^{-1}}^\dagger M_{\delta_1^{-1}} = 0 \tag{67}$$

$$M_{\delta_2} M_{\delta_1}^\dagger + M_{\delta_1} M_{\delta_2}^\dagger + M_{\delta_2^{-1}} M_{\delta_1^{-1}}^\dagger + M_{\delta_1^{-1}} M_{\delta_2^{-1}}^\dagger = 0 \tag{68}$$

$$\sum_\delta M_\delta^\dagger M_\delta = \sum_\delta M_\delta M_\delta^\dagger = \mathbb{1} \tag{69}$$

This set of equations admits solutions with a one dimensional internal space, and the evolution operator can be written as

$$W = \frac{1}{2}(e^{i\theta}(\tau_1 \pm \tau_2) + e^{i\varphi}(\tau_1^{-1} \mp \tau_2^{-1})) \tag{70}$$

where τ_1 and τ_2 are the displacements in the directions δ_1 and δ_2. However, as can be seen from the form of the evolution operator, this example is equivalent to a quantum walk on $\mathbb{Z}$ with a two dimensional internal space by grouping together pairs of second neighbours. What is interesting here is that even on a graph where all sites are equivalent, there may exist scalar solutions provided all second neighbours are multiply connected. The minimal dimension of the internal space would still however have to be questioned since it strongly depends on the choice of the graph and various descriptions appear to be equivalent.

3.3.2. The hypercube We consider the group presentation

$$\Gamma = \langle \delta_1, \cdots \delta_n | \delta_i^2 = e \, \forall i; \, \delta_i \delta_j \delta_i^{-1} \delta_j^{-1} = e \, \forall i \neq j \rangle \tag{71}$$

whose Cayley graph is the hypercube in n dimensions. The condition equations become:

$$M_{\delta_i}^\dagger M_{\delta_j} + M_{\delta_j}^\dagger M_{\delta_i} = 0 \tag{72}$$

$$M_{\delta_i} M_{\delta_j}^\dagger + M_{\delta_j} M_{\delta_i}^\dagger = 0 \tag{73}$$

$$\sum_\delta M_\delta^\dagger M_\delta = \mathbb{1} \tag{74}$$

Equations (72) and (73) are valid for all pairs of generators δ_i, δ_j. Solutions originating from those for a free group of n generators have been studied by various authors ([13]-[14]).

Proposition 3 *There exists a unitary quantum walk operator (2) on the Cayley graph of the group (71) such that the internal operators are of the form* $M_{\delta_i} = \frac{1}{\sqrt{n}} \sigma_i U$ *where* U *is a unitary matrix of dimension* $dim(\mathcal{H}_I)$ *and* $\{\sigma_1 \ldots \sigma_n\}$ *is a set of anticommuting matrices.*

Proof: If one requires that all the matrices M_δ be Hermitian (or anti-hermitian) then the first set of equations (72)-(73) takes the form of an anticommutation relation between all pairs of matrices. Hermitian anticommuting matrices generate a Clifford algebra, it is therefore natural to find solutions among their matrix representations. Let $\{\sigma_1 \ldots \sigma_n\}$ such a set of anticommuting matrices and U an unitary matrix. A possible choice for the matrices M_δ is then $M_{\delta_i} = \frac{1}{\sqrt{n}} \sigma_i U$. □

For example, equations for $n = 3$ are solved by $M_i = \frac{1}{\sqrt{3}}\sigma_i U$ where each σ_i is one of the three Pauli matrices and U a unitary matrix in two dimensions. While the dimension of the matrix representation is rather large, (at least $2^{[\frac{n}{2}]}$), such solution may nevertheless be useful.

4. A generalised model of quantum walk

A quantum walk is a model for the motion of a quantum particle jumping (quantically) over a graph. A particle having a fixed number of internal degrees of freedom, one is naturally led to attach to each point x of the graph a copy of some Hilbert space $\mathcal{H}_I$ describing them. This is obviously not a necessary hypothesis in the context of a network of quantum processors, and even if we will retain here most of the terminology of quantum walks, we will not base our approach in this section on the interpretation of our quantum object as a physical particle. A second important property is the choice of a discrete time evolution, again motivated by the idea that quantum processors as their classical equivalents would exchange information at discrete times.
We will continue to consider discrete time evolution but we want to note that quantum walks with continuous time has also been introduced in the context of quantum algorithmics [15] [16]. As for the discrete time model, the succes of these walks performing particular tasks is dependent on characteristics such as the initial vector state [17], thus indicating that a classification of this model may also be of some interest. Some properties of one dimensional walks have been determined as for example the revival time [18] and a limit theorem demostrated by [19].
We consider an oriented graph $G = (X, E)$, X the set of vertices, and E the set of oriented edges. To each vertex $x \in X$, we attach a (finite) Hilbert space $\mathcal{H}_x$, and define the quantum evolution over $\mathcal{H} = \oplus_{x\in X}\mathcal{H}_x$ as follows: For each oriented pair (x, y), we define a linear map $M_{x,y}$ from $\mathcal{H}_x$ to $\mathcal{H}_y$, extend it on $\mathcal{H}$ by setting $M_{x,y} = 0$ on $\mathcal{H}_x^{\perp}$. We define its conjugate $M_{x,y}^{\dagger}$ as the map such that

$$\langle\Psi'|M_{x,y}\Psi\rangle = \langle M_{x,y}^{\dagger}\Psi'|\Psi\rangle \tag{75}$$

for all $|\Psi\rangle$, $|\Psi'\rangle$ in $\mathcal{H}$. Then we define the evolution of the quantum walk over $\mathcal{H}$ as:

$$|\Psi(t+1)\rangle = W|\Psi(t)\rangle \tag{76}$$

where $|\Psi(t)\rangle$ is the state of the system at time t and W is the unitary operator

$$W = \sum_{(x,y)\in E} M_{x,y} \tag{77}$$

In order to restrict the sum to the pairs of neighbouring sites and impose W to be unitary we require the following three properties:

$$M_{x,y} \neq 0 \text{ if and only if } (x, y) \in E \tag{78}$$

$$\sum_y M_{x,y}^{\dagger}M_{z,y} = \sum_y M_{y,x}M_{y,z}^{\dagger} = 0 \text{ for all } x \neq z \tag{79}$$

$$\sum_y M^\dagger_{x,y} M_{x,y} = \sum_y M_{y,x} M^\dagger_{y,x} = \mathbf{1}_x \tag{80}$$

where $\mathbf{1}_x$ is the projector over $\mathcal{H}_x$. Conditions (79) and (80) are necessary and sufficient conditions for W to be unitary. Here, it is already interesting to note that even in this more general context quantum "coin" solutions exist provided that on each site the number of incoming edges equals the number of outgoing ones. The construction can be done in the following way: we first set the dimension of all local Hilbert spaces equal to the number of incoming (or equivalently outgoing) neighbours,

$$dim(\mathcal{H}_x) = |E^{in}_x| = |E^{out}_x| \tag{81}$$

where we have set

$$E^{in}_x = \{y \in X : (y,x) \in E\} \tag{82}$$

$$E^{out}_x = \{y \in X : (x,y) \in E\} \tag{83}$$

For all $x \in X$ we fix two orthonormal basis $\mathcal{B}^{in}_x$ and $\mathcal{B}^{out}_x$ in $\mathcal{H}_x$ an label its elements using the list of neighbours,

$$\mathcal{B}^{in}_x = \{|\varphi^{in}_x(y)\rangle\}_{y \in E^{in}_x} \tag{84}$$

$$\mathcal{B}^{out}_x = \{|\varphi^{out}_x(y)\rangle\}_{y \in E^{out}_x} \tag{85}$$

Now setting

$$M_{x,y} = |\varphi^{in}_y(x)\rangle\langle\varphi^{out}_x(y)| \tag{86}$$

just satisfies all conditions (79), (80) and defines a general quantum "coin" solution even outside the context of a quantum particle on a lattice. In fact we get some more insight on how such solutions works from the point of view of a quantum network: first, each node splits the (partial) wave function along the vectors of a fixed basis $\mathcal{B}^{out}_x$ and send the resulting complex number to each of its neighbours; then a (partial) wave function is recomposed using the received numbers and the other fixed basis $\mathcal{B}^{in}_x$. We now want to recover previous definition of quantum walks on a Cayley graph, so we naturally suppose that the properties of the graph are transferred to the walk. In particular all local Hilbert spaces are copies of the same space,

$$\mathcal{H}_x = \mathcal{H}_0 \tag{87}$$

for all x in X and the complete Hilbert space is equivalent to the direct product of the local space $\mathcal{H}_0$ with a position space $\mathcal{H}_X$.

$$\mathcal{H} \approx \mathcal{H}_0 \otimes \mathcal{H}_X \tag{88}$$

Furthermore, the maps $M_{x,y}$ will depend only on the edge colour and direction of the edge (x,y) (i.e. only on the generator $\delta = x^{-1}y$) and not in the starting vertex x:

$$M_{x,y} = T_{0,y} M_{x^{-1}y} T_{x,0} \text{ for all } (x,y) \in E \tag{89}$$

where $M_{x^{-1}y}$ is a map on $\mathcal{H}_0$ and $T_{x,y}$ is the canonical shift map sending $\mathcal{H}_x$ onto $\mathcal{H}_y$. Thus the evolution operator W on $\mathcal{H}$ as a product space reads

$$W = \sum_{\delta \in \Delta} M_\delta \otimes T_\delta \tag{90}$$

5. Conclusion

We have considered quantum walks on Cayley graphs of groups and addressed the problem of classifying them as a function of the group presentation and the choice of the internal space. A first result is that the smallest possible dimension of the internal space depends strongly on the generating set chosen for constructing the Cayley graph. In the case of free groups, we succeeded in classifying all possible solutions. Standard quantum walk definition is recovered and correspond to an internal space of dimension equal to the number of neighbours (its smallest value) and a free group with a set of generators containing elements of the group different from the identity. When the identity element is present in the generating set used to define the Cayley graph of a free grop, or on other Cayley graphs, we showed that different solutions do exist for which we give a partial characterisation. We presented a few examples of solutions which does not enter in the previously known solutions and which become available as soon as there exist closed paths of length 4 on the graph, with alternating orientation. In particular, we found solutions with a smaller internal dimension that what is usually expected and a new kind of quantum walks on the hypercube based on Clifford algebra representation. We hope that these new possibilities will prove useful in the context of the relationship between quantum walks and quantum algorithms.

6. Acknowledgements

We are grateful to Z. Nagy and F. Millet for helping us in finding Clifford solutions on the hypercube and to J. Avan, J.-P. Kownacki, M. Schürmann and N. Weatherall for useful discussions.
Research partially supported by European Commission HPRN-CT-2002-00279, RTN QP Applications.

References

[1] Ambainis A 2003 *Int. J. Quantum Information* **1** 507
[2] Aharonov D, Ambainis A, Kempe J and Vazirani U 2001 *Proc. STOC*
(Aharonov D, Ambainis A, Kempe J and Vazirani U 2000 *Preprint* quant-ph/0012090)
[3] Shenvi N, Kempe J and BirgittaWhaley K 2003 *Phys. Rev. A* **67** 052307
[4] Ambainis A, Kempe J and Rivosh A 2005 *Proc. SODA*
(Ambainis A, Kempe J and Rivosh 2004 *Preprint* quant-ph/0402107)
[5] Brun T A, Carteret H A and Ambainis A 2003 *Phys. Rev. A* **67** 052317
[6] Wójcik D K and Dorfman J R 2003 *Phys. Rev. Let* **90** 230602
[7] Wójcik D K and Dorfman J R 2004 *Physica D* **187** 223
[8] Meyer D A 1996 *Phys. Lett. A* **223** 5-345
[9] Barenco A, Bennett C H, Cleve R, Divicenzo D P, Margolus N, Shor P, Sleator T, Smolin J A, Weinfurter H 1995 *Phys. Rev. A.* **52** 3457
[10] White A T *Graphs of groups on surfaces* (North-Holland)
[11] Meyer D A 1997 *Phys. Rev. E* **55** 5-5261
[12] Bialynicki-Birula I 1994 *Phys. Rev. D* **49** 12-6920

[13] Kempe J 2003 *Proc. RANDOM*
(Kempe J 2002 *Preprint* quant-ph/0205083)
[14] Moore C and Russell A 2002 *Proc. RANDOM*
(Moore C and Russell A 2001 *Preprint* quant-ph/0104137)
[15] Farhi E and Gutmann S 1998 *Phys. Rev. E* **58** 915
[16] Childs A M, Farhi E and Gutmann S 2002 *Quant. Inf. Process* **1** 35
[17] Mülken O and Blumen A 2005 *Phys. Rev. E* **71** 016101
[18] Mülken O and Blumen A 2005 *Phys. Rev. E* **71** 036128
[19] Konno N 2005 *Phys. Rev. E* **72** 026113