Chapitre 1

Modèles de Calcul Quantique

Pablo Arrighi
Simon Perdrix

Des phénomènes mis en évidence par la physique quantique dans le comportement des particules élémentaires sont désormais considérés sous l'angle de leur exploitation pour représenter, traiter et communiquer l'information. Feynman a inventé le concept d'ordinateur quantique [36] avec une application en tête : la simulation de système quantique, un domaine où l'ordinateur classique se révèle particulièrement peu efficace. Depuis, des résultats algorithmiques [40, 65], théoriques [19] puis expérimentaux soulignent l'intérêt d'un fondement quantique des sciences de l'information. Ces résultats montrent bien que des problèmes hors de portée de l'informatique classique peuvent être traités en exploitant ce paradigme de calcul non classique. Cela ouvre des perspectives scientifiques et technologiques immenses.

Après une introduction au calcul quantique, nous nous concentrerons sur le thème de la simulation quantique [37]. Ce thème fait appel à des modèles de calcul quantique massivement parallèle type automates cellulaires. Nous étudierons un premier algorithme de simulation quantique par une marche quantique.

1.1 Les postulats de la mécanique quantique

La formalisation de la mécanique quantique date du début du siècle passé. Même si de nombreuses questions fondamentales continuent à animer la communauté scientifique travaillant sur les fondements de la physique quantique (unification de la mécanique quantique et relativité générale, ou interprétation de la

mesure quantique par exemple), le formalisme de la mécanique quantique est particulièrement solide et éprouvé : elle est la théorie physique la plus fidèle à la réalité dans le sens où cette théorie permet de prédire les résultats expérimentaux avec très grande précision.

Dans cette section nous allons adopter une présentation de la mécanique quantique adaptée aux informaticiens : nous considèrerons uniquement des systèmes discrets et finis (le cas non-fini sera abordé en section 1.5), où la brique de base de l'information est le bit quantique, ou *qubit*. Après avoir décrit les états possibles d'une mémoire quantique, nous verrons comment la mesure agit sur l'état d'un registre, et enfin nous verrons comment évolue l'état d'un système quantique isolé.

1.1.1 Etats Quantiques

Le bit quantique

La brique de base en théorie de l'information est le *bit*. La mécanique quantique nous enseigne qu'un tel système ayant deux états classiques possibles **0** et **1** peut également être dans une superposition de **0** et de **1**, c'est-à-dire dans un état que nous noterons $\alpha\,|\mathbf{0}\rangle + \beta\,|\mathbf{1}\rangle$ où $\alpha, \beta \in \mathbb{C}$ avec $|\alpha|^2 + |\beta|^2 = 1$. De façon plus abstraite, l'espace des états possibles d'un bit quantique (*qubit*) est donc la sphère unité de $\mathbb{C}^{\{\mathbf{0},\mathbf{1}\}}$, le $\mathbb{C}$-espace vectoriel de dimension 2 engendré par $|\mathbf{0}\rangle$ et $|\mathbf{1}\rangle$ et muni de la norme euclidienne.

Plus généralement l'état d'un registre de n bits quantiques est une superposition des 2^n états classiques possibles :

Définition 1.1.1. *L'état $|\varphi\rangle$ d'un registre quantique de taille n est un vecteur unité de $\mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n}$:*

$$|\varphi\rangle = \sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} \alpha_x\,|x\rangle \quad \textit{tel que} \quad \| \,|\varphi\rangle\, \| = \sqrt{\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} |\alpha_x|^2} = 1$$

Exemple 1.1.2.

$$\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$

$$\frac{1}{\sqrt{3}}(|00\rangle + i\,|01\rangle + |11\rangle)$$

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Remarque 1.1.3 (Notation de Dirac)**.** *Le symbole $|x\rangle$ se prononce 'ket' x. On utilise également le symbole $\langle x|$ qui se prononce 'bra' x pour parler de l'adjoint*

$|x\rangle^\dagger$ *de* $|x\rangle$. *Les termes 'bra' et 'ket' proviennent de la décomposition du mot 'bracket' utilisé pour parler du produit scalaire canonique* $\langle u|v\rangle = u^\dagger v$, *ainsi le produit de* $\langle x|$ *('bra') et* $|y\rangle$ *('ket') est le produit scalaire ('bracket') des deux vecteurs, i.e.* $\langle x|y\rangle = \langle x|\,|y\rangle$.

Système composé

L'état d'un registre classique dont on connait l'état des sous-registres est obtenu par simple concaténation de ces états : par exemple un registre de 3 bits dont les deux premiers sont dans l'état **01** et le troisième est dans l'état **1**, est dans l'état **011**. La composition des états quantiques s'obtient à l'aide du produit tensoriel :

Définition 1.1.4. *Soit* $|\varphi_1\rangle$ *l'état d'un registre de* n *qubits et* $|\varphi_2\rangle$ *celui d'un registre de* m *qubits, l'état du registre composé de* $(n+m)$ *qubits est*

$$|\varphi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$$

avec $\cdot \otimes \cdot$ *bilinéaire et* $\forall x \in \{\mathbf{0},\mathbf{1}\}^n, \forall y \in \{\mathbf{0},\mathbf{1}\}^m, |x\rangle \otimes |y\rangle = |xy\rangle$

L'état d'un registre composé d'un premier sous registre dans l'état $\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} \alpha_x |x\rangle$ et d'un second dans l'état $\sum_{y\in\{\mathbf{0},\mathbf{1}\}^m} \beta_y |y\rangle$ est donc $\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n, y\in\{\mathbf{0},\mathbf{1}\}^m} \alpha_x\beta_y |xy\rangle$.

Exemple 1.1.5. *Dans les exemples qui suivent nous utilisons deux couleurs dans un but pédagogique pour mettre en évidence le premier registre (en bleu) et le second (en rouge).*

$$|\mathbf{0}\rangle \otimes \frac{|\mathbf{0}\rangle - |\mathbf{1}\rangle}{\sqrt{2}} = \frac{|\mathbf{0}\rangle\otimes|\mathbf{0}\rangle - |\mathbf{0}\rangle\otimes|\mathbf{1}\rangle}{\sqrt{2}} = \frac{|\mathbf{00}\rangle - |\mathbf{01}\rangle}{\sqrt{2}}$$

$$\frac{|\mathbf{0}\rangle + i|\mathbf{1}\rangle}{\sqrt{2}} \otimes \frac{|\mathbf{00}\rangle - i|\mathbf{10}\rangle}{\sqrt{2}} = \frac{|\mathbf{000}\rangle - i|\mathbf{010}\rangle + i|\mathbf{100}\rangle + |\mathbf{110}\rangle}{2}$$

L'état d'un registre sur plusieurs qubits n'est pas toujours décomposable en l'état de chacun de ses qubits. Par exemple pour tous $|\varphi_1\rangle$, $|\varphi_2\rangle$ états quantiques sur un qubit, $|\varphi_1\rangle \otimes |\varphi_2\rangle \neq \frac{1}{\sqrt{2}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle)$. En effet, soient $|\varphi_1\rangle = a\,|\mathbf{0}\rangle + b\,|\mathbf{1}\rangle$ et $|\varphi_2\rangle = c\,|\mathbf{0}\rangle + d\,|\mathbf{1}\rangle$, on a $|\varphi_1\rangle \otimes |\varphi_2\rangle = ac\,|\mathbf{00}\rangle + ad\,|\mathbf{01}\rangle + bc\,|\mathbf{10}\rangle + cd\,|\mathbf{11}\rangle$. Comme le système $\{ac = 1/\sqrt{2}; ad = 0; bc = 0; cd = 1/\sqrt{2}\}$ n'a pas de solution, l'état $\frac{1}{\sqrt{2}}(|\mathbf{00}\rangle + |\mathbf{11}\rangle)$ est indécomposable, on dit qu'il est *intriqué*. La découverte mathématique de tels états par Einstein, Podolsky et Rosen [34] en 1935 les a conduit à remettre en cause le formalisme de la mécanique quantique. Dans les années 60, John Bell [17] a proposé une expérience permettant de décider si de tels états existent ou non dans la nature. Malheureusement cette expérience était irréalisable avec les technologies de l'époque. En 1982, Alain Aspect et son équipe [16] réalisent l'expérience de Bell et démontrent expérimentalement l'existence de tels états quantiques intriqués.

L'intrication est un phénomène essentiel en informatique quantique : elle est utilisée dans le protocole de téléportation par exemple. Elle est également indispensable au calcul quantique : un ordinateur quantique dont la mémoire serait à tout moment séparable (c'est-à-dire sans intrication) peut être simulé efficacement par un ordinateur classique.

Etats graphes

Représenter et manipuler un état quantique n'est pas toujours aisé : un état quantique sur n qubits est représenté par 2^n nombres complexes. Concrètement, la description d'un état sur 20 qubits peut nécessiter jusqu'à plus d'un million de nombres complexes. Certains états quantiques admettent cependant une représentation plus compacte, c'est le cas des états graphes [42]. Les états graphes sont des états quantiques représentés par des graphes simples non orientés où chaque sommet correspond à un qubit et chaque arête représente intuitivement l'intrication entre les qubits. Formellement, étant donné un graphe $G = (V, E)$ d'ordre $n = |V|$, l'état quantique $|G\rangle$ représenté par ce graphe est

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{\mathbf{0},\mathbf{1}\}^V} (-1)^{|G[x]|} |x\rangle$$

où $|G[x]|$ est la taille du sous graphe induit par le support de x, autrement dit $|G[x]|$ est le nombre d'arêtes (u, v) de G telles que $x_u = x_v = 1$.

1.1.2 Mesure quantique

La mécanique quantique nous dit que si un système peut être dans deux états – par exemple un bit dans l'état 0 ou 1 ; ou un chat vivant ou mort – alors ce système peut être dans une superposition de ces deux états. Or, dans la vie de tous les jours nous observons rarement des superpositions de 0 et de 1 et encore moins des chats à la fois vivants et morts ! Une explication à cela : l'observation, aussi appelée mesure quantique, obéit à un postulat qui ne rend que les états *classiques* directement obervables. Si un qubit dans l'état $\alpha |\mathbf{0}\rangle + \beta |\mathbf{1}\rangle$ est mesuré alors avec probabilité $|\alpha|^2$ la valeur **0** est observée et avec probabilité $|\beta|^2$ la valeur **1** est observée. De plus, la mesure projette l'état du qubit dans l'état observé, à savoir $|\mathbf{0}\rangle$ dans le premier cas et $|\mathbf{1}\rangle$ dans le second.

$\alpha |\mathbf{0}\rangle + \beta |\mathbf{1}\rangle$ $\xrightarrow{|\alpha|^2}$ $|\mathbf{0}\rangle$ *on mesure* **0**

$\xrightarrow{|\beta|^2}$ $|\mathbf{1}\rangle$ *on mesure* **1**

Dans le cas des états intriqués, la mesure d'un qubit modifie globalement l'état du système : par exemple si le premier qubit de l'état $\frac{|\mathbf{00}\rangle+|\mathbf{11}\rangle}{\sqrt{2}}$ est mesuré, avec probabilité $1/2$ le premier qubit sera projeté dans l'état $|\mathbf{0}\rangle$ (resp. $|\mathbf{1}\rangle$) et donc l'état global du système sera $|\mathbf{00}\rangle$ (resp. $|\mathbf{11}\rangle$). Ainsi l'état du second qubit dépend du résultat de la mesure du premier qubit. Il y a ici un effet de bord instantané de la mesure du premier qubit sur le second et ce quelque soit la distance physique entre ces deux qubits. Bien qu'ayant contribué au scepticisme face à l'existence des états intriqués, cette non localité de la mesure quantique ne viole pas le principe de causalité car elle ne permet pas de transmettre d'information plus vite que la vitesse de la lumière. La raison est essentiellement que le résultat de la mesure est probabiliste, on ne peut donc pas 'choisir' de projeter l'état du second qubit dans un état ou dans un autre.

La définition suivante décrit l'action de la mesure d'un des qubits d'un registre quantique :

Définition 1.1.6. *La mesure du $i^{ième}$ qubit de $\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} \alpha_x |x\rangle$ produit le résultat $r \in \{0,1\}$ avec probabilité $p_r = \sum_{x\in\{\mathbf{0},\mathbf{1}\}^n \mid x_i=r} |\alpha_x|^2$, l'état du registre après la mesure [1] est alors $\frac{1}{\sqrt{p_r}} \sum_{x\in\{\mathbf{0},\mathbf{1}\}^n \mid x_i=r} \alpha_x |x\rangle$.*

On peut donc voir la mesure du $i^{\text{ième}}$ qubit comme la transition probabiliste suivante :

$$\sum_{x\in\{\mathbf{0},\mathbf{1}\}^n} \alpha_x |x\rangle \quad \xrightarrow[p_r]{} \quad \frac{1}{\sqrt{p_r}} \sum_{x\in\{\mathbf{0},\mathbf{1}\}^n \mid x_i=r} \alpha_x |x\rangle$$

La mesure décrite ci-dessus est une mesure dans la base dite *standard* $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$. Plus généralement, on peut faire des mesures dans toute base $\{|\psi_0\rangle, |\psi_1\rangle\}$ orthonomée ($\langle\psi_0|\,|\psi_1\rangle = 0$, où $\langle\psi_0| := |\psi_0\rangle^\dagger$). D'un point de vue physique, mesurer dans une autre base signifie mesurer une autre quantité : mesurer l'énergie ou la position d'une particule correspond à des mesures dans des bases différentes.

1.1.3 Evolution unitaire

En l'absence de mesure, c'est à dire quand le système est isolé, l'état d'un sytème quantique évolue de façon unitaire : son évolution est linéaire et préserve la condition de normalisation.

1. Lorsque $p_r = 0$ l'état du registre après la mesure n'est pas défini (division par 0), mais la mesure ne produit, par définition, jamais ce cas là.

Définition 1.1.7. *L'état d'un registre isolé évolue de façon unitaire.* $U : \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n} \to \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n}$ *est unitaire si*

— U *est linéaire :* $U(\alpha |\phi\rangle + \beta |\psi\rangle) = \alpha U |\phi\rangle + \beta U |\psi\rangle$;

— U *préserve la norme euclidienne :* $\|U |\phi\rangle\| = \||\phi\rangle\|$.

Exemple 1.1.8. *Les opérations unitaires sur* 1 *qubit les plus simples sont les opérations de Pauli* X, Y, Z *:*

$$\begin{array}{rcl} X : |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{array} \qquad \begin{array}{rcl} Z : |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{array} \qquad \begin{array}{rcl} Y = iXZ : |0\rangle & \mapsto & i|1\rangle \\ |1\rangle & \mapsto & -i|0\rangle \end{array}$$

D'autres exemples sont la transformation d'Hadamard (H) *et une extension de Pauli* Z *appelé rotation autour de* Z *:*

$$\begin{array}{rcl} H : |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array} \qquad \begin{array}{rcl} R_z(\theta) : |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & e^{i\theta}|1\rangle \end{array}$$

Le Control-Not (ΛX) *est une transformation unitaire agissant sur* 2 *qubits. Intuitivement une négation (Pauli* X*) est appliquée sur le second qubit si le premier est dans l'état* $|1\rangle$ *:*

$$\begin{array}{rcl} \Lambda X : |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$$

La transformation d'Hadamard est particulièrement utile en informatique quantique car elle permet de produire des états superposés à partir d'états de bases (états classiques). Si l'on applique Hadamard une seconde fois,

$$HH|0\rangle = H\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{H|0\rangle + H|1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle + |0\rangle - |1\rangle}{2} = |0\rangle$$

on voit apparaitre un autre phénomène spécifiquement quantique, l'interférence entre $+|1\rangle$ et $-|1\rangle$, pour obtenir l'état classique $|0\rangle$.

Propriété 1.1.9. $U : \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n} \to \mathbb{C}^{\{\mathbf{0},\mathbf{1}\}^n}$ *est unitaire si et seulement si* $U^\dagger = U^{-1}$ *où* $U^\dagger$ *est l'adjoint – c'est à dire la transposée conjuguée – de* U.

L'évolution d'un système isolé est donc inversible.

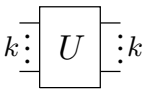
La composition spaciale de transformations unitaires est obtenue grâce au produit tensoriel :

Définition 1.1.10. *Soient* U *l'évolution unitaire d'un registre de* n *qubits et* V *celle d'un registre de* m *qubits, l'évolution globale du registre composé de* $(n+m)$ *qubits est* $U \otimes V$ *avec* $\forall x \in \{\mathbf{0},\mathbf{1}\}^n, \forall y \in \{\mathbf{0},\mathbf{1}\}^m, (U \otimes V)|x,y\rangle = (U|x\rangle) \otimes (V|y\rangle)$.

1.2 Circuits quantiques

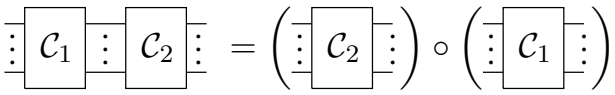
Les portes d'un circuit quantique sont des transformations unitaires. Tout circuit quantique est réversible, il possède autant d'entrées que de sorties. Etant donné une famille $\mathcal{F}$ de transformations unitaires, un circuit quantique peut être défini inductivement de la façon suivante :

— Porte $U \in \mathcal{F}$ d'arité k :

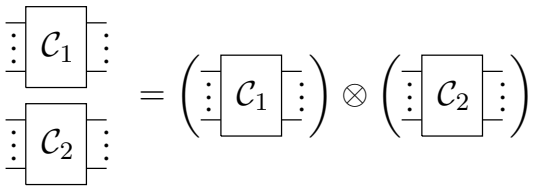


— L'identité :

— Composition séquentielle de deux circuits $\mathcal{C}_1$ et $\mathcal{C}_2$, agissant tous deux sur n qubits :



— Composition parallèle de deux circuits $\mathcal{C}_1$ et $\mathcal{C}_2$:



Le nombre de portes d'un circuit est appelé sa taille. Un circuit quantique peut comporter des qubits auxilliaires qui sont initialisés à $|0\rangle$. Un circuit quantique ayant n qubits d'entrées et m qubits auxiliaires réalise la transformation unitaire $U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ si pour tout $x \in \{0,1\}^n$, le circuit transforme l'état $|x\rangle \otimes |0^m\rangle$ en $(U|x\rangle) \otimes |0^m\rangle$, c'est à dire que les qubits auxiliaires doivent être dans l'état $|0\rangle$ en fin de calcul.

Théorème 1.2.1. *La famille de portes unitaires $\{H, \Lambda X, R_z(\alpha) : \alpha \in [0, 2\pi[\}$ est universelle : pour tout n, et pour toute transformation unitaire U sur n qubits, il existe un circuit quantique réalisant U dont chaque porte est H, ΛX ou $R_z(\alpha)$.*

La famille $\{H, \Lambda X, R_z(\alpha) : \alpha \in [0, 2\pi[\}$ est universelle mais infinie non dénombrable. Il n'est pas très raisonnable de définir un modèle de calcul en autorisant des angles qui ne sont pas calculables, de plus en pratique aucune technologie ne permet d'implémenter une rotation selon un angle fixé α_0 avec une infinie précision. Si l'on se contente d'un nombre fini d'opérations, par exemple $\{H, \Lambda X, R_z(\pi/4)\}$ alors le modèle ne peut être universel : le nombre de circuits

possibles est dans ce cas dénombrable alors que l'ensemble des opérations unitaires sur n qubits, pour $n > 0$ fixé, ne l'est pas. Cependant une universalité approchée est possible :

Théorème 1.2.2. *La famille de portes unitaires $\{H, \Lambda X, R_z(\pi/4)\}$ est approximativement universelle : pour tout n, pour tout transformation unitaire U sur n qubits et pour toute $\epsilon > 0$, il existe un circuit quantique réalisant une transformation unitaire U_0 telle que $\|U - U_0\| < \epsilon$, où $\|V\| = \sup_{|\phi\rangle \neq 0} \frac{\|V|\phi\rangle\|}{\||\phi\rangle\|}$.*

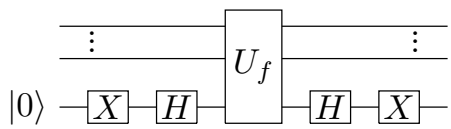
La réversibilité des circuits quantiques est-elle une contrainte ? Tous les circuits classiques sont-ils simulables par des circuits quantiques ? Un circuit classique ayant n entrées et m sorties calcule une fonction $f : \{0,1\}^n \to \{0,1\}^m$ et ne peut donc pas être réversible dès que $n > m$. Une technique standard pour rendre ce circuit réversible consiste à garder une copie de l'entrée et écrire le résultat de la fonction sur un registre auxiliaire. Cette méthode permet d'obtenir une transformation unitaire : $\forall x \in \{0,1\}^n, \forall y \in \{0,1\}^m, U_f |x, y\rangle \mapsto |x, f(x) \oplus y\rangle$, où $\cdot \oplus \cdot$ désigne le XOR bit à bit. Cette opération est sa propre inverse : $U_f(U_f |x, y\rangle) = U_f(|x, y \oplus f(x)\rangle) = |x, y \oplus f(x) \oplus f(x)\rangle = |x, y\rangle$. U_f simule f dans le sens où un appel à U_f sur $|x, 0\rangle$ produit $|x, f(x)\rangle$. De plus implémenter cette version unitaire de f n'est pas significativement plus compliqué que de calculer f :

Théorème 1.2.3. *Si $f : \{0,1\}^n \to \{0,1\}^m$ est calculée par un circuit classique de taille t alors son extension quantique $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$ est réalisée par un circuit quantique de taille $O(t)$.*

Dans le cas des fonctions booléennes, c'est à dire avec un seul bit de sortie et qui permettent de résoudre des problèmes de décision, il peut être intéressant de considérer une extension quantique alternative qui n'utilise pas de registre auxiliaire :

Lemme 1.2.4. *Si $f : \{0,1\}^n \to \{0,1\}$ est calculée par un circuit classique de taille t alors son extension quantique $U'_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$ est réalisée par un circuit quantique de taille $O(t)$.*

Démonstration. La preuve de ce lemme est l'occasion d'une première manipulation de circuit quantique. Etant donné l'extension $U_f : \mathbb{C}^{2^{n+1}} \to \mathbb{C}^{2^{n+1}}$ de f, on considère le circuit suivant, où le dernier qubit est un qubit auxiliaire initialisé dans l'état $|0\rangle$.



Pour tout $x \in \{0,1\}^n$,

$$\begin{aligned}
|x,0\rangle &\xmapsto{I_n \otimes X} |x,1\rangle \\
&\xmapsto{I_n \otimes H} \frac{1}{\sqrt{2}} \left(|x,0\rangle - |x,1\rangle\right) \\
&\xmapsto{U_f} \frac{1}{\sqrt{2}} \left(|x,f(x)\rangle - |x,1 \oplus f(x)\rangle\right) \\
&= \frac{(-1)^{f(x)}}{\sqrt{2}} \left(|x,0\rangle - |x,1\rangle\right) \\
&\xmapsto{I_n \otimes H} \frac{(-1)^{f(x)}}{2} \left(|x,0\rangle + |x,1\rangle - |x,0\rangle + |x,1\rangle\right) \\
&= (-1)^{f(x)} |x,1\rangle \\
&\xmapsto{I_n \otimes X} (-1)^{f(x)} |x,0\rangle
\end{aligned}$$

Ce circuit réalise donc $U'_f :: |x\rangle \mapsto (-1)^{f(x)} |x\rangle$. De plus d'après le théorème 1.2.3 il existe un circuit de taille $O(t)$ qui implémente U_f, donc il existe un circuit de taille $O(t)$ qui implémente U'_f. □

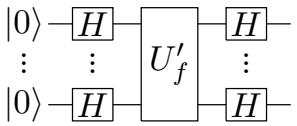
1.3 Quelques algorithmes quantiques

1.3.1 Deutsch-Jozsa

On se donne une fonction booléenne $f : \{0,1\}^n \to \{0,1\}$ avec la promesse que la fonction est soit constante ($\forall x, y \in \{0,1\}^n, f(x) = f(y)$) soit équilibrée ($|f^{(-1)}(0)| = |f^{(-1)}(1)|$). L'objectif est de déterminer si f est constante ou équilibrée.

Un algorithme classique déterministe consiste à appeler f sur $2^{n-1} + 1$ entrées différentes (c'est-à-dire sur la moitié plus une entrées). Si toutes les valeurs sont identiques la fonction est constante, sinon elle est équilibrée. Cet algorithme déterministe est optimal en nombre d'appels à la fonction f car on ne peut pas décider si la fonction est équilibrée ou constante en explorant moins de la moitié des entrées.

Deutsch et Jozsa [30] ont proposé un algorithme quantique permettant de décider si f est équilibrée ou constante en un seul appel à l'extension quantique de f :



La première étape de cet algorithme consiste à appliquer $H^{\otimes n}$, c'est-à-dire H sur n qubits en parallèle. Pour tout $x \in \{0,1\}^n$, $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\bullet y} |y\rangle$, avec $x \bullet y = \sum_{i=1}^{n} x_i y_i \bmod 2$. Comme pour tout $y \in \{0,1\}^n$ on a $0^n \bullet y = 0$, la première étape de cet algorithme produit une superposition uniforme ; par linéarité l'appel à U'_f permet une certaine forme de parallélisme quantique en associant à chaque vecteur $|x\rangle$ de la superposition l'amplitude $(-1)^{f(x)}$; enfin, la seconde application de $H^{\otimes n}$ engendre des interférences qui permettent en mesurant l'état final du registre de déterminer si la fonction est constante ou équilibrée. Plus précisément :

$$\begin{aligned}
|0^n\rangle &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\xrightarrow{U'_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \\
&\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H^{\otimes n} |x\rangle \\
&= \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)+x\bullet y} |y\rangle \\
&= \sum_{y\in\{0,1\}^n} \alpha_y |y\rangle
\end{aligned}$$

où $\alpha_y = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+x\bullet y}$. On remarque que $\alpha_{0^n} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$. Si f est équilibrée il y a autant de "-1" que de "1" dans cette somme donc $\alpha_{0^n} = 0$, en revanche si f est constante, alors $|\alpha_{0^n}| = 1$. Ainsi la mesure du registre à la fin du calcul produit le résultat classique 0^n si et seulement si f est constante.

Cet algorithme a été le premier permettant de montrer une séparation entre les algorithmes classiques déterministes et les algorithmes quantiques. Cependant il existe des algorithmes probabilistes beaucoup plus efficaces que les algorithmes déterministes pour résoudre ce problème. Par exemple étant donné un entier k, l'algorithme de Monte Carlo qui consiste à appeler f sur k entrées choisies aléatoirement et à répondre que la fonction est constante si et seulement si les k valeurs obtenues sont identiques permet de résoudre le problème avec grande probabilité. Si la fonction est constante la probabilité d'erreur est nulle ; si la fonction est équilibrée la probabilité d'erreur est de $1/2^{k-1}$. Par exemple pour $k = 11$ la probabilité d'erreur sera inférieure à $1/1000$. Dans les sections suivantes sont présentés des problèmes pour lesquels les algorithmes quantiques sont plus rapides que les algorithmes classiques, même probabilistes.

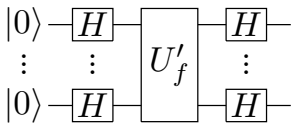
1.3.2 Bernstein-Vazirani

On veut identifier les fausses pièces parmi un ensemble de n pièces. On sait qu'une vraie pièce a une masse de $8g$ contre $7,5g$ pour une fausse. La seule balance à notre disposition est défectueuse, son écran n'indique que les décimales de la masse en gramme : par exemple ".0" pour $8g$; ".5" pour $22.5g$. Ainsi on ne peut connaître que la parité du nombre de fausses pièces posées sur le plateau de la balance. Combien de pesées doit-on effectuer pour identifier l'ensemble des fausses pièces ?

Pour modéliser ce problème, on va représenter chaque sous ensemble des n pièces par un mot binaire de longueur n : le ième bit de ce mot est 1 si et seulement si la ième pièce est dans l'ensemble. Appelons $a \in \{0,1\}^n$ l'ensemble des mauvaises pièces. On peut modéliser la balance à l'aide de la fonction f : $\{0,1\}^n \to \{0,1\}$ qui à un ensemble x associe la parité du nombre de mauvaises pièces dans x. On a $f(x) = x \bullet a = \sum_{i=1}^{n} x_i a_i \bmod 2$.

Un algorithme classique consiste à mesurer chaque pièce indépendamment et ainsi déterminer si elle est fausse ou non. Cet algorithme permet d'identifier les fausses pièces en n pesées. Cet algorithme naïf est optimal car tout algorithme classique, même probabiliste avec faible probabilité d'erreur, requiert n pesées pour des raisons de théorie de l'information : chaque pesée donne au plus un bit d'information alors que la réponse contient n bits d'information.

Cependant, nous vivons dans un monde quantique, nous pouvons donc a priori utiliser cette balance en régime quantique par exemple en posant une superposition de sous ensembles de pièces sur son plateau. Combien de pesées sont nécessaires pour déterminer l'ensemble des fausses pièces à l'aide de cette balance quantique ? Bernstein et Vazirani [20] ont proposé le circuit quantique suivant, qui est en fait le même que celui utilisé par Deutsch-Jozsa :



La première étape de cet algorithme consiste à appliquer $H^{\otimes n}$, c'est-à-dire H sur n qubits en parallèle. Pour tout $x \in \{0,1\}^n$, $H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \bullet y} |y\rangle$, avec $x \bullet y = \sum_{i=1}^{n} x_i y_i \bmod 2$. Comme pour tout $y \in \{0,1\}^n$ $0^n \bullet y = 0$, la première étape de cet algorithme produit une superpo-

sition uniforme :

$$\begin{aligned}
|0^n\rangle &\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \\
&\xrightarrow{U'_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet a} |x\rangle \\
&\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\bullet a} H^{\otimes n} |x\rangle \\
&= \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{x\bullet a + x\bullet y} |y\rangle \\
&= \frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{x\bullet (a\oplus y)} |y\rangle \\
&= \sum_{y\in\{0,1\}^n} \alpha_y |y\rangle
\end{aligned}$$

où $\alpha_y = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\bullet(a\oplus y)}$. On remarque que $\alpha_a = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\bullet 0^n} = \frac{\sum_{x\in\{0,1\}^n}(-1)^0}{2^n} = 1$. De plus, comme $\sum_{y\in\{0,1\}^n}|\alpha_y|^2 = 1$, on en déduit que pour tout $y \neq a$, $\alpha_y = 0$. Ainsi l'état du registre à la fin du calcul est $|a\rangle$. On peut mesurer ce résultat et obtenir l'ensemble a des fausses pièces. Cet algorithme quantique utilise une seule pesée là où un algorithme classique nécessite un nombre linéaire de pesées.

Bernstein et Vazirani [20] ont également défini une version récursive de ce problème qui peut être résolu de façon exacte en utilisant un nombre polynomial de pesées alors que tout algorithme probabiliste nécessite un nombre superpolynomial de pesées.

1.3.3 Grover

Avec ce troisième algorithme quantique nous abordons un problème classique en informatique, celui de la recherche. Il s'agit d'un problème très général : étant donné une base de données de 2^n éléments non structurée on cherche un élément particulier. Par exemple on cherche à trouver un mot dans un dictionnaire à partir de sa définition ; ou le nom d'une personne dans un annuaire à partir de son numéro de téléphone. Le problème peut être modélisé de la façon suivante : soit une fonction booléenne $f : \{0,1\}^n \to \{0,1\}$ telle que $|f^{(-1)}(1)| = 1$, trouver $x_0 \in \{0,1\}^n$ tel que $f(x_0) = 1$.

Comme on ne suppose aucune structure sur les éléments, tout algorithme classique nécessite $N-1$ appels à f ($N/2$ en moyenne), où $N = 2^n$ est le nombre

d'éléments de la base de données. Grover a introduit un algorithme quantique [40] permettant de déterminer cet élément en $O(\sqrt{N})$ appels à U'_f. L'algorithme est le suivant :

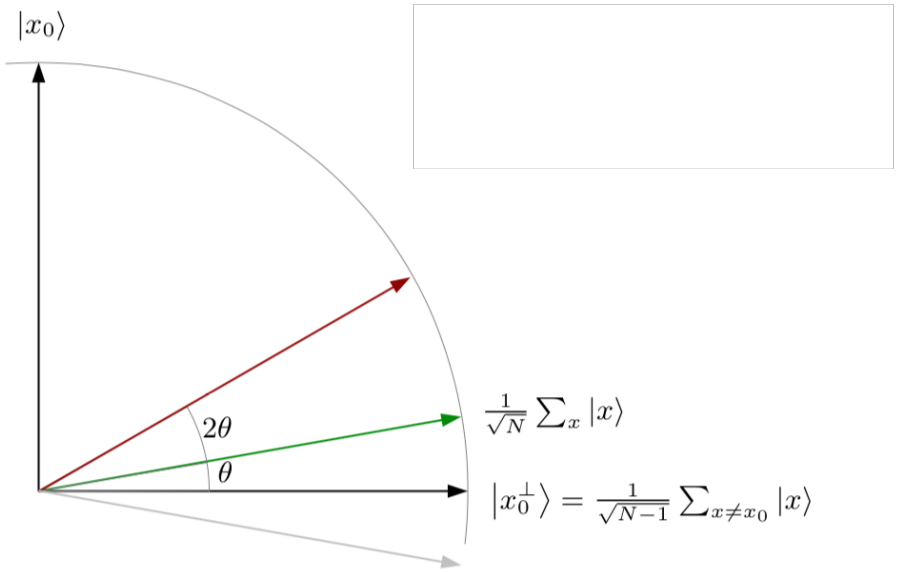
1. Préparer un registre de n qubits dans l'état $\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n} |0 \dots 0\rangle$

2. Répéter $\frac{\pi\sqrt{N}}{4}$ fois :
   – (a) Appliquer $U'_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$
   – (b) Appliquer $D : |x\rangle \mapsto -|x\rangle + \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle$

3. Mesurer le registre. Si le résultat z ne vérifie pas $f(z) = 1$, recommencer à l'étape 1.

Une preuve graphique de l'algorithme de Grover a été proposée par Aharonov [] : l'idée est de projeter l'espace complexe de dimension 2^n sur l'espace de dimension 2 engendré par $|x_0\rangle$ (x_0 est l'élément recherché) et $\left|x_0^\perp\right\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$, la superposition uniforme de tous les autres éléments. L'état initial du registre est la superposition uniforme $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt{N}} |x_0\rangle + \frac{\sqrt{N-1}}{\sqrt{N}} \left|x_0^\perp\right\rangle$, un vecteur (représenté en vert dans la figure ci-dessous) qui forme un angle $\theta = \arcsin(\frac{1}{\sqrt{N}}) \approx \frac{1}{\sqrt{N}}$ avec le vecteur $\left|x_0^\perp\right\rangle$.

La clé de cette preuve graphique est d'interpréter graphiquement U'_f et D dans cet espace de dimension 2. On remarque que $U'_f \left|x_0^\perp\right\rangle = \left|x_0^\perp\right\rangle$ et $U'_f |x_0\rangle = -|x_0\rangle$, U'_f est donc une réflexion par rapport à $\left|x_0^\perp\right\rangle$. L'application de U'_f transforme donc l'état initial en vert dans la figure ci dessous en l'état représenté en gris. Dans cette représentation D est une réflexion par rapport à la superposition uniforme : $D \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} D |x\rangle = -\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle + N \frac{2}{N} \sum_{y \in \{0,1\}^n} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$. Ainsi l'application de D produit l'état représenté en rouge sur la figure ci dessous, qui forme un angle 2θ avec l'état initial en vert. La composition de deux réflexions étant une rotation, chaque passage dans la boucle (2) de l'algorithme de Grover correspond à une rotation d'angle 2θ. Pour optimiser la probabilité de mesurer l'état $|x_0\rangle$ à la fin de l'algorithme il faut que l'état du système soit le plus proche possible de l'état $|x_0\rangle$, il faut donc que le nombre de passages k dans la boucle vérifie $k \times 2\theta \approx \pi/2$, donc $k \approx \frac{\pi}{4\theta} \approx \frac{\pi\sqrt{N}}{4}$.



1.3.4 Shor

Pour terminer ce rapide panorama des algorithmes quantiques nous évoquons l'algorithme de Shor [65] qui est sans aucun doute l'algorithme quantique le plus emblématique. Cet algorithme permet de factoriser efficacement un entier (non premier) de taille n, en trouvant un facteur non trivial en temps $O(n^3)$. On ne connait pas d'algorithme classique polynomial permettant de factoriser des nombres. Ce problème a même été supposé difficile et est au coeur de systèmes de cryptographie à clés publiques comme RSA [63] largement utilisés aujourd'hui. L'avènement d'un ordinateur quantique remet donc en cause la sécurité de nombreux systèmes communications communément utilisés.

A noter qu'un protocole de cryptographie quantique introduit par Bennett et Brassard [18] permet d'échanger de l'information de façon sûre. La sécurité de ce protocole est inconditionnelle, elle repose sur les postulats de la mécanique quantique.

L'algorithme de Shor est beaucoup plus élaboré que les autres algorithmes quantiques présentés dans ce chapitre, en conséquence nous référons à [54] pour une description détaillée de cet algorithme. A noter que cet algorithme se généralise à une classe de problèmes dit des sous groupes cachés [35, 44, 43].

1.3.5 Encore d'autres algorithmes quantiques...

Nous avons passé en revue quelques algorithmes quantiques 'traditionnels'. La recherche de nouveaux algorithmes quantiques est encore aujourd'hui un domaine en plein développement, nous pouvons par exemple citer l'utilisation de

techniques de marches quantiques [1] (généralisation de marches aléatoires) pour obtenir des algorithmes quantiques efficaces, par exemple pour la recherche de triangles dans les graphes [46, 45].

1.4 Modèles de Calcul Quantique

Dans cette section nous faisons un rapide tour d'horizon non exhaustif des modèles de calcul quantique. Nous avons déjà évoqué le modèle des circuits quantiques que nous avons utilisé pour présenter quelques algorithmes quantiques simples dans la section précédente. Historiquement, le premier modèle de calcul quantique a en fait été celui des machines de Turing quantiques. Le modèle des automates cellulaires quantiques est quant à lui un modèle massivement parallèle et permettant une modélisation assez fidèle des systèmes quantiques : il s'agit essentiellement d'une discrétisation en temps et en espace d'un système quantique. Il existe également des modèles de calcul quantique qui ne sont pas des 'quantisations' de modèles classiques, en particulier le modèle de calcul par mesures qui contrairement aux autres modèles de calcul évoqués jusqu'ici, n'utilise pas les évolutions unitaires mais les mesures comme moteur du calcul.

1.4.1 Machine de Turing Quantique

La machine de Turing quantique a été le premier modèle de calcul quantique. Introduit par Deutsch en 1985 [29], le modèle a été formalisé par Bernstein et Vazirani [20] au début des années 1990. Une machine de Turing quantique généralise la machine de Turing classique : la configuration d'une machine de Turing quantique est une superposition de configurations classiques : non seulement son ruban, mais aussi sa tête de lecture/écriture et son état interne sont en superposition. Concrètement l'évolution d'une machine de Turing est décrite par sa fonction de transition quantique qui décrit une superposition de transitions possibles. L'une des difficultés techniques à utiliser une machine de Turing quantique est que la fonction de transition doit vérifier des conditions de bonne formation pour que la description locale des transitions engendre bien une évolution de la machine globalement unitaire.

D'autres difficultés s'ajoutent à l'utilisation des machines de Turing quantique. Leur évolution étant unitaire il n'est pas possible pour l'utilisateur de savoir si l'état terminal de la machine est atteint. De plus, cet état terminal peut éventuellement être atteint par certaines configurations de la superposition mais pas par d'autres. Il existe des solutions à ces problèmes, en restreignant par exemple l'ensemble des machines de Turing quantiques à celles qui atteignent un état final sur toutes les configurations en superposition de façon synchronisée. L'ajout qu'un qubit d'arrêt que l'on peut observer pour déterminer si la machine a atteint

son état final ou non, sans perturber de façon significative le calcul est aussi possible [55]. Des variantes permettant l'observation de tout ou partie de la machine ont été introduites [57, 58] permettant d'une part de formaliser l'utilisation ad-hoc du qubit d'arrêt et également de tenir compte de modèles de calcul quantique plus récent où la mesure est au coeur du calcul (voir section 1.4.2).

En résumé, le modèle des machines de Turing quantiques est puissant mais difficile à utiliser et appréhender. Un résultat de Yao [73] montre qu'en terme de puissance de calcul les machines de Turing sont équivalentes au circuits quantiques. Ces derniers beaucoup plus intuitifs sont en général privilégié dès que possible.

1.4.2 Calcul par mesures

Dans les modèles traditionnels de calcul quantique comme les machines de Turing quantiques et les circuits quantiques, les évolutions unitaires jouent un rôle essentiel, la mesure quantique étant rejetée à la fin du calcul comme opération ne servant qu'à observer le résultat du calcul mais sans y contribuer réellement. Nielsen a montré [53] que la mesure quantique peut également être utilisée comme brique de base du calcul. En effet, comme la mesure quantique a la particularité de transformer le système mesuré, pourquoi ne pas utiliser cette transformation pour mener un calcul ? Tout comme les opérations unitaires H, $R_z(\pi/4)$ et ΛX sont universelles pour les circuits quantiques (théorème 1.2.2), il existe des familles de mesures sur 1 et 2 qubits qui sont universelles pour le calcul quantique [56].

Un autre modèle de calcul par mesures a été introduit par Raussendorf et Briegel [62]. Ce modèle utilise uniquement des mesures locales (sur un qubit) mais nécessite une ressource initiale intriquée, en l'occurence un état graphe (définition 1.1.1). Ce modèle est très prometteur en termes d'implémentation physique [60, 71]. Afin d'étudier les propriétés de ce modèle de calcul original, un formalisme dédié, le *measurement-calculus* [27, 28] a été développé. Ce formalisme a permis de mieux comprendre comment des stratégies spécifiques [25, 51] dépendant de l'intrication initiale permettent d'obtenir une évolution globalement déterministe alors que la brique de base du calcul, la mesure, ne l'est pas. Une séparation en terme de profondeur de calcul a également été mise en évidence [26] entre calcul par mesures et circuit quantique : le calcul par mesures favorise la parallélisation des opérations quantiques.

1.4.3 Automates cellulaires quantiques

Les Automates Cellulaires ont été introduits par Von Neumann [70]. Il s'agit d'une grille de cellules, chacune d'entre elles pouvant être dans un certain état, pris parmi un nombre fini d'états possibles. La grille entière évolue en pas de

temps discrets, en itérant une fonction globale G. En plus on demande que ce G soit shift-invariant (agit partout pareil) et causal (l'information ne peut pas être transmise plus vite que la vitesse de la lumière). Voir Figure 1.1. Comme il s'agit d'un modèle de de calcul proche de la physique, Feynman [37], puis Margolus [49], ont suggéré très tôt dans le développement du calcul quantique qu'il serait judicieux d'avoir une version quantique de ce modèle : les Automates Cellulaires Quantiques (QCA). Cela pour deux raisons. Premièrement, parcequ'ils constituent un cadre naturel pour faire de la simulation quantique [21, 23, 48, 50], dont on sait qu'elle sera l'une des applications phares du calcul quantique. Deuxièmement, car ce sont des architectures avantageuses d'implémentation physique d'un ordinateur quantique [24, 52, 67, 69] : dans un QCA, le calcul se produit sans contrôle externe, ce qui élimine une source de bruit. Mais il y a bien d'autres raisons d'étudier les QCA : en tant que modèle de calcul distribué quantique (pour étudier les problèmes sensibles aux dispositions spatiales) ou comme un outil privilégié pour comprendre les liens entre enchevêtrement et causalité [12, 13][41]. Enfin il y a aussi la perspective de la physique théorique, où les QCAs sont de bons candidats pour proposer des modèles jouets quantiques de l'espace-temps.

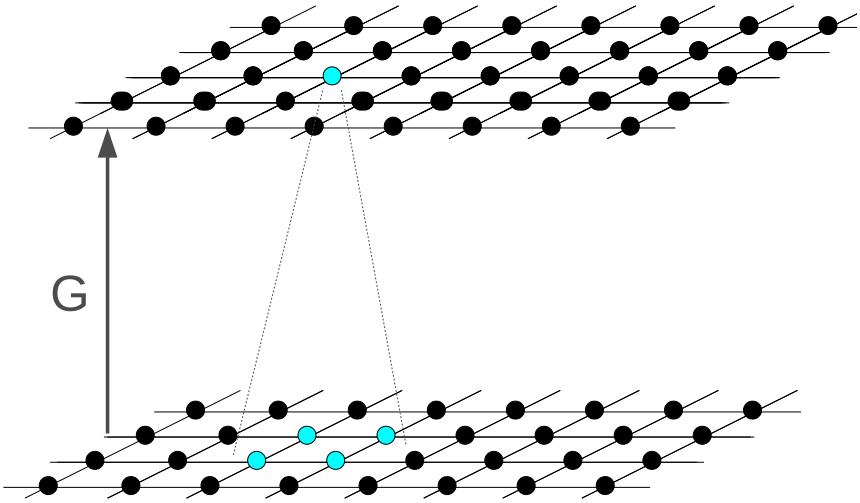


FIGURE *1.1 – Automates Cellulaires Quantiques, en dimensions* $2+1$ *(deux dimensions d'espace, une de temps).*

Un Automate Cellulaire Quantique (QCA) est donc une grille de systèmes quantiques, chacun de dimension finie. La grille entière évolue en pas de temps discrets, en itérant un opérateur unitaire global G. On demande encore que ce G soit shift-invariant (agit partout pareil) et causal (l'information ne peut pas être transmise plus vite que la vitesse de la lumière). Voir Figure 1.1. Si cette définition peut sembler naturelle, sa formalisation n'a pas été aisée. Les premières tentatives de formalisation [32, 72][2] se sont avérées briser la causalité [14], et furent remplacées par une approche plus axiomatique d'une part [64][14, 15, 12, 13] et

des définitions opérationnelles ad hoc d'autre part, [24, 59, 52, 61, 68, 72]. Dans [12, 13, 11] nous sommes parvenus à unifier ces approches, en établissant un théorème de portée générale, selon lequel « L'unitarité plus la causalité impliquent la localisabilité » . Il s'agit d'un théorème de représentation s'appliquant à toute unitaire causale, pour la mettre sous forme d'un circuit de profondeur composé de portes unitaires de locales. Dans [5, 6, 9, 8, 10] nous avons étudié la simulation intrinsèque des QCA. Autrement dit, nous avons construit des QCA capables de simuler tous les autres QCA.

1.5 Simulation quantique

Enjeux. Les ordinateurs mettent généralement des jours, voire des mois à simuler le résultat d'une experience de physique quantique qui, si elle est effectuée sur un table optique, se produit en un instant. Alors qu'il était confronté à cette situation, le prix Nobel de physique Richard Feynman une idée à la fois simple et géniale : ces simulations devraient être faisables plus rapidement par un ordinateur qui exploiterait lui même les bizarreries de la physique quantique, pour augmenter sa puissance de calcul. Autrement dit quoi de plus efficace, pour simuler un système quantique, que d'en utiliser un autre ? Les systèmes quantiques sont, en effet, de par leur nature, coûteux à représenter classiquement, étant donné que la description de n qubits requière que l'on spécifie 2^n nombres complexes. Les calculs, sur ces données de taille exponientielle, nécessitent donc eux-même en temps exponentiel. Classiquement, on ne peut pas espérer simuler plus de quelques particules. Pourtant le fait de pouvoir simuler des systèmes quantiques est un enjeu majeur. En (bio)chimie, physique des particules ou des matériaux, un simulateur quantique permettrait de comprendre des systèmes quantiques qui ne nous sont pas faciles d'accès, parce qu'on ne les a pas encore fabriqués (synthèse de nouvelles molécules), ou parce qu'ils sont hors d'atteinte (particules sur l'horizon d'un trou noir).

La décohérence. Actuellement les physiciens construisent de petits simulateurs quantiques constitués d'une dizaine de qubits, et parviennent à reproduire des phénomènes connus. Le principal obstacle, pour passer à l'échelle et envisager les applications mentionnées, c'est la décohérence. Comme nous l'avons vu, en physique quantique, l'observation modifie irréversiblement le système, elle le « classicise » . Donc, tant que le système est petit ses chances de « rester totalement incognito » , c'est-à-dire de ne pas interagir, même avec un photon de passage, sont fortes. Il reste alors dans le régime quantique. Un grand système par contre a nettement moins de chance de rester incognito : il est « observé » par l'environnement avec lequel il interagit. C'est ce qui explique que la physique quantique reste cantonnée aux petites échelles (particules, atomes). Néanmoins, même en

présence de décohérence, la simulation quantique peut rester utile. En effet, les systèmes que l'on souhaite simuler pour des applications comme la chimie quantique, biochimie, la synthèse de nouvelles molécules, les nanotechnologies etc. sont tous de relativement grande taille, en ce sens qu'ils sont eux-même soumis à la décohérence. Un exemple célèbre est celui du transport de l'énergie lors de la photosynthèse des plantes, qui est de nature mi-quantique, mi-classique. Bref, si l'on veut simuler un système quantique imparfait, nul besoin d'attendre l'ordinateur quantique parfait. L'implémentation expérimentale de la simulation quantique a d'ailleurs déjà commencé.

Expériences. Décrivons trois manipulations expérimentales, parmi de nombreuses autres, mais dont les performances laissent entrevoir le futur de la simulation.

- Les trappes d'ions sont apparues il y a une dizaine d'années. Dans ces manipulations, une dizaine d'ions sont piégés dans un champ électromagnétique et manipulés par des lasers. Les trappes d'ions permettent de simuler l'équation de Dirac qui gouverne les électrons et d'y constater, par exemple, la manière dont ils oscillent (phńomène dit du Zitterbewegung [39]). Récemment des propositions d'expériences sur trappes d'ion ont été formulées qui visent à simuler des versions discrétisées du modèle standard de la physique des particules.
- Les circuits optiques intégrés sont des gravures 3D de guides optiques qui conduisent des photons, comme de la fibre optique. Quand deux guides sont proches les photons peuvent sauter d'un guide à l'autre par effet tunnel. On pense à ces sauts comme au mouvement de la particule que l'on modélise. Ce système permet apparemment de faire de l'« échantillonnage de boson », c'est-à-dire de générer une certaine distribution de probabilité dont on peut prouver qu'elle ne suarait être générée efficacement de manière classique. La difficulté, c'est que l'on a pas vraiment de moyen de contrôler qu'il s'agit bien là d'une distribution issue de l'échantillonnage de boson — puis que c'est trop long à vérifier classiquement.
- Les réseaux optiques permettent de manipuler très précisément les atomes. Un atome placé sur un tel réseau est prisonnier dans des puits de potentiel (on dit qu'il est « froid »), et manipulé à l'aide de lasers. On peut ensuite déplacer l'atome dans une superposition de directions : à la fois vers la gauche et vers la droite. Cette technique a permis de simuler une particule chargée dans un champs électrique [38]. Dans le futur elle devrait permettre de simuler des particules quantiques en interactions.

Aspects théoriques. Au-delà de ces défis expérimentaux il y a de nombreux défis théoriques. En effet, toute simulation, même classique, d'un système physique, sur un ordinateur, nécessite une modélisation, c'est-à-dire qu'il faut parvenir à représenter les états du système par une suite de bits, et représenter l'évolution

de ce système par un algorithme. Très fréquemment on modélise le système à l'aide d'un automate cellulaire : un modèle où le temps et l'espace sont discrets (l'espace est découpé en cellules, et l'on saute du temps t au temps t+1). L'état de chaque cellule au temps suivant est alors calculé via une règle locale qui prend comme argument l'état actuel de la cellule et celui de ces voisines. Maintenant que l'on cherche à modéliser les systèmes quantiques, les mêmes problématiques émergent : quels sont les systèmes quantiques qui se prêtent à une modélisation discrète ? Est-ce que tous peuvent être simulés par des modèles de type automates cellulaires quantiques ? Actuellement nous avons par exemple mis au point les premiers algorithme de simulation d'un fermion sans masse à l'approche d'un trou noir [31, 4]. Prenons maintenant un exemple concret de modélisation d'un système physique par un algorithme quantique apparenté à un automate cellulaire : une marche quantique.

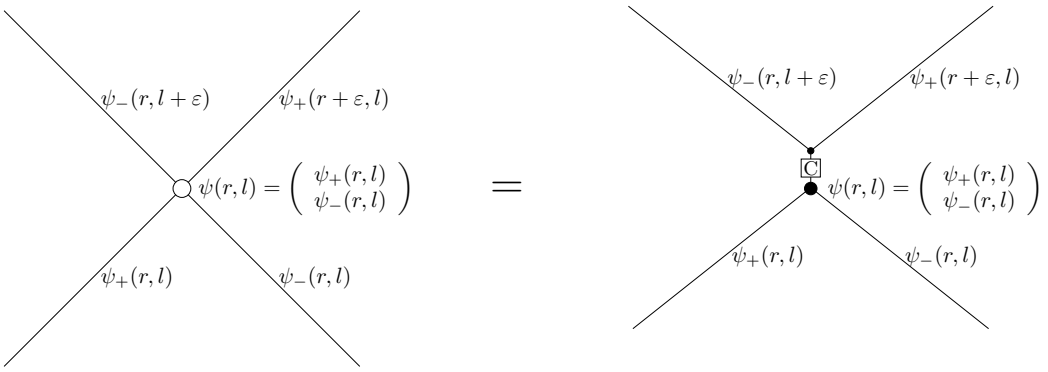
Exemple de simulation par une marche quantique

Nous allons expliquer comment simuler, avec une marche quantique, le comportement d'un électron, en $1+1$ dimensions (une dimension d'espace, une dimension de temps). Les électrons se déplacent selon l'équation de Dirac :

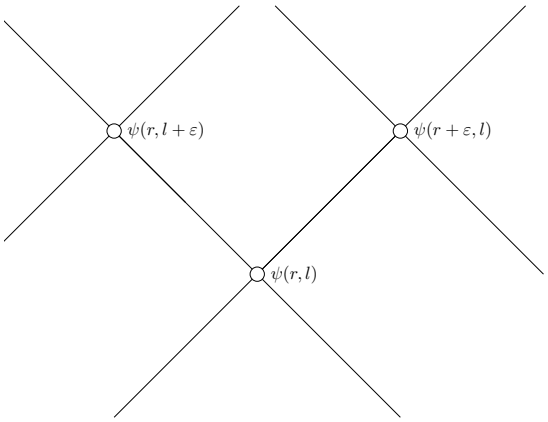
$$\partial_t \psi = -\mathrm{i} m X \psi - Z \partial_x \psi, \tag{1.1}$$

avec ∂_y la dérivée partielle selon y, m la masse et $\psi = \psi(t,x)$ sa fonction d'onde en espace-temps, de $\mathbb{R}^{1+1}$ vers $\mathbb{C}^2$. Voici comment interpréter une fonction d'onde : $\psi(x,t)$ est un vecteur de nombres complexes $(\alpha(x,t) \quad \beta(x,t))^T$. Le nombre complex $\alpha(x,t)$ est l'amplitude quantique pour que la particule se trouve au lieu x au temps t et qu'elle soit sur le point de partir vers la droite. Idem pour la gauche, avec β. Ce formalisme, des fonctions d'onde, est le plus courant chez les physiciens, puisqu'ils étudient le plus souvent des espace-temps continus. Il est donc un peu différent du formalisme des kets, bras et qubits que nous avons vu jusqu'alors. Mais, pour faire le lien, il suffit d'imaginer une fonction d'onde discrétisée par pas de ε à un temps donné, donc une fonction ψ de $\varepsilon\mathbb{Z}$ vers $\mathbb{C}^2$. $\psi(x)$ est donc un vecteur de nombres complexes $(\alpha(x) \quad \beta(x))^T$. Maintenant, en termes de kets et de bras, et comme nous ne considérons ici qu'une particule, mais qui peut-être dans deux états internes possibles (disons $|u\rangle$ quand elle est sur le point d'aller à droite, et $|d\rangle$ quand elle est sur le point d'aller à gauche), les états de base possibles sont de la forme $|\ldots 00u00\ldots\rangle$, $|\ldots 00d00\ldots\rangle$, $|\ldots 000u0\ldots\rangle$, etc. Un état général du système, $|\psi\rangle$, est donc donné par une superposition de ces états de base, et dont les amplitudes sont donnnées par la fonction d'onde ψ. Par exemple, si l'on superposait les trois états de base ci-dessus avec différentes amplitudes $\alpha(3)$, $\beta(3)$, $\alpha(4)$, on obtiendrait

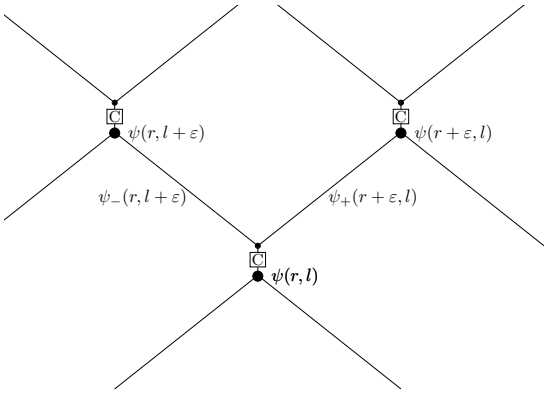
$$|\psi\rangle = \alpha(3)\,|\ldots 00u00\ldots\rangle + \beta(3)\,|\ldots 00u00\ldots\rangle + \alpha(4)\,|\ldots 000u0\ldots\rangle\,.$$



(a) Chaque point blanc (gauche) représente le circuit correspondant (droite).



(b) Une fonction d'onde ψ en espace-temps en coordonnées lumière. Le temps s'écoule vers le haut.



(c) Une représentation explicite, sous forme de circuit, de la relation entre les vecteurs à chaque points. La matrice C est appliquée à chaque vecteur d'entrée, tandis que les lignes propagent chaque composante du vecteur de sortie à la vitesse de la lumière.

FIGURE *1.2* – Marche quantique pour l'équation de Dirac.

C'est donc ainsi qu'il faut comprendre les fonctions d'ondes ψ : elles fournissent les amplitudes de superposition des cas de base qui composent $|\psi\rangle$.

Effectuons le changement de coordonnées $r = (t + x)/2$ et $l = (t - x)/2$. C'est ce qu'on appelle les coordonnées « lumière » , car les lignes à r constant ne sont autres que les trajectoires des photons lancés vers la gauche, et réciproquement. Redéfinissons la fonction d'onde : $\psi(r + l, r - l) \to \psi(r, l)$. Alors l'Eq. (1.1) devient

$$\begin{pmatrix} \partial_r & 0 \\ 0 & \partial_l \end{pmatrix} \psi = -\mathrm{i}mX\psi. \tag{1.2}$$

On note $e^{\varepsilon\partial_\mu}$ la translation par ε selon l'axe μ (avec $\mu = 0, 1$), i.e.

$(e^{\varepsilon\partial_\mu}\psi)(x_\mu) = \psi(x_\mu + \varepsilon)$. Cette notation est justifiée par la définition de l'exponentielle en tant que série de Taylor. Il est clair que $(e^{\varepsilon\partial_\mu}\psi) = \psi + \varepsilon\partial_\mu\psi$.

En utilisant le développement au premier ordre de l'exponentielle, on obtient que la fonction d'onde est une ψ est solution de l'équation de Dirac equation si et seulement si, quand $\varepsilon \to 0$,

$$\begin{aligned}\begin{pmatrix} e^{\varepsilon\partial_r} & 0 \\ 0 & e^{\varepsilon\partial_l} \end{pmatrix}\psi &= \left(\mathrm{Id} + \begin{pmatrix} \varepsilon\partial_r & 0 \\ 0 & \varepsilon\partial_l \end{pmatrix}\right)\psi + O(\varepsilon^2) \\ &= (\mathrm{Id} - \mathrm{i}m\varepsilon X)\psi + O(\varepsilon^2). \end{aligned} \tag{1.3}$$

De façon équivalente si on denote $\psi = (\psi_+, \psi_-)^{\mathsf{T}}$, alors ψ est solution de l'équation de Dirac equation si et seulement si, au premier ordre en ε et quand $\varepsilon \to 0$,

$$\begin{aligned} \psi_+(r+\varepsilon, l) &= \psi_+(r,l) - \mathrm{i}m\varepsilon\psi_-(r,l) \\ \text{and} \quad \psi_-(r, l+\varepsilon) &= \psi_-(r,l) - \mathrm{i}m\varepsilon\psi_+(r,l). \end{aligned} \tag{1.4}$$

Si maintenant ε est considéré comme fixe, et ψ est une fonction d'onde de $(\varepsilon\mathbb{Z})^2$ vers $\mathbb{C}^2$, alors Eq. (1.4) est un simple schéma aux différences finies pour l'équation de Dirac. On peut le voir comme un système dynamique illustré en Fig. 1.2 avec :

$$C = \begin{pmatrix} 1 & -\mathrm{i}\varepsilon m \\ -\mathrm{i}\varepsilon m & 1 \end{pmatrix}. \tag{1.5}$$

Mais nous aurions pu faire un petit bout de chemin supplémentaire à partir de Eq. (1.3). En effet, en reconnaissant dans le membre droit une expansion au premier ordre d'une exponentielle, on obtient :

$$\begin{pmatrix} e^{\varepsilon\partial_r} & 0 \\ 0 & e^{\varepsilon\partial_l} \end{pmatrix}\psi = e^{-\mathrm{i}m\varepsilon X}\psi + O(\varepsilon^2). \tag{1.6}$$

De fait, ψ est solution de l'équation de Dirac equation si et seulement si, quand $\varepsilon \to 0$, l'Eq. (1.6) est satisfaite. Si une fois de plus on considère ε comme fixé, alors l'Eq. (1.6) definit une Marque Quantique pour l'équation de Dirac (Dirac QW) [66, 21, 50, 22, 7]. C'est en effet un système dynamique, illustré encore en Fig. 1.2 mais cette fois avec :

$$C = e^{-\mathrm{i}m\varepsilon X} = \begin{pmatrix} \cos(\varepsilon m) & -\mathrm{i}\sin(\varepsilon m) \\ -\mathrm{i}\sin(\varepsilon m) & \cos(\varepsilon m) \end{pmatrix}, \tag{1.7}$$

qui est exactement unitaire, à tous les ordres de ε.

De retour en coordonnées (t, x), la marche de quantique de Dirac est donnée par $\psi(t+\varepsilon, x) = TC\psi(t,x)$, avec $T = e^{-\varepsilon\partial_x\sigma_3}$ l' opération de shift partiel. Ce

$W = TC$ est appelé « opérateur de la marche » : il est shift-invariant et unitaire. C est appelé « opérateur de pièce » : il agit sur le degré de liberté interne $\mathcal{H} \cong \mathbb{C}^2$. Au global les composantes du vecteur sont donc « mélangées » par l'opérateur de pièce, puis la composante du haut bouge à droite à la vitesse de la lumière, et la composante de bas bouge à gauche à la vitesse de la lumière.

Pourquoi préférer la marche quantique, obtenue dans un second temps, au schéma aux différences finies obtenu en premier lieu ? Parceque le schéma aux différences finies n'est pas « physique » : il n'est pas unitaire, les nombres que l'on y fait évoluer représentent certes des approximations d'amplitudes quantiques, mais ne peuvent pas être implémentées comme tels. A l'inverse, la marche quantique est unitaire, il s'agit donc d'une évolution physique réaliste. On peut donc implémenter cette évolution sur un système quantique dont les amplitudes de superpositions sont les nombres que l'on fait évoluer. Autrement dit la marche quantique est un algorithme de simulation quantique valable pour simuler l'électron sur un simulateur quantique. Par ailleurs, la marche quantique peut donc prétendre à être un modèle « jouet » valable du comportement de l'électron : une explication espace-temps discrets valable pour son comportement.

Conclusion. Le domaine de la simulation quantique est entré dans une phase fascinante, phase où les théoriciens parviennent à modéliser toujours plus de physique quantique, et les expérimentateurs parviennent à implémenter ces modèles avec toujours plus de succès. Reste encore à passer à l'échelle, à parvenir à des simulateurs avec 100 ou 1000 qubits, et faire en sorte que la décohérence, inévitable dans l'état actuel de nos capacités techniques, soit utilisée pour émuler la décohérence qui a lieu dans le système à simuler. A plus long terme, un simulateur quantique universel permettrait, avec une seule machine physique, de simuler tout système quantique, et donc de remplacer bon nombre d'expériences coûteuses par un seul dispositif.

Bibliographie

[1] A. Ambainis. Quantum walk algorithm for element distinctness. *SIAM Journal on Computing*, 37(1) :210–239, 2007.

[2] P. Arrighi. Algebraic characterizations of unitary linear quantum cellular automata. In *Proceedings of Mathematical Foundations of Computer Science, Lecture Notes in Computer Science*, volume 4162, page 122. Springer, 2006.

[3] P. Arrighi and S. Facchini. Decoupled quantum walks, models of the klein-gordon and wave equations. *EPL (Europhysics Letters)*, 104(6) :60004, 2013.

[4] P. Arrighi, S. Facchini, and M. Forets. Quantum walks in curved spacetime. *Pre-print arXiv :1505.07023*, 2015.

[5] P. Arrighi and R. Fargetton. Intrinsically universal one-dimensional quantum cellular automata. In *Proceedings of DCM*, 2007.

[6] P. Arrighi, R. Fargetton, and Z. Wang. Intrinsically universal one-dimensional quantum cellular automata in two flavours. *Fundamenta Informaticae*, 21 :1001–1035, 2009.

[7] P. Arrighi, M. Forets, and V. Nesme. The Dirac equation as a Quantum Walk : higher-dimensions, convergence. Pre-print arXiv :1307.3524, 2013.

[8] P. Arrighi and J. Grattage. A quantum Game of Life. In *Second Symposium on Cellular Automata "Journées Automates Cellulaires" (JAC 2010), Turku, December 2010. TUCS Lecture Notes 13, 31-42, (2010).*, 2010.

[9] P. Arrighi and J. Grattage. A Simple n-Dimensional Intrinsically Universal Quantum Cellular Automaton. *Language and Automata Theory and Applications, Lecture Notes in Computer Science*, 6031 :70–81, 2010.

[10] P. Arrighi and J. Grattage. Intrinsically universal n-dimensional quantum cellular automata. *J. of Computer and Systems Sciences*, 78 :1883–1898, 2012.

[11] P. Arrighi and J. Grattage. Partitioned Quantum Cellular Automata are Intrinsically Universal. *Natural Computing*, 11 :13–22, 2012.

[12] P. Arrighi, V. Nesme, and R. Werner. Unitarity plus causality implies localizability. *J. of Computer and Systems Sciences*, 77 :372–378, 2010. QIP 2010 (long talk).

[13] P. Arrighi, V. Nesme, and R. Werner. Unitarity plus causality implies localizability (full version). *Journal of Computer and System Sciences*, 77(2) :372–378, 2011.

[14] P. Arrighi, V. Nesme, and R. F. Werner. Quantum cellular automata over finite, unbounded configurations. In *Proceedings of LATA, Lecture Notes in Computer Science*, volume 5196, pages 64–75. Springer, 2008.

[15] P. Arrighi, V. Nesme, and R. F. Werner. One-dimensional quantum cellular automata. *IJUC*, 7(4) :223–244, 2011.

[16] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25) :1804–1807, 1982.

[17] J. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1 :195, 1964.

[18] C. H. Bennett and G. Brassard. Quantum cryptography : Public key distribution and coin tossing. In *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing, Bangalore, India*, page 175, New York, 1984. IEEE Press.

[19] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70 :1895–1899, 1993.

[20] E. Bernstein and U. Vazirani. Quantum complexity theory. In *Proceedings of the 25th Annual ACM Symposium on the Theory of Computation*, pages 11–20, New York, 1993. ACM press.

[21] I. Bialynicki-Birula. Weyl, Dirac, and Maxwell equations on a lattice as unitary cellular automata. *Phys. Rev. D.*, 49(12) :6920–6927, 1994.

[22] A. Bisio, G. M. D'Ariano, and A. Tosini. Dirac quantum cellular automaton in one dimension : Zitterbewegung and scattering from potential. *Physical Review A*, 88(3) :032301, 2013.

[23] B. M. Boghosian and W. Taylor. Quantum lattice-gas model for the many-particle Schrödinger equation in d-dimensions. *Phys. Rev. E.*, 57(1) :54–66, 1998.

[24] G. K. Brennen and J. E. Williams. Entanglement dynamics in one-dimensional quantum cellular automata. *Phys. Rev. A.*, 68(4) :042311, Oct 2003.

[25] D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New Journal of Physics (NJP)*, 9(8), 2007.

[26] D. E. Browne, E. Kashefi, and S. Perdrix. Computational depth complexity of measurement-based quantum computation. In *Theory of Quantum Computation, Communication, and Cryptography (TQC'10)*, volume 6519, pages 35–46. LNCS, 2011.

[27] V. Danos, E. Kashefi, and P. Panangaden. The measurement calculus. *J. ACM*, 54(2), 2007.

[28] V. Danos, E. Kashefi, P. Panangaden, and S. Perdrix. *Extended Measurement Calculus*. Cambridge University Press, 2010.

[29] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A*, 400 :97–117, 1985.

[30] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. 439 :553–558, 1992.

[31] G. Di Molfetta, M. Brachet, and F. Debbasch. Quantum walks as massless dirac fermions in curved space-time. *Physical Review A*, 88(4) :042301, 2013.

[32] C. Dürr, H. Le Thanh, and M. Santha. A decision procedure for well-formed linear quantum cellular automata. In *Proceedings of STACS 96, Lecture Notes in Computer Science*, pages 281–292. Springer, 1996.

[33] J. Eakins. Quantum cellular automata, the EPR paradox and the Stages paradigm. In *Proceedings of NATO ARW, The Nature of Time : Geometry, Physics and Perception*, volume 95, page 323. Kluwer, 2003.

[34] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of reality be considered complete ? *Phys. Rev.*, 47(10) :777–780, May 1935.

[35] M. Ettinger, P. Høyer, and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1) :43–48, 2004.

[36] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6) :467–488, 1982.

[37] R. P. Feynman. Quantum mechanical computers. *Foundations of Physics (Historical Archive)*, 16(6) :507–531, 1986.

[38] M. Genske, W. Alt, A. Steffen, A. H. Werner, R. F. Werner, D. Meschede, and A. Alberti. Electric quantum walks with individual atoms. *Physical review letters*, 110(19) :190601, 2013.

[39] R. Gerritsma, G. Kirchmair, F. Zähringer, E. Solano, R. Blatt, and C. Roos. Quantum simulation of the dirac equation. *Nature*, 463(7277) :68–71, 2010.

[40] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Found. Phys Phys Rev Lett*, 79 :325, 1993.

[41] J. Gütschow, S. Uphoff, R. F. Werner, and Z. Zimborás. Time asymptotics and entanglement generation of Clifford quantum cellular automata. *Journal of Mathematical Physics*, 51(1) :015203, 2010.

[42] M. Hein, J. Eisert, and H. J. Briegel. Multi-party entanglement in graph states. *Physical Review A*, 69 :062311, 2004.

[43] G. Ivanyos, L. Sanselme, and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups. In *STACS 2007*, pages 586–597. Springer, 2007.

[44] P. Koiran, V. Nesme, and N. Portier. The quantum query complexity of the abelian hidden subgroup problem. *Theoretical computer science*, 380(1) :115–126, 2007.

[45] F. Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 216–225. IEEE, 2014.

[46] T. Lee, F. Magniez, and M. Santha. Improved quantum query algorithms for triangle finding and associativity testing. In *Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1486–1502. SIAM, 2013.

[47] S. Lloyd. A potentially realizable quantum computer. *Science*, 261(5128) :1569–1571, 1993.

[48] P. Love and B. Boghosian. From Dirac to Diffusion : decoherence in Quantum Lattice gases. *Quantum Information Processing*, 4(4) :335–354, 2005.

[49] N. Margolus. Parallel quantum computation. In *Complexity, Entropy, and the Physics of Information : The Proceedings of the 1988 Workshop on Complexity, Entropy, and the Physics of Information, May-June 1989, in Santa Fe, New Mexico*, pages 273–293. Perseus Books, 1990.

[50] D. A. Meyer. From quantum cellular automata to quantum lattice gases. *J. Stat. Phys*, 85 :551–574, 1996.

[51] M. Mhalla and S. Perdrix. Finding optimal flows efficiently. In *the 35th International Colloquium on Automata, Languages and Programming (ICALP), LNCS*, volume 5125, pages 857–868, 2008.

[52] D. Nagaj and P. Wocjan. Hamiltonian quantum cellular automata in one dimension. *Phy. Rev. A.*, 78(3) :032311, 2008.

[53] M. A. Nielsen. Universal quantum computation using only projective measurement, quantum memory, and preparation of the 0 state. *Phys. Rev. A*, 308 :96–100, 2003.

[54] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.

[55] M. Ozawa. Halting of quantum Turing machines. In *UMC*, pages 58–65, 2002.

[56] S. Perdrix. State transfer instead of teleportation in measurement-based quantum computation. *International Journal of Quantum Information*, 3(1) :219–223, 2005.

[57] S. Perdrix. Partial observation of quantum turing machines and a weaker well-formedness condition. *Electronic Notes in Theoretical Computer Science*, 270(1) :99–111, 2011.

[58] S. Perdrix. Towards Observable Quantum Turing Machines : Fundamentals, Computational Power, and Universality. *International Journal of Unconventional Computing*, 7(4) :291–311, 2011. Special Issue : New Worlds of Computation - http ://www.oldcitypublishing.com/IJUC/IJUCcontents/IJUCv7n4contents.html.

[59] C. Pérez-Delgado and D. Cheung. Local unreversible cellular automaton ableitary quantum cellular automata. *Phys. Rev. A.*, 76(3) :32320, 2007.

[60] R. Prevedel, P. Walther, F. Tiefenbacher, P. Bohi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445(7123) :65–69, Jan. 2007.

[61] R. Raussendorf. Quantum cellular automaton for universal quantum computation. *Phys. Rev. A.*, 72(2) :22301, 2005.

[62] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86 :5188–5191, 2001.

[63] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2) :120–126, 1978.

[64] B. Schumacher and R. Werner. Reversible quantum cellular automata. arXiv pre-print quant-ph/0405174, 2004.

[65] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, pages 303–332, 1999.

[66] S. Succi and R. Benzi. Lattice boltzmann equation for quantum mechanics. *Physica D : Nonlinear Phenomena*, 69(3) :327–332, 1993.

[67] J. Twamley. Quantum cellular automata quantum computing with endohedral fullerenes. *Phys. Rev. A.*, 67(5) :52318–52500, 2003.

[68] W. Van Dam. Quantum cellular automata. Masters thesis, University of Nijmegen, The Netherlands, 1996.

[69] K. G. H. Vollbrecht and J. I. Cirac. Reversible universal quantum computation within translation-invariant systems. *Phys. Rev. A.*, 73(1), 2006.

[70] J. von Neumann. *Theory of Self-Reproducing Automata*. University of Illinois Press, Champaign, IL, USA, 1966.

[71] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030) :169–176, Mar. 2005.

[72] J. Watrous. On one-dimensional quantum cellular automata. *Complex Systems*, 5(1) :19–30, 1991.

[73] A. Yao. Quantum circuit complexity. In *Proc. 34th IEEE Symposium on Foundation of Computer Science*, 1993.