

Introduction à l'algorithmique quantique

François Schwarzentruber

4 mai 2022

“I think I can safely say that nobody understands quantum mechanics.”

Richard Feynman

<https://francoisschwarzentruber.github.io/quantumalgorithmcats/>

1 Motivation

1.1 Quelques applications

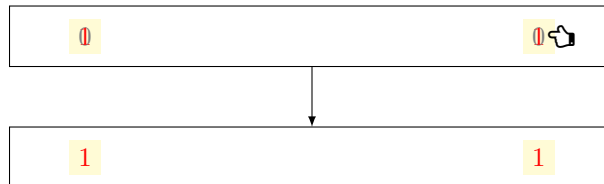
- Problème de factorisation d'un nombre entiers : Algorithme de Shor [Sho94]
- Problème de recherche d'une solution : Algorithme de Grover [Gro96]
- Simulation numérique pour développer de nouveaux médicaments [LWG⁺10]
- Utilisation d'un ordinateur quantique pour comprendre la matière et la physique quantique [PODDB⁺12] [SKPK19]
- Apprentissage automatique quantique [BWP⁺17]

1.2 Avantage de la physique quantique

Superposition : le système est dans plusieurs états physiques



Intrication : quand changer un qubit en affecte un autre



Archétype d'un algorithme quantique qui parallélise le calcul

5	3		7				
6		1	9	5			
	9	8				6	
8			6				3
4		8	3				1
7			2				6
	6				2	8	
		4	1	9			5
			8			7	9

construction d'état quantique superposé

5	3		7				
6		1	9	5			
	9	8				6	
8			6				3
4		8	3				1
7			2				6
	6				2	8	
		4	1	9			5
			8			7	9

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

mesure

Amplification de la bonne solution

1.3 Un effort industriel

IBM	https://quantum-computing.ibm.com Bibliothèque Python3 qiskit Open Quantum Assembly Language (OpenQASM)
Atos	Bibliothèque Python3 pyAQASM aQASM
Microsoft	Q#
Google	https://quantumai.google/

1.4 Comparaison ordinateur classique VS quantique

	ordinateur classique	ordinateur quantique
unité d'information	bit $\in \{0, 1\}$	qubit $\in \mathbb{C}^{\{0,1\}}$
mémoire	n bits	n qubits
état d'un programme	état physique $s \in \{0, 1\}^n$	superposition d'états physiques $s \in \mathbb{C}^{\{0,1\}^n}$
calcul	déterministe	déterministe
mesure	déterministe	probabiliste

2 États quantiques

Définition 1 (état quantique) Un état quantique¹ sur n qubits est un vecteur de $\mathbb{C}^{\{0,1\}^n}$ de norme 1. Les coordonnées sont repérées par des suites de bits de longueur n .

Notation 2 (notation de Dirac - bra-ket) On utilise la notation $|\alpha\rangle$ pour désigner un vecteur $\alpha \in \mathbb{C}^{\{0,1\}^n}$. Si $|\alpha\rangle \in \mathbb{C}^{\{0,1\}^n}$, on note $|\alpha\rangle = \sum_{u \in \{0,1\}^n} \alpha_u |u\rangle$.

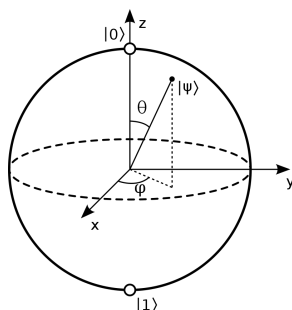
Notation 3 (état classique) Soit $u \in \{0, 1\}^n$. Le vecteur unité où toutes les coordonnées sont nulles sauf la u -coordonnée qui vaut 1 se note $|u\rangle$. Un tel vecteur représente un *état classique*.

2.1 Exemple d'un qubit ($n = 1$)

Notation 4

- $|0\rangle$ est le vecteur $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et désigne le qubit avec spin up.
- $|1\rangle$ est le vecteur $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et désigne le qubit avec spin down.
- Un état quantique d'un qubit est un vecteur $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$, noté $a|0\rangle + b|1\rangle$ où $a, b \in \mathbb{C}$ avec $|a|^2 + |b|^2 = 1$.

Remarque 5 (sphère de Bloch) L'état quantique d'un qubit est un point sur la sphère de Bloch :



$$\cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle$$

1. En réalité, c'est modulo un décalage de phase donc il faut quotienter l'ensemble des vecteurs de norme 1 de $\mathbb{C}^{\{0,1\}^n}$ par la relation \sim définie par $|x\rangle \sim |y\rangle$ ssi il existe $\alpha \in \mathbb{C}$ de norme 1 avec $|x\rangle = \alpha|y\rangle$. Mais, nous n'avons pas besoin de cette lourdeur administrative dans ce cours.

2.2 Exemple de deux qubits

Notation 6 (état classique) Avec 2 qubits, les quatre états classiques sont $|00\rangle$, $|01\rangle$, $|10\rangle$ et $|11\rangle$ qui sont :

$$|00\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Ainsi, l'état quantique de deux qubits est un vecteur $\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ de \mathbb{C}^4 que l'on note $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

où $a, b, c, d \in \mathbb{C}$ avec $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

Exemple 7 (état de Bell) L'état de Bell est l'état d'intrication suivant : $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

2.3 Exemple de trois qubits

Avec 3 qubits, les états physiques sont $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$ qui sont :

$$|000\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |001\rangle := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |010\rangle := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |011\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |100\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |101\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |110\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |111\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Un état quantique de 3 qubits est un vecteur $\sum_{x \in \{0,1\}^3} \alpha_x |x\rangle$ dans $\mathbb{C}^{\{0,1\}^3}$ avec $\sum_{x \in \{0,1\}^3} |\alpha_x|^2 = 1$:

$$\alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \alpha_{010} |010\rangle + \alpha_{011} |011\rangle + \alpha_{100} |100\rangle + \alpha_{101} |101\rangle + \alpha_{110} |110\rangle + \alpha_{111} |111\rangle.$$

3 Mesure

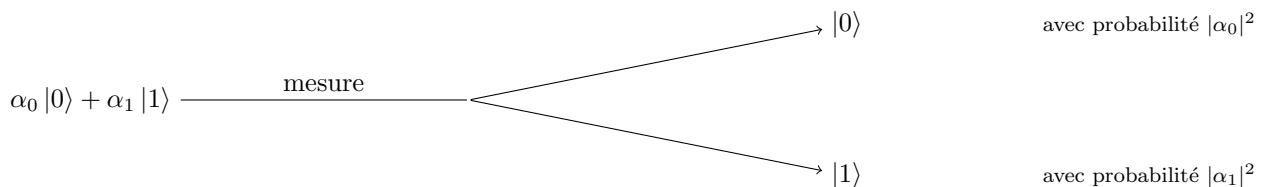
3.1 Mesure complète d'un état

Définition 8 (mesure complète) Considérons l'état $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$ où $\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$.

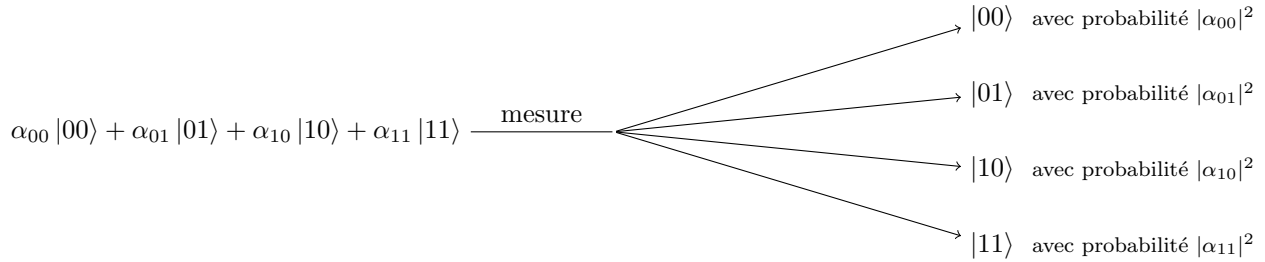
La mesure de cet état s'effectue comme suit :

1. le système choisit $x \in \{0, 1\}^n$ avec une probabilité de $|\alpha_x|^2$;
2. l'utilisateur lit cette valeur de x ;
3. le nouveau état devient l'état physique $|x\rangle$.

3.1.1 Mesure d'un qubit

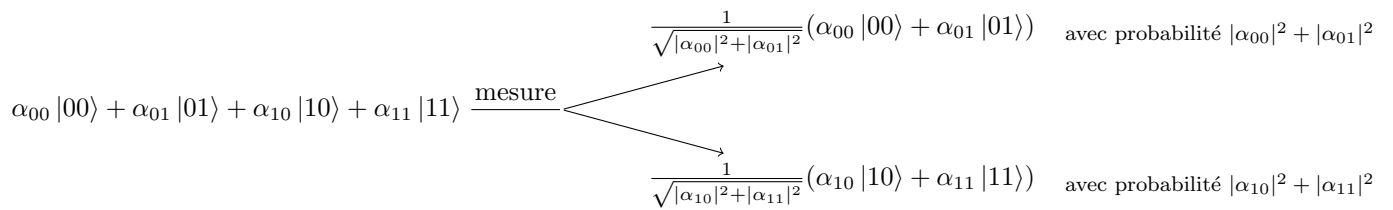


3.1.2 Mesure de deux qubits



3.2 Mesure partielle

3.2.1 Mesure partielle du premier bit parmi deux qubits



3.3 En général

Définition 9 (mesure d'un sous-ensemble de qubits) Soit l'état $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$ où $\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$.

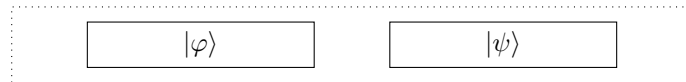
La mesure des qubits $J \subseteq \{1, \dots, n\}$ s'effectue comme suit :

1. la nature choisit $(y_j)_{j \in J} \in \{0, 1\}^J$ avec une probabilité de $\sum_{x \in \{0,1\}^n |x_J = y_J} |\alpha_x|^2$.
2. L'utilisateur lit la valeur choisie $(y_j)_{j \in J} \in \{0, 1\}^J$.
3. Le nouvel état est :

$$\frac{1}{\sqrt{\sum_{x \in \{0,1\}^n |x_J = y_J} |\alpha_x|^2}} \sum_{x \in \{0,1\}^n |x_J = y_J} \alpha_x |x\rangle.$$

4 Intrication et produit tensoriel

Soit deux systèmes indépendants (*non intriqués*) d'états quantiques respectifs $|\varphi\rangle$ et $|\psi\rangle$. Le produit tensoriel $|\varphi\rangle \otimes |\psi\rangle$ représente l'état quantique du système global.



Définition 10 (produit tensoriel) Soit $|\varphi\rangle = \sum_{x \in \{0,1\}^n} \varphi_x |x\rangle$ dans \mathbb{C}^{2^n} et $|\psi\rangle = \sum_{y \in \{0,1\}^k} \psi_y |y\rangle$ dans \mathbb{C}^{2^k} .

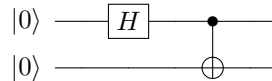
Le produit tensoriel de $|\varphi\rangle$ et $|\psi\rangle$ est le vecteur $\mathbb{C}^{2^{n+k}}$ défini par :

$$|\varphi\rangle \otimes |\psi\rangle = \sum_{x \in \{0,1\}^n, y \in \{0,1\}^k} \varphi_x \psi_y |xy\rangle.$$

5 Circuits quantiques

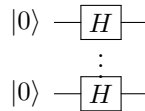
Porte	Effet	Matrice (unitaire)
Négation	$ 0\rangle \xrightarrow{\text{NOT}} 1\rangle$ $ 1\rangle \xrightarrow{\text{NOT}} 0\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Hadamard	$ 0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} 0\rangle + \frac{1}{\sqrt{2}} 1\rangle$ $ 1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} 0\rangle - \frac{1}{\sqrt{2}} 1\rangle$	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Non contrôlé	$ 00\rangle \xrightarrow{\text{CNOT}} 00\rangle$ $ 10\rangle \xrightarrow{\text{CNOT}} 11\rangle$ $ 01\rangle \xrightarrow{\text{CNOT}} 01\rangle$ $ 11\rangle \xrightarrow{\text{CNOT}} 10\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Décalage de phase contrôlé	$ 00\rangle \xrightarrow{\text{CNOT}} 00\rangle$ $ 10\rangle \xrightarrow{\text{CNOT}} 10\rangle$ $ 01\rangle \xrightarrow{\text{CNOT}} 01\rangle$ $ 11\rangle \xrightarrow{\text{CNOT}} e^{i\theta} 11\rangle$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$

Exemple 11 (mon premier circuit quantique)



Exemple 12 (portes de Hadamard en parallèle) Sur $|0\dots 0\rangle$, l'application de n portes de Hadamard en parallèle donne :

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}^n} \sum_{u \in \{0,1\}^n} |u\rangle.$$



6 Algorithme de Grover

Dans toute cette section, n désigne le nombre de qubits et $M = 2^n$ le nombre d'états physiques possibles.

6.1 Problème de recherche d'une solution

Recherche d'une solution

entrée : une boîte noire implémentant $f : \{0, 1\}^n \rightarrow \{0, 1\}$ telle qu'il existe un unique $\sigma \in \{0, 1\}^n$ tel que $f(\sigma) = 1$.
 sortie : l'élément σ

Exemple 13 Considérons une grille de Sudoku qui admet une unique solution σ .

5	3		7					
6			1	9	5			
	9	8				6		
8			6					3
4			8		3			1
7			2					6
	6					2	8	
			4	1	9			5
			8				7	9

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

solution σ

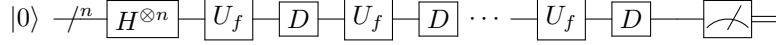
On considère la fonction

$$f : \{0, 1\}^n \rightarrow \begin{cases} \{0, 1\} \\ 1 & \text{si } x \text{ respecte les contraintes du Sudoku} \\ 0 & \text{sinon} \end{cases}$$

Proposition 14 L'algorithme déterministe naïf pour décider la recherche d'une solution est en temps $\Theta(2^n)$ dans le pire cas, si on suppose que la boîte noire est en $O(1)$.

6.2 Principe de l'algorithme

Algorithme de Grover



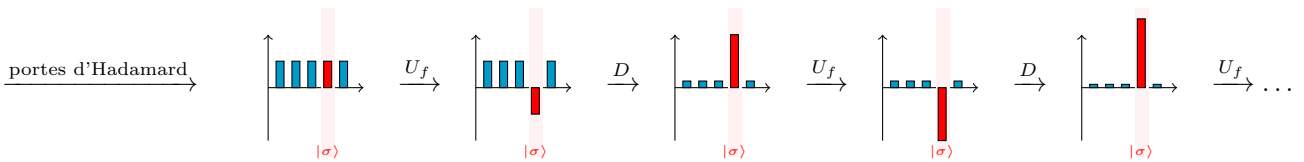
où

- $H^{\otimes n}$ représente n portes Hadamard en parallèle, une sur chaque qubit ;
- U_f est un circuit qui représente la fonction f de la façon suivante :

$$U_f(x) = \begin{cases} -x & \text{si } x = \sigma \\ x & \text{sinon} \end{cases}$$

- D est appelé l'opérateur de diffusion de Grover défini par la matrice :

$$\begin{pmatrix} 2/M - 1 & 2/M & \cdots & 2/M \\ 2/M & 2/M - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 2/M \\ 2/M & \cdots & 2/M & 2/M - 1 \end{pmatrix}$$



Remarque 15 (implémentation de D) On a :

$$D = H^{\otimes n} R H^{\otimes n}$$

où $H^{\otimes n}$ est la matrice pour n portes Hadamard en parallèle et $R = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & \cdots & 0 & -1 \end{pmatrix}$.

6.3 Effet des itérations

Notation 16 (somme des états physiques autres que σ) $|\rho\rangle := \sum_{x \in \{0,1\}^n, x \neq \sigma} |x\rangle$.

Proposition 17 La k -ème itération de $U_f D$ est :

$$s_{k-1}|\sigma\rangle + r_{k-1}|\rho\rangle \xrightarrow{U_f} -s_{k-1}|\sigma\rangle + r_{k-1}|\rho\rangle \xrightarrow{D} s_k|\sigma\rangle + r_k|\rho\rangle$$

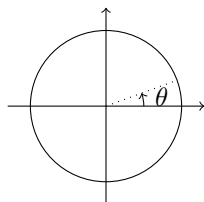
avec $s_0 = r_0 = \frac{1}{\sqrt{M}}$;

$s_{k+1} := \left(\frac{M-2}{M}s_k + 2\frac{M-1}{M}r_k\right)$ et $r_{k+1} := \left(-\frac{2}{M}s_k + \frac{M-2}{M}r_k\right)$.

6.4 Calcul du nombre d'itérations

Proposition 18 Soit $\theta \in]0, \frac{\pi}{2}[$ l'angle tel que $\sin \theta = \frac{1}{\sqrt{M}}$. Pour tout entier $k \geq 0$, on a :

$$s_k = \sin((2k+1)\theta) \quad r_k = \frac{1}{\sqrt{M-1}} \cos((2k+1)\theta)$$



Théorème 19 Après $O(\sqrt{M})$ itérations, on mesure σ avec une probabilité $\geq 1 - \frac{1}{M}$.

7 Transformée de Fourier quantique

7.1 Rappel du problème

Soit $M = 2^n$.

Définition 20 Transformée de Fourier

entrée : $(a_0, \dots, a_{M-1}) \in \mathbb{C}^M$, une racine M -ème primitive de l'unité ω ;
sortie : $A(\omega^0), A(\omega), \dots, A(\omega^{M-1})$ où $A = \sum_{i=0}^{M-1} a_i X^i$.

7.2 Algorithme classique

entrée : des nombres a_0, \dots, a_{M-1} , et une racine M -ème de l'unité primitive ω

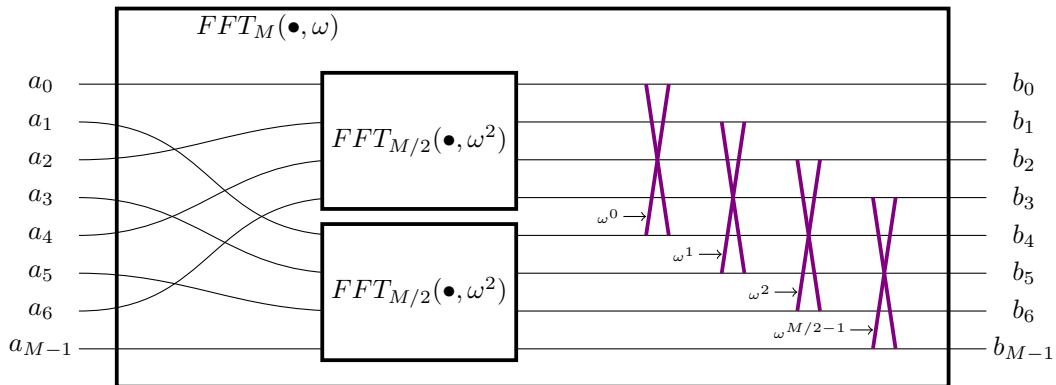
sortie : $A(\omega^0), A(\omega), \dots, A(\omega^{M-1})$ où $A = \sum_{i=0}^{M-1} a_i X^i$

fonction $FFT(a_0, \dots, a_{M-1}, \omega)$

```

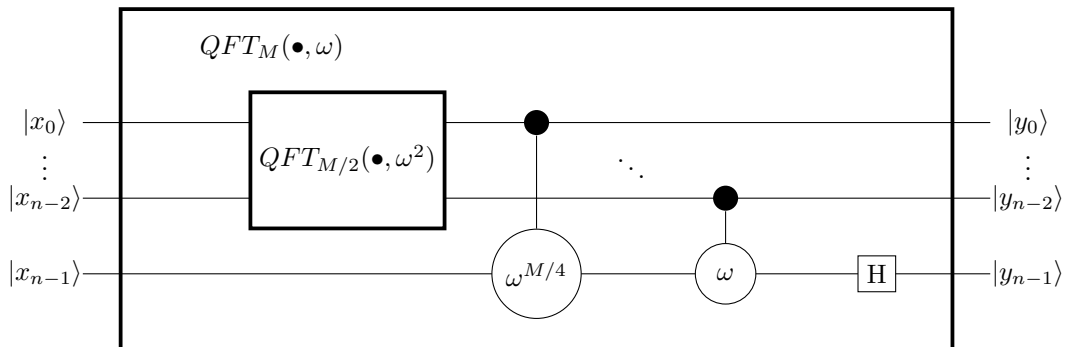
si  $M = 1$ 
  renvoyer  $a_0$ 
sinon
   $(s_0, \dots, s_{M/2-1}) := FFT(a_0, a_2, \dots, a_{M-2}, \omega^2)$ 
   $(s'_0, \dots, s'_{M/2-1}) := FFT(a_1, a_3, \dots, a_{M-1}, \omega^2)$ 
  pour  $k = 0$  à  $M/2 - 1$ 
     $b_k := s_k + \omega^k s'_k$ 
     $b_{k+M/2} := s_k - \omega^k s'_k$       opération papillon
  renvoyer  $b_0, \dots, b_{M-1}$ 
  
```

Proposition 21 La FFT réalise le calcul en $O(M \log M)$.



7.3 Circuit quantique

Le circuit est composé d'abord de l'appel récursif qui réalise la "FFT en parallèle" sur les $n - 1$ premiers qu-bits. Puis on a des portes de changement de phase contrôlé. Par exemple, la première porte vient modifier la phase en multipliant par $\omega^{M/4}$ pour toutes les coordonnées x où $x_0 = x_{n-1} = 1$. Pour les autres coefficients x , cette porte ne modifie pas le coefficient devant x . La deuxième porte vient modifier la phase en multipliant par $\omega^{M/8}$ pour toutes les coordonnées x où $x_1 = x_{n-1} = 1$, etc. Cette suite de changement de phase correspond au calcul de $\omega^j s'_k$ qui est un préalable à l'opération papillon. Enfin, les opérations papillon sont réalisées par une porte d'Hadamard sur le dernier qu-bit (oui oui, ça marche, on le verra plus calmement dans la démonstration de correction!).



En sortie, on récupère le résultat de la FFT mais normalisée (car il faut que le module du vecteur soit 1).

Proposition 22 *QFT* est en temps $O(\log^2 M)$.

Théorème 23 Pour tout (a_0, \dots, a_{M-1}) ,

$$QFT_{M,\omega} \left(\sum_{u \in \{0,1\}^n} a_u |u\rangle \right) = \frac{1}{\sqrt{M}} \sum_{u \in \{0,1\}^n} b_u |u\rangle$$

où $(b_0, \dots, b_{M-1}) = FFT(a_0, \dots, a_{M-1}, \omega)$.

8 Notes bibliographiques

Le dernier chapitre de [DPV06] est plaisant et a été beaucoup utilisé pour fabriquer ce cours. Le seul souci est qu'il présente l'algorithme de Shor : très intéressant mais rien n'est fait proprement, et pour cause, l'algorithme de Shor requiert un peu de théorie des nombres, et beaucoup de calculs avec la FFT etc. J'ai donc relayé la QFT et Shor à la fin. J'ai préféré présenter au début l'algorithme de Grover, plus simple à comprendre. L'algorithme de Grover a été proposé en 1996 [Gro96]. Attention la démonstration de correction dans l'article original [Gro96] contient quelque erreurs. L'algorithme de Grover est optimal (dans un certain sens) [BBBV97]. Pour des informations sur l'implémentation, consulter [NO10] et [CEP⁺18].

Références

- [BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5) :1510–1523, 1997.
- [BWP⁺17] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671) :195–202, 2017.
- [CEP⁺18] Patrick J. Coles, Stephan J. Eidenbenz, Scott Pakin, Adetokunbo Adedoyin, John Ambrosiano, Petr M. Anisimov, William Casper, Gopinath Chennupati, Carleton Coffrin, Hristo N. Djidjev, David Gunter, Satish Karra, Nathan Lemons, Shizeng Lin, Andrey Y. Lokhov, Alexander Malyzhenkov, David Dennis Lee Mascarenas, Susan M. Mniszewski, Balu Nadiga, Dan O'Malley, Diane Oyen, Lakshman Prasad, Randy Roberts, Philip Romero, Nandakishore Santhi, Nikolai Sinitsyn, Pieter Swart, Marc Vuffray, Jim Wendelberger, Boram Yoon, Richard J. Zamora, and Wei Zhu. Quantum algorithm implementations for beginners. *CoRR*, abs/1804.03719, 2018.
- [DPV06] S. Dasgupta, C.H. Papadimitriou, and U.V. Vazirani. Algorithms. 2006.
- [Gro96] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.
- [LWG⁺10] Benjamin P Lanyon, James D Whitfield, Geoff G Gillett, Michael E Goggin, Marcelo P Almeida, Ivan Kassal, Jacob D Biamonte, Masoud Mohseni, Ben J Powell, Marco Barbieri, et al. Towards quantum chemistry on a quantum computer. *Nature chemistry*, 2(2) :106–111, 2010.
- [NO10] Mikio Nakahara and Tetsuo Ohmi. *Quantum computing : from linear algebra to physical realizations*. Taylor & Francis, 2010.
- [PODDB⁺12] Alejandro Perdomo-Ortiz, Neil Dickson, Marshall Drew-Brook, Geordie Rose, and Alán Aspuru-Guzik. Finding low-energy conformations of lattice protein models by quantum annealing. *Scientific reports*, 2(1) :1–7, 2012.
- [Sho94] Peter W. Shor. Algorithms for quantum computation : Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134. IEEE Computer Society, 1994.
- [SKPK19] Adam Smith, MS Kim, Frank Pollmann, and Johannes Knolle. Simulating quantum many-body dynamics on a current digital quantum computer. *npj Quantum Information*, 5(1) :1–13, 2019.