Théorie des nombres algorithmique

2024-2025

Table des matières

Introduction

Le cours discute l'algorithmique quantique et le but c'est l'algo de Shor [Sho97] !

Révolution du XXe en physique

Experience de Young :

- Un atome par un à travers les fentes de Young. Les atomes semblent interférer avec les autres anciencs atomes.

Invariance de la vitesse de la lumière par rapport au référentiel (Boltzmann$\to$Einstein).

Expèrience de Dirac :

- Polarisation des photons : plan polarisé agit comme un produit scalaire pour laisser passer la lumière.

Heisenberg-Schrödinger

L'état d'un système physique est décrit par une fonction d'onde (vecteur unitaire) d'un espace de Hilbert dépendant du système. Pour

- une seule particule, l'espace de Hilbert associé à une particule est

  $$\mathscr{H}_1 = L^2(\mathbb{R}^3, \mathbb{C})$$

  Où la probabilité de position dans l'espace de la particule.

- Pour deux particules

  $$\mathscr{H}_2 = L^2(\mathbb{R}^3 \times \mathbb{R}^3, \mathbb{C})$$

  qui n'est pas isomorphe à $\mathscr{H}_1 \times \mathscr{H}_1$, l'idée est que les deux particules peuvent être intriquées, par contre

  $$\mathscr{H}_2 = \mathscr{H}_1 \otimes \mathscr{H}_2$$

- Pour une polarisation : $\mathscr{H} = \mathbb{C}^2 = \mathbb{C}|\uparrow> \oplus \mathbb{C}|\rightarrow>$.
- Pour deux polarisations : $\mathscr{H} = \mathbb{C}^4 = \mathbb{C}|\uparrow\uparrow> \oplus \mathbb{C}|\uparrow\rightarrow> \otimes \mathbb{C}|\rightarrow\uparrow> \otimes \mathbb{C}|\rightarrow\rightarrow>$
- Pour n polarisations : $\mathbb{C}^{2^n}$ avec 2^n états.

Si on regarde maintenant l'équation de Schrödinger

$$\frac{d|\psi>}{dt} = H|\psi>$$

où H est l'Hamiltonien $H\colon \mathscr{H} \to \mathscr{H}$ qui est linéaire auto-adjoint. On a la notion de mesure encodée par un observable

$$O\colon \mathscr{H} \to \mathscr{H}$$

auto-adjoint, on a $|\psi> \in \mathscr{H} = \bigoplus_\lambda \mathscr{H}_\lambda$ et

$$\begin{aligned} |\psi> &= \sum_\lambda \psi_\lambda \\ &= \sum_\lambda ||\psi_\lambda^2|| = 1 \end{aligned}$$

Ce que ca dit c'est que deux mesures du même système peuvent être différentes, et surtout, quand on *mesure*, on est projetés sur un état et les nouvelles mesures sont projetées au même endroit. On obtient λ en sortie avec $||\psi_\lambda||^2$. Après la mesure, la fonction d'onde devient $\frac{\psi_\lambda}{||\psi_\lambda||^2}$.

Avec l'exemple d'une particule, $\mathscr{H} = L^2(\mathbb{R}^3, \mathbb{C})$:

- La position en x : $O\colon \mathscr{H} \to \mathscr{H}; f \mapsto x.f$.
- La vitesse en x : $O\colon \mathscr{H} \to \mathscr{H}; f \mapsto \partial f/\partial x$.

!!! Pour avoir des mesures cohérentes faut que les observables commutent. Et la par exemple les deux commutent pas!

Aussi, Einstein Podoloski ROsen (EPR) croyaient pas à ce formalisme. La raison c'est la fonction à trappe $|\psi> = |\uparrow\uparrow> + |\rightarrow\rightarrow>$ qui au moment de la mesure d'une des deux polarisations on projette sur un des deux facteurs de sorte que la deuxième polarisation doit être la même! (Key agreement existe!!)

Références pour le cours

Un livre : N. Mermin, Quantum Computer Science, an introduction.

Chapitre 1

L'ordinateur quantique

1.1 Les qubits (q-bits)

Définition 1.1.1. Soit $n \geq 1$. Un n-qubit est une somme formelle de la forme

$$w \in 0, 1^n a_w | w >$$

avec $a_w \in \mathbb{C}$. Il est normalisé si $\sum_{w \in \{0,1\}^n} |a_w|^2 = 1$.

Exemple 1.1.2. Si $n = 1$, on peut avoir $\alpha|0> +\beta|1>$, $\alpha, \beta \in \mathbb{C}$.

L'ensemble des n-qubits est un espace de Hilbert de dimension 2^n, i.e. c'est un $\mathbb{C}$-espace vectoriel avec un produit hermitien : $< \sum_w a_w|w > , \sum_w b_w|w >>= \sum_w \bar{a}_w b_w$ où la base est supposée orthogonale. On a aussi un produit tensoriel donné par la concaténation des chaines de bits.

Remarque 1. *Le* 2*-qubit*

$$|00> +|11>$$

n'est pas un produit de 1*-qubits! Cet état est dit intriqué, l'idée est que sinon on peut réduire le calcul à celui sur les* 1*-qubits.*

1.2 Les portes

Pour pouvoir imaginer des portes utilisables en pratique, on doit avoir des portes qui sont des isomorphismes et des isométries;

Définition 1.2.1. La porte X inverse $|0>$ et $|1>$.

Définition 1.2.2. La porte CX, où C est pour *controlled* tel que

- $|00> \mapsto |00>$

- $|01> \mapsto |01>$
- $|10> \mapsto |11>$
- $|11> \mapsto |01>$

Faut imaginer que le premier bit agit sur le deuxième par une porte X si c'est 1.

Définition 1.2.3. La porte CCX,

- $|00x> \mapsto |00x>$
- $|01x> \mapsto |01x>$
- $|10x> \mapsto |11x>$
- $|110> \mapsto |111>$
- $|111> \mapsto |110>$

Pareil qu'avant mais avec les deux premiers bits. Apparemment on a tout les algorithmes classiques avec ces trois portes. La prochaine est non classique.

Définition 1.2.4. La porte de Hadamard H,

- $|0> \mapsto \frac{|0>+|1>}{2}$
- $|1> \mapsto \frac{|0>-|1>}{2}$

avec lequel on obtient des états intriqués.

Définition 1.2.5. La porte de changement de phase R_θ avec $\theta \in \mathbb{R}$,

- $|0> \mapsto |0>$
- $|1> \mapsto e^{i\theta}|1>$

Définition 1.2.6 (Porte booléenne). Soit $f\colon \{0,1\}^n \to \{0,1\}^m$, on déf la porte

$$U_f(|x>|y>) = |x>|y \oplus f(x)>$$

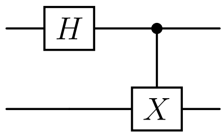
sur une base, puis on étend par linéarité.

Remarque 2. *C'est bien une bijection peu importe f.*

1.3 Circuits

Un fil est censé représenter une entrée, en pratique on met un fil pour une entrée de n-bits mais vaudrait mieux en mettre n pour les portes CX par exemple.

Exemples 1.3.1. Un exemple avec la porte hadamard :



On a

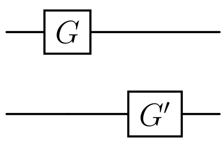
$$|00> \mapsto \frac{|0> + |1>}{\sqrt{2}}|0> \mapsto \frac{|00> + |11>}{\sqrt{2}}$$

Autrement dit on peut créer l'état EPR avec deux portes, c'est la force d'un ordinateur quantique! La deuxième partie du calcul c'est parce que c'est une porte CX. On a aussi

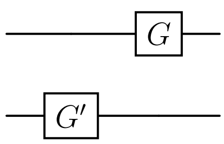
$$|01> \mapsto \frac{|01> + |10>}{\sqrt{2}}.$$

Les portes Hadamard, X, CX ont ordre 2 et R_θ est additive.

Exemple 1.3.2. Attention au diagramme :



qui équivaut à



Le point c'est juste que $G\colon |x > |y > \mapsto G(|x >)|y >$ et pas $G\colon |x > |y > \mapsto |G(x) > |y >$ par exemple si G est la porte Hadamard.

1.4 Mesures

Ça a l'air compliqué mdr. On assume qu'on a un n-qubit normalisé q. On veut mesurer le premier bit. Faut rappeler que

$$q = \sum_{w \in \{0,1\}^n} a_w |w>$$

ducoup c'est pas clair *mesurer le premier bit.* On réecrit

$$q = |0> \otimes q_0 + |1> \otimes q_1$$

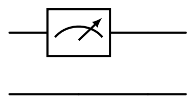
, on peut le faire là on a juste distingué les deux premierrs bits. On remarque qu'alors

$$||q_0||^2 + ||q_1||^2 = ||q||^2 = 1$$

La mesure est censée donner 0 avec probabilité $||q_0||^2$ et donner 1 avec probabilité $||q_1||^2$.

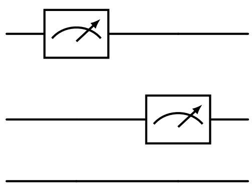
À ce stade q est détruit et on a remplacé q par $|i> \otimes \frac{q_i}{||q_i||^2}$. Autrement dit, si on refait la mesure on obtient i avec probabilité 1.

Définition 1.4.1 (Mesure)**.** On écrit

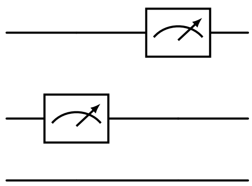


Pour dire qu'on fait une mesure.

Proposition 1.4.2. *] Les mesures de premier et deuxième bit*

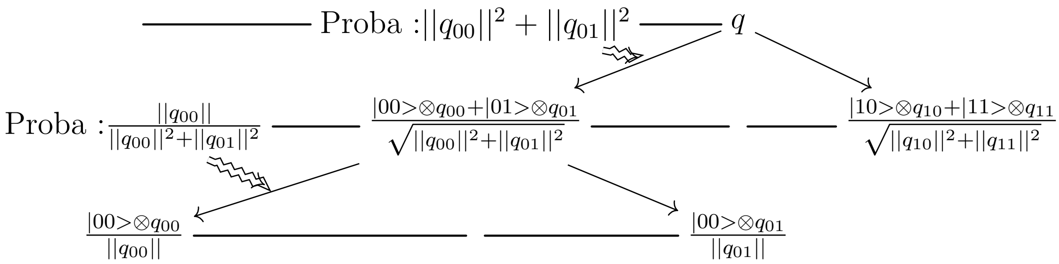


et



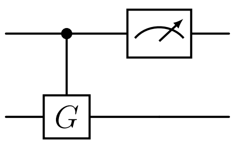
sont équivalentes.

Preuve. Si on écrit $q = |00> \otimes q_{00} + |01> \otimes q_{01} + |10> \otimes q_{10} + |11> \otimes q_{11}$, on peut écrire :

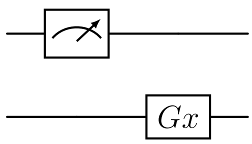


En particulier, on a ij avec proba $||q_{ij}||^2$! □

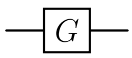
Proposition 1.4.3. *Les deux circuits*



et



sont équivalents. Où Gx est donnée par



Si $x = 1$ et

sinon.

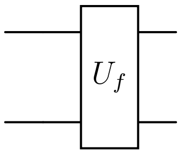
Chapitre 2

Premiers algorithmes quantiques

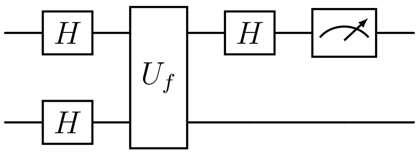
2.1 L'algorithme Deutsch-Jozsa

Problème 1. Étant donné $f\colon \{0,1\} \to \{0,1\}$ décider si $f(0) = f(1)$.

L'idée c'est que dans le monde classique, on est obligés de calculer $f(0)$ et $f(1)$ alors que dans le monde quantique on peut le faire en une fois. La fonction f est représentée par la porte



Proposition 2.1.1 (Circuit Deutsch)**.** *Le circuit*



résoud le problème précédent.

Preuve. On fait rentrer $|0>$ sur les deux inputs. On a à l'étape 1

$$
\begin{aligned}
|0>|0> \mapsto & (\frac{|0> + |1>}{\sqrt{2}}) \otimes (\frac{|0> - |1>}{\sqrt{2}}) \\
= & \frac{1}{2}(|00> - |01> + |10> - |11>)
\end{aligned}
$$

Puis à l'étape 2

$$\begin{aligned} U_f(|x>|y>) &= |x>|y \oplus f(x)> \\ &= \frac{1/2}{(}|0>|f(0)> - |0>|\bar{f}(0)> \\ &+ |1>|f(1)> - |1>|\bar{f}(1)>) \end{aligned}$$

À l'étape 3 on a un gros truc

$$\begin{aligned} \frac{1}{2\sqrt{2}}&(|0>|f(0)> + |1>|f(0)> \\ &- |0>|\bar{f}(0)> - |1>|\bar{f}(0)> \\ &+ |0>|f(1)> - |1>|f(1)> \\ &- |0>|\bar{f}(1)> + |1>|\bar{f}(1)>) \end{aligned}$$

Si $f(0) = f(1) = a$, on obtient

$$\begin{aligned} \frac{1}{2\sqrt{2}}&([0a> + |1a> - |0\bar{a}> - |1\bar{a}> \\ &+ |0a> - |1a> - |0\bar{a}> + |1\bar{a}>) \\ &= \frac{1}{2\sqrt{2}}(|0a> - |0\bar{a}>) \end{aligned}$$

Sinon avec $f(0) = a$ et $f(1) = \bar{a}$, on obtient

$$\frac{1}{\sqrt{2}}(|1a> - |1\bar{a}>)$$

On mesure donc le premier bit à 0 avec probabilité 1 si $f(0) = f(1)$ et on mesure 1 avec probabilité 1 si $f(0) = \bar{(}f(1))$. □

Problème 2. Étant donné une fonction booléenne $f\colon \{0,1\}^n \to \{0,1\}$ avec la promesse que f est constante, ou équilibrée $\#f^{-1}(0) = \#f^{-1}(1)$. Décider si f est équilibrée ou constante.

Dans le cas classique, on est plus ou moins obligé de tester f sur la moitié des entrées. Dans le cas quantique, on peut le faire en une évaluation.

Bibliographie

[Sho97] Peter W. Shor. « Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer ». In : *SIAM Journal on Computing* 26.5 (oct. 1997), p. 1484-1509. ISSN : 1095-7111. DOI : 10.1137/s0097539795293172. URL : http://dx.doi.org/10.1137/S0097539795293172.