Programmation quantique

Master informatique & GPEX MINERVE

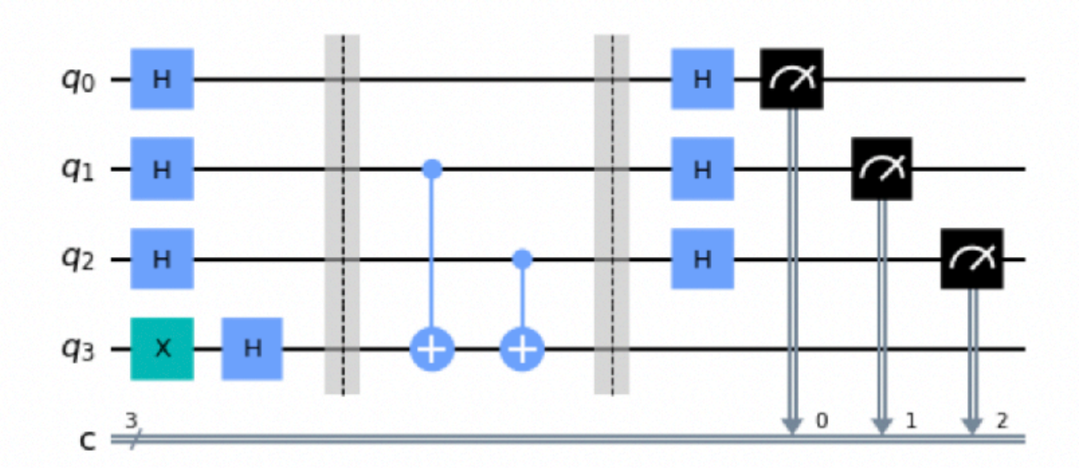
Nicolas Ollinger, Ioan Todinca

2024-2025

Découvrir l'informatique quantique à travers la programmation de circuits quantiques

Différence quantique/classique

- qubit, portes quantiques, circuits quantiques vs. bit, portes logiques, circuits booléens
- particularités du quantique : superposition, interférence, intrication, etc.
- éléments de programmation en Qiskit (notebook Python)



Volet plus culturel : promesses et enjeux du calcul quantique

Travaux pratiques à effectuer sur machine, en Qiskit

Plan

1. Promesses et enjeux du calcul quantique
2. Calcul quantique : différences avec le modèle classique
   - qubit, portes quantiques, circuits quantiques. Bases mathématiques.
   - Superposition. Intrication. Interférences « destructives »
3. Le problème de Bernstein-Vazirani et son algorithme quantique
4. Algorithme de Grover :
   - Accélération polynomiale mais…
   - … ce serait l'un des algorithmes les plus utiles dans la pratique
5. Impact du quantique sur l'informatique d'aujourd'hui et de demain
6. Conclusion et conseils de lecture

1. Promesses et enjeux du calcul quantique

- Plusieurs scientifiques s'interrogent au début des années 1980 sur l'utilisation de processus quantiques pour faire du calcul.
- Richard Feynman (prix Nobel de physique, fameux pour ses recherches mais aussi pour ses enseignements), "Simulating physics with computers." International Journal of Theoretical Physics, 1981 :
  "Can you do it with a new kind of computer — a quantum computer? Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements. It's not a Turing machine, but a machine of a different kind."
- David Deutsch. "Quantum theory, the Church–Turing principle and the universal quantum computer", 1985.
  Formalise la notion d'ordinateur quantique et pose la question d'avantages en termes de vitesse de calcul (complexité quantique versus classique). Premiers algorithmes surprenants.

1. Promesses et enjeux du calcul quantique

Ordinateur quantique : calcule les mêmes choses qu'avec une machine classique, en étant potentiellement plus efficace (complexité en temps) pour certains calculs.
1992-1997

- E. Bernstein et U. Vazirani. Accélération (polynomiale) d'un certain problème… cf. suite.
- L. Grover. Recherche d'une valeur en temps $O(\sqrt{N})$ — les algos classiques ont besoin de $\Theta(N)$.
- D. Simons. Accélération **exponentielle** d'un autre problème : calculer la période s d'une fonction $f : \{0,1\}^n \to \{0,1\}^n$ telle que $\forall x \neq y, f(x) = f(y) \Rightarrow x \oplus y = s$. Le problème semble artificiel mais…
- P. Shor s'en sert pour décomposer un nombre N en facteurs premiers, en temps polynomial par rapport à $\log N$. Calcule l'ordre r d'un nombre a, c-à-d le r minimum t.q. $a^r \equiv 1 \bmod N$, en
  On ne sait pas le faire avec un ordinateur classique. Si c'était faisable, de nombreux protocoles cryptographiques deviendraient facile à casser.

Si l'on avait des ordinateurs quantiques…

Certains calculs se feraient exponentiellement plus rapidement que sur des machines classiques. Il faudrait complètement revoir la cryptographie des cartes bancaires et autres !

Communication et cryptographie quantique : domaine le plus avancé (mais nous n'en parlerons presque pas).

Est-ce réalisable ?

- S. Haroche, J.-M. Raimond. Quantum computing: dream or nightmare? Physics Today, 49(8):51–54, 1996. Décohérence, erreurs inhérentes aux phénomènes quantiques. Ordinateur quantique : "The computer scientist's dream [but] the experimenter's nightmare."
- P. Shor (le même) : codes correcteurs d'erreurs, quantiques. En théorie, on peut avancer.
- En pratique ? L'algorithme de Shor a été implémenté en 2021 pour décomposer le nombre… 21. Il paraît que ça a donné 7×3. Pas de menace imminente sur la crypto…
- Des annonces de « suprématie quantique » pour des problèmes spécifiques… Discutables.
- Restons zen, l'avenir nous le dira. Beaucoup d'obstacles à franchir. Mais ça mérite de s'y pencher !

NISQ : Noisy Intermediate-Scale Quantum

L'état actuel des ordinateurs quantiques

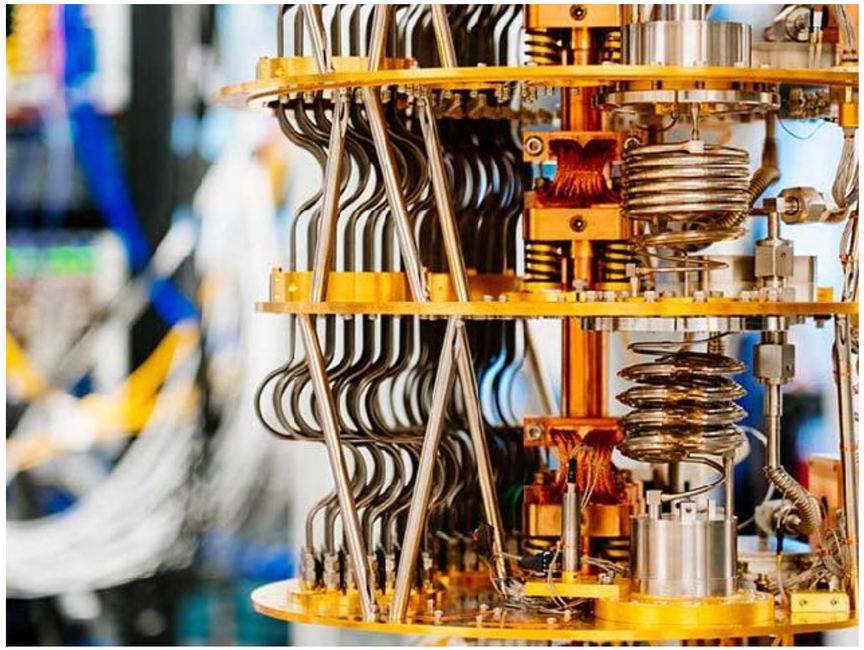


Image Google, Quantum AI Lab, Santa Barbara, USA

- Intermediate-scale : quelques dizaines de qubits
- Noisy : pas de correction d'erreurs
- Sycamore (Google), 53 qubits disposés selon une grille 2D. L'intrication d'un qubit est possible avec ses voisins sur la grille. Circuits avec une vingtaine de niveaux de portes, mesure à la fin.
- Héron (IBM), 133 puis 156 qubits, grille 2D
- Pasqual : ordinateur à base de recuit quantique

Exemples d'entreprises en France et à l'étranger

France : fortes compétences en physique (S. Haroche, A Aspect et « descendants »)

PASQAL

IBM

QUANDELA

Google

ALICE & BOB

D:WAVE
The Quantum Computing Company™

C12

QILIMANJARO
QUANTUM · TECH

IQuEra
COMPUTING INC.

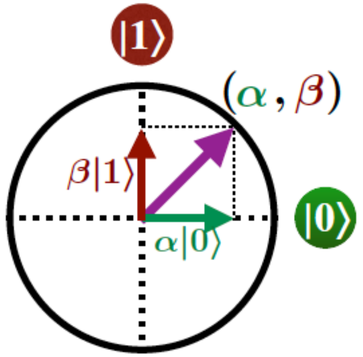
EVIDEN

émulation

parityqc

2. Calcul quantique — qubit, superposition

Ici : les calculs seront faits à l'aide de circuits quantiques. C'est un modèle universel. Pas le seul, cf. thèse Atos (Eviden, Bull)/LIFO d'Arthur Braida sur le **recuit quantique**.



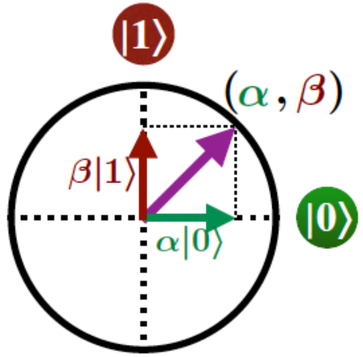
[F. Magniez, exposé Collège de France]

- qubit : **superposition** de $|0\rangle$ et de $|1\rangle$. Vecteur à 2 dimensions !
  $\alpha|0\rangle + \beta|1\rangle \quad$ avec $\quad \alpha, \beta \in \mathbb{C} \quad$ tels que $\quad |\alpha|^2 + |\beta|^2 = 1$
- La **superposition** est un phénomène quantique systématiquement exploité dans les algorithmes, à travers des états tels que
  $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ ou $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

2. Calcul quantique — qubit, mesure

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

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



La **mesure** d'un qubit donnera $|0\rangle$ ou $|1\rangle$... avec les probabilités ci-dessus.

Exercice. Décrire les issues possibles, avec leurs probabilités respectives, après avoir mesuré chacun des qubits suivants :

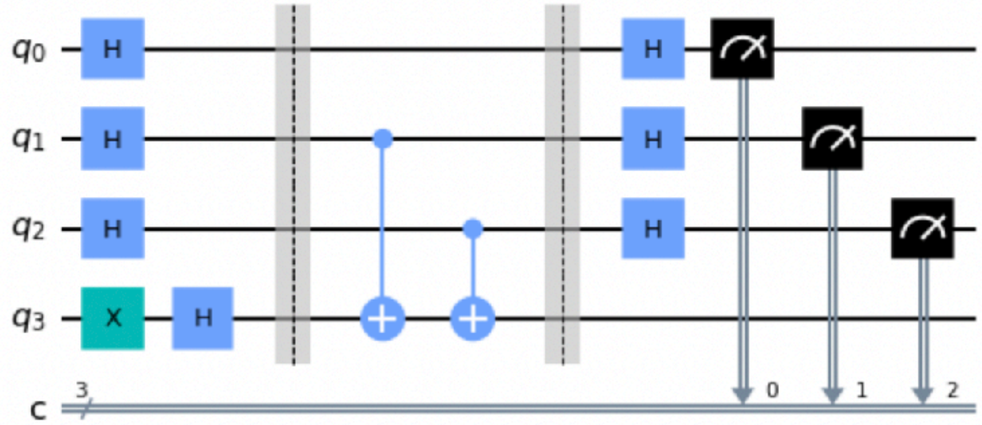
a. $|0\rangle$ b. $|1\rangle$ c. $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ d. $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

2. Calcul quantique — circuits, portes

Registre de n qubits, initialement tous à $|0\rangle$. Cela fait $N = 2^n$ possibilités, après mesure.

Portes : transformations $U : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$, unitaires, c.-à.-d. préservation de la norme + linéarité : $U\left(\alpha|\varphi\rangle + \beta|\psi\rangle\right) = \alpha U|\varphi\rangle + \beta U|\psi\rangle$

- composition séquentielle : produit de matrices
- composition parallèle : produit tensoriel, $|x\rangle \otimes |y\rangle = |xy\rangle$



N.B. Matrices de taille 2^n à coefficients complexes. Par linéarité, **il suffit de connaître le comportement pour tout $|x\rangle = |x_1 x_2 \ldots x_n\rangle$, avec x_i booléens**

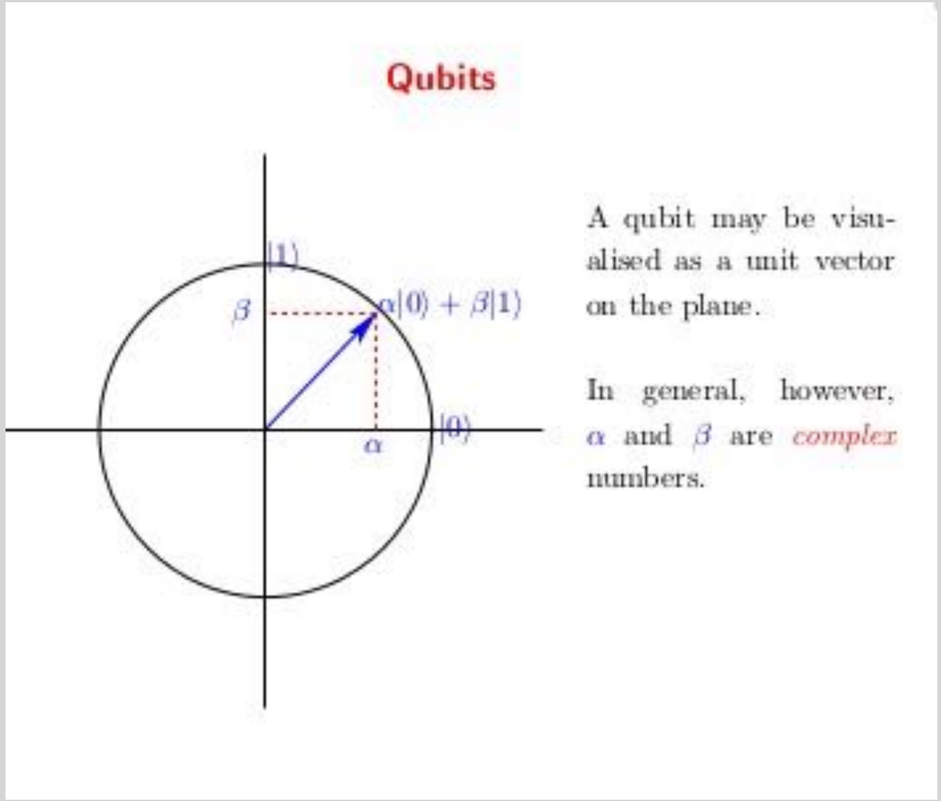
Sur les mathématiques derrière ces notations

« compliqué mais pas difficile » ; pas franchement intuitif

Un registre de n qubits correspond à un vecteur de dimension $N = 2^n$, à coefficients complexes.

Pour un qubit : $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$

Exemple : $\frac{|0\rangle + |1\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$



quora.com

Plusieurs qubits — notation de Dirac

(ou bra-ket)

Composition parallèle : produit tensoriel.

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\begin{bmatrix}0\\1\end{bmatrix}\\0\begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}$$

Les états de la forme $|x\rangle = |x_1 x_2 \ldots x_n\rangle$ avec $x_i \in \{0,1\}$ forment une base de l'espace vectoriel. Tout autre état s'écrit comme

$$|\varphi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle, \text{ avec } \alpha_x \in \mathbb{C} \text{ et } \sqrt{\sum_{x\in\{0,1\}^n} |\alpha_x|^2} = 1$$

Produit tensoriel $A \otimes B$ de deux matrices de taille $m \times n$ et $p \times q$: une matrice de taille $mp \times nq$

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$

Expression par rapport aux vecteurs de base

$$|\varphi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Exemple (état de Bell) :

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|00\ldots00\rangle \iff \left.\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}\right\} 2^n, \quad |00\ldots01\rangle \iff \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad \cdots$$

$$\cdots \quad , \quad |11\ldots10\rangle \iff \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}, \quad |11\ldots11\rangle \iff \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

An Introduction to Quantum Computing, P. Kaye, R. Laflamme, M. Mosca

Portes. Séquence : produit matrices

X

(porte NOT)

$|0\rangle \mapsto |1\rangle$

$|1\rangle \mapsto |0\rangle$

Matrice :

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

H

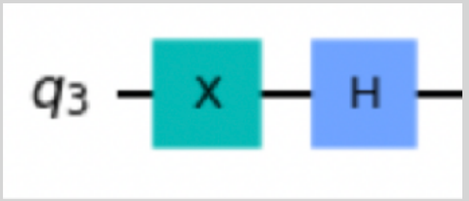
(Hadamard)

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Matrice :

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

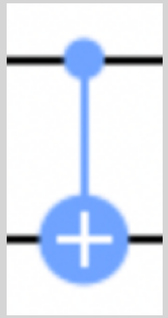


$$H(X|0\rangle) = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Portes — plusieurs qubits

composition séquentielle : produit de matrices



$$|xy\rangle \mapsto |x\rangle|x \oplus y\rangle$$

$$CX$$

(Controlled-NOT)

$$|00\rangle \mapsto |00\rangle$$

$$|01\rangle \mapsto |01\rangle$$

$$|10\rangle \mapsto |11\rangle$$

$$|11\rangle \mapsto |10\rangle$$

Matrice :

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Heron

Quantum volume: 512

At 156 qubits, Heron is an Eagle-sized upgrade to Egret that pulls in substantial innovations in signal delivery that were previously deployed in Osprey. The signals required to enable the fast, high-fidelity two-qubit and single-qubit control are delivered with high-density flex cabling.

- View available Heron processors ↗
- Native gates and operations: `cz`, `id`, `delay`, `measure`, `reset`, `rz`, `sx`, `x`, `if_else`, `for_loop`, `switch_case`

Revisions

`r2` (July 2024) This is a revision of the original Heron processor. The chip has been redesigned to include 156 qubits in a heavy-hexagonal lattice. While continuing to make use of the innovations of the original Heron processors, it also introduces a new TLS mitigation feature that controls the TLS environment of the chip, thereby improving coherence and stability across the whole chip.

IBM

Qubits supraconducteurs

Portes avec des impulsions micro-ondes

Alignement en grille carrée 2D sur la version antérieure, grille hexagonale maintenant

Très peu de portes implémentées physiquement ;

- à 2 qubits : CZ ($|11\rangle \mapsto -|11\rangle$, les autres inchangés)
- 1 qubit : X, SX, RZ

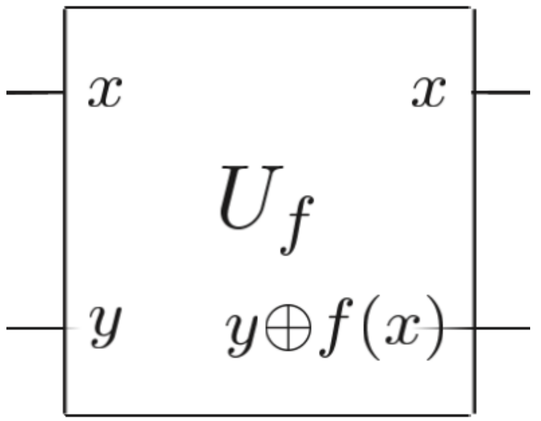
Les autres sont simulées, cf. TP

https://docs.quantum.ibm.com/

2. Du classique au quantique (compatibilité)

Toute fonction classique $f : \{0,1\}^n \to \{0,1\}^m$ peut être simulée par un circuit quantique U_f de taille similaire, à $n + m$ qubits, tel que

$$|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$

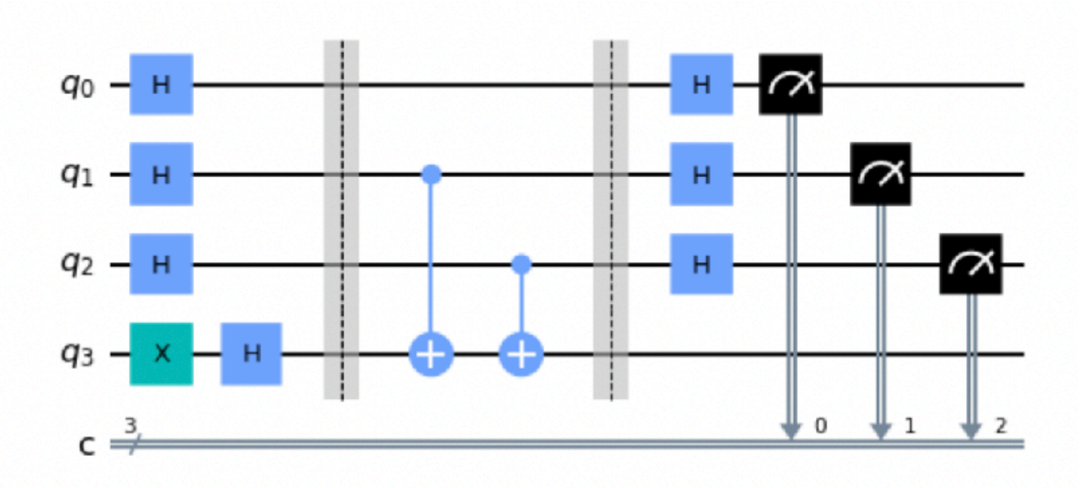


N.B. Cela revient à programmer avec des outils très basiques, comme si l'on programmait en assembleur...

2. Calcul quantique — « parallélisme quantique»

« La plupart des **algorithmes quantiques** fonctionnent sur le principe suivant :

- créer une superposition pertinente de qubits à partir de $|00\cdots0\rangle$
- effectuer en **parallèle** un calcul classique sur la superposition des entrées ;
- effectuer une **transformation quantique pertinente** ;
- observer le résultat grâce à des **mesures**. »

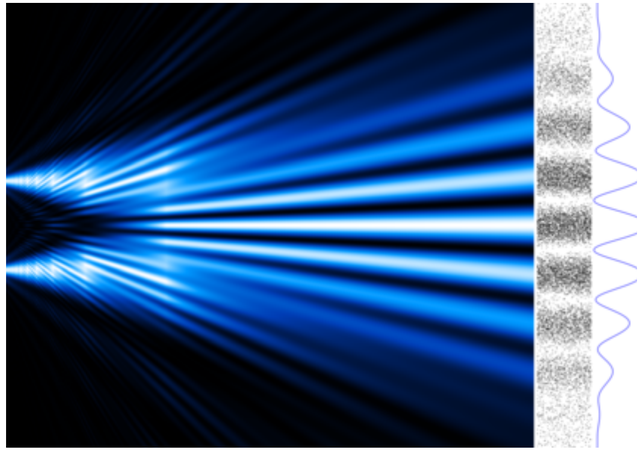


Exercice.

Rappeler les états $H|0\rangle$ et $H|1\rangle$. Montrer que $H^{\otimes n}|00\cdots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$

2. Interférence

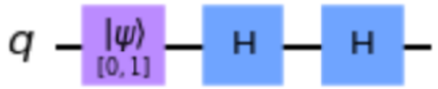
dont interférence « destructive »



Fentes de Young - Wikipedia

Interférence : combinaison de deux ondes.
Cf. expérience des fentes de Young :
interférences « constructives » et
« destructives »

Exercice. Analyser la succession de deux portes H :
calculer $H(H|0\rangle)$ et $H(H|1\rangle)$.

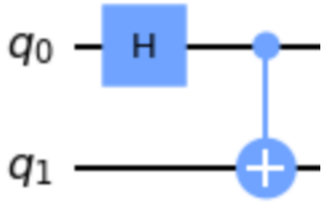


2. Intrication quantique

ou « enchevêtrement » ; *entanglement*, en anglais

Etat de Bell : $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

Un circuit qui construit cet état :



- Chacun des deux qubits a une probabilité de $\frac{1}{2}$ d'être mesuré à 0, pareil pour 1.
- Supposons que le premier qubit a été mesuré à 0. Que donnera la mesure du 2ème qubit ? Conclure que les propriétés des deux qubits sont corrélées.

Perturbant car on peut éloigner arbitrairement les deux qubits tout en préservant l'intrication...
Controverse Bohr - Einstein ; prix Nobel 2022 J. Clauser, **Alain Aspect** et A. Zeiliger.

3. Algorithme de Bernstein-Vazirani

Parce que suffisamment surprenant (accélération quantique) mais (relativement) abordable

Le problème

- Donnée : une fonction $f : \{0,1\}^n \to \{0,1\}$
- Promesse : il existe un $s \in \{0,1\}^n$ tel que $f(x) = x \cdot s$
- Sortie : trouver s

Exercice.

Proposer un algorithme classique pour résoudre ce problème. De combien d'appels à la fonction f avez-vous besoin ?

Rappel : pour $x = x_1 x_2 \cdots x_n$ et $s = s_1 s_2 \cdots s_n$ on note $x \cdot s$ leur produit scalaire :

$$x \cdot s = x_1 \cdot s_1 \oplus x_2 \cdot s_2 \oplus \cdots \oplus x_n \cdot s_n$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} \to XOR\left(\begin{bmatrix} x_1 \cdot s_1 \\ x_2 \cdot s_2 \\ x_3 \cdot s_3 \\ x_4 \cdot s_4 \end{bmatrix} \right)$$

3. Algorithme de Bernstein-Vazirani

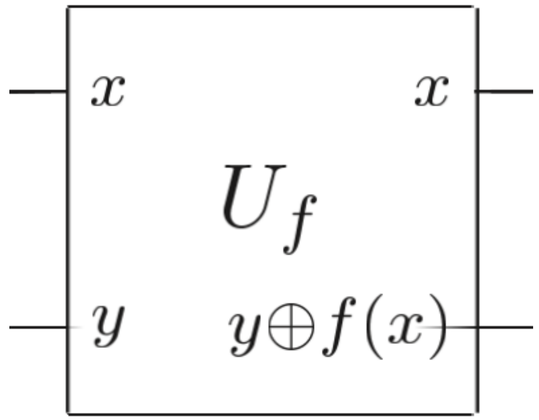
L'algorithme quantique : un seul appel à la fonction f

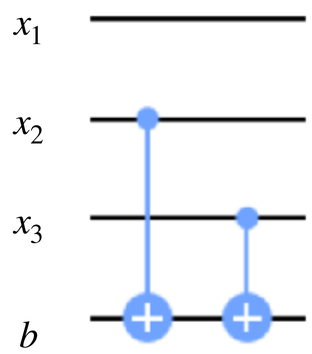
$f(x) = x \cdot s$ pour un vecteur « inconnu » $s \in \{0,1\}^n$

1. **On construit d'abord** $U_f : |xb\rangle \to |x\rangle\,|b \oplus f(x)\rangle$
2. Remplacer l'entrée b par $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. On a :

$$U_f : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \to (-1)^{f(x)}\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

3. Appliquer des portes H sur les n premiers qubits, à l'entrée. Qu'obtient-on, sans mesurer ?
4. Appliquer des portes H sur les n premiers bits, à la sortie. Mesurer ces bits et montrer que l'on obtient s.





$s = 011$

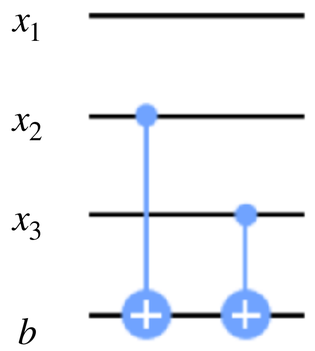
3. Algorithme de Bernstein-Vazirani

$f(x) = x \cdot s$ pour un vecteur « inconnu » $s \in \{0,1\}^n$

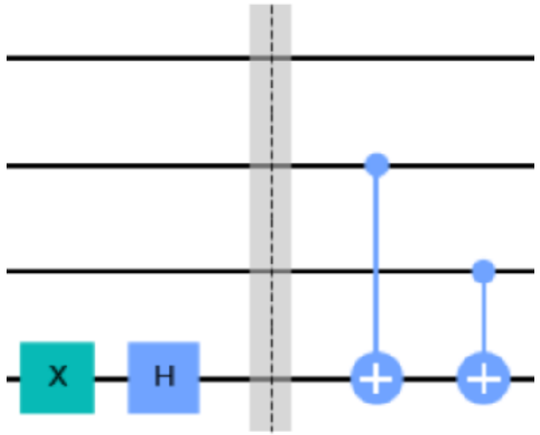
1. On construit d'abord $U_f : |xb\rangle \to |x\rangle\,|b \oplus f(x)\rangle$
2. **Remplacer l'entrée b par $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. On a :**

$$U_f : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \to (-1)^{f(x)}\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

3. Appliquer des portes H sur les n premiers qubits, à l'entrée. Qu'obtient-on, sans mesurer ?
4. Appliquer des portes H sur les n premiers bits, à la sortie. Mesurer ces bits et montrer que l'on obtient s.



$s = 011$



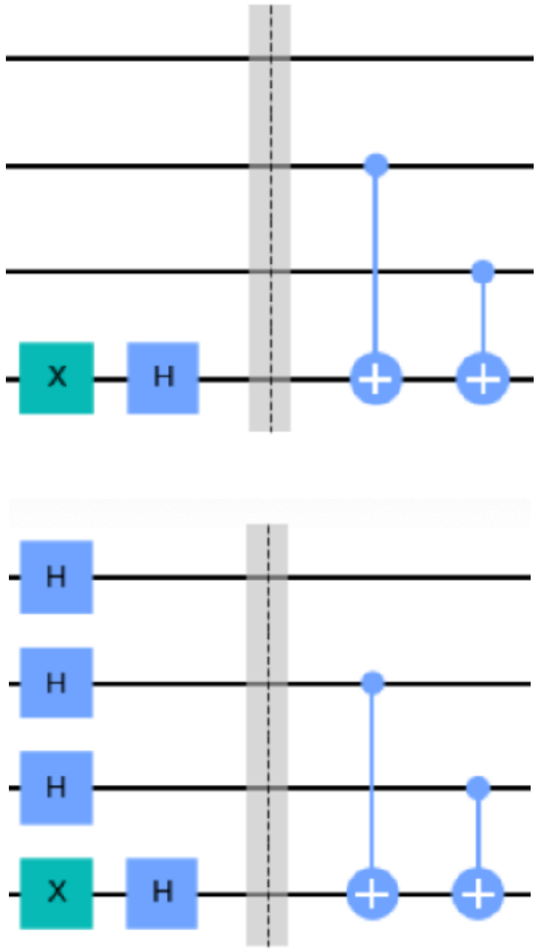
3. Algorithme de Bernstein-Vazirani

$f(x) = x \cdot s$ pour un vecteur « inconnu » $s \in \{0,1\}^n$

1. On construit d'abord $U_f : |xb\rangle \to |x\rangle\,|b \oplus f(x)\rangle$
2. Remplacer l'entrée b par $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. On a :

$$U_f : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \to (-1)^{f(x)}\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

3. **Appliquer des portes H sur les n premiers qubits, à l'entrée. Qu'obtient-on, sans mesurer ?**
4. Appliquer des portes H sur les n premiers bits, à la sortie. Mesurer ces bits et montrer que l'on obtient s.



3. Algorithme de Bernstein-Vazirani

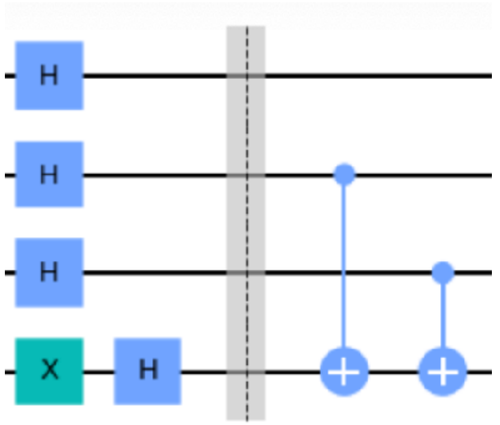
$f(x) = x \cdot s$ pour un vecteur « inconnu » $s \in \{0,1\}^n$

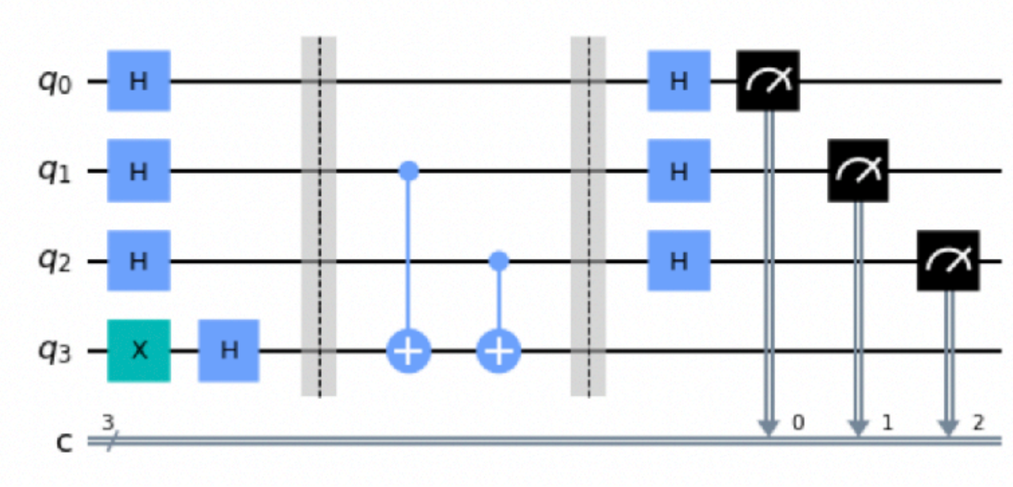
1. On construit d'abord $U_f : |xb\rangle \rightarrow |x\rangle\,|b \oplus f(x)\rangle$
2. Remplacer l'entrée b par $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. On a :

$$U_f : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \rightarrow (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

3. Appliquer des portes H sur les n premiers qubits, à l'entrée. Qu'obtient-on, sans mesurer ?
4. **Appliquer des portes H sur les n premiers bits, à la sortie. Mesurer ces bits et montrer que l'on obtient s.**

L'algorithme mesure s avec probabilité 1.





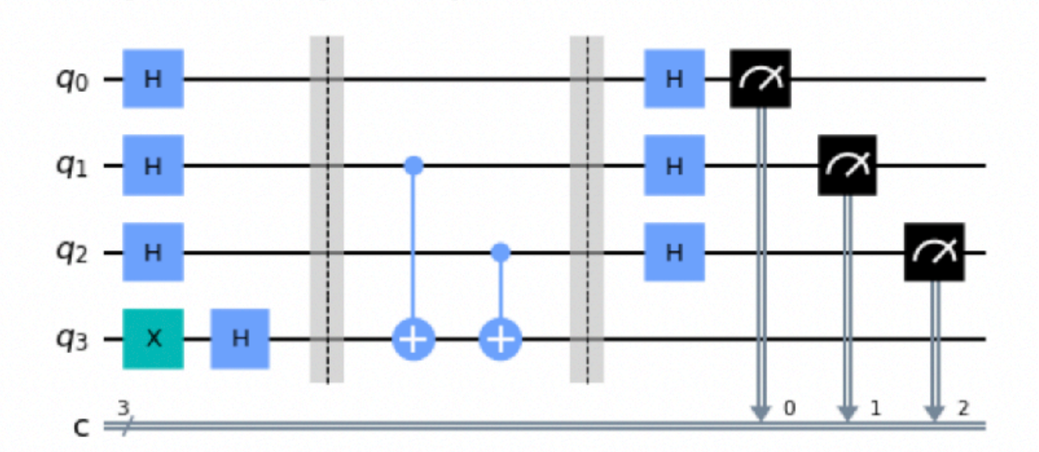
Mesure : 011

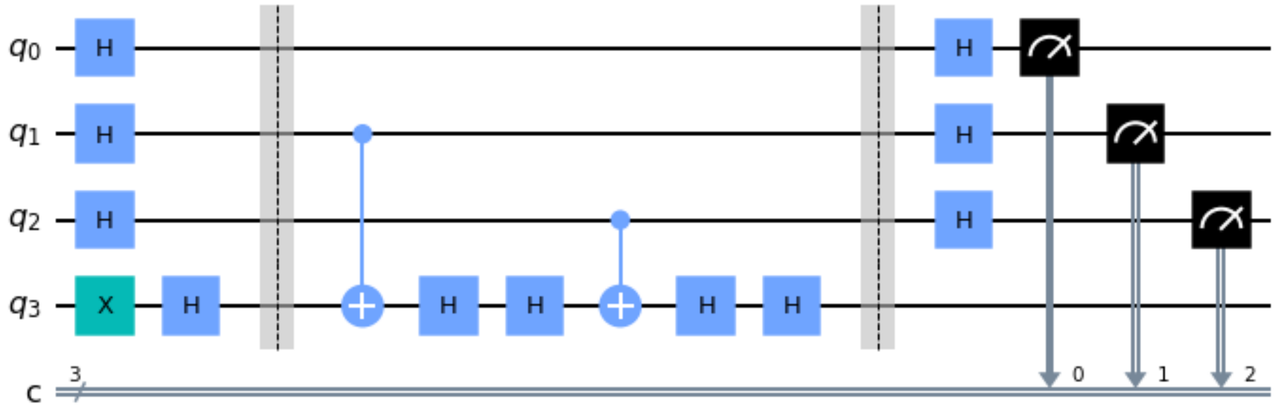
3. Preuve algo de Bernstein-Vazirani

Pourquoi ça marche ? Une preuve presque combinatoire

Lemme 1 :

≡ Identité

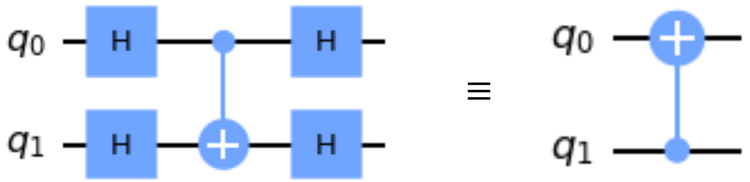




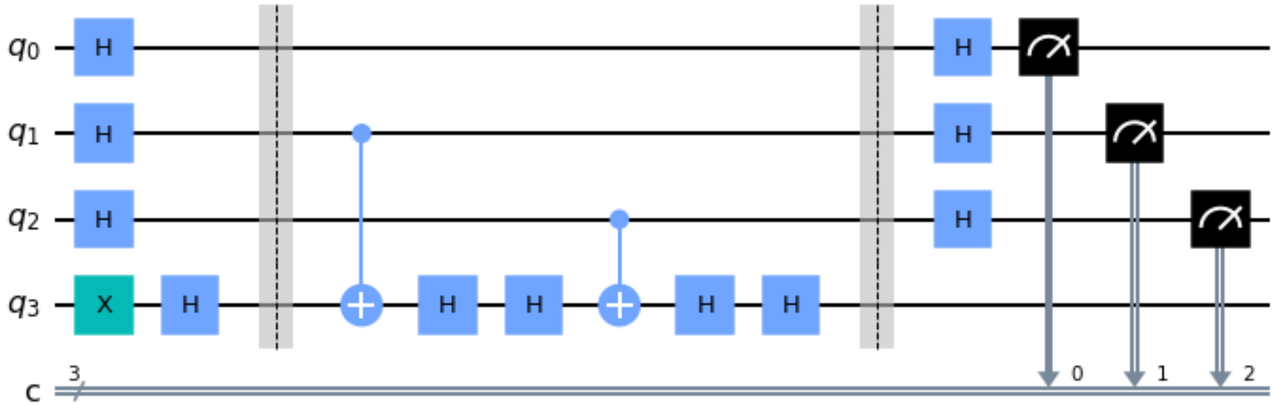
3. Preuve algo de Bernstein-Vazirani

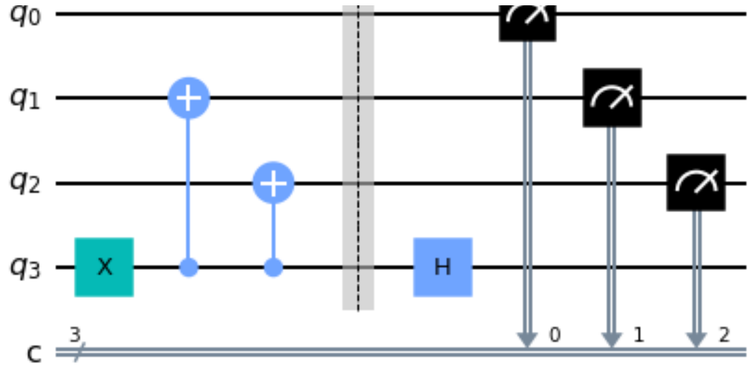
Pourquoi ça marche ? Une preuve presque combinatoire

Lemme 2 :



In fine, c'est comme si l'on avait inversé toutes les portes CNOT, sachant que le dernier qubit est à $|1\rangle$





Sortie : 011

4. Algorithme de Grover

Le problème. On dispose d'une fonction $f : \{0,1\}^n \to \{0,1\}$. L'objectif est de trouver, s'il existe, un vecteur $x \in \{0,1\}^n$ tel que $f(x) = 1$.

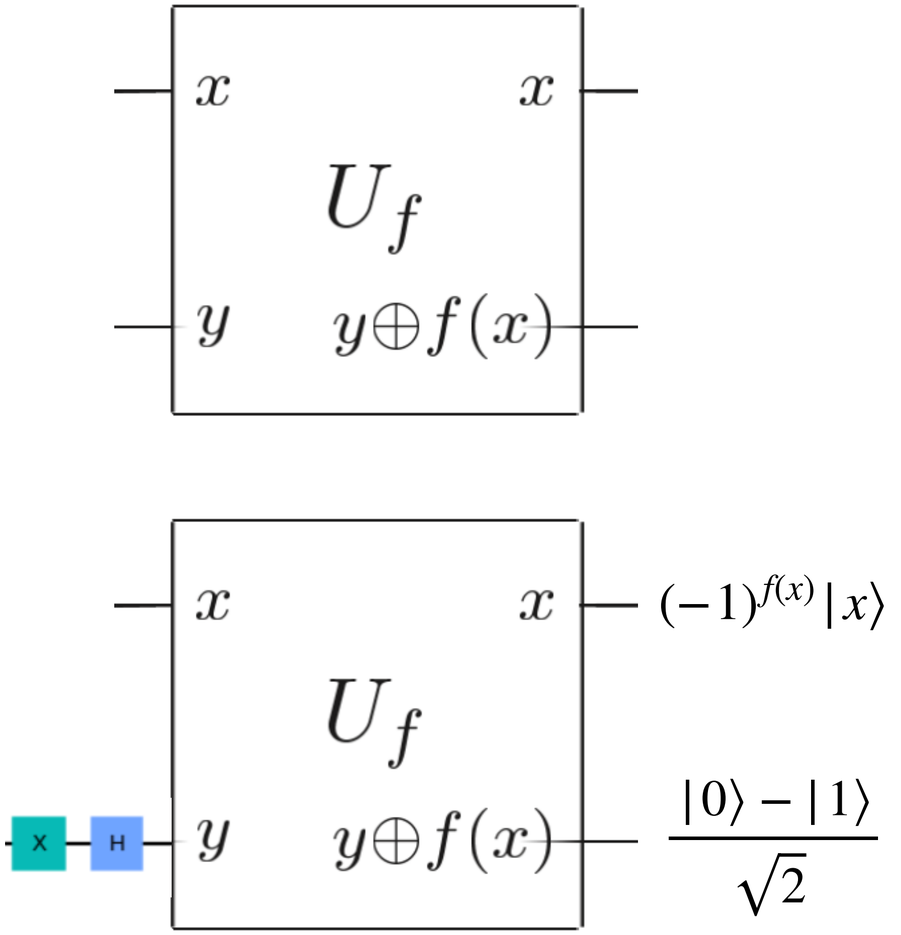
L'algorithme de Grover (1996) permet de résoudre le problème en temps $O(\sqrt{2^n})$ alors que tout algorithme classique requiert un temps $\Theta(2^n)$.

C'est un algorithme probabiliste : il trouve la solution avec une probabilité au moins 2/3.
Des techniques standard d'amplification permettent de la ramener aussi près de 1 que l'on veut.

Problème SAT (satisfiabilité), en classique : même si f est une fonction booléenne connue, on ne sait pas faire mieux que $\Theta(2^n)$...

Grover serait l'un des algorithmes les plus utiles pour accélérer (polynomialement) de nombreux algorithmes classiques.

4. Algorithme de Grover - outils de base

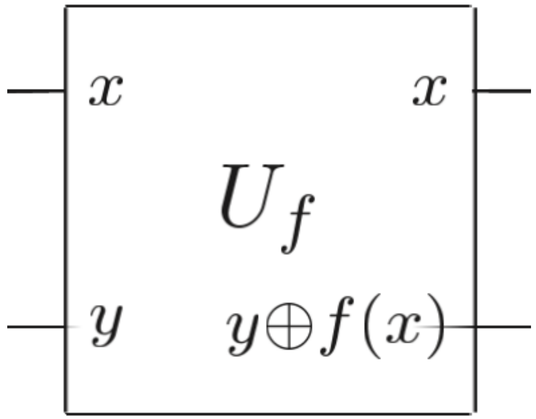


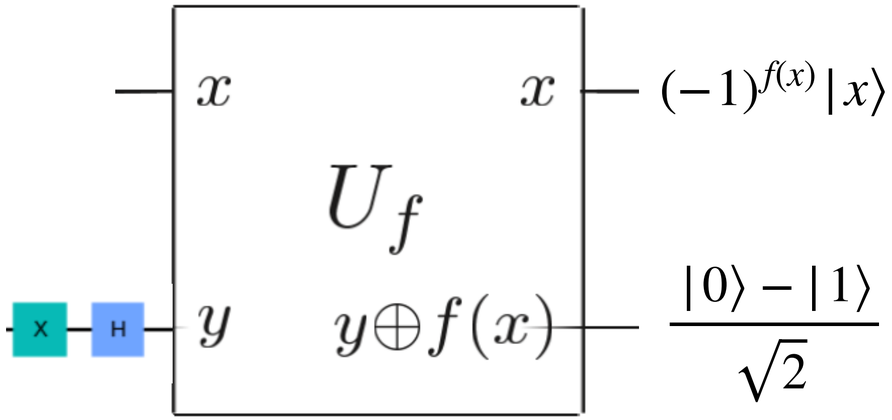
Oracle Z_f

Rappel TD/cours

- Pour toute fonction booléenne f, on peut construire l'oracle (le circuit)
  $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$
- On note $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- **En mettant $y = |-\rangle$, on obtient en sortie l'état $(-1)^{f(x)}|x\rangle|-\rangle$**
- **Ce nouvel oracle sera noté Z_f.**

4. Algorithme de Grover - outils de base





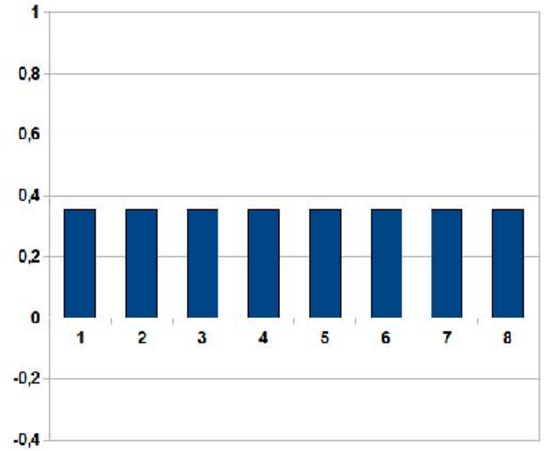
Oracle Z_f

Hypothèse simplificatrice. Supposons que notre fonction $f : \{0,1\}^n \to \{0,1\}$ est telle qu'il existe un seul x_1 tel que $f(x_1) = 0$.

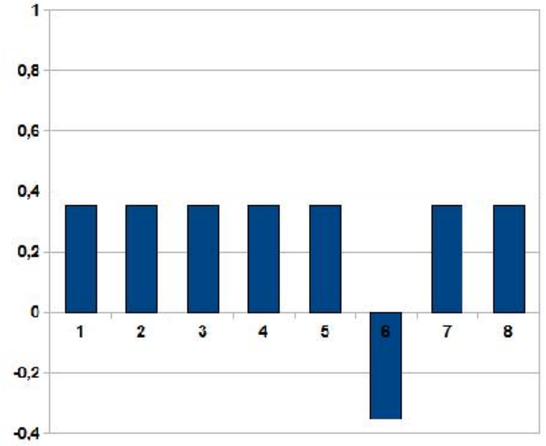
(On peut résoudre le cas général, mais cela nécessite une analyse plus poussée.)

Exercice. Quel est l'état de sortie du circuit Z_f si l'on met une porte H sur chacun des n qubits en entrée ?

4. Algorithme de Grover — première observation



Etat initial après H



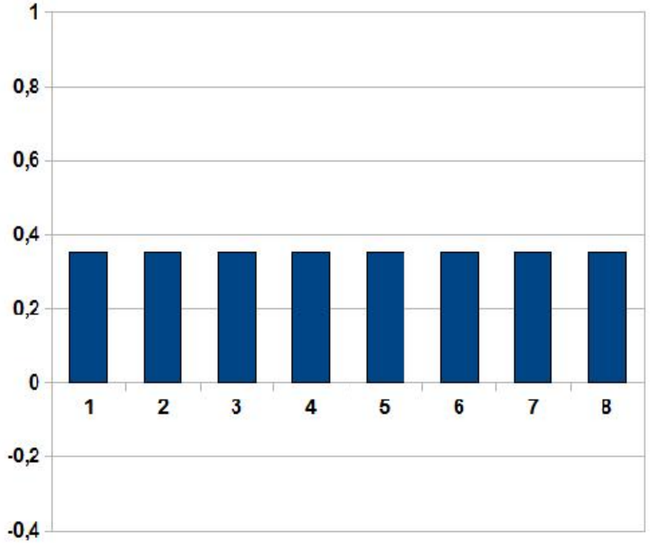
Sortie

Images : https://fr.wikipedia.org/wiki/Algorithme_de_Grover

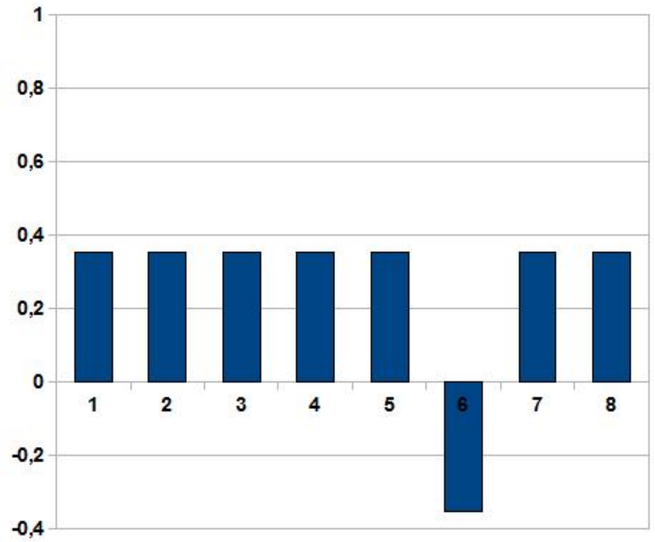
Hypothèse simplificatrice (rappel). Pour notre fonction $f : \{0,1\}^n \to \{0,1\}$ il existe un seul x_1 tel que $f(x_1) = 0$.

Exercice. Quel est l'état de sortie du circuit Z_f si l'on met une porte H sur chacun des n qubits en entrée ?

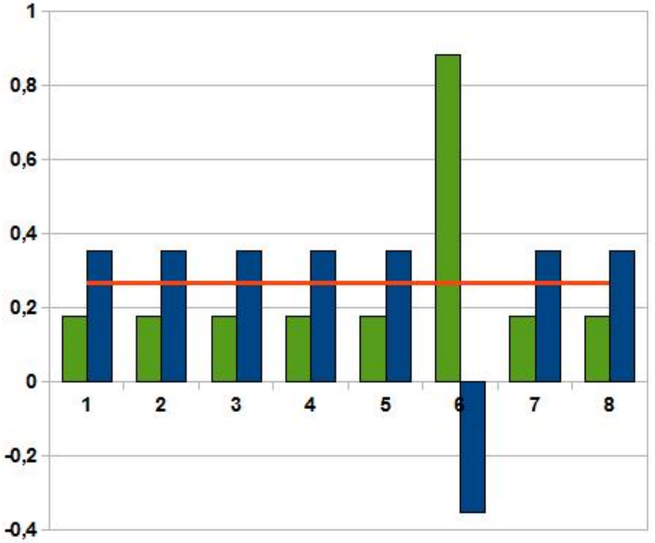
- Etat « initial », après les portes H
- Etat de sortie : l'amplitude de x_1 voit son signe inversé



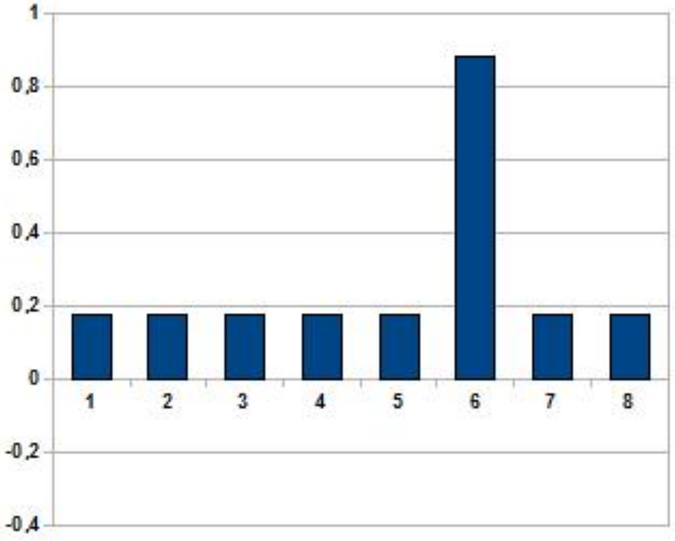
Etat initial après H



Sortie circuit Z_c



Miroir autour de la moyenne

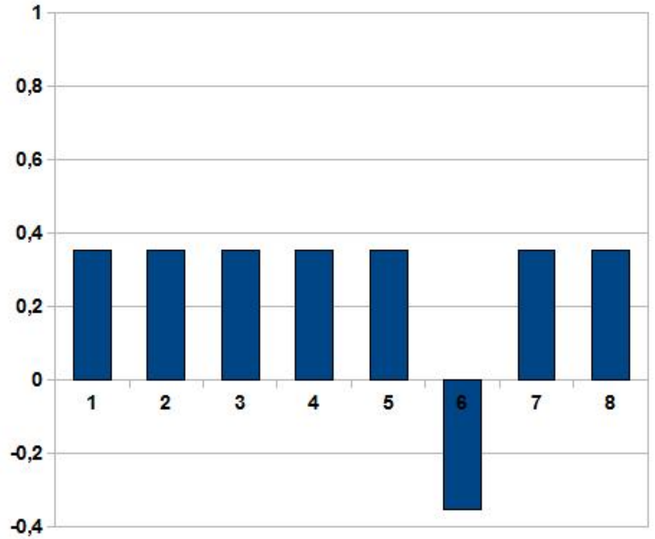


Nouvel état après l'opération

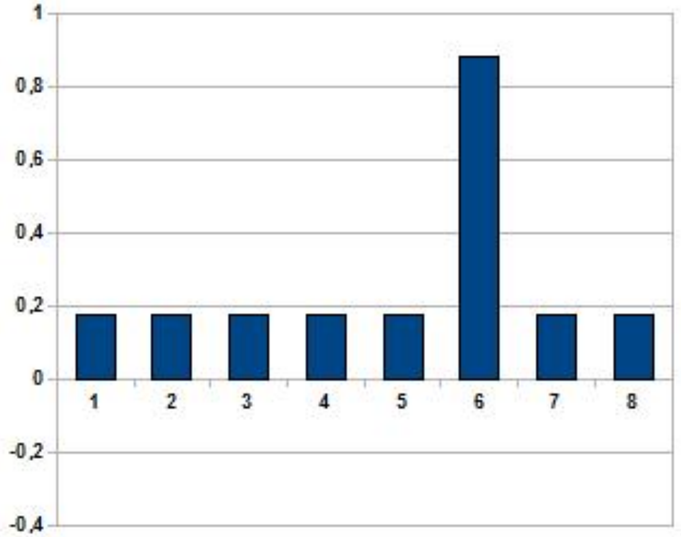
4. Algorithme de Grover — miroir autour de la moyenne

Opérateur de Grover

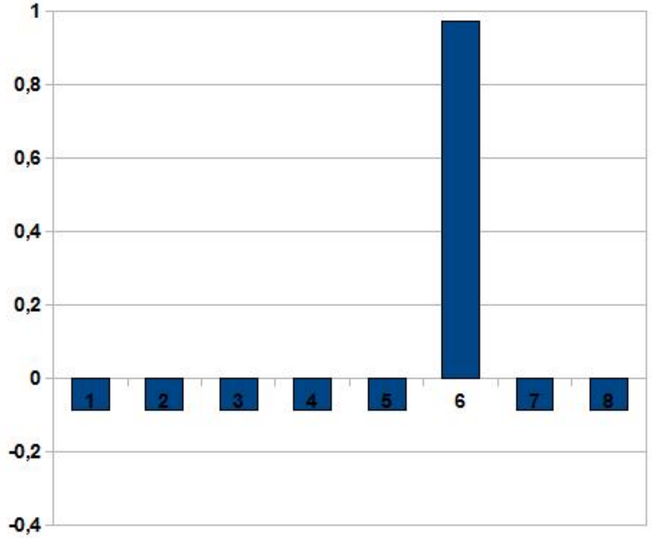
- Intuition : comme si l'on calculait la moyenne des amplitudes, et que l'on appliquait un « miroir autour de la moyenne »
- Nous verrons ultérieurement l'implémentation et les preuves



Sortie circuit Z_f



Etat après une opération « de Grover »



Etat après deux opérations « de Grover »

4. Algorithme de Grover — répéter

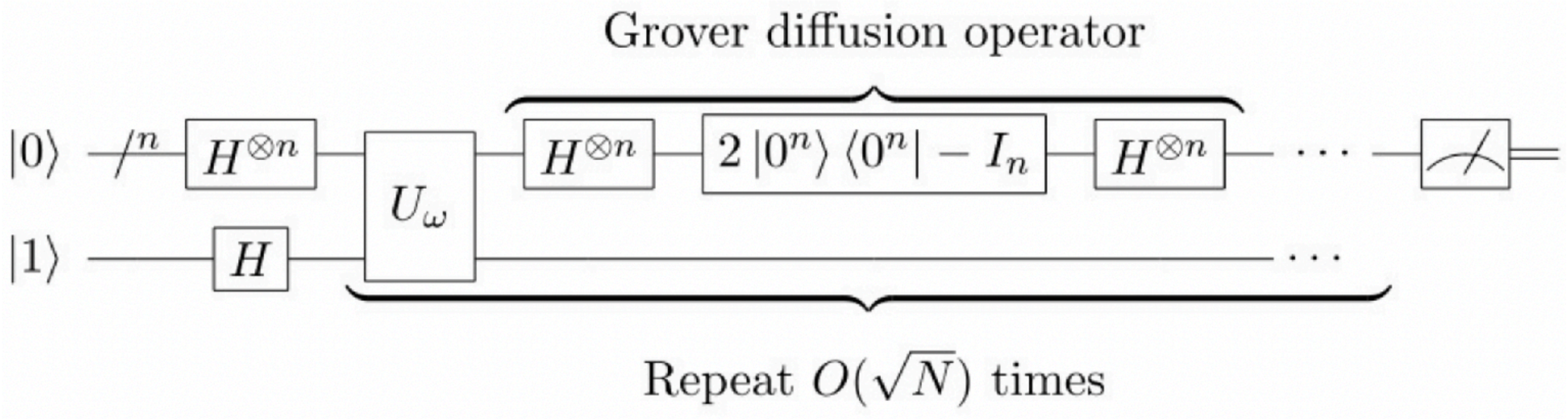
… le bon nombre de fois

- Sur l'exemple, on mesure x_1 avec probabilité supérieure à 90 %

Encore faut-il :

- Détailler l'implémentation
- Transformer l'exemple en preuve systématique

4. Algorithme de Grover



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Schéma général. Dans ce schéma U_ω est simplement une autre notation pour U_f.

L'opérateur de diffusion de Grover réalise le « miroir autour de la moyenne ». Son implémentation assez simple :

$$H^{\oplus n} Z_{OR} H^{\oplus n}$$

Encore un peu de mathématiques

Notation « bra » et projections

Rappelons qu'un état $|\psi\rangle = |a_1 a_2 \ldots a_n\rangle$ représente un vecteur (colonne).

On note par $\langle\psi| = \langle a_1 a_2 \ldots a_n|$ sa transposée conjuguée : le vecteur est vu « en ligne ». Pour chaque coordonnée on prend sa conjuguée... qui reste inchangée dans le cas des vecteurs a coordonnées réelles.

$\langle 0^n|$ représente $\langle 00\ldots0|$, avec n zéros : matrice $[10\ldots0]$, une ligne et 2^n colonnes.

Le produit scalaire des vecteurs réels $|\phi\rangle$ et $|\psi\rangle$ aussi noté $\langle\varphi|\psi\rangle$.

Opérateur projection : $|\psi\rangle\langle\psi|$. C'est le produit tensoriel entre les deux matrices.

Le **produit scalaire** des vecteurs réels $|\phi\rangle$ et $|\psi\rangle$ est égal à $\langle\varphi| \times |\psi\rangle$, noté $\langle\varphi|\psi\rangle$.

Opérateur projection : $|\psi\rangle\langle\psi|$. C'est le produit tensoriel entre les deux matrices.

Propriétés (du produit tensoriel) :

- $(|\psi\rangle\langle\psi|)|\varphi\rangle = |\psi\rangle(\langle\psi|\varphi\rangle)$ est la projection du vecteur $|\varphi\rangle$ sur $|\psi\rangle$
- Pour deux matrices A, B de taille $N \times N$,

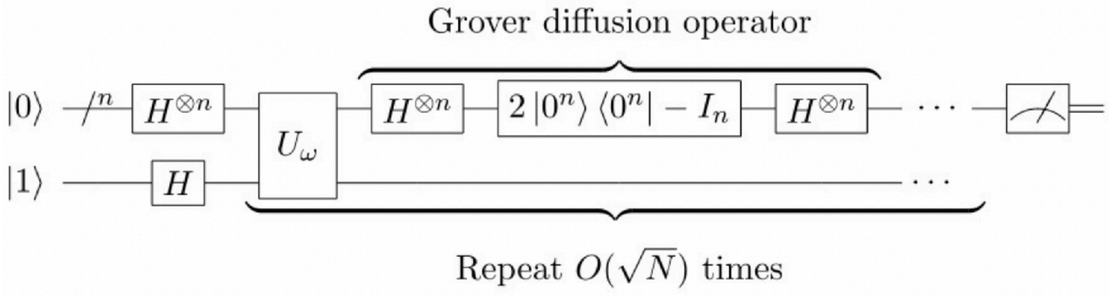
$$A(|\psi\rangle\langle\psi|)B = (A|\psi\rangle) \otimes (\langle\psi|B)$$

Exercice 1. Ecrire la matrice de $|0^n\rangle\langle 0^n|$, puis celle de $2|0^n\rangle\langle 0^n| - I_n$.

Exercice 2. Montrer que $2|0^n\rangle\langle 0^n| - I_n$ correspond à l'oracle Z_{OR} de la fonction OR_n.

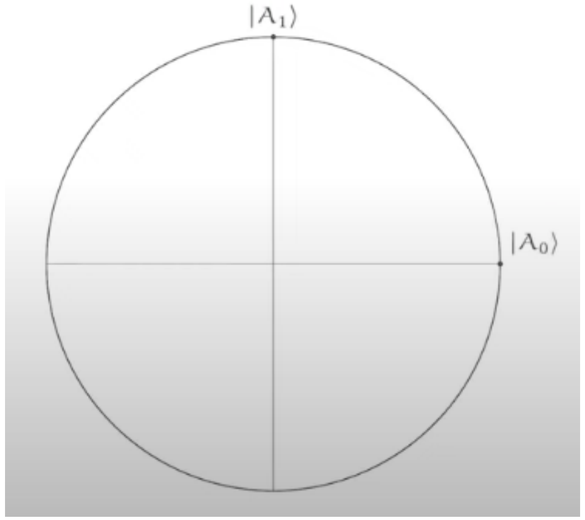
Exercice 3. Montrer que $H^{\oplus n}(2|0^n\rangle\langle 0^n| - I_n)H^{\oplus n} = 2|u\rangle\langle u| - I_n$, où $u = H^{\oplus n}|0^n\rangle$.

4. Algorithme de Grover : la preuve



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

On note $A_1 = \{x_1\}$ et
$A_0 = \{x \in \{0,1\}^n : f(x) = 0\}$

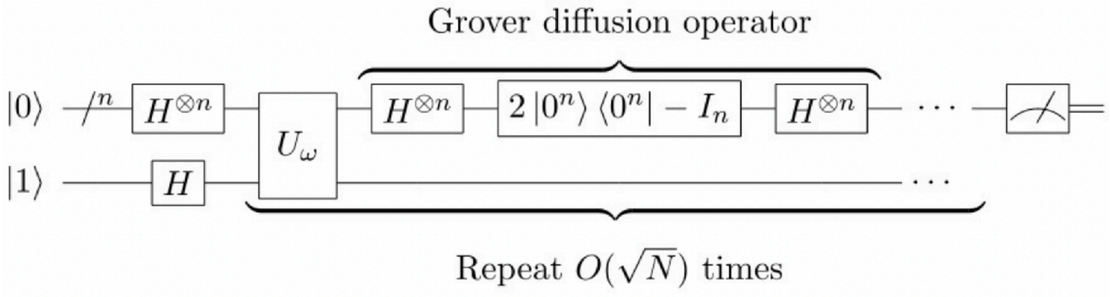


John Watrous, IBM, vidéo YouTube

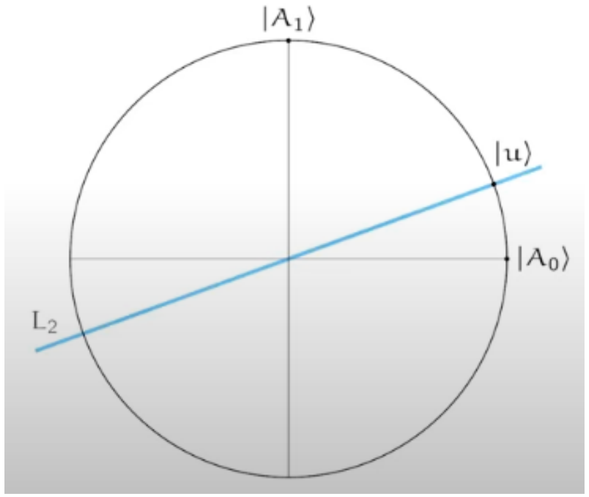
Pour un ensemble de vecteurs booléens A notons $|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle$.

Observer que les vecteurs $|A_0\rangle$ et $|A_1\rangle$ sont orthogonaux.

4. Algorithme de Grover : la preuve



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



John Watrous, IBM

Soit $|u\rangle = H^{\otimes n}|0^n\rangle$, le vecteur « uniforme »

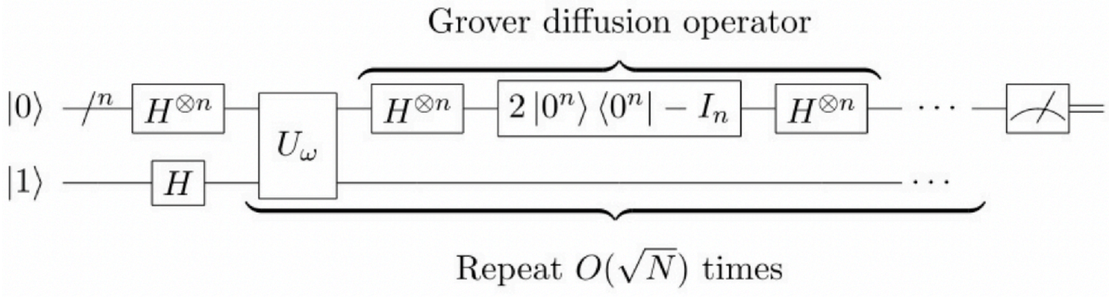
$$|u\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$|u\rangle = \frac{1}{\sqrt{N}} \left(\sum_{x_0\in A_0} |x_0\rangle + \sum_{x_1\in A_1} |x_1\rangle \right)$$

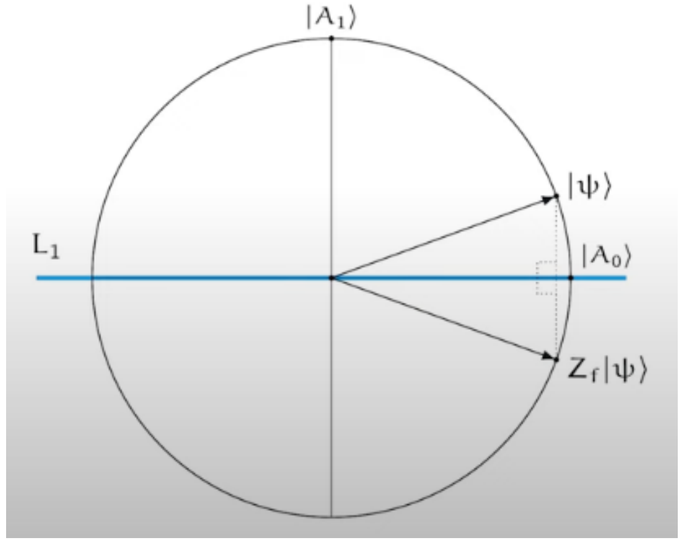
$$|u\rangle = \frac{\sqrt{|A_0|}}{\sqrt{N}} |A_0\rangle + \frac{\sqrt{|A_1|}}{\sqrt{N}} |A_1\rangle$$

$|u\rangle$ est une combinaison linéaire de $|A_0\rangle$ et $|A_1\rangle$

4. Algorithme de Grover : la preuve



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



John Watrous, IBM

Comprendre l'opération $Z_f|\psi\rangle$: symétrie autour de $|A_0\rangle$.

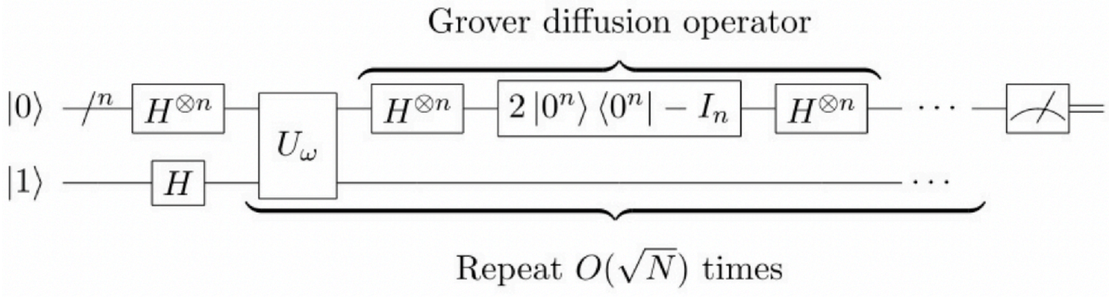
$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$$

$$|\psi\rangle = \sum_{x_0\in A_0} \alpha_{x_0} |x_0\rangle + \sum_{x_1\in A_1} \alpha_{x_1} |x_1\rangle$$

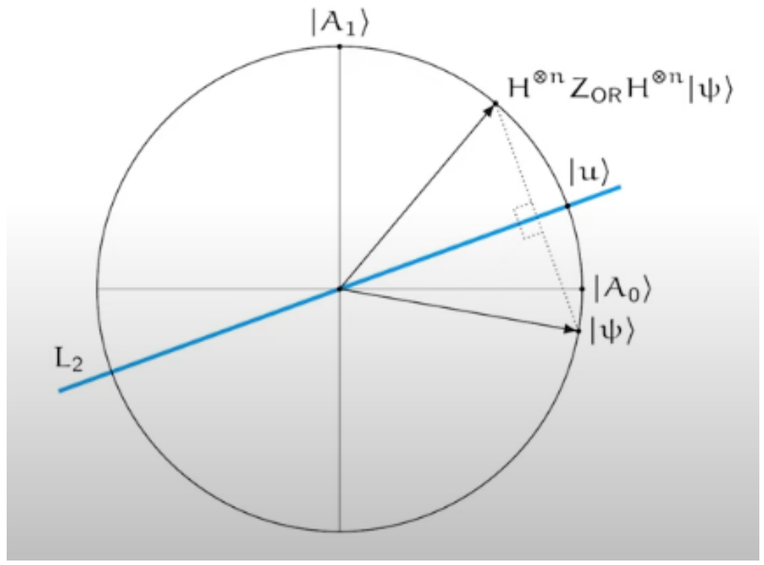
$$Z_f|\psi\rangle = \sum_{x_0\in A_0} \alpha_{x_0}(-1)^{f(x_0)} |x_0\rangle + \sum_{x_1\in A_1} \alpha_{x_1}(-1)^{f(x_1)} |x_1\rangle$$

$$Z_f|\psi\rangle = \sum_{x_0\in A_0} \alpha_{x_0} |x_0\rangle - \sum_{x_1\in A_1} \alpha_{x_1} |x_1\rangle$$

4. Algorithme de Grover : la preuve



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



John Watrous, IBM

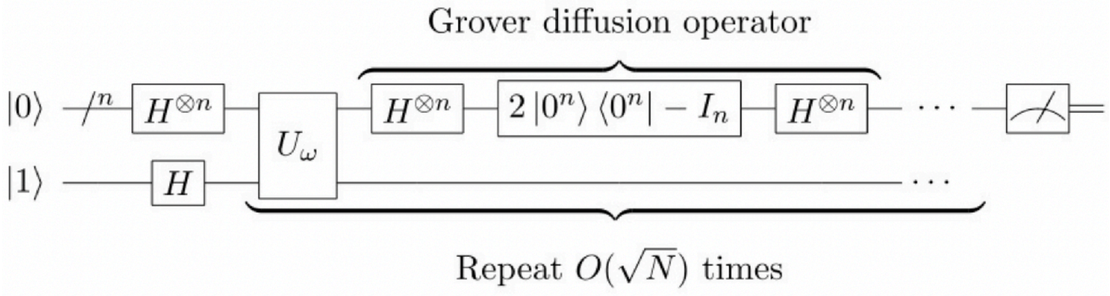
Comprendre l'opération $H^{\oplus n} Z_{OR} H^{\oplus n} |\psi\rangle$: symétrie autour de $|u\rangle$.

$$Z_{OR} = 2\,|0^n\rangle\langle 0^n| - I$$

$$\begin{aligned} H^{\oplus n} Z_{OR} H^{\oplus n} |\psi\rangle &= H^{\oplus n}(2\,|0^n\rangle\langle 0^n| - I)H^{\oplus n} \\ &= 2H^{\oplus n}(|0^n\rangle\langle 0^n|)H^{\oplus n} - H^{\oplus n} I H^{\oplus n} \\ &= 2\,|u\rangle\langle u| - I \end{aligned}$$

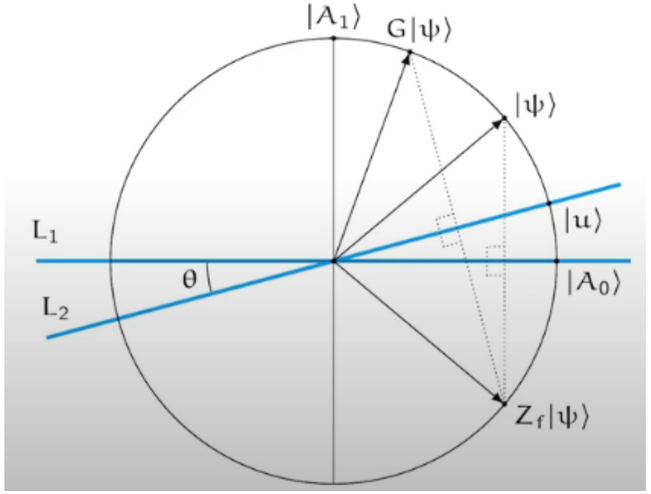
On a utilisé le fait que $H^{\oplus n}|0^n\rangle = |u\rangle$

4. Algorithme de Grover : la preuve



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Comprendre une itération complète :
$(H^{\oplus n} Z_{OR} H^{\oplus n}) Z_f |\psi\rangle$

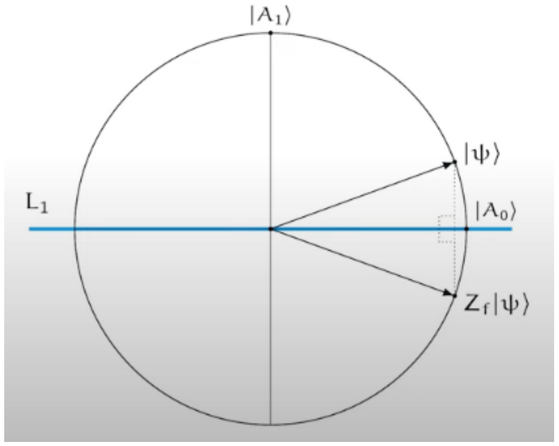


John Watrous, IBM

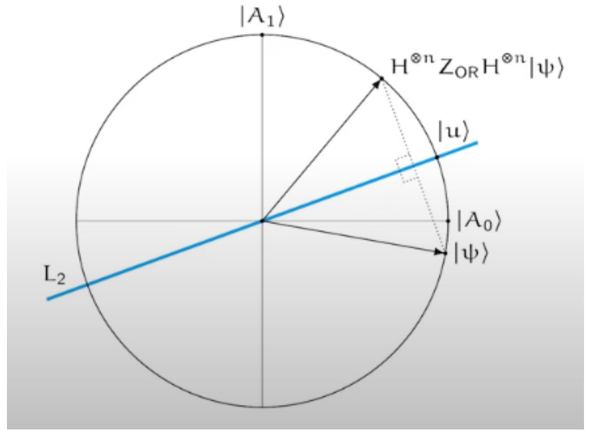
1. Symétrie autour de $|A_0\rangle$
2. Symétrie autour de $|u\rangle$

Equivalent à une rotation du vecteur $|\psi\rangle$ d'angle 2θ, où θ est l'angle entre les vecteurs $|u\rangle$ et $|A_0\rangle$

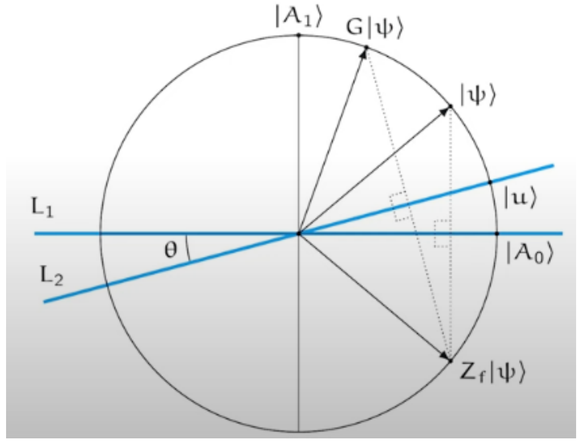
4. Algorithme de Grover : la preuve



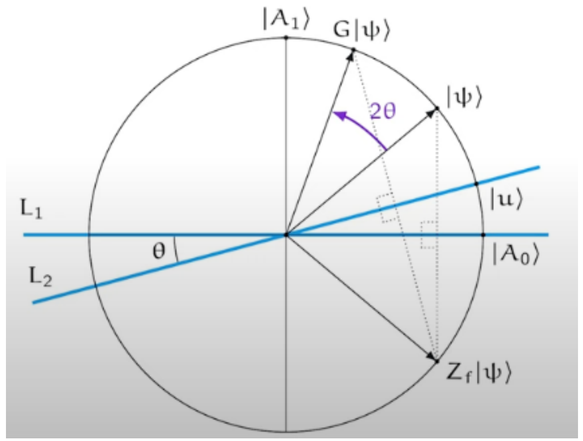
1. On applique Z_f



2. Puis $H^{\oplus n} Z_{OR} H^{\oplus n}$



3. La combinaison des deux produit...



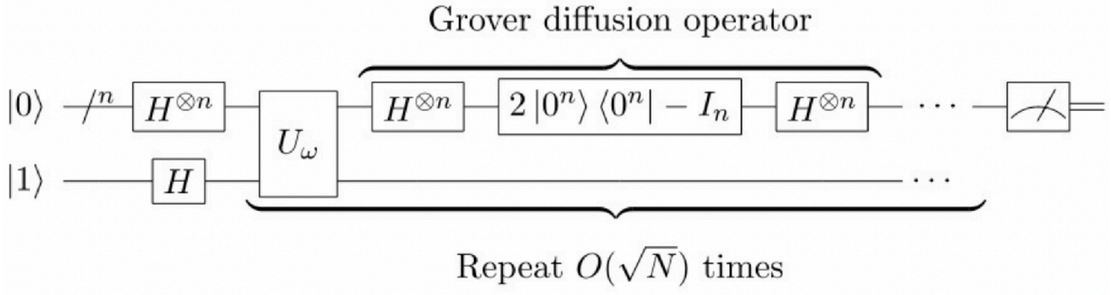
Une rotation d'angle 2θ

Comprendre une itération complète : $(H^{\oplus n} Z_{OR} H^{\oplus n}) Z_f |\psi\rangle$

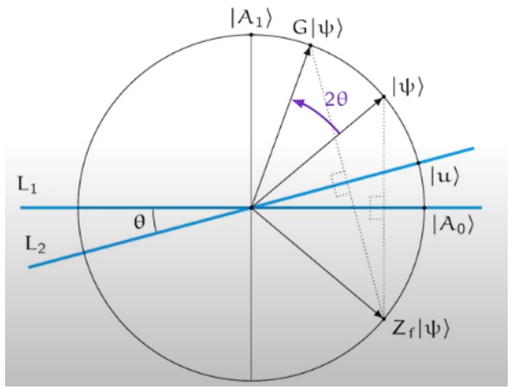
1. Symétrie autour de $|A_0\rangle$
2. Symétrie autour de $|u\rangle$

Equivalent à une rotation du vecteur $|\psi\rangle$ d'angle 2θ, où θ est l'angle entre les vecteurs $|u\rangle$ et $|A_0\rangle$

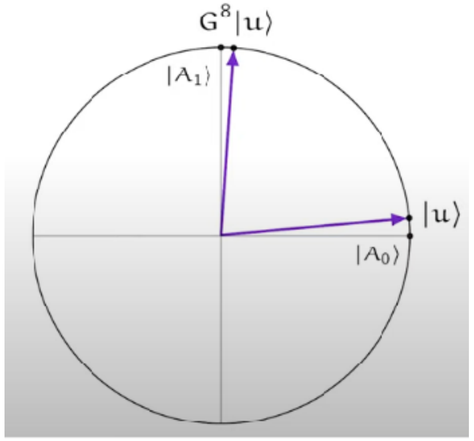
4. Algorithme de Grover : choisir le nombre d'itérations



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



Une rotation d'angle 2θ



$N = 128, t = 8$

1. On part de $\psi_0 = |u\rangle$, d'angle θ avec $|A_0\rangle$
2. Après t itérations, l'angle devient $(2t+1)\theta$ $|A_0\rangle$
3. On voudrait mesurer A_1, donc on veut que cet angle soit à peu près 90°, soit $\pi/2$

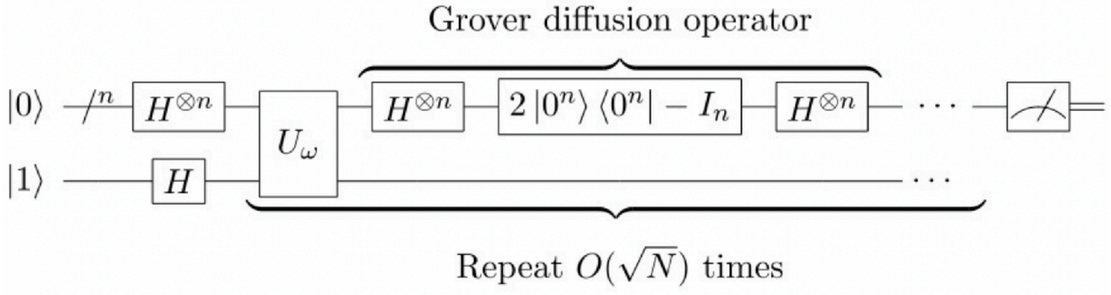
$$|u\rangle = \frac{1}{\sqrt{N}}|A_1| + \frac{\sqrt{N-1}}{\sqrt{N}}|A_0\rangle$$

$$|u\rangle = \sin(\theta)|A_1| + \cos(\theta)|A_0\rangle$$

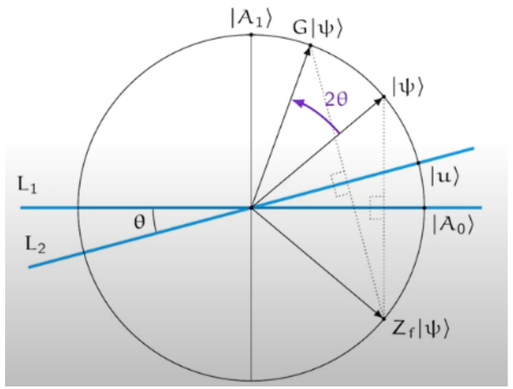
Donc $\sin(\theta) = \frac{1}{\sqrt{N}}$, et pour N grande $\theta \sim \frac{1}{\sqrt{N}}$.

On choisit $t = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$

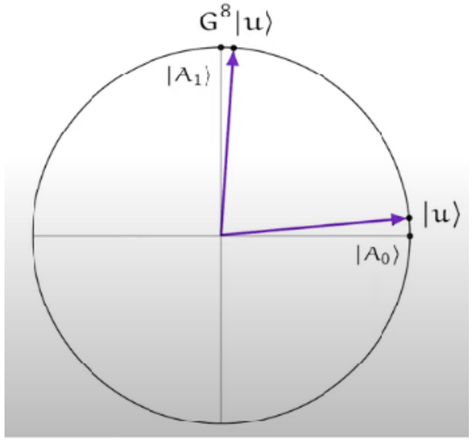
4. Algorithme de Grover complet



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



Une rotation d'angle 2θ



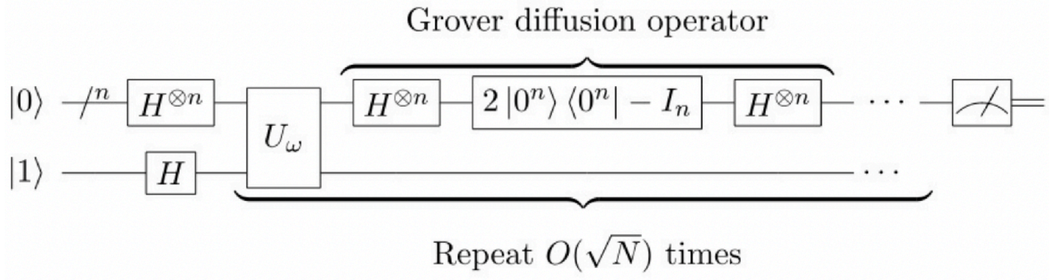
$N = 128, t = 8$

Construction Circuit Grover

1. Appliquer $H^{\oplus n}$: portes H sur n premiers qubits
2. Enchaîner $t = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ fois le circuit G :
3. ajouter Z_f
4. ajouter $H^{\oplus n}$
5. ajouter Z_{OR}
6. ajouter $H^{\oplus n}$

On utilise le dernier qubit à $|-\rangle$ pour Z_f et Z_{OR}

4. Algorithme de Grover complet



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Théorème. L'algorithme de Grover mesure x_1 avec probabilité au moins $1 - \frac{1}{N}$, où $N = 2^n$.

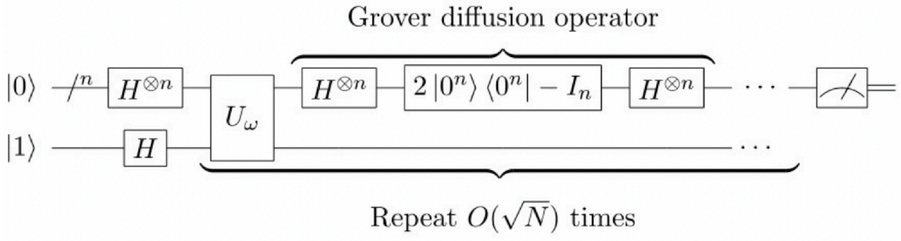
Construction Circuit Grover

1. Appliquer $H^{\oplus n}$ sur n premiers qubits
2. Enchaîner $t = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ fois le circuit G :
3. ajouter Z_f puis $H^{\oplus n}$ puis Z_{OR} puis $H^{\oplus n}$

Extensions

- Si f a un nombre arbitraire de solutions, choisir le nombre t d'itérations uniformément au hasard dans $\{1,\ldots,\pi\sqrt{N}/4\}$, proba succès $\geq 40\,\%$.
- On peut faire mieux, cf. [John Watrous, YouTube].
- Optimisation : $f : \{0,1\}^n \to \mathbb{N}$, calculer x tel que $f(x)$ soit maximum : même complexité, [Dürr, Høyer '97].
- Nombreuses applications mais... $2^{n/2}$ portes.

4. Algorithme de Grover : exercices



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Théorème. L'algorithme de Grover mesure x_1 avec probabilité au moins $1 - \frac{1}{N}$, où $N = 2^n$.

Exercice 1.

1. Décrire complètement le circuit pour l'algorithme de Grover, dans notre cas restreint.
2. L'appliquer pour une fonction ayant 2 bits en entrée. Analyser l'évolution des amplitudes après chaque étape. Quelle est la probabilité de trouver la solution ?
3. Même question pour une fonction à 1 bit.

Exercice 2. Considérons maintenant que la fonction f en entrée est sans restriction particulière.

1. Rappeler l'algorithme mixte, classique/quantique, qui trouve une solution x_1 telle que $f(x_1) = 1$ avec probabilité $\geq 40\%$, si un tel x_1 existe.
2. Modifier l'algorithme pour obtenir une solution avec probabilité au moins $1 - 1/N$. Préciser sa complexité en temps.

5. Impact du quantique

à court et moyen terme

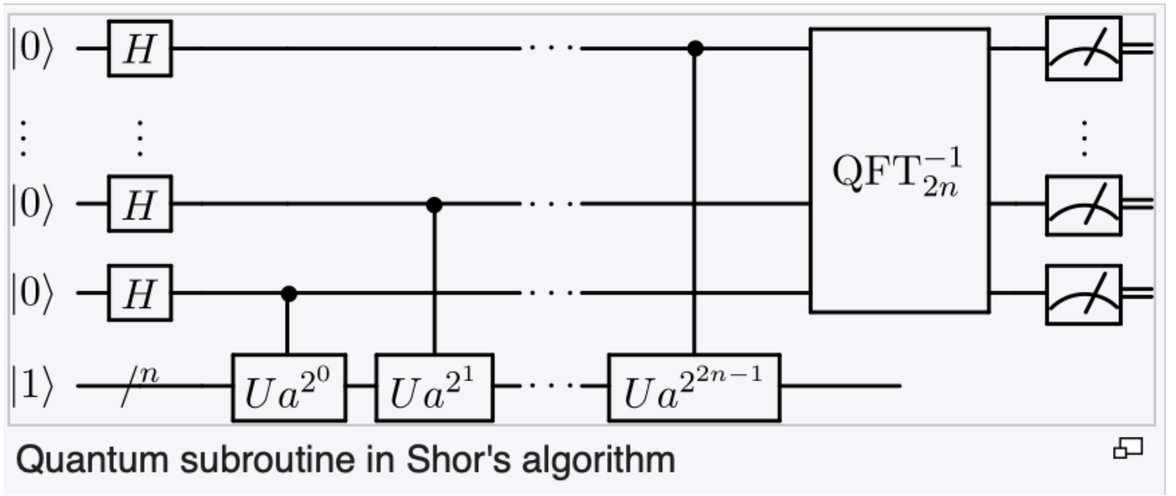
Objectif : analyser les conséquences des outils de programmation quantique sur l'informatique d'aujourd'hui, et rentrer plus dans les détails d'une algorithmique « mixte » qui utiliserait parfois du code quantique

A. Algorithme de Shor : factorisation et logarithme discret. Conséquences sur la cryptographie, cryptographie « post quantique ».
B. Echange quantique de clés : algorithme BB84.
C. Outils pour une programmation mixte, classique/quantique : zoom sur l'algorithme de Grover, s'il fallait l'adapter aux applications.

A. Algorithme de Shor [P. Shor '94]

Il permet de résoudre en temps polynomial par rapport au nombre de bits en entrée :

- Le problème Factorisation(N): trouver un diviseur de N, différent de 1 et de N, s'il en existe
- Le problème du logarithme discret modulo N, $\log_b(a) = x$ tel que $b^x = a \mod N$.



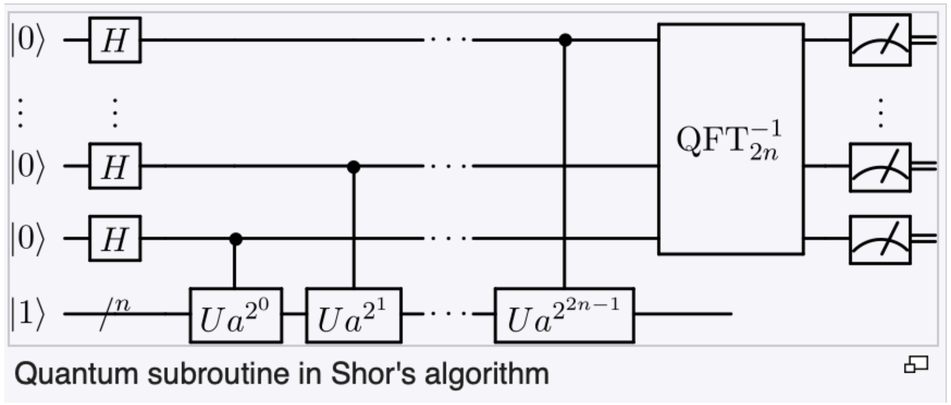
Wikipedia, Algorithme de Shor

La partie « quantique » calcule, pour un nombre a, le plus petit nombre r tel que $a^r = 1 \mod N$. Le reste est classique. Complexité $O(n^2) = O((\log N)^2)$.

A. Conséquence : besoin de crypto post-quantique

S'il était implémentable, il rendrait caducs deux protocoles cryptographiques très utilisés :

- **Protocole de chiffrement RSA** [Rivest, Shamir, Adelman '77], dont la sécurité repose sur la difficulté à décomposer un (grand) nombre en facteurs premiers.
- **Protocole d'échange de clé de Diffie-Hellman** [Diffie, Hellman '76], dont la sécurité repose sur la difficulté à calculer le logarithme discret.



Wikipedia, Algorithme de Shor

La plupart des protocoles utilisés actuellement se basent sur ces deux problèmes...

Emergence de la **cryptographie post-quantique**, qui n'a rien de quantique et qui propose d'autres protocoles, résistants à ce type d'attaque.

Exemples : CRYSTALS-Kyber (clés), CRYSTALS-Dilithium (signature), basés sur des « réseaux euclidiens structurés ».

B. Echange de clé [Bennett-Brassard 84]

Pour l'échange sécurisé de clés, il existe déjà une solution quantique.

Lecture et vidéos recommandées : cours de Frédéric Magniez au Collège de France, https://www.college-de-france.fr/chaire/frederic-magniez-informatique-et-sciences-numeriques-chaire-annuelle/events

Objectif de l'échange de clé : A et B doivent se mettre d'accord sur une clé (suite aléatoire de bits).

- Hypothèse que A et B sont bien identifiés (pas d'usurpation d'identité).
- A la fin du protocole, A et B doivent avoir la clé partagée et doivent être les seul à la posséder. Si quelqu'un a écouté la conversation entre A et B, ils doivent s'en rendre compte.

Pourquoi BB84 ?

4

1. On peut le présenter en 20’
   - en simplifiant beaucoup…
   - mais sans le massacrer, j’espère
2. Fait appel à plusieurs propriétés de qubits :
   - aspect vectoriel (superposition, mesure)
   - théorème de non-clonage
3. **Il est déjà implémenté !**
   - qubits : photons
   - fibre optique

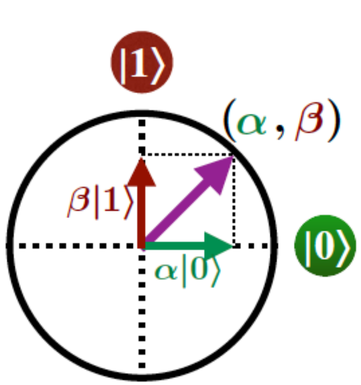
C. Bennet

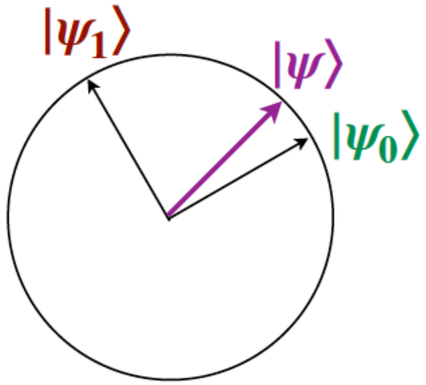
G. Brassard

1èr outil : mesures en différentes bases

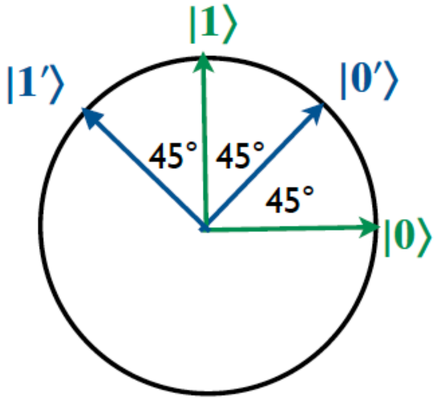
[Les images sont extraites des exposés de F. Magniez.]

Mesure et base de mesure : un qubit peut être mesuré dans n'importe quelle base orthogonale !





Nous allons choisir deux bases $|0\rangle, |1\rangle$ et avec $|0'\rangle, |1'\rangle$ une rotation de 45°.

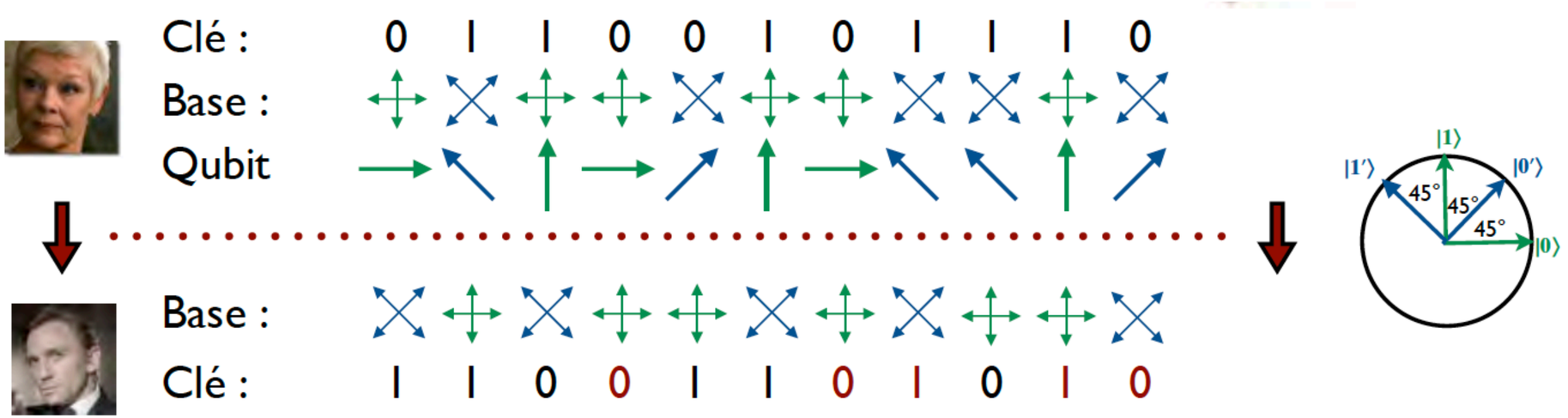


Observation : le qubit $|0'\rangle$ mesuré dans la base $|0\rangle, |1\rangle$ donne $|0\rangle$ avec proba 1/2 et $|1\rangle$ avec proba 1/2. Pareil pour tout autre combinaison.

BB84 en cachant les détails sous le tapis (1)

Communication quantique **d'Alice vers Bob.**

Alice choisit une suite de bits de clé (uniformément au hasard), une suite de bases et une suite de qubits. Elle communique ces derniers.

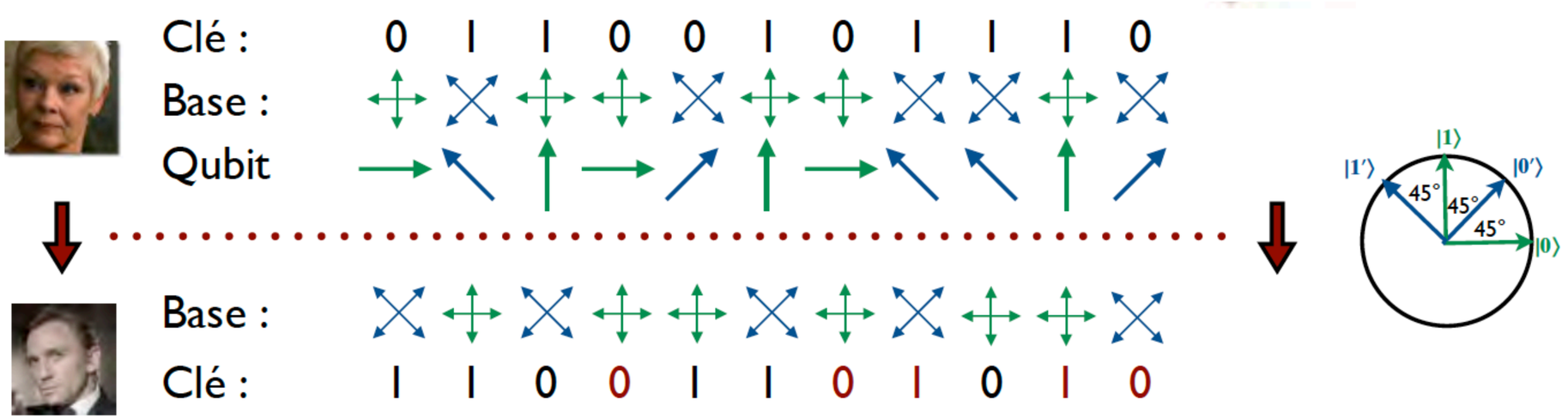


Extrait exposé F. Magniez

BB84 en cachant les détails sous le tapis (2)

Bob choisit une suite de bases et mesure les bits reçus dans la base respective.

Alice et Bob communiquent la suite de bases que chacun a choisi.

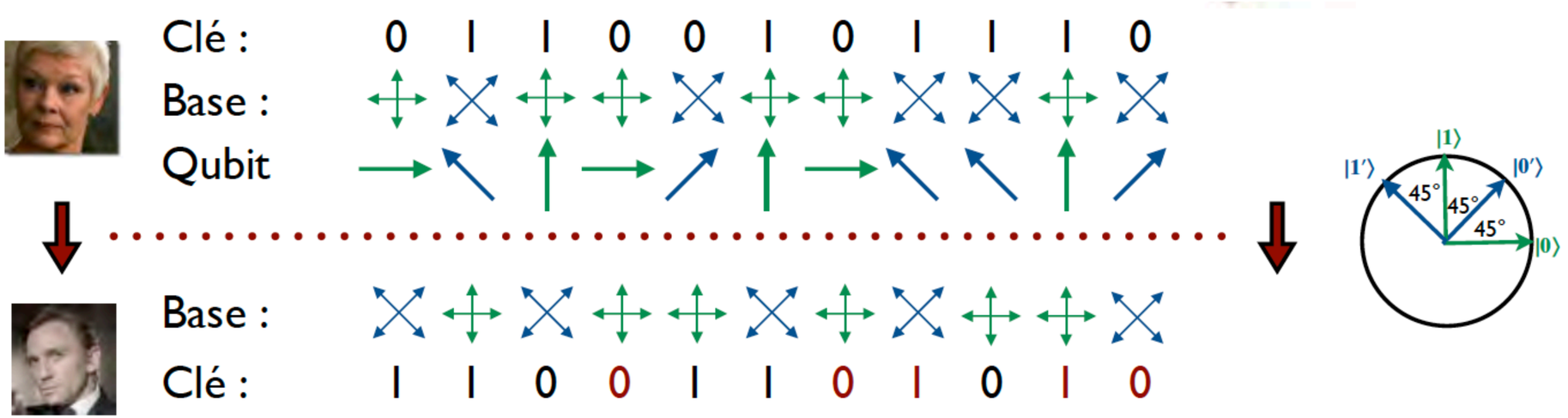


Extrait exposé F. Magniez

BB84 en cachant les détails sous le tapis (3)

En moyenne, la moitié des bases choisies par Alice et Bob coincident. On ne garde comme clé que ces bits-là. Conclusion : Alice et Bob se sont mis d'accord sur la moitié des bits ! (Enfin, modulo erreurs, mais **ce n'est pas le sujet du jour**).

Mais **quid des intrus ???**

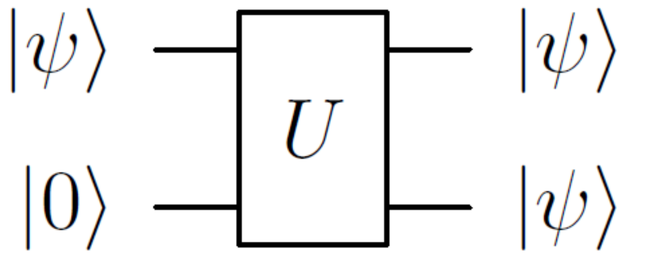


Extrait exposé F. Magniez

2ème outil : le théorème de non clonage

Théorème. Il est impossible de dupliquer un qubit.

- Informellement : si on le mesure, on le détruit, on perd son aspect vectoriel
- Formellement : utiliser la linéarité des transformations. Cf. travaux dirigés.



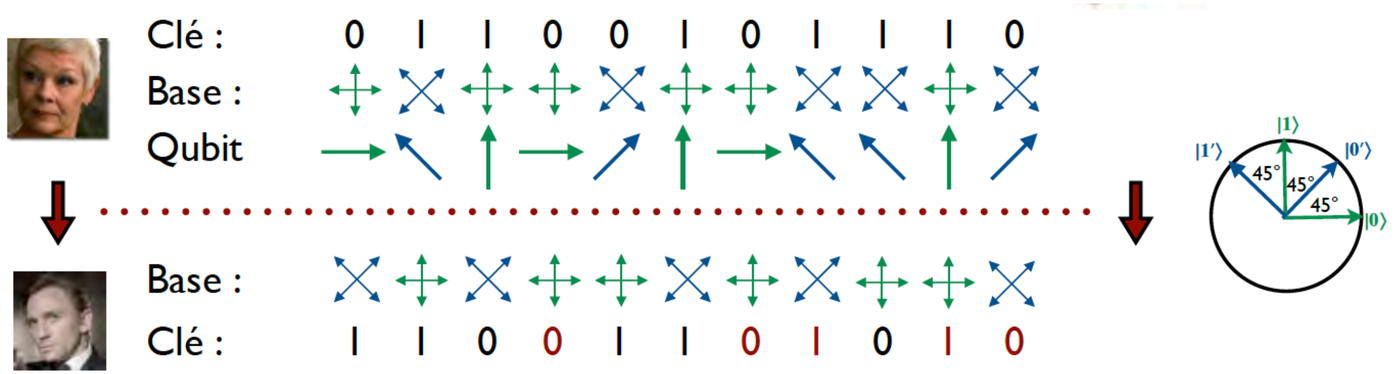
Contre-intuitif mais pas difficile à montrer, par linéarité.

Conséquences du non clonage sur BB84

Admettons qu'un intrus ait écouté les échanges secrets d'Alice vers Bob.

Il lui sera impossible de les « remettre » dans le canal les qubits interceptés sans en modifier une large proportion. Et cela se verra.

Extrait exposé F. Magniez



Extrait exposé F. Magniez

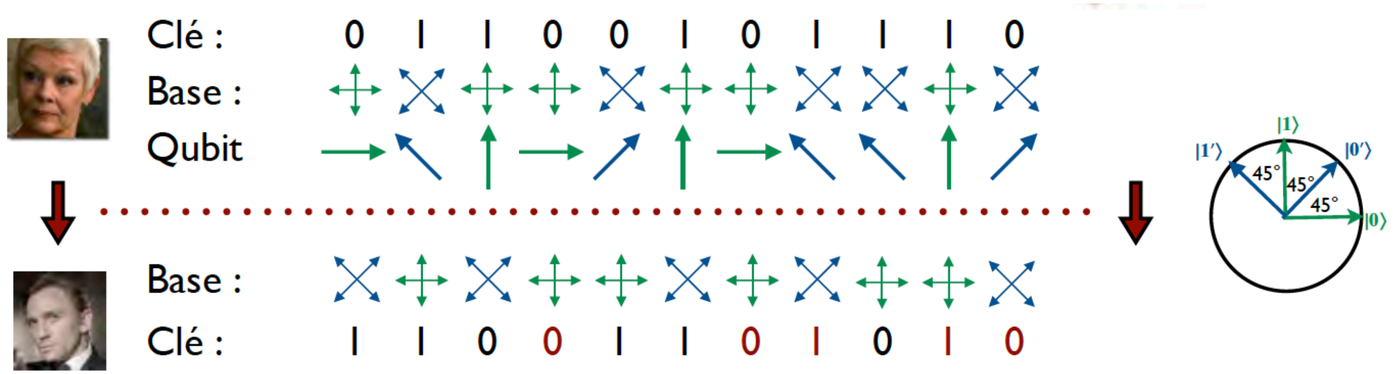
Informel mais ça se transforme en preuve, même si l'intrus a des stratégies futées.
On peut en parler plus en détail !

Conséquences du non clonage sur BB84

Admettons qu'un intrus, Eve (Evil) ait écouté les échanges secrets d'Alice vers Bob.

Option 1. L'intrus, Eve mesure au hasard le qubit dans l'une des deux bases, et le « remet » dans le canal de communication dans la même base.

Extrait exposé F. Magniez



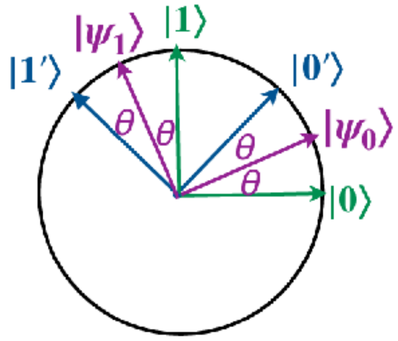
Exercice. Calculer la probabilité pour que le qubit remis par Eve soit identique au qubit émis par Alice. Calculer la probabilité que le bit lu par Eve soit égal à celui émis par Alice.

Comment ferait Bob pour détecter l'intrusion, si Eve a lu k qubits ?

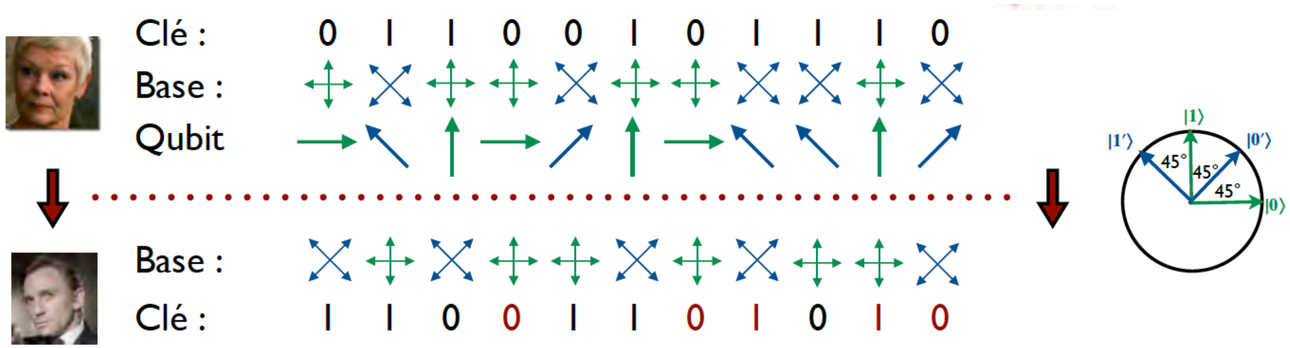
Conséquences du non clonage sur BB84

Admettons qu'Eve adopte une stratégie plus sophistiquée.

Option 2. Eve choisit une autre base ($|\psi_0\rangle, |\psi_1\rangle$), dans laquelle elle mesure le qubit intercepté et le remet dans la même base. Notons θ l'angle avec la base « canonique ».



Extrait exposé F. Magniez



Extrait exposé F. Magniez

Exercice. Quelle est la probabilité que le bit lu par Bob soit celui émis par Alice, malgré l'intrusion ? Quelle est la proba pour que le bit lu par Eve soit celui émis par Alice ? Comment détecter l'intrus ?

C. Algorithme de Grover dans les approches mixtes

1. Introduction Consider the following problem from a crossword puzzle:

_ _ r _ n h _ (Solution - piranha)

You have an online dictionary with 1, 000, 000 words in which the words are arranged alphabetically. You could program it to look for the solution to the puzzle so that it typically solves it after looking through 500, 000 words. It is very difficult to do much better than this. But that is: only if you limit yourself to a classical computer. A quantum computer can be in multiple states at the same time and, by proper design, can carry out multiple computations simultaneously. In case the above dictionary were available on a quantum computer, it would be possible to carry out the search in only about 1, 000 steps by using the quantum search algorithm.

Lov Grover, From Schrödinger's Equation to the Quantum Search Algorithm, ArXiV 2001.

Théorème.
L'algorithme de Grover mesure x_1 tel que $f(x_1) = 1$ avec probabilité au moins $1 - \frac{1}{N}$, où $N = 2^n$.

Exercice. Imaginons qu'on devrait implémenter pour de bon le puzzle proposé par Grover. Nous avons largement discuté de l'implémentation du circuit quantique de Grover.

1. Quel serait le travail à faire par un informaticien qui dispose uniquement de Qiskit et d'un ordinateur quantique ?
2. Comment encoder ne serais-ce qu'un tableau d'entiers, voire de booléens ? Même inefficace ?

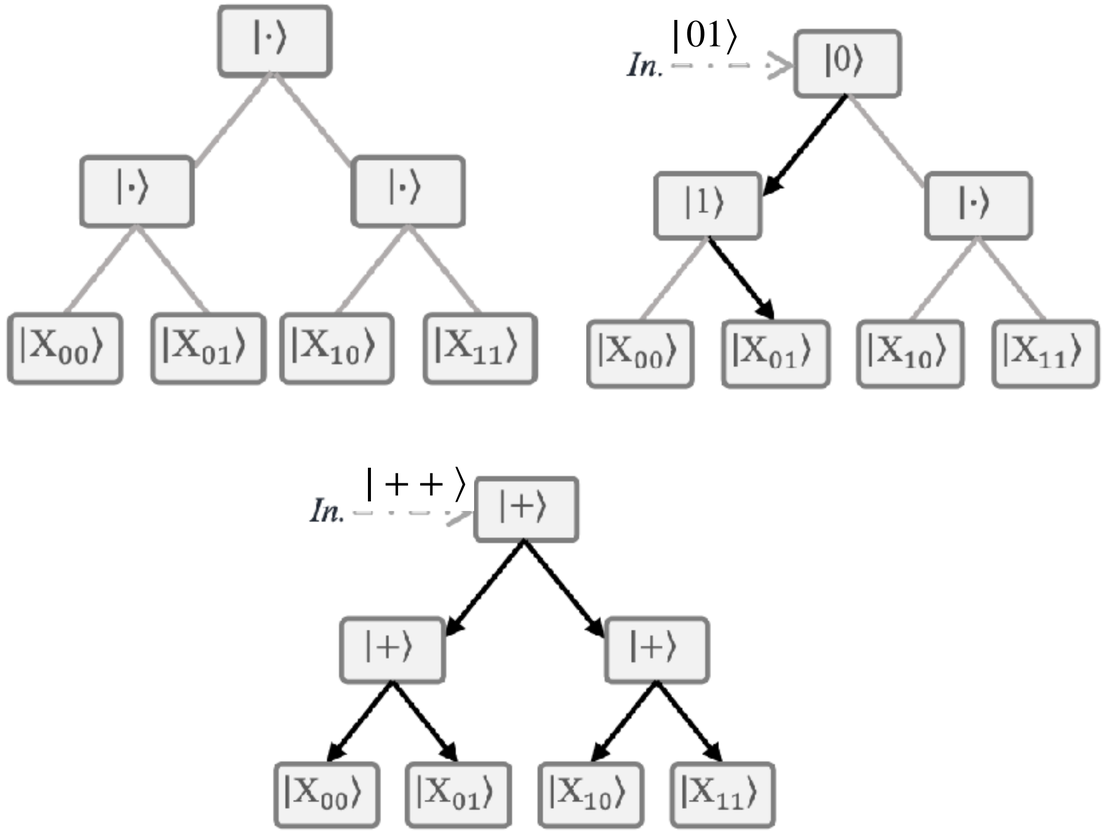
C. Quantum RAM : principe

Pour pouvoir implémenter Grover avec un tableau, on aurait besoin d'une « QRAM » où l'on puisse stocker un tableau X de booléens (entiers, etc.) de taille $N = 2^n$ et accéder à $X[i]$ et temps poly(n).

$$|i\rangle \mapsto |i\rangle\,|X[i]\rangle$$

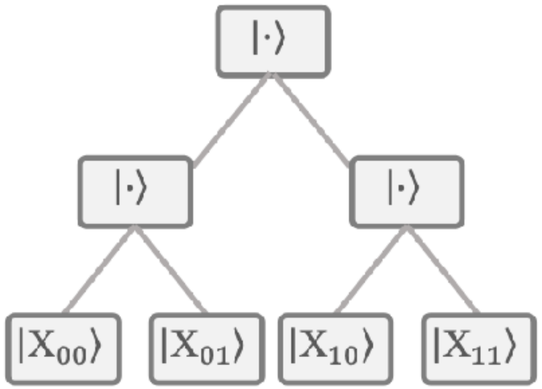
Mais en plus, on doit pouvoir « superposer » :

$$\sum_{i=0}^{N-1} \alpha_i\,|i\rangle \mapsto |\sum_{i=0}^{N-1} \alpha_i i\rangle\,|X[i]\rangle$$



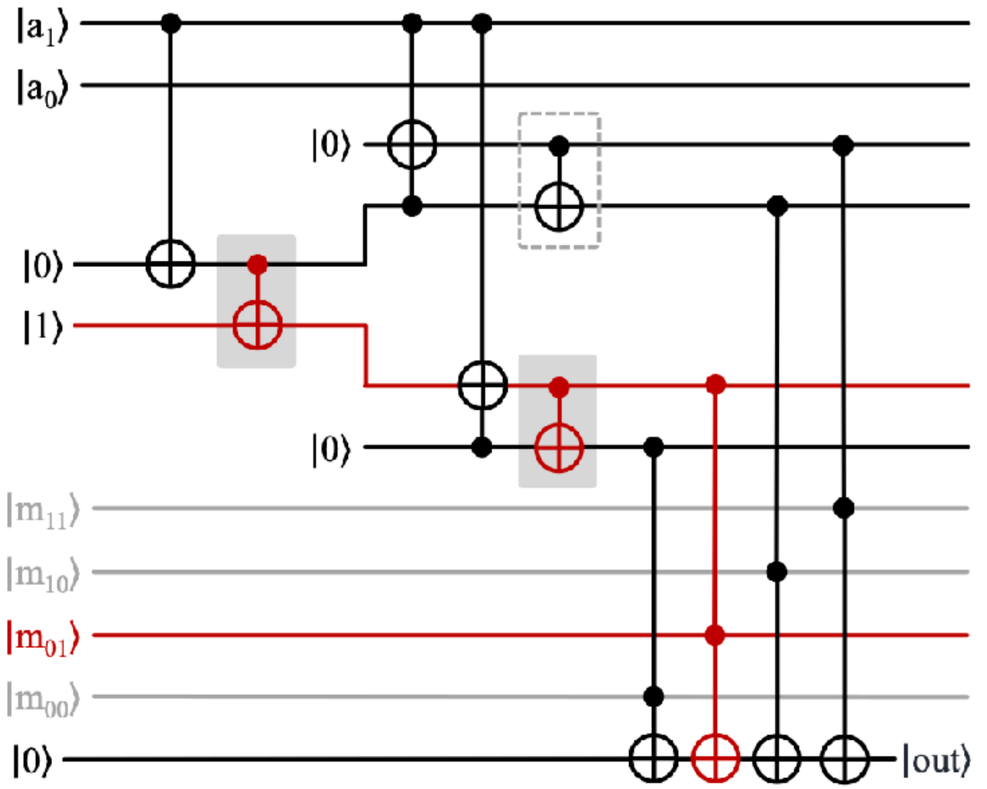
Phalak, Chatterjee, Ghosh, Quantum Random Access Memory For Dummies, ArXiV 2023

C. Quantum RAM : implémentation



Extrait de Phalak, Chatterjee, Ghosh, Quantum Random Access Memory For Dummies, ArXiV 2023.

Cf. également Arunachalam *et al.*, On the robustness of bucket brigade quantum RAM, ArXiV 2015



Implémentation par circuit de la QRAM pour un tableau de taille 4.
En rouge, les portes activées lorsqu'on lit l'adresse $|01\rangle$.

6. Conclusion

Pour aller plus loin

1. Algorithmes quantiques : circuits, qubits, portes quantiques.
2. Atypiques voire contre-intuitifs mais pas forcément des maths sophistiquées…
3. Pas trop compliqué : algo de Simons (trouve la période d'une fonction à n bits en entrée et en sortie, nombre polynomial d'appels).
4. Plus subtile : algorithme de Shor (factorisation), transformée de Fourrier quantique.
5. Cryptographie quantique, envoi de clé, « téléportation » d'un qubit. Intrication quantique, non clonage, mesure dans des bases différentes.

Exposés de Frédéric Magniez, Collège de France. Livres, par ex. [Kaye, Laflamme, Mosca, *An Introduction to Quantum Computing*, 2007; Nielsen, Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010].

Exposés d'Arthur Braida (Eviden/LIFO) pour le calcul adiabatique.

Exposés et documents de John Watrous (IBM) sur YouTube.

Matériel supplémentaire

- Petit focus sur l'intrication quantique

7. Intrication quantique

Cf. prix Nobel d'Alan Aspect.

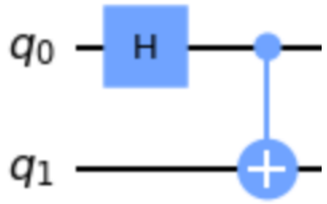
Etats de Bell (2 qubits intriqués) : que se passe-t-il si l'on éloigne les deux qubits ?

Eh bien… en mesurant le premier, on est sûrs que le deuxième donne la même mesure.

(Sérieux) doutes d'Einstein [Einstein, Podolsky, Rosen '35], qui trouve(nt) que cela contredit le principe de localité.

A. Aspect réalise une expérience à Orsay (avec Grangier, Roger et Dalibard) confirmant l'existence de ces états.

Applications à la cryptographie (plus avancées). « Téléportation » quantique.



Etat de Bell :

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$