Quantum Computer Science

David Mermin

Pôle Projet : Calcul Quantique

19 décembre 2019

Sommaire

Chapitre 1

Qu'est-ce qu'un ordinateur quantique ?

Définition

Un ordinateur quantique utilise les propriétés quantiques de la matière, telle que la superposition, afin d'effectuer des opérations sur des données.

Qu'est-ce qu'un ordinateur quantique ?

Propriété

Dans un ordinateur quantique, la physique qui code l'information (le bit) ne doit avoir aucune interaction physique qui n'est pas sous le contrôle complet du programme. La moindre interaction introduit d'importantes erreurs. C'est l'un des principaux obstacles à la création de l'ordinateur quantique.

Qu'est-ce qu'un ordinateur quantique ?

Deux points font que la situation n'est pas désespérée :

- L'isolation d'un système atomique est facile à réaliser
- Les erreurs introduites par les interactions extérieures peuvent être corrigées si elles ne sont pas trop récurrentes.

Cbit

Définition

Cbit est une information codée sur deux états distinguables et sans ambiguïté. Un Cbit est représenté en informatique par un état 0 ou 1

Cbit

Définition

Cbit est une information codée sur deux états distinguables et sans ambiguïté. Un Cbit est représenté en informatique par un état 0 ou 1

Exemple :
Un ordinateur classique utilise une suite de Cbits : 011101010001010

Cbit

Définition

Cbit est une information codée sur deux états distinguables et sans ambiguïté. Un Cbit est représenté en informatique par un état 0 ou 1

Exemple :
Un ordinateur classique utilise une suite de Cbits : 011101010001010

Le Qbit

Le Qbit est un bit quantique.

Qbit

Représentation

On représente l'état d'un Cbit dans une boîte appelée "ket" $|\,\rangle$ dans lequel on place l'état du Cbit $|0\rangle$ ou $|1\rangle$.
Ces deux etats peuvent être représentés sous forme matricielle :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; et \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Qbit

Représentation

On représente l'état d'un Cbit dans une boîte appelée "ket" $|\,\rangle$ dans lequel on place l'état du Cbit $|0\rangle$ ou $|1\rangle$.
Ces deux etats peuvent être représentés sous forme matricielle :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; et \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Représentation :

Pour un même état, il y a trois façons de le représenter ;

- $|1\rangle\,|0\rangle\,|1\rangle$
- $|101\rangle$
- $|5\rangle_3$

Produit tensoriel

Définition

On définit le produit tensoriel entre trois 1-Cbit :

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \otimes \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 z_0 \\ x_0 y_0 z_1 \\ x_0 y_1 z_0 \\ x_0 y_1 z_1 \\ x_1 y_0 z_0 \\ x_1 y_0 z_1 \\ x_1 y_1 z_0 \\ x_1 y_1 z_1 \end{pmatrix}$$

Produit tensoriel

Exemple :

$$|5\rangle_3 = |101\rangle = |1\rangle\,|0\rangle\,|1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix}$$

On peut remarquer que $|5\rangle_3$ est représenté sous forme vectorielle par que des zeros sauf à la $(5+1)^{ieme}$ position parce qu'il y a le zéro à la première position.

Cette propriété est généralisable.

propriétés

propriétés

$$(\mathbf{a} \otimes \mathbf{b}) |xy\rangle = (\mathbf{a} \otimes \mathbf{b}) |x\rangle \otimes |y\rangle = \mathbf{a} |x\rangle \otimes \mathbf{b} |y\rangle$$

et,

$$(\mathbf{a} \otimes \mathbf{b})(\mathbf{c} \otimes \mathbf{d}) = (\mathbf{ac}) \otimes (\mathbf{bd})$$

introduction

Operation réversible

L'ordinateur quantique base ses calculs sur des opérations réversibles qui transforme un Cbit dans un état initial en un Cbit dans son état final portant l'information recherchée.
Toutes les actions menées sur le Cbit peuvent être inversées.

CNOT operation

opération CNOT

L'opération CNOT est une opération réversible appliquée à un seul Cbit qui permet d'inverser l'état du Cbit. L'opérateur est noté **X**

$$\mathbf{X} : |x\rangle \rightarrow |\tilde{x}\rangle\,;\, \tilde{1} = 0 \; et \; \tilde{0} = 1$$

CNOT operation

opération CNOT

L'opération CNOT est une opération réversible appliquée à un seul Cbit qui permet d'inverser l'état du Cbit. L'opérateur est noté **X**

$$\mathbf{X} : |x\rangle \rightarrow |\tilde{x}\rangle \,;\, \tilde{1} = 0 \textit{ et } \tilde{0} = 1$$

Réversibilité

$$\mathbf{X}^2 = \mathbf{Id}$$

L'opération est réversible avec $\mathbf{X}^{-1} = \mathbf{X}$

CNOT operation

opération CNOT

L'opération CNOT est une opération réversible appliquée à un seul Cbit qui permet d'inverser l'état du Cbit. L'opérateur est noté **X**

$$\mathbf{X} : |x\rangle \rightarrow |\tilde{x}\rangle \, ; \tilde{1} = 0 \textit{ et } \tilde{0} = 1$$

Réversibilité

$$\mathbf{X}^2 = \mathbf{Id}$$

L'opération est réversible avec $\mathbf{X}^{-1} = \mathbf{X}$

Forme matriciel

On peut écrire l'opérateur **X** sous forme matricielle :

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

SWAP operation

opération SWAP

Change les états des bits i et j. L'opérateur est noté $\mathbf{S}_{ij}$

$$\mathbf{S}_{10}\,|xy\rangle = \mathbf{S}_{01}\,|xy\rangle = |yx\rangle$$

SWAP operation

opération SWAP

Change les états des bits i et j. L'opérateur est noté $\mathbf{S}_{ij}$

$$\mathbf{S}_{10}\,|xy\rangle = \mathbf{S}_{01}\,|xy\rangle = |yx\rangle$$

Forme matriciel

On peut écrire l'opérateur $\mathbf{S}_{10} = \mathbf{S}_{01}$ sous forme matricielle :

$$\mathbf{S}_{10} = \mathbf{S}_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

cNOT operation

opération cNOT

Si le bit i (bit de controle) est à l'etat $|1\rangle$ alors le bit j change d'état. Sinon, si le bit de controle est à l'état $|0\rangle$ alors le bit j reste inchangé. L'opérateur est noté $\mathbf{C}_{ij}$

$$\mathbf{C}_{10} |x\rangle |y\rangle = |x\rangle |y \oplus x\rangle , \qquad \mathbf{C}_{01} |x\rangle |y\rangle = |x \oplus y\rangle |y\rangle$$

où $\oplus$ est l'addition modulo 2

propriétés

Forme matricielle

On peut écrire l'opérateur $\mathbf{S}_{01}$ *et* $\mathbf{S}_{10}$ sous forme matricielle :

$$\mathbf{S}_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \mathbf{S}_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

propriétés

Forme matricielle

On peut écrire l'opérateur $\mathbf{S}_{01}$ *et* $\mathbf{S}_{10}$ sous forme matricielle :

$$\mathbf{S}_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \mathbf{S}_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Construire S

On peut construire **S** à l'aide de l'opérateur **C**

$$\mathbf{S}_{ij} = \mathbf{C}_{ij}\mathbf{C}_{ji}\mathbf{C}_{ij}$$

opération **n**

opération **n**

L'opérateur **n** permet la projection de l'état :

$$\mathbf{n}\,|x\rangle = x\,|x\rangle\,, \quad x = 0 \textit{ or } 1$$

opération **n**

opération **n**

L'opérateur **n** permet la projection de l'état :

$$\mathbf{n}\,|x\rangle = x\,|x\rangle\,, \quad x = 0 \text{ } or \text{ } 1$$

Forme matricielle

On peut écrire l'opérateur **n** sous forme matricielle :

$$\mathbf{n} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \tilde{\mathbf{n}} = \mathbf{n} - 1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

propriétés

propriétés

$$\mathbf{n}^2 = \mathbf{n}, \quad \tilde{\mathbf{n}}^2 = \tilde{\mathbf{n}}, \quad \mathbf{n}\tilde{\mathbf{n}} = \tilde{\mathbf{n}}\mathbf{n} = \mathbf{0}, \quad \mathbf{n} + \tilde{\mathbf{n}} = \mathbf{Id}$$

$$\mathbf{n}\mathbf{X} = \mathbf{X}\tilde{\mathbf{n}}, \quad \tilde{\mathbf{n}}\mathbf{X} = \mathbf{X}\mathbf{n}$$

propriétés

propriétés

$$\mathbf{n}^2 = \mathbf{n}, \quad \tilde{\mathbf{n}}^2 = \tilde{\mathbf{n}}, \quad \mathbf{n}\tilde{\mathbf{n}} = \tilde{\mathbf{n}}\mathbf{n} = \mathbf{0}, \quad \mathbf{n} + \tilde{\mathbf{n}} = \mathbf{Id}$$

$$\mathbf{n}\mathbf{X} = \mathbf{X}\tilde{\mathbf{n}}, \quad \tilde{\mathbf{n}}\mathbf{X} = \mathbf{X}\mathbf{n}$$

Association des opérateurs **n** et **X**

Avec des blocs **n** et **X** on peut contruire l'opérateur **S** et **C**

$$\mathbf{S}_{ij} = \mathbf{n}_i\mathbf{n}_j + \tilde{\mathbf{n}}_i\tilde{\mathbf{n}}_j + (\mathbf{X}_i\mathbf{X}_j)(\mathbf{n}_i\tilde{\mathbf{n}}_j + \tilde{\mathbf{n}}_i\mathbf{n}_j)$$

$$\mathbf{C}_{ij} = \tilde{\mathbf{n}}_i + \mathbf{X}_j\mathbf{n}_i$$

Z operation

opérateur **Z**

Cet opérateur n'existe pas sur les ordinateurs traditionnels. Il est défini par sa représentation matricielle :

$$\mathbf{Z} = \tilde{\mathbf{n}} - \mathbf{n} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

propriétés

propriétés

$$\mathbf{ZX} = -\mathbf{XZ}$$

$$\mathbf{nX} = \mathbf{X\tilde{n}}, \quad \mathbf{\tilde{n}X} = \mathbf{Xn}$$

propriétés

propriétés

$$\mathbf{ZX} = -\mathbf{XZ}$$

$$\mathbf{nX} = \mathbf{X\tilde{n}}, \quad \mathbf{\tilde{n}X} = \mathbf{Xn}$$

Association des opérateurs **n** et **X**

$$\textit{(1)}\ \mathbf{S}_{ij} = \mathbf{n}_i\mathbf{n}_j + \mathbf{\tilde{n}}_i\mathbf{\tilde{n}}_j + (\mathbf{X}_i\mathbf{X}_j)(\mathbf{n}_i\mathbf{\tilde{n}}_j + \mathbf{\tilde{n}}_i\mathbf{n}_j)$$

$$\textit{(2)}\ \mathbf{C}_{ij} = \mathbf{\tilde{n}}_i + \mathbf{X}_j\mathbf{n}_i$$

$$\textit{(3)}\ \mathbf{n} = \frac{1}{2}(\mathbf{Id} - \mathbf{Z}), \qquad \mathbf{\tilde{n}} = \frac{1}{2}(\mathbf{Id} + \mathbf{Z})$$

$$\textit{(4)}\ \mathbf{C}_{ij} = \frac{1}{2}(\mathbf{Id} + \mathbf{Z}_i) + \frac{1}{2}\mathbf{X}_j(\mathbf{Id} - \mathbf{Z}_i)$$

$$= \frac{1}{2}(\mathbf{Id} + \mathbf{X}_j) + \frac{1}{2}\mathbf{Z}_i(\mathbf{Id} - \mathbf{X}_j)$$

H operation

opérateur H

La transformation d'hadamard permet entre autre de changer l'opérateur $\mathbf{C}_{ij}$ en $\mathbf{C}_{ji}$. Cette transformation est définie par :

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

propriétés

réversibilité

$$\mathsf{H}^2 = \mathsf{Id}$$

H est bien réversible.

propriétés

réversibilité

$$\mathbf{H}^2 = \mathbf{Id}$$

H est bien réversible.

action sur **X** et **H**

$$\mathbf{HXH} = \mathbf{Z}, \qquad \mathbf{HZH} = \mathbf{X}$$

propriétés

réversibilité

$$\mathbf{H}^2 = \mathbf{Id}$$

H est bien réversible.

action sur X et H

$$\mathbf{HXH} = \mathbf{Z}, \qquad \mathbf{HZH} = \mathbf{X}$$

Association d'opérateurs pour retrouver C

$$\mathbf{C}_{ji} = (\mathbf{H}_i\mathbf{H}_j)\mathbf{C}_{ij}(\mathbf{H}_i\mathbf{H}_j)$$

propriétés

réversibilité

$$\mathbf{H}^2 = \mathbf{Id}$$

H est bien réversible.

action sur **X** et **H**

$$\mathbf{HXH} = \mathbf{Z}, \qquad \mathbf{HZH} = \mathbf{X}$$

Association d'opérateurs pour retrouver **C**

$$\mathbf{C}_{ji} = (\mathbf{H}_i\mathbf{H}_j)\mathbf{C}_{ij}(\mathbf{H}_i\mathbf{H}_j)$$

Action de **H** sur les etats à 1 Cbit

$$\mathbf{H}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad \mathbf{H}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Controlled-Z operation

opérateur Controlled-Z

Par analogie avec l'opérateur cNOT, si le bit de contrôle i est à l'état $|0\rangle$ alors il ne se passe rien et i le bit de contrôle est à l'état $|1\rangle$, on applique l'opérateur Z.
Pour un duo de Cbit :

$$\mathbf{C}_{ij}^{Z} = \mathbf{C}_{ji}^{Z}$$

Controlled-Z operation

opérateur Controlled-Z

Par analogie avec l'opérateur cNOT, si le bit de contrôle i est à l'état $|0\rangle$ alors il ne se passe rien et i le bit de contrôle est à l'état $|1\rangle$, on applique l'opérateur Z.
Pour un duo de Cbit :

$$\mathbf{C}^Z_{ij} = \mathbf{C}^Z_{ji}$$

Combinaison d'opérateurs

$$\mathbf{H}_j\mathbf{C}_{ij}\mathbf{H}_j = \mathbf{C}^Z_{ij}, \qquad \mathbf{H}_i\mathbf{C}_{ji}\mathbf{H}_i = \mathbf{C}^Z_{ji}$$

forme alternative de SWAP

SWAP avec $\mathbf{Z}$ et $\mathbf{X}$

$$\mathbf{S}_{ij} = \frac{1}{2}(\mathbf{Id} + \mathbf{Z}_i\mathbf{Z}_j) + \frac{1}{2}(\mathbf{X}_i\mathbf{X}_j)(\mathbf{Id} - \mathbf{Z}_i\mathbf{Z}_j)$$

forme alternative de SWAP

SWAP avec $\mathbf{Z}$ et $\mathbf{X}$

$$\mathbf{S}_{ij} = \frac{1}{2}(\mathbf{Id} + \mathbf{Z}_i\mathbf{Z}_j) + \frac{1}{2}(\mathbf{X}_i\mathbf{X}_j)(\mathbf{Id} - \mathbf{Z}_i\mathbf{Z}_j)$$

Définition de $\mathbf{Y}$

On peut simplifier l'expression en définissant :

$$\mathbf{Y} = i\mathbf{X}\mathbf{Z} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

forme alternative de SWAP

SWAP avec **Z** et **X**

$$\mathbf{S}_{ij} = \frac{1}{2}(\mathbf{Id} + \mathbf{Z}_i\mathbf{Z}_j) + \frac{1}{2}(\mathbf{X}_i\mathbf{X}_j)(\mathbf{Id} - \mathbf{Z}_i\mathbf{Z}_j)$$

Définition de **Y**

On peut simplifier l'expression en définissant :

$$\mathbf{Y} = i\mathbf{X}\mathbf{Z} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

forme alternative de SWAP

$$\mathbf{S}_{ij} = \frac{1}{2}(\mathbf{Id} + \mathbf{X}_i\mathbf{X}_j + \mathbf{Y}_i\mathbf{Y}_j + \mathbf{Z}_i\mathbf{Z}_j)$$

États des Qbits

État d'un Qbit : Vecteur de dimension 2

$$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

États des Qbits

État d'un Qbit : Vecteur de dimension 2

$$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

État de n Qbits : Vecteur de dimension 2^n

$$|\Psi\rangle = \sum_{x=0}^{2^n} \alpha_x |x\rangle_n \qquad \sum_{x=0}^{2^n} |\alpha_x|^2 = 1$$

États des Qbits

État d'un Qbit : Vecteur de dimension 2

$$|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |\alpha_0|^2 + |\alpha_1|^2 = 1$$

État de n Qbits : Vecteur de dimension 2^n

$$|\Psi\rangle = \sum_{x=0}^{2^n} \alpha_x |x\rangle_n \qquad \sum_{x=0}^{2^n} |\alpha_x|^2 = 1$$

État d'une paire de Qbits : Produit de Kronecker des états

$$|\Psi\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$$

Opérations Réversibles sur les Qbits

Opérateurs Unitaires

Pour pouvoir utiliser les Qbits, il est nécessaire de ne les manipuler qu'avec des opérateurs réversibles. On utilise les opérateurs unitaires, vérifiant :

$$\mathbf{u}\mathbf{u}^{\dagger} = \mathbf{u}^{\dagger}\mathbf{u}$$

Opérations Réversibles sur les Qbits

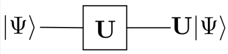
Opérateurs Unitaires

Pour pouvoir utiliser les Qbits, il est nécessaire de ne les manipuler qu'avec des opérateurs réversibles. On utilise les opérateurs unitaires, vérifiant :

$$\mathbf{u}\mathbf{u}^\dagger = \mathbf{u}^\dagger\mathbf{u}$$

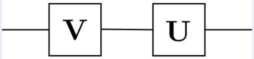
Représentation Circuit

On représente l'action de l'opérateur **u** sur un état $|\Psi\rangle$ par le circuit suivant :



Association d'Opérateurs

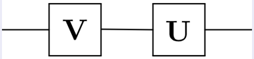
En Série



$\Longleftrightarrow$

Association d'Opérateurs

En Série



$\Longleftrightarrow$

En Parallèle

$$\mathbf{U}|\Psi\rangle \otimes \mathbf{V}|\Phi\rangle = (\mathbf{U} \otimes \mathbf{V})|\Psi\Phi\rangle$$

La Règle de Born

Règle de Born pour la mesure d'un Qbit

Étant donné un état $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, la probabilité de mesurer le Qbit dans l'état $|x\rangle$ est $p(x) = |\alpha_x|^2$, $x \in \{0, 1\}$

La Règle de Born

Règle de Born pour la mesure d'un Qbit

Étant donné un état $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, la probabilité de mesurer le Qbit dans l'état $|x\rangle$ est $p(x) = |\alpha_x|^2$, $x \in \{0, 1\}$

Superposition d'États

Le Qbit ne peut être vu comme étant dans l'état $|0\rangle$ **ou** l'état $|1\rangle$ avec une certaine probabilité : il est dans un **état superposé** et la mesure n'aboutit qu'à un seul état.

La Règle de Born

Règle de Born pour la mesure d'un Qbit

Étant donné un état $|\Psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, la probabilité de mesurer le Qbit dans l'état $|x\rangle$ est $p(x) = |\alpha_x|^2$, $x \in \{0, 1\}$

Superposition d'États

Le Qbit ne peut être vu comme étant dans l'état $|0\rangle$ **ou** l'état $|1\rangle$ avec une certaine probabilité : il est dans un **état superposé** et la mesure n'aboutit qu'à un seul état.

Règle de Born Généralisée

On peut généraliser ce qui précède dans le cas où il y a $n+1$ Qbits $|\Psi\rangle_{n+1} = \alpha_0|0\rangle|\Phi_0\rangle + \alpha_1|1\rangle|\Phi_1\rangle$ et où l'on n'en mesure qu'un. Le résultat est $|x\rangle|\Phi_x\rangle$ avec la probabilité $p = |\alpha_x|^2$.

Chapitre 4

Recherche avec un Ordinateur Quantique

Objectif :

Écrire des algorithmes de recherche de nombres ayant une complexité infèrieure à celle d'algorithmes classiques.

Exemple de recherche d'un nombre unique (boite noire) :

Algorithme classique : O(N) $\rightarrow$ **Calcul quantique :** O($\sqrt{N}$)
(plus précisément $\frac{\pi}{4}\sqrt{N}$, pour N assez grand)

Méthode de Grover : "Black-box subroutine"

Exemple de la recherche d'un nombre unique

Description du problème :

Une fonction "boite noire" f, d'opérateur $\mathbf{U}_f$, définie par :
f(x)=1 si $x = a$, $f(x) = 1$ si $x \neq a$, a étant un entier inconnu qu'on cherche à déterminer (on posera $a < 2^n$).

Idée générale :

On utilisera un processus itératif qui passe par deux opérateurs **V** et **W**. $\mathbf{U}_f$ n'agit que sur l'unique Qbit d'output, alors que **V** et **W** n'agissent que sur les n Qbits d'input. On obtient un résultat ayant une forte probabilité d'être correct.

Définition de **V** et **W**

Définition de **V** :

$\mathbf{V}|\psi\rangle$ renvoie le symétrique de $|\psi\rangle$ par rapport à l'axe $|a_\perp\rangle$,
i.e. : $\mathbf{V} = \mathbf{1} - 2|a\rangle\langle a|$
On a alors : $\mathbf{V}\,|a\rangle = -\,|a\rangle$ et $\mathbf{V}|a_\perp\rangle = |a_\perp\rangle$
V est construit à partir de *$\mathbf{U}_f$, qui n'est pas utilisé directement dans l'algorithme.

Définition de **W** :

$\mathbf{W}|\psi\rangle$ renvoie le symétrique de ψ par rapport à l'axe $|\phi\rangle$,
où $|\phi\rangle = \mathbf{H}^{\otimes n}\,|0\rangle_n = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n$ (superposition uniforme des entrées possibles)
i.e. : $\mathbf{W} = 2\,|\phi\rangle\langle\phi| - \mathbf{1}$

Implémentation de l'algorithme

Initialisation :

L'entrée sera composée de n Qbits et notée $|x\rangle$ et le Qbit de sortie sera noté $|y\rangle$. Initialement, on aura $|x\rangle = |\phi\rangle$. On prendra aussi : $|y\rangle = \mathbf{H}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, qui permet de tester l'égalité à a (cf le problème de Bernstein–Vazirani, chap 2).

Prcessus itératif :

On applique simplement l'opérateur **WV** un grand nombre de fois. L'ensemble de Qibts $|x\rangle$ converge vers $|a\rangle$, de sorte que la probabilité d'obtenir a lors de la mesure après un grand nombre d'itérations est très proche de 1.

Construction de **V** et de **W**

Construction de **V** :

V est construit à partir de $\mathbf{U}_f$: On prend $|y\rangle = \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, forme pour laquelle appliquer $\mathbf{U}_f$ revient à appliquer un opérateur linéaire **V** aux n Qbits de départ. L'opérateur est alors défini par :
$\mathbf{V}|x\rangle = (-1)^{f(x)} \otimes \mathbf{H}|1\rangle$

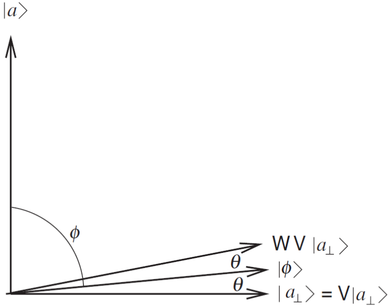
Avantage de l'opérateur **H**

H permet à $\mathbf{U}_f$ de n'agir que sur les n Qbits de départ en laissant inchangé le Qbit de sortie.

Construction de **V** et de **W**

Situation de départ

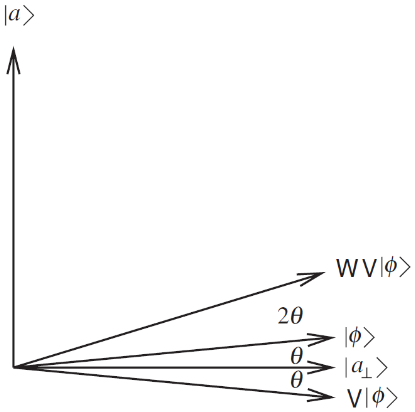
On initialise l'algorithme avec $|\psi\rangle = \frac{1}{2^{n/2}} \times \sum_{x=0}^{2^n-1} |x\rangle_n$
$|\psi\rangle$ est presque orthogonal à $|a\rangle$, en effet :
$\langle\psi|a\rangle = \cos\phi = \frac{1}{2^{n/2}} = 1/\sqrt{N}$
$\theta = \pi/2 - \phi$ ie $\theta \simeq 2^{-n/2}$



Construction de **V** et de **W**

Objectif

On compose successivement par **WV** (rotation) pour atteindre $|a\rangle$ avec $WV^k|\phi\rangle$



Construction de **V** et de **W**

Construction de W

Est l'identité pour tous les états sauf $|00...00\rangle$: multiplie par -1

$-\mathbf{W} = \mathbf{H}^{\otimes n}\mathbf{X}^{\otimes n}(\mathbf{c}^{n-1}\mathbf{Z})\mathbf{X}^{\otimes n}\mathbf{H}^{\otimes n}$

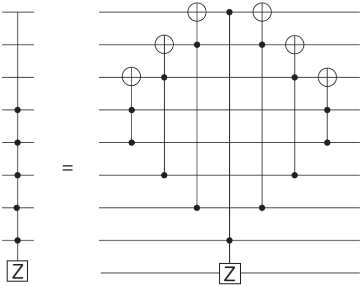


Figure – Schéma logique de **W**

Construction de **V** et de **W**

Construction de W

Schéma précédent = QBits auxiliaires doivent être tous égaux à 0
$\rightarrow$ contraignant
S'affranchir de cela avec une structure symétrique

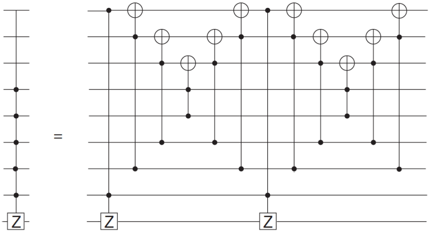


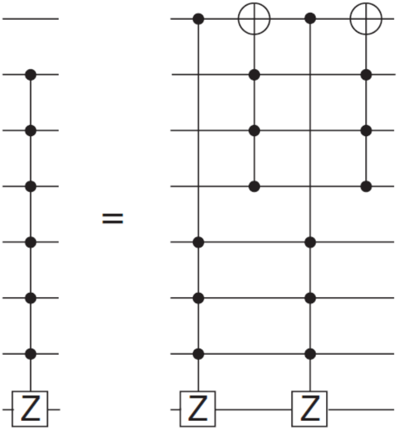
Figure – Nouveau schéma logique de **W**

Construction de **V** et de **W**

Construction de W

On peut réduire le nombre de Qbits auxiliaires à 1

Performances accrues



Généralisation à plusieurs entiers inconnus

Nouvelle écriture du problème

La fonction "boite noire" f devient :

$$f(x) = 0 \quad si \quad x \neq a_1, ..., a_m \quad ; \quad f(x) = 1, x = a_1, ..., a_m$$

V devient :

$$\mathbf{V}|x\rangle = |x\rangle \quad si \quad x \neq a_1, ..., a_m \quad ; \quad \mathbf{V}|x\rangle = -|x\rangle \; si \quad x = a_1, ..., a_m$$

Enfin $|a\rangle$ devient :

$$|\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |a_i\rangle$$

Généralisation à plusieurs entiers inconnus

Convergence

Angle θ entre $|\psi_\perp\rangle$ *et* $|\phi\rangle$:

$$\sin\theta = \langle\psi|\phi\rangle = \sqrt{m/2^n}$$

Si $m/2^n << 1$ on converge très proche de $|\psi\rangle$ avec $(\pi/4)2^{n/2}/\sqrt{m}$

Inconvénient

Méthode nécessite de connaître m à l'avance
$\rightarrow$ on peut contourner le problème avec une transformée de Fourier quantique

Cas de recherche d'un élément parmi 4

Formulation rapide

Avec n=2 ou N= 4, $\sin\theta = 1/2$, ie : $\theta = 30$
3*30 = 90 : résolution exacte avec une itération
Ordinateurs classiques : tester tous les cas possibles