3

Calculs quantiques

3.1 Notion de calculateur

Un état de n bits d'un calculateur classique ou registre classique de taille n, ne peut stocker, en instant donné, qu'un seul entier $i \in [0,\ 2^n - 1]$ décrit en notation binaire par

$$\begin{aligned} i &= i_{n-1}2^{n-1} + i_{n-2}2^{n-2} + ... + i_1 2^1 + i_0 2^0 \\ &= \sum_{m=0}^{n-1} i_m 2^m \end{aligned} \tag{3.1}$$

où $i_m \in [0,\ 1]$. Ainsi, 3 bits physiques peuvent etre préparés dans $2^3 = 8$ configurations différentes, représentant les nombres de 0 à 7, par exemple, les chaines binaires

$$011$$

$$111$$

représentent respectivement les nombres 3 et 7.

Un calculateur quantique est une collection de n qubits qui représente un registre quantique de taille n. L'état de n qubits d'un calculateur quantique est

$$\begin{aligned} |\psi_1\rangle &= \sum_{i=0}^{2^n-1} c_i |i\rangle \\ &= \sum_{i_{n-1}=0}^{1} ... \sum_{i_1=0}^{1} \sum_{i_0=0}^{1} c_{n-1}...c_1 c_0 |i_{n-1}\rangle \otimes |i_{n-2}\rangle ... \otimes |i_0\rangle \\ &= \sum_{i_{n-1},...c_1 c_0=0}^{1} c_{n-1,...1,0} |i_{n-1} i_{n-2} ... i_1 i_0\rangle \end{aligned} \tag{3.2}$$

avec la contrainte (complétude)

$$\sum_{i=0}^{2^n-1} |c_i|^2 = 1$$

Ainsi, en vertu du principe de superposition clairement visible dans l'équation précédente, un registre quantique de n qubits peut être préparé non seulement dans l'état $|i\rangle$ de la base de calcul, mais aussi dans une superposition d'états et donc stocker 2^n nombres, qui augmente exponentiellement avec le nombre de qubits. Par conséquent, le principe se superposition offre de nouvelles possibilités de calculs comme d'un grand nombre d'opérations.

Par exemple: pour n=2, un état générique de 2 qubits d'un calculateur quantique s'écrit:

$$\begin{aligned} |\psi\rangle &= (c_0 |0\rangle + c_1 |1\rangle) \otimes (c'_0 |0\rangle + c'_1 |1\rangle) \\ &= c_{0,0} |0\rangle |0\rangle + c_{0,1} |0\rangle |1\rangle + c_{1,0} |1\rangle |0\rangle + c_{1,1} |1\rangle |1\rangle \\ &= c_{0,0} |00\rangle + c_{0,1} |01\rangle + c_{1,0} |10\rangle + c_{1,1} |11\rangle \end{aligned} \tag{3.3}$$

Pour effectuer un calcul quantique, il faut effectuer les trois étapes de base suivantes.

· La préparation de n qubits dans l'état initial $|\psi_i(t)\rangle$ (input state) au temps t_0. Le vecteur d'état initial est un vecteur de l'espace de Hilbert à 2^n dimensions $H^{\otimes n}$.

· L'implémentation de la transformation unitaire désirée ou souhaitée $U(t, t_0)$ qui agira sur l'état initial en évitant tout interaction avec l'environnement, $|\psi_f(t)\rangle = U(t, t_0) |\psi_i(t_0)\rangle$

· La mesure à l'instant t sur les n qubits afin d'obtenir l'état final (ouput state).

Il est à noter que l'évolution unitaire $U(t, t_0)$ réversible: connaissant le vecteur d'état au temps t, on peut remonter à celui au temps t_0 par

$$U^-(t,\ t_0) = U(t_0, t)$$

$$|\psi_i(t_0)\rangle \rightarrow \boxed{U(t,\ t_0)} \rightarrow |\psi_f(t)\rangle$$

Un calcul quantique est évolution quantique.

3.2 Les circuits quantiques

3.2.1 Energie-information-réversibilité

L'information, malgré son caractère abstrait est portée par un support physique. Il est donc intéressant de se demander s'il est possible de calculer sans dissiper de l'énergie.

Principe Landeur: Chaque fois qu'un bit d'information est effacé, la quantité d'énergie dissipé dans l'environnement vaut au moins $k_B T \ln 2$.

Puisque le principe de landeur est lié à l'invisibilité, il est légitime de se poser la question de savoir si les opérations logiques habituelles peuvent être conduites de façon réversible, et donc sans dissipation de l'énergie.

En effet toute fonction irréversible

$$f: \ \{0,\ 1\}^m \rightarrow \ \{0,\ 1\}^n$$

peut être en fonction réversible en définissant une fonction

$$\widetilde{f}: \ \{0,\ 1\}^{m+n} \rightarrow \ \{0,\ 1\}^{m+n}$$

telle que

$$\widetilde{f}\,(x, y) = (x, y \oplus^n f(x))$$

où $\oplus^n$est l'addition modulo 2^n, x représente m bits lorsque y et $f(x)$ représente n bits.

Puisque $\widetilde{f}$ transforme des entrées distinctes en sorties distinctes, elle est une fonction (m+n) bits inversible.

En effet puisque $f(x) + f(x) = 0 \ \forall f(x)$

$$(x, y) \rightarrow (x,\ y \oplus f(x)) \rightarrow (x,\ y \oplus f(x) \oplus f(x)) = (x, y)$$

Il est donc possible de trouver une porte logique universelle.

3.3 Parallélisme quantique

Dans la notation $|x\rangle$, où le nombre x est un des huit nombres (en binaire)

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$$

un registre quantique de taille 3 peut stocker les entiers individuels comme 3 ou 7

$$\begin{aligned} |0\rangle \otimes |1\rangle \otimes |1\rangle &\equiv |011\rangle \equiv |3\rangle \\ |1\rangle \otimes |1\rangle \otimes |1\rangle &\equiv |111\rangle \equiv |7\rangle \end{aligned}$$

mais, aussi les stocker simultanément. On parle alors de parallélisme quantique. En effet, si au lieu de prendre le premier single-qubit dans l'état $|0\rangle$ ou $|1\rangle$, on le prend plutôt dans l'état superposé $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, alors

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle \equiv \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle) \equiv \frac{1}{\sqrt{2}}(|3\rangle + |7\rangle)$$

on peut évidement préparer ce registre de taille 3 dans une superposition d'état des huit entiers, en mettant chaque single-qubit dans l'état superposé $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$;

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ = \; & \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\ = \; & \frac{1}{\sqrt{2^3}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle) \\ = \; & \frac{1}{\sqrt{2^3}} \sum_{i=0}^{2^3-1} |i\rangle \end{aligned} \tag{3.4}$$

3.3.1 Portes single-qubits

Les opérateurs sur un single-qubit (1-qubit) sont décrites par des matrices de Pauli X, Y, Z, la porte de Walsh-Hadamard et la porte Phase Shift.

Porte de Walsh-Hadamard

La porte de walsh-Hadamard, définie par la matrice

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

permet de transformer les états de base $\{|0\rangle\,,\ |1\rangle\}$ en état superposés

$$\begin{aligned} W|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ W|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

soit sous forme compacte

$$\begin{aligned} W|k\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^k|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left((-1)^k|k\rangle + |1-k\rangle\right), \qquad k = \{0,1\} \end{aligned}$$

ou schématiquement par le diagramme

$$|0\rangle \rightarrow \boxed{\text{W}} \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

comme $W^2 = I$, la transformation inverse $W^{-1} = W$, la forme de la matrice W montre que W est hermitien.

Le diagramme précédent représente un circuit quantique de taille 3 qui affecte la transformation de walsh-Hadamard à 3 single-qubits,

$$W^{\otimes 3}|000\rangle = W|0\rangle \otimes W|0\rangle \otimes W|0\rangle$$

$$\left.\begin{array}{l} |0\rangle \rightarrow \boxed{\text{W}} \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |0\rangle \rightarrow \boxed{\text{W}} \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |0\rangle \rightarrow \boxed{\text{W}} \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \end{array}\right\} \Rightarrow \frac{1}{\sqrt{2^3}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\right)$$

Le résultat (output) est une superposition de tous les huit entiers de 0 à 7.

exemple:

$$\begin{aligned} W^{\otimes 3}|101\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \\ &= \frac{1}{\sqrt{2^3}}\left(|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle\right) \\ &= \frac{1}{\sqrt{2^3}}\left(|0\rangle - |1\rangle + |2\rangle - |3\rangle - |4\rangle + |5\rangle - |6\rangle + |7\rangle\right) \end{aligned}$$

En générale, si initialement on a un registre de taille n dans un état $y = \{0,1\}^n$, alors

$$\begin{aligned} W^{\otimes n}|y\rangle &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^3-1}(-1)^{yx}|x\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^3-1}e^{i\pi yx}|x\rangle \end{aligned}$$

où le produit de $y = (y_{n-1}y_{n-2}...y_1y_0)$ et de $x = (x_{n-1}x_{n-2}...x_1x_0)$

$$yx = y_{n-1}x_{n-1} + y_{n-2}x_{n-2} + ... + y_1x_1 + y_0x_0$$

Si l'on prend $|0_m\rangle$ comme état initial du registre de résultats, alors

$$U|x \otimes 0_m\rangle = |x \otimes f(x)\rangle$$

si on applique W sur le registre de données dans l'état $|0_n\rangle$ avant U, le vecteur d'état dans l'état final sera par linéarité

$$\begin{aligned} \left|\psi_{fin}\right\rangle &= U|W0_n \otimes 0_m\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^3-1} |x \otimes f(x)\rangle \end{aligned}$$

Remarque 1 La rotation par une angle δ sur l'axe $\widehat{u}$ s'écrit comme:

$$\begin{aligned} R_{\widehat{u}}(\delta) &= e^{-i\frac{\delta}{2}(\widehat{u}\cdot\ \sigma)} \\ &= I\ \cos\left(\frac{\delta}{2}\right) - i\,(\widehat{u}\cdot\ \sigma)\sin\left(\frac{\delta}{2}\right) \end{aligned} \tag{3.5}$$

on note que la porte de walsh-Hadamard est une opération de rotation d'angle $(\delta = \pi)$ autour de l'axe $\widehat{u}' = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$. En effet;

$$W = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = -iR_{\widehat{u}'}(\pi) \tag{3.6}$$

Remarque 2 L'application de la porte W à un single-qubit arbitraire $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ est un exemple de l'interférence quantique qui se manifeste mathématiquement par l'addition des amplitudes de probabilités. En effet

$$W|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

Par exemple:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^x|1\rangle\right), \qquad x \in \{0,1\}.$$

pour $x = 0$, $W|\psi\rangle = \frac{1}{\sqrt{2}}W(|0\rangle + |1\rangle) = |0\rangle$.

Porte Phase Shift

La porte Phase-Shift définie par la matrice

$$R_Z(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}$$

et symboliquement représentée par le diagramme suivant:

$$|k\rangle \rightarrow \boxed{R_Z(\delta)} \rightarrow e^{i\,k\,\delta}\,|k\rangle$$

laisse inchangée l'état de base $|0\rangle$ et change la phase globale de l'état $|0\rangle$, $e^{i\,\delta}\,|1\rangle$.

· La porte de Walsh-Hadamard et la porte Phase-Shift peuvent être combinées pour construire le circuit de taille 4, qui génère au facteur de phase globale $e^{i\,\frac{\theta}{2}}$ près le single qubit générique

$$\begin{aligned} |k\rangle &\rightarrow \boxed{W} \rightarrow \boxed{R_Z(\theta)} \rightarrow \boxed{W} \rightarrow \boxed{R_Z\left(\tfrac{\pi}{2}+\varphi\right)} \rightarrow |\psi\rangle \\ |\psi\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\,\varphi}\,|1\rangle \end{aligned}$$

Ce circuit quantique s'écrit vectoriellement sous la forme

$$R_Z\left(\frac{\pi}{2}+\varphi\right) W\; R_Z(\theta)\, W\,|0\rangle = |\psi\rangle = e^{i\,\frac{\theta}{2}}\left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\,\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle\right)$$

Et d'un manière générale, ces deux portes (la porte de Walsh-Hadamard et la porte phase-Shift) peuvent être utilisées pour transformer l'état initial $|0_1\rangle\,|0_2\rangle\cdots|0_n\rangle$ d'un registre de n qubits en n'importe quel état de type $|\psi_1\rangle\,|\psi_2\rangle\cdots|\psi_n\rangle$, où $|\psi_i\rangle$ est un état superposé arbitraire de $|0\rangle$ et $|1\rangle$.

Ce sont ces états n qubits qu'on appelle états produit tensoriel ou état séparables.

Le tableau suivant présent les portes unitaires single-qubit les plus usuelles.

Nom	Diagramme	Matrice dans $\{\|0\rangle, \|1\rangle\}$
$Walsh$ $-Hadamard$	$\|k\rangle \rightarrow \boxed{W} \rightarrow \frac{1}{\sqrt{2}}\left((-1)^k \|k\rangle + \|1-k\rangle\right)$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
$Pauli\ X$	$\|k\rangle \rightarrow \boxed{X} \rightarrow \|1-k\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$Pauli\ Y$	$\|k\rangle \rightarrow \boxed{Y} \rightarrow i\,(-1)^k \|1-k\rangle$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
$Pauli\ Z$	$\|k\rangle \rightarrow \boxed{Z} \rightarrow (-1)^k \|k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$Phase$	$\|k\rangle \rightarrow \boxed{S} \rightarrow (i)^k \|k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$Phase-Shift$	$\|k\rangle \rightarrow \boxed{R_Z(\delta)} \rightarrow e^{i\,k\,\delta} \|k\rangle -$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}$

3.3.2 Portes de contrôle et génération d'intrication

En générale, un registre de taille $n > 1$ peut être préparé dans des états corrélés (intriqués).

On rappelle que, pour $n = 2$, l'état

$$\alpha\,|00\rangle + \beta\,|01\rangle = |0\rangle \otimes (\alpha\,|0\rangle + \beta\,|1\rangle)$$

est séparable en $|\psi_1\rangle = |0\rangle$ et $|\psi_2\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle)$.

Par contre, l'état

$$\alpha\,|00\rangle + \beta\,|11\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

est corrélés $(\alpha,\ \beta \neq 0)$.

Afin d'intriquer au moins deux qubits, il nous faut étendre notre répertoire de portes logiques aux portes logiques 2-qubits qui réalise une dynamique conditionnelle.

Ces portes sont des portes de contrôle U qui traduisent quantiquement

$$|x\rangle\,|y\rangle \rightarrow |x\rangle\,U^x\,|y\rangle$$

qui correspond, pour $x, y \in \{0, 1\}$ à

$$\begin{aligned} |0\rangle |0\rangle &\rightarrow |0\rangle |0\rangle \\ |0\rangle |1\rangle &\rightarrow |0\rangle |1\rangle \\ |1\rangle |0\rangle &\rightarrow |1\rangle U |y\rangle \\ |1\rangle |1\rangle &\rightarrow |1\rangle U |y\rangle \end{aligned}$$

Usuellement, on l'appelle porte controlled-U ou CU et on la représente sous formes de décomposition spectrale et matricielle, dans la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, par

$$|0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes U = \begin{pmatrix} I & O \\ O & U \end{pmatrix}$$

$$\begin{array}{ccc} |x\rangle & \rightarrow \bullet \rightarrow & |x\rangle \\ & | & \\ |y\rangle & \rightarrow \boxed{U} \rightarrow & U^x |y\rangle \end{array}$$

Porte CU

où I, O, U sont des matrices 2×2.

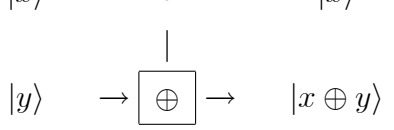
Le premier bit $|x\rangle$ agit comme contrôle et sa valeur reste inchangée à la sortée. Le second bit $|y\rangle$ est appelé cible. Sur le diagramme, le contrôle est représenté le point noir.

Porte CNOT La plus populaire des portes CU est la porte $CNOT$ où CX qui opère la transformation décrite par

$$\begin{aligned} CNOT &= CX = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes X \\ &= \begin{pmatrix} I & O \\ O & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

autrement qui inverse le bit cible $|y\rangle$ lorsque le bit de contrôle $|x\rangle$ est dans l'état $|1\rangle$, on l'a résume par

$$CNOT |x\rangle |y\rangle = |x\rangle |x \oplus y\rangle, \quad x, y \in \{0, 1\}$$



x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Porte CNOT

on note sur la table de vérité que lorsque le cible est dans l'état $|1\rangle$, la porte $CNOT$ devient la porte $COPY$

$$|x\rangle |0\rangle \rightarrow |x\rangle |x\rangle , \qquad x \in \{0, 1\}$$

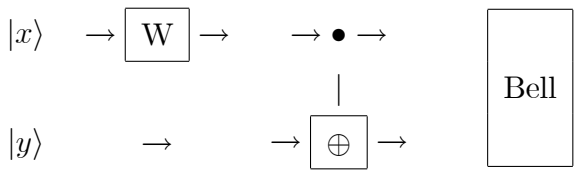
par conséquent

$$CNOT (\alpha |0\rangle + \beta |1\rangle) |0\rangle = \alpha |00\rangle + \beta |11\rangle$$

Basse de Bell La basse de Bell est définie comme:

$$\begin{aligned} \left|\phi^+\right\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ \left|\phi^-\right\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\ \left|\psi^+\right\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \\ \left|\psi^-\right\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \end{aligned}$$

par les portes logiques dans la base $\{|0\rangle , \ |1\rangle\}$, nous pouvons travers le circuit:



Il est facile de vérifier que ce circuit produit les transformations

$$|00\rangle \rightarrow \left|\phi^+\right\rangle ; \ |10\rangle \rightarrow \left|\phi^-\right\rangle ; \ |01\rangle \rightarrow \left|\psi^+\right\rangle ; \ |11\rangle \rightarrow \left|\psi^-\right\rangle$$

On note que cette transformation peut être inversée simplement en exécutant le circuit de la droite vers la gauche, puisque les portes $CNOT$ et de Walsh-Hadamard sont inversibles.

Porte controlled Phase Shift La deuxième porte CU usuelle est la porte controlled Phase-Shift définie, dans la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ par

$$CPS = \begin{pmatrix} I & O \\ O & R_Z(\delta) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\delta} \end{pmatrix}$$

$$\begin{array}{ccccc} |x\rangle & & \rightarrow \bullet \rightarrow & & |x\rangle \\ & & | & & \\ |y\rangle & \rightarrow & \boxed{R_Z(\delta)} & \rightarrow & e^{ixy\delta}|y\rangle \end{array}$$

$Porte \quad CPS$

Elle applique la phase global $e^{i\delta}$ lorsque le qubit de contrôle $|y\rangle$ est dans l'état $|1\rangle$

$$CPS\ |11\rangle = e^{i\delta}|11\rangle$$

Remarque 3: La porte CZ ou $CMINUS$ est définie par $CPS(\pi) = CZ$, soit

$$CZ = \begin{pmatrix} I & O \\ O & Z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$\begin{array}{ccccccc} |x\rangle & \rightarrow & & \rightarrow \bullet \rightarrow & & \rightarrow & |x\rangle \\ & & & | & & & \\ |y\rangle & \rightarrow \boxed{W} \rightarrow & & \rightarrow \boxed{X} \rightarrow & & \rightarrow \boxed{W} \rightarrow & (-1)^{xy}|y\rangle \end{array}$$

$Porte \quad CZ$

cette porte est importante en ce sens qu'elle est plus facile à implémenter de la porte CX.

on a les relations suivantes entre CX et CZ

$$\begin{aligned} CZ &= (I \otimes W)(CX)(I \otimes W) \\ CX &= (I \otimes W)(CZ)(I \otimes W) \end{aligned}$$

3.3.3 Portes quantiques universelles

L'intérêt de ces portes universelles est de faciliter l'intégration à partir de portes pré-caractérisées.

Nous avons déjà que n'importe quelle fonction peut être synthétisée à l'aide de:

· Porte $NAND$, constantes 0 et 1 dans le cas classique.

· Porte $CNOT$, portes single-qubit (W, $R_U(\delta)$) dans le cas quantique. On dit que ($CNOT$, W, $R_U(\delta)$) forme un ensemble infini de portes quantiques universelles.

Il existe cependant d'autres ensembles de portes quantiques universelles.

Porte CV

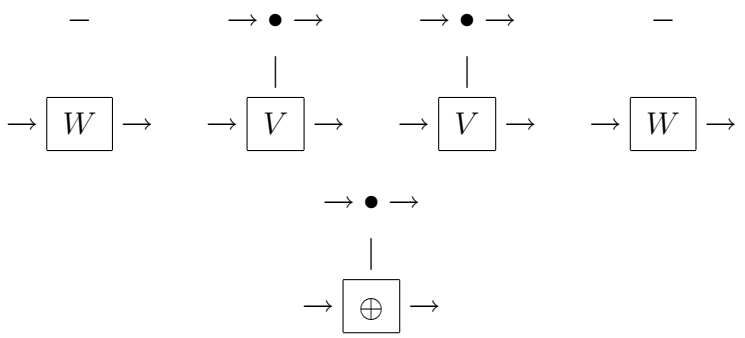
Toute porte quantique qui peut intriquer deux qubits peut être utilisée comme porte quantique universelle. Mathématiquement, un choix élégant consiste en une paire de portes de Walsh-Hadamard

et des portes CV, où V est la matrice

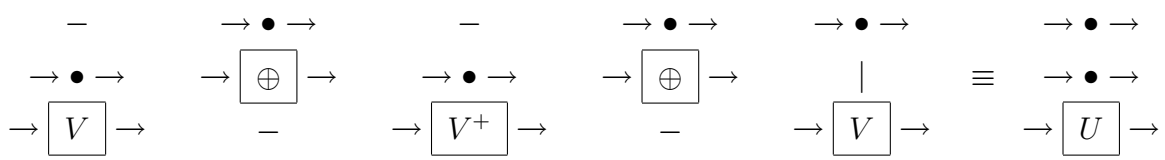
$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = R_Z\left(\frac{\pi}{2}\right)$$

Lorsqu'on applique quatre fois CV, on obtient l'identité, ainsi trois applications consécutives de CV donne l'inverse de CV où CV^+

On construit une porte $CNOT$ à partir des portes W et CV de la manière suivante:



On montre que toute matrice 2×2 unitaire U, telle que $U = V^2$, peut être simulée par la circuit:



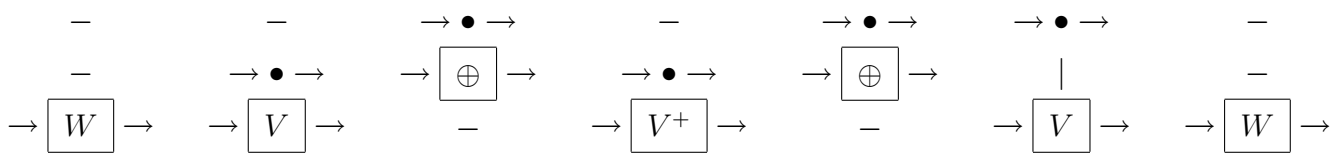
construction de Sleator -Weinfurter

Il est noter que

$$CCU\,|xyz\rangle = |xy\rangle\, U^{xy}\,|z\rangle\,.$$

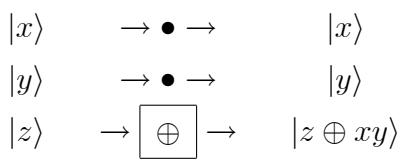
Porte de TOFFOLI

Les portes W et CV permettent aussi de construire une porte fort utile, à trois bits d'entrée et de sortée, appelée de TOFFOLI ou porte Controlled-Controlled-NOT($CCNOT$, C^2NOT)



Implémentation de la porte de TOFFOLI

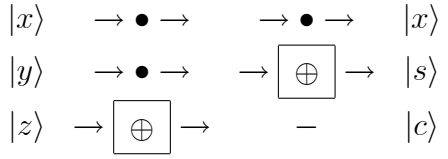
Cette porte, dont les deux bits de contrôle x et y restent inchangés alors que le bit cible z est inversé lorsque les deux bits de contrôle sont à 1, c'est-à-dire $Z' = Z \oplus xy$, est représentée par la table de vérité suivante.



Porte de TOFFOLI

N	x	y	z	x	y	$z \oplus xy$
	0	0	0	0	0	0
	0	0	1	0	0	1
	0	1	0	0	1	0
	0	1	1	0	1	1
	1	0	0	1	0	0
	1	0	1	1	0	1
	1	1	0	1	1	1
	1	1	1	1	1	0

Exercice: Donner les expressions et les tables de vérité de s et c du circuit suivant:



3.4 Evaluation quantique d'une fonction

Pour évaluer une fonction $f: \ \{0,\ 1\}^n \rightarrow \ \{0,\ 1\}^m$, on a besion d'au moins deux registres. Le premier, le registre de donner (input register) de taille n pour stocker les arguments x de la fonction f. le second, le registre de résultat (output register) de taille m pour stocker les valeurs de $f(x)$. la fonction d'évolution est une évolution unitaire des deux registres. $|xy\rangle \rightarrow |x \quad y + f(x)\rangle \bmod 2^m \quad y \in \{0,\ 1\}^m$.

par exemple, le circuit calculant la fonction

$$\begin{aligned} f: \qquad & \{0,\ 1\}^2 \rightarrow \ \{0,\ 1\}^3 \\ & x \rightarrow \ f(x) = x^2 \end{aligned}$$

agit ainsi qu'il suit

$$\begin{aligned} |00\rangle |000\rangle \ &\rightarrow \ |00\rangle |000\rangle \\ |01\rangle |000\rangle \ &\rightarrow \ |10\rangle |001\rangle \\ |10\rangle |000\rangle \ &\rightarrow \ |01\rangle |100\rangle \\ |11\rangle |000\rangle \ &\rightarrow \ |11\rangle |001\rangle \end{aligned}$$

on peut l'écrire sous la forme

$$|x\ 0\rangle \rightarrow \left|x \quad x^2 \ mod\ 2^3\right\rangle$$

comme $3^2 \bmod 2^3 = 1$, on écrit $|11\rangle |000\rangle \ = \ |11\rangle |001\rangle$

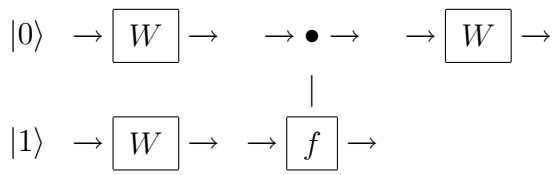
Ce qui rend intéressant l'évolution quantique d'une fonction est son action sur la superposition d'état des différents inputs x.

Par exemple,

$$\sum_x |x\ 0\rangle \rightarrow \sum_x |x \quad f(x)\rangle$$

Algorithme de Deutsch-Jozsa

Le but est tester la parité de la fonction $f: \ \{0,\ 1\} \rightarrow \ \{0,\ 1\}$ ou la condition $f(0) = f(1)$, ce qui équivant à vérifier $f(0) \oplus f(1)$. Si cela zéro alors f est constante, sinon f est équilibrée.



1- L'algorithme commence avec deux qubits dans l'état $|0\rangle |1\rangle$.

2- Une transformation de Walsh-Hadamard est d'abord appliquée à chaque qubit. Cela donne

$$W|0\rangle W|1\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

3- Une implémentation quantique (oracle) de la fonction f permet de passer de $|x\rangle |y\rangle$ à $|x\rangle \mid y + f(x)\rangle$, le second qubit est inversé si seulement si $f(x) = 1$. Soit pour $x \in \{0,\ 1\}$

$$U_f \ |x\rangle (|0\rangle - |1\rangle) = (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)$$

où le facteur $(-1)^{f(x)}$ s'est retropropagé (kicked back) devant le premier qubit. Ainsi l'évolution de la fonction nous donne

$$\begin{aligned} & \frac{1}{2}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right](|0\rangle - |1\rangle) \\ = \ & (-1)^{f(0)}\frac{1}{2}\left[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right](|0\rangle - |1\rangle) \end{aligned}$$

Le second qubit n'est plus utile, de meme que le facteur de phase global, on peut donc les ignorer, on a alors l'état

$$\frac{1}{\sqrt{2}}\left[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right]$$

4- En appliquant une transformation de Walsh Hadamard à cet état, on a

$$\begin{aligned} & \frac{1}{2}\left[|0\rangle + |1\rangle + (-1)^{f(0)\oplus f(1)}|0\rangle - (-1)^{f(0)\oplus f(1)}|1\rangle\right](|0\rangle - |1\rangle) \\ = \ & \frac{1}{2}\left[\left(1 + (-1)^{f(0)\oplus f(1)}\right)|0\rangle + \left(1 - (-1)^{f(0)\oplus f(1)}\right)|1\rangle\right] \end{aligned}$$

$f(0) \oplus f(1) = 0$, $f(0) = f(1)$ si et seulement si on observe $|0\rangle$.

5- Donc, l'état final du premier qubit est $\mid f(0) \oplus f(1)\rangle$ et la fonction est constante si et seulement si on mesure $|0\rangle$.

Comme on le constante, la parité de la fonction $f(x)$ a été encodé par un single-qubit après une seule invocation de f. Ceci parce qu'un calculateur quantique peut évaluer simultanément $f(0)$, $f(1)$. Les deux chemins alternatifs ou complémentaires sont recombinés par la dernière porte de Walsh-Hadamard. L'interférence est constructive pour l'une des valeurs de $f(0) \oplus f(1)$ et destructive pour la valeur alternative.

Dans le cas générale, on a $n+1$ bit dans l'état $|0\rangle^{\otimes n}|1\rangle$. Les premiers n bits sont tous dans l'état $|0\rangle$ et les derniers bit dans l'état $|1\rangle$. Nous appliquons ensuite la transformation de Walsh-Hadamard à chaque qubit, pour obtenir

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle\left(|0\rangle-|1\rangle\right)$$