Portes quantiques

Vidéo ■ partie 9.1. Portes quantiques - Théorie
Vidéo ■ partie 9.2. Portes quantiques - Oracle

Nous approfondissons nos connaissances théoriques des portes quantiques en étudiant ce qu'elles peuvent réaliser (ou pas !).

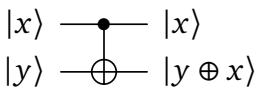
1. La porte de Toffoli est universelle

1.1. Quelques portes quantiques

Nous présentons de nouvelles portes et leur lien avec des portes déjà rencontrées.

Porte CNOT. Nous connaissons bien la porte $CNOT$.

On rappelle que la porte $CNOT$ est une porte NOT conditionnelle, si sur la première ligne on a le qubit $|0\rangle$ alors la seconde ligne est inchangée ; par contre si le qubit de la première ligne est $|1\rangle$ alors la seconde échange le qubit $|0\rangle$ en $|1\rangle$ et inversement. Si x, y ont pour valeurs 0 ou 1, alors l'action sur la seconde ligne est en fait $y \oplus x$ où « $\oplus$ » est l'addition binaire (et ne doit pas être confondue avec l'addition de qubits).

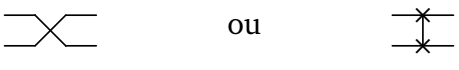


$$|0.0\rangle \xmapsto{CNOT} |0.0\rangle \qquad |0.1\rangle \xmapsto{CNOT} |0.1\rangle \qquad |1.0\rangle \xmapsto{CNOT} |1.1\rangle \qquad |1.1\rangle \xmapsto{CNOT} |1.0\rangle$$

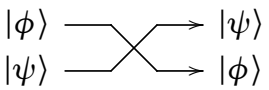
Voici la matrice de la transformation de $CNOT$ (dans la base $(|0.0\rangle, |0.1\rangle, |1.0\rangle, |1.1\rangle)$) :

$$M = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

Porte SWAP. La porte $SWAP$ échange deux qubits. Voici sa notation :

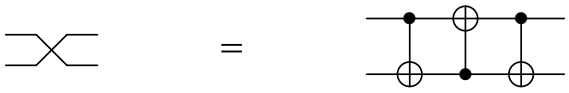


Comme on l'a dit, cette porte échange deux qubits :



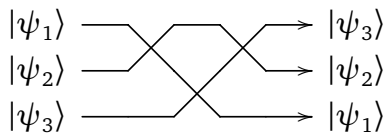
Exercice.
Calculer l'image des 2-qubits de la base canonique $(|0.0\rangle, |0.1\rangle, |1.0\rangle, |1.1\rangle)$ et en déduire la matrice 4×4 de la porte $SWAP$.

Exercice.
Montrer qu'une porte $SWAP$ est équivalente à un circuit réalisé à partir de trois portes $CNOT$.



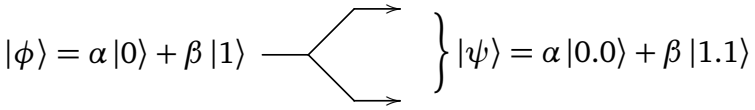
Indication. Il suffit de le vérifier sur les 2-qubits de la base canonique.

Exercice.
Montrer que le circuit suivant, construit à partir de trois portes $SWAP$ correspond à une porte $SWAP_3$ qui renverse l'ordre de 3 qubits, c'est-à-dire $(|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle) \mapsto (|\psi_3\rangle, |\psi_2\rangle, |\psi_1\rangle)$.



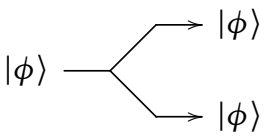
Il existe un circuit qui, à partir de portes $SWAP$, réalise une porte $SWAP_n$ renversant l'ordre de n qubits, c'est-à-dire $(|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle) \mapsto (|\psi_n\rangle, \ldots, |\psi_2\rangle, |\psi_1\rangle)$. Construire un tel circuit pour $n = 4$.

Porte FANOUT. La porte $FANOUT$ transforme un 1-qubit en un 2-qubit. Dans un circuit quantique, cela permet d'augmenter le nombre de lignes quantiques.



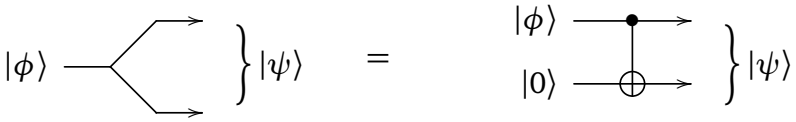
Piège. La porte $FANOUT$ envoie $|0\rangle$ sur $|0.0\rangle$ et $|1\rangle$ sur $|1.1\rangle$.

Cependant, il faut bien comprendre la porte $FANOUT$ ne réalise pas un copier-coller du 1-qubit d'entrée.

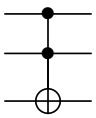
Ceci n'est pas vrai : 

D'ailleurs, une telle porte ne peut pas exister ! Ce sera prouvé par le théorème de non-clonage quantique en fin de chapitre.

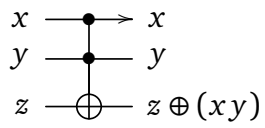
Exercice.
Montrer qu'une porte $FANOUT$ peut être réalisée à partir d'une porte $CNOT$ initialisée par $|0\rangle$ sur sa seconde ligne.



Porte de Toffoli (CCNOT). La porte de Toffoli est similaire à une porte $CNOT$ mais avec trois lignes. Si les deux premiers qubits sont $|1\rangle$, alors on applique une porte X (c'est-à-dire NOT) au troisième qubit.



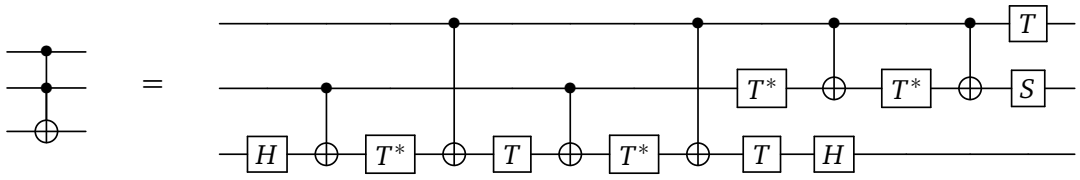
Voici l'action d'une porte de Toffoli lorsque x, y, z sont des bits 0 ou 1 (noter que $xy = 1$ si et seulement si $x = 1$ et $y = 1$ et alors $1 \oplus z = NOT(z)$).



$$M = \left(\begin{array}{cc|cc|cc} 1 & 0 & & & & \\ 0 & 1 & & & & \\ \hline & & 1 & 0 & & \\ & & 0 & 1 & & \\ \hline & & & & 1 & 0 \\ & & & & 0 & 1 \\ \hline & & & & 0 & 1 \\ & & & & 1 & 0 \end{array}\right)$$

Exercice.
Montrer qu'une porte Toffoli permet de réaliser une porte $CNOT$. Il suffit d'imposer le qubit $|1\rangle$ en entrée de la seconde ligne.

Exercice (Difficile)**.**
On peut réaliser une porte de Toffoli à partir de plusieurs portes $CNOT$ et de portes élémentaires S, H, T et son adjointe T^*.



Essayer de prouver cette construction, soit par un calcul théorique, soit expérimentalement à l'aide d'un ordinateur (voir le chapitre « Utiliser un ordinateur quantique (avec Qiskit) »).

On rappelle qu'une porte H de Hadamard est définie par la matrice :

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

La porte S est appelé « porte phase » et est définie par la matrice :

$$S = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix}.$$

La porte $\frac{\pi}{8}$ est définie par la matrice unitaire :

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

et donc

$$T^* = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix}.$$

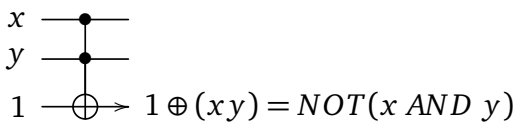
1.2. Théorème d'universalité

Théorème 1.
La porte de Toffoli est universelle : n'importe quelle fonction logique $f : \{0,1\}^n \to \{0,1\}$ peut être réalisée par un circuit quantique ne comportant que des portes de Toffoli.

Remarque. La réalisation pratique requiert l'ajout de lignes auxiliaires.
Preuve.

- On sait que n'importe quelle fonction logique $f : \{0,1\}^n \to \{0,1\}$ peut être réalisée par un circuit classique ne comportant que des portes $NAND$ (voir le chapitre « Informatique classique »).

- On réalise facilement l'équivalent d'une porte $NAND$ à l'aide d'une porte de Toffoli en l'initialisant avec un 1 sur la troisième ligne. L'entrée correspond aux deux premières lignes et la sortie à la troisième ligne.



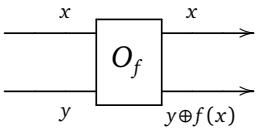
  Pour vérifier que cela fonctionne, il faut remarquer que pour des bits x, y valant 0 ou 1 alors xy est la même chose que $x\ AND\ y$, et donc $1 \oplus (xy) = NOT(x\ AND\ y)$.
- Conclusion : on réalise la fonction $f : \{0,1\}^n \to \{0,1\}$ en substituant chaque porte $NAND$ par une porte de Toffoli, avec un 1 sur sa troisième ligne.

2. Oracle

2.1. Définition

Le groupe $\mathbb{Z}/n\mathbb{Z}$.
Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ correspond à l'ensemble des entiers modulo n. On peut représenter ce groupe par l'ensemble $\{0, 1, \ldots, n-1\}$, avec la convention que $n \equiv 0$, $n+1 \equiv 1, \ldots$ La loi de ce groupe est l'addition. On a déjà rencontré le groupe $\mathbb{Z}/2\mathbb{Z}$ (cas $n = 2$) qui est l'ensemble $\{0,1\}$ muni de l'addition binaire notée « $\oplus$ » (en préférence à « $+$ ») qui vérifie $1 \oplus 1 = 0$, ce qui est cohérent car $1 + 1 = 2 \equiv 0$ modulo 2.
Oracle.
Nous allons associer à une fonction f un *oracle*. L'oracle d'une fonction f est un circuit quantique dont on explicite seulement l'entrée et la sortie (qui dépend de f). C'est une sorte de boîte noire, car nous n'avons pas besoin de connaître les détails du circuit qui réalise un oracle.
Cas $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.
C'est le cas déjà rencontré dans le chapitre « Un premier algorithme quantique », la fonction était alors notée $f : \{0,1\} \to \{0,1\}$.

Voici la transformation effectuée par un oracle, lorsque les entrées sont des bits classiques 0 ou 1 :



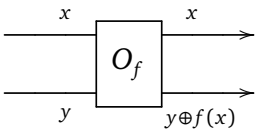
Il y a deux lignes pour l'entrée de l'oracle et deux lignes pour la sortie. La première sortie laisse la première entrée inchangée. Pour la seconde sortie : si x et y sont 0 ou 1 alors la seconde sortie est $y \oplus f(x)$; c'est donc y si $f(x) = 0$ et $NON(y)$ si $f(x) = 1$.
Ainsi l'oracle associé à f fournit une fonction

$$\begin{array}{rccc} F: & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ & (x,y) & \longmapsto & \big(x, y \oplus f(x)\big) \end{array}$$

Nous verrons plus tard comment cela définit naturellement une transformation quantique sur les 2-qubits.
Pour l'instant nous généralisons l'oracle au cas d'autres fonctions.

Cas $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

Cette situation correspondra à l'algorithme de Grover. On fixe $n \geqslant 2$ et on considère une fonction quelconque $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ que l'on peut aussi voir comme une fonction $f : \{0, 1, \ldots, n-1\} \to \{0, 1\}$.
La transformation de l'oracle, pour $x \in \mathbb{Z}/n\mathbb{Z}$ et $y \in \mathbb{Z}/2\mathbb{Z}$, renvoie une nouvelle fois x (élément de $\mathbb{Z}/n\mathbb{Z}$) et $y \oplus f(x)$ (élément de $\mathbb{Z}/2\mathbb{Z}$).



On obtient ainsi :

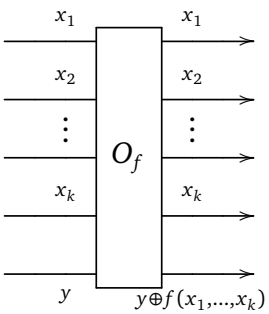
$$\begin{array}{rccc} F: & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ & (x,y) & \longmapsto & \big(x, y \oplus f(x)\big) \end{array}$$

Exemple.
Fixons $\ell \in \{0, \ldots, n-1\}$ un entier et $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ tel que $f(x) = 0$ pour tout x, sauf $f(\ell) = 1$.
Alors :

- pour $x \neq \ell$ et $y = 0$ on a $y \oplus f(x) = 0$,
- pour $x \neq \ell$ et $y = 1$ on a $y \oplus f(x) = 1$,
- pour $x = \ell$ et $y = 0$ on a $y \oplus f(x) = 1$,
- pour $x = \ell$ et $y = 1$ on a $y \oplus f(x) = 1 \oplus 1 = 0$.

Cas $f : (\mathbb{Z}/2\mathbb{Z})^k \to \mathbb{Z}/2\mathbb{Z}$.

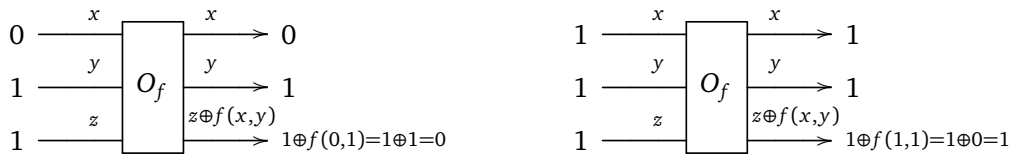
Cette situation correspondra à l'algorithme de Deutsch–Jozsa.
On fixe $k \geqslant 1$ et on considère une fonction quelconque $f : \big(\mathbb{Z}/2\mathbb{Z}\big)^k \to \mathbb{Z}/2\mathbb{Z}$ que l'on peut aussi voir comme une fonction $f : \{0,1\}^k \to \{0,1\}$.
La transformation de l'oracle, pour $x = (x_1, \ldots, x_k) \in (\mathbb{Z}/2\mathbb{Z})^k$ et $y \in \mathbb{Z}/2\mathbb{Z}$, renvoie $x = (x_1, \ldots, x_k)$ (élément de $(\mathbb{Z}/2\mathbb{Z})^k$) et $y \oplus f(x)$ (élément de $\mathbb{Z}/2\mathbb{Z}$).



On obtient ainsi :

$$\begin{array}{rccc} F: & (\mathbb{Z}/2\mathbb{Z})^k \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & (\mathbb{Z}/2\mathbb{Z})^k \times \mathbb{Z}/2\mathbb{Z} \\ & (x_1,\dots,x_k,y) & \longmapsto & \big(x_1,\dots,x_k,y\oplus f(x_1,\dots,x_k)\big) \end{array}$$

Exemple.
On considère $f:\big(\mathbb{Z}/2\mathbb{Z}\big)^2 \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(x,y) = x\ XOR\ y$. Voici quelques exemples d'action de l'oracle :



Autrement dit $F(0,1,1) = (0,1,0)$ et $F(1,1,1) = (1,1,1)$.

On pourrait généraliser l'oracle au cas d'une fonction $f: E \to E'$ pour lequel l'oracle associé serait une fonction $F: E \times E' \to E \times E'$ défini par $F(x,y) = (x, y \oplus f(x))$ où « $\oplus$ » est une addition dans E'.

2.2. L'oracle est bijectif

Quel peut être l'intérêt d'un oracle ? Plus précisément quel est l'avantage de la fonction F par rapport à f ? Considérons une fonction $f: E \to \mathbb{Z}/2\mathbb{Z}$ quelconque. En particulier elle n'est pas supposée bijective, par contre la fonction F associée à l'oracle va l'être.

Lemme 1.
Soit $f: E \to \mathbb{Z}/2\mathbb{Z}$ une fonction quelconque, alors la fonction $F: E \times \mathbb{Z}/2\mathbb{Z} \to E \times \mathbb{Z}/2\mathbb{Z}$ définie par $F(x,y) = (x, y \oplus f(x))$ est bijective.

Démonstration. Il suffit de trouver la bijection réciproque de F : nous allons montrer que cette réciproque est F elle-même.
Partons de

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

donc

$$F\big(F(x,y)\big) = F(x, y \oplus f(x)) = (x, y \oplus f(x) \oplus f(x)) = (x,y).$$

En effet, pour $a \in \mathbb{Z}/2\mathbb{Z}$ on a $a \oplus a = 2a = 0$ (car $0 \oplus 0 = 0$ et $1 \oplus 1 = 0$), donc $x \oplus a \oplus a = x$. Ainsi F est bijective et de plus $F^{-1} = F$ (autrement dit $F \circ F = \mathrm{id}$). □

Exemple.
Reprenons $f:\big(\mathbb{Z}/2\mathbb{Z}\big)^2 \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(x,y) = x\ XOR\ y$. Alors F est bien bijective :

$$\begin{array}{llll} (0,0,0) \overset{F}{\longmapsto} (0,0,0) & & (0,0,1) \overset{F}{\longmapsto} (0,0,1) \\ (0,1,0) \overset{F}{\longmapsto} (0,1,1) & & (0,1,1) \overset{F}{\longmapsto} (0,1,0) \\ (1,0,0) \overset{F}{\longmapsto} (1,0,1) & & (1,0,1) \overset{F}{\longmapsto} (1,0,0) \\ (1,1,0) \overset{F}{\longmapsto} (1,1,0) & & (1,1,1) \overset{F}{\longmapsto} (1,1,1) \end{array}$$

Exemple.
Soit $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ telle que $f(x) = 0$ pour tout x, sauf $f(\ell) = 1$, pour un entier $\ell \in \{0,\dots,n-1\}$ fixé.

- Pour $x \neq \ell$, $f(x) = 0$ donc $F(x,y) = (x, y \oplus f(x)) = (x,y)$.
- pour $x = \ell$, $f(x) = 1$ donc $F(x,y) = (x, y \oplus 1) = (x, NON(y))$.

L'application F est bijective.

2.3. Transformation quantique

Considérons le cas d'une fonction $f : (\mathbb{Z}/2\mathbb{Z})^k \to \mathbb{Z}/2\mathbb{Z}$. L'oracle fournit une fonction $F : (\mathbb{Z}/2\mathbb{Z})^{k+1} \to (\mathbb{Z}/2\mathbb{Z})^{k+1}$ en ayant considéré $(\mathbb{Z}/2\mathbb{Z})^k \times \mathbb{Z}/2\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^{k+1}$. Voyons la transformation quantique associée sur les $(k+1)$-qubits.
Les $(k+1)$-qubits sont engendrés par la base canonique formée des 2^{k+1} qubits de base :

$$\underbrace{|0.0\ldots0\rangle}_{k+1 \text{ bits}} \qquad |0.0\ldots1\rangle \qquad \ldots \qquad |1.1\ldots1\rangle\,.$$

La fonction F (définie sur des $(k+1)$-bits) s'étend naturellement en une fonction $\tilde{F}$ sur les vecteurs de la base des $(k+1)$-qubits :

$$\begin{aligned}
|e_0\rangle = |0.0\ldots0\rangle &\overset{\tilde{F}}{\longmapsto} |F(0,0,\ldots,0)\rangle = |f_0\rangle \\
|e_1\rangle = |0.0\ldots1\rangle &\overset{\tilde{F}}{\longmapsto} |F(0,0,\ldots,1)\rangle = |f_1\rangle \\
&\ldots \\
|e_{2^{k+1}-1}\rangle = |1.1\ldots1\rangle &\overset{\tilde{F}}{\longmapsto} |F(1,1,\ldots,1)\rangle = |f_{2^{k+1}-1}\rangle
\end{aligned}$$

Maintenant que $\tilde{F}$ est définie sur les vecteurs de la base par la relation $\tilde{F}(|e_i\rangle) = |F(e_i)\rangle = |f_i\rangle$, elle s'étend par linéarité à tous les $(k+1)$-qubits. Ainsi on obtient

$$\tilde{F} : \mathbb{C}^{2^{k+1}} \longrightarrow \mathbb{C}^{2^{k+1}}$$

et pour un $(k+1)$-qubit

$$|\psi\rangle = \sum_{i=0}^{2^{k+1}-1} \alpha_i\,|e_i\rangle\,,$$

avec $\alpha_i \in \mathbb{C}$, on obtient le $(k+1)$-qubit :

$$\tilde{F}(|\psi\rangle) = \sum_{i=0}^{2^{k+1}-1} \alpha_i\,|f_i\rangle\,.$$

Comme F est bijective alors $\tilde{F}$ envoie l'ensemble des vecteurs de la base canonique sur ces mêmes vecteurs de la base canonique (autrement dit $\tilde{F}$ permute les vecteurs de la base). Ainsi $\tilde{F}$ est une transformation unitaire (voir la section 3).

Exemple.
Reprenons l'exemple de la fonction $f : \left(\mathbb{Z}/2\mathbb{Z}\right)^2 \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(x,y) = x\ XOR\ y$. Nous avons déjà calculé F, ce qui donne les valeurs de $\tilde{F}$ sur les 3-qubits de base. Par exemple $\tilde{F}\,|0.1.0\rangle = |0.1.1\rangle$, $\tilde{F}\,|0.1.1\rangle = |0.1.0\rangle$,... Pour un 3-qubit quelconque :

$$|\psi\rangle = \alpha_0\,|0.0.0\rangle + \alpha_1\,|0.0.1\rangle + \alpha_2\,|0.1.0\rangle + \alpha_3\,|0.1.1\rangle + \alpha_4\,|1.0.0\rangle + \alpha_5\,|1.0.1\rangle + \alpha_6\,|1.1.0\rangle + \alpha_7\,|1.1.1\rangle$$

alors

$$\tilde{F}\,|\psi\rangle = \alpha_0\,|0.0.0\rangle + \alpha_1\,|0.0.1\rangle + \alpha_3\,|0.1.0\rangle + \alpha_2\,|0.1.1\rangle + \alpha_5\,|1.0.0\rangle + \alpha_4\,|1.0.1\rangle + \alpha_6\,|1.1.0\rangle + \alpha_7\,|1.1.1\rangle\,.$$

2.4. Matrice de l'oracle

Nous allons calculer la matrice de l'oracle, c'est-à-dire la matrice de l'application $\tilde{F}$.
On rappelle que

$$(x,y) \overset{F}{\longmapsto} (x, y \oplus f(x))$$

où $x = (x_1, \dots, x_k)$ est un k-bit et y un 1-bit. La fonction F est naturellement étendue aux qubits de base par la formule :

$$|x.y\rangle \overset{\tilde{F}}{\longmapsto} |x.y \oplus f(x)\rangle$$

Calculons explicitement l'image de chacun des vecteurs $|e_i\rangle$ de la base canonique de $(k+1)$-qubits.

$$|e_0\rangle = |\underbrace{0\dots0}_{x}.\underbrace{0}_{y}\rangle \overset{\tilde{F}}{\longmapsto} |\underbrace{0\dots0}_{x}.\underbrace{0 \oplus f(0,\dots,0)}_{0 \text{ ou } 1}\rangle = \begin{cases} |e_0\rangle & \text{si } f(0,\dots,0) = 0 \\ |e_1\rangle & \text{si } f(0,\dots,0) = 1 \end{cases}$$

De même

$$|e_1\rangle = |\underbrace{0\dots0}_{x}.\underbrace{1}_{y}\rangle \overset{F}{\longmapsto} |\underbrace{0\dots0}_{x}.\underbrace{1 \oplus f(0,\dots,0)}_{1 \text{ ou } 0}\rangle = \begin{cases} |e_1\rangle & \text{si } f(0,\dots,0) = 0 \\ |e_0\rangle & \text{si } f(0,\dots,0) = 1 \end{cases}$$

De façon générale

$$\begin{cases} |e_{2i}\rangle \overset{\tilde{F}}{\longmapsto} |e_{2i}\rangle \\ |e_{2i+1}\rangle \overset{\tilde{F}}{\longmapsto} |e_{2i+1}\rangle \end{cases} \quad \text{ou} \quad \begin{cases} |e_{2i}\rangle \overset{\tilde{F}}{\longmapsto} |e_{2i+1}\rangle \\ |e_{2i+1}\rangle \overset{\tilde{F}}{\longmapsto} |e_{2i}\rangle \end{cases}$$

La sous-matrice de $\tilde{F}$ dans la base (e_{2i}, e_{2i+1}) est donc

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{ou} \qquad J_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

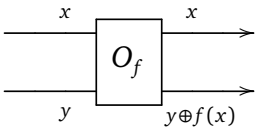
Ainsi la matrice de $\tilde{F}$ dans la base canonique des $(k+1)$-qubits est la matrice suivante, qui est une matrice diagonale par blocs, chaque bloc étant I_2 ou J_2 :

$$A = \begin{pmatrix} I_2/J_2 & & & & \\ & I_2/J_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & I_2/J_2 \end{pmatrix} \in M_{2^{k+1}}(\mathbb{C}).$$

On a bien sûr $I_2^2 = I_2$, mais aussi $J_2^2 = I_2$ et $J_2^* = J_2$, donc $A^*A = I$, ce qui prouve que A est une matrice unitaire. (On le savait déjà car l'application associée $\tilde{F}$ est unitaire, voir ci-dessus.)

2.5. Oracle pour $f = NOT$

Considérons $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ défini par $f(0) = 1$ et $f(1) = 0$. C'est donc la négation : $f(x) = NOT(x) = 1 \oplus x$. Décrivons l'oracle de f.



L'application F est :

$$\begin{array}{rccc} F: & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ & (x,y) & \longmapsto & \big(x, y \oplus f(x)\big) = \big(x, 1 \oplus x \oplus y\big). \end{array}$$

ce qui donne concrètement :

$$\begin{array}{lll}(0,0) & \overset{F}{\longmapsto} & (0,1)\\ (0,1) & \overset{F}{\longmapsto} & (0,0)\\ (1,0) & \overset{F}{\longmapsto} & (1,0)\\ (1,1) & \overset{F}{\longmapsto} & (1,1)\end{array} \quad \text{donc} \quad \begin{array}{lll}|0.0\rangle & \overset{\tilde{F}}{\longmapsto} & |0.1\rangle\\ |0.1\rangle & \overset{\tilde{F}}{\longmapsto} & |0.0\rangle\\ |1.0\rangle & \overset{\tilde{F}}{\longmapsto} & |1.0\rangle\\ |1.1\rangle & \overset{\tilde{F}}{\longmapsto} & |1.1\rangle\end{array}$$

Ainsi la matrice de l'oracle est :

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

2.6. Oracle pour $f = AND$

Exercice.
Effectuer le même travail mais cette fois avec la fonction de deux variables f définie par AND.
Soit $f : (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(x,y) = x\ AND\ y = xy$.
Nous allons voir que l'oracle associé à ce f est exactement une porte de Toffoli ($CCNOT$).

En détails :

1. Calculer l'image par l'oracle de chacun des vecteurs de la base des 3-qubits : $|0.0.0\rangle$, $|0.0.1\rangle$,...,$|1.1.1\rangle$.
2. En déduire que l'oracle associé à ce f est équivalent à une porte de Toffoli, en vérifiant que le résultat est le même que l'action de la porte de Toffoli sur les 3-qubits de base.
3. Vérifier que l'application F (ou $\tilde{F}$) est bijective alors que f ne l'est pas.
4. Calculer la matrice de l'oracle (et retrouver la matrice de la porte de Toffoli).

3. Matrices unitaires

Nous reprenons l'étude des matrices unitaires, ici de taille quelconque, les matrices 2×2 ayant déjà été étudiées dans le chapitre « Vecteurs et matrices ».

3.1. Produit scalaire hermitien

Rappelons quelques définitions et propriétés.

- Le ***produit scalaire hermitien*** $\langle u|v\rangle$ des deux vecteurs u et v est défini par :

$$u = \begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix} \qquad v = \begin{pmatrix}y_1\\y_2\\\vdots\\y_n\end{pmatrix} \qquad \langle u|v\rangle = x_1^* \cdot y_1 + x_2^* \cdot y_2 + \cdots + x_n^* \cdot y_n = \sum_{i=1}^{n} x_i^* \cdot y_i.$$

- Le produit scalaire permet de calculer la norme : $\|u\|^2 = \langle u|u\rangle$.
- Le produit scalaire est anti-linéaire à gauche et linéaire à droite. Pour $\lambda \in \mathbb{C}$:

$$\langle \lambda u|v\rangle = \lambda^* \langle u|v\rangle \quad \text{et} \quad \langle u|\lambda v\rangle = \lambda \langle u|v\rangle .$$

- La ***matrice adjointe*** de A est la matrice A^* obtenue par transposition et conjugaison complexe :

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{np} \end{pmatrix} \qquad A^* = \begin{pmatrix} a_{11}^* & a_{21}^* & \dots & a_{n1}^* \\ a_{12}^* & a_{22}^* & \dots & a_{n2}^* \\ \vdots & \vdots & & \vdots \\ a_{1p}^* & a_{2p}^* & \dots & a_{np}^* \end{pmatrix}.$$

- La notation « ket » $|\phi\rangle$ désigne un vecteur écrit sous forme colonne :

$$|\phi\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

- La notation « bra » $\langle\phi|$ désigne un vecteur ligne, obtenu comme l'adjoint :

$$\text{si} \quad |\phi\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \text{alors} \qquad \langle\phi| = |\phi\rangle^* = \begin{pmatrix} x_1^* & \cdots & x_n^* \end{pmatrix}.$$

- Ainsi l'écriture $\langle\cdot|\cdot\rangle$ désigne de façon cohérente à la fois le produit scalaire hermitien et la multiplication matricielle d'un vecteur ligne par un vecteur colonne (qui donne un scalaire) :

$$|\phi\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \qquad \langle\phi|\psi\rangle = x_1^* \cdot y_1 + x_2^* \cdot y_2 + \cdots + x_n^* \cdot y_n.$$

Proposition 1.

$$\boxed{\langle Au|v\rangle = \langle u|A^*v\rangle}$$

Démonstration. Si $A = (a_{ij})$ et $u = (x_i)$ alors Au est un vecteur dont le terme de rang i est $(Au)_i = \sum_{j=1}^n a_{ij}x_j$. Ainsi si $v = (y_i)$ alors $\langle Au|v\rangle$ est la somme sur i de termes

$$\left(\sum_{j=1}^n a_{ij}x_j\right)^* y_i,$$

et donc

$$\langle Au|v\rangle = \sum_{i=1}^n \sum_{j=1}^n a_{ij}^* x_j^* y_i.$$

D'autre part $\langle u|A^*v\rangle$ est la somme sur i de termes

$$x_i^* \left(\sum_{j=1}^n a_{ij}^* y_j\right),$$

ce qui prouve que $\langle u|A^*v\rangle = \langle Au|v\rangle$. □

3.2. Caractérisation des matrices unitaires

Définition.
Une matrice $A \in M_n(\mathbb{C})$ est ***unitaire*** si :

$$\boxed{A^*A = I}$$

On note U_n l'ensemble des matrices unitaires.

Si A est une matrice unitaire alors on a

$$A^{-1} = A^* \qquad \text{et} \qquad AA^* = I.$$

Proposition 2.
L'ensemble des matrices unitaires forme un groupe. En particulier $I \in U_n$ et si $A, B \in U_n$ alors $AB \in U_n$ et $A^{-1} \in U_n$.

Pour la suite nous aurons besoin de la notion suivante :

Définition.
Les vecteurs $(e_1, e_2, \dots, e_n)$ forment une ***base orthonormale*** de $\mathbb{C}^n$ si

$$\langle e_i | e_j \rangle = 0 \quad \text{pour tout } i \neq j \qquad \text{et} \qquad \|e_i\| = 1 \quad \text{pour tout } i = 1, \dots, n.$$

On peut rassembler les deux conditions en une seule

$$\langle e_i | e_j \rangle = \delta_{i,j}$$

où $\delta_{i,j}$ est le symbole de Kronecker :

$$\delta_{i,j} = 0 \quad \text{si } i \neq j \quad \text{et} \quad \delta_{i,i} = 1.$$

Proposition 3.
Les assertions suivantes sont équivalentes :
(i) La matrice $A \in M_n(\mathbb{C})$ est unitaire.
(ii) A préserve le produit scalaire hermitien : $\langle Au | Av \rangle = \langle u | v \rangle$ quels que soient $u, v \in \mathbb{C}^n$.
(iii) A préserve les longueurs : $\|Au\| = \|u\|$ quel que soit $u \in \mathbb{C}^n$.
(iv) Si (e_i) est une base orthonormale de $\mathbb{C}^n$, alors (Ae_i) est aussi une base orthonormale.
(v) Les vecteurs colonnes (f_i) de A forment une base orthonormale de $\mathbb{C}^n$.

Démonstration.
- (i) $\implies$ (ii) $\langle Au | Av \rangle = \langle u | A^* A v \rangle = \langle u | v \rangle$
- (ii) $\implies$ (iii) $\|Au\|^2 = \langle Au | Au \rangle = \langle u | u \rangle = \|u\|^2$
- (iii) $\implies$ (iv) Notons $f_i = Ae_i$. Alors $\|f_i\| = \|e_i\| = 1$. Soit $i \neq j$, comme $\|e_i + e_j\|^2 = 2$ alors $\|f_i + f_j\|^2 = \|A(e_i + e_j)\|^2 = \|e_i + e_j\|^2 = 2$. Or

$$\begin{aligned} \|f_i + f_j\|^2 &= \langle f_i + f_j | f_i + f_j \rangle = \langle f_i | f_i \rangle + \langle f_i | f_j \rangle + \langle f_j | f_i \rangle + \langle f_j | f_j \rangle \\ &= \|f_i\|^2 + \langle f_i | f_j \rangle + \langle f_i | f_j \rangle^* + \|f_j\|^2 = \|f_i\|^2 + 2\,\mathrm{Re}\big(\langle f_i | f_j \rangle\big) + \|f_j\|^2 \end{aligned}$$

  Comme $\|f_i + f_j\|^2 = 2$, $\|f_i\|^2 = 1$ et $\|f_j\|^2 = 1$ alors $2\,\mathrm{Re}\big(\langle f_i | f_j \rangle\big) = 0$.
  De même

$$\|f_i + \mathrm{i} f_j\|^2 = \|f_i\|^2 - 2\,\mathrm{Im}\big(\langle f_i | f_j \rangle\big) + \|f_j\|^2$$

  alors $2\,\mathrm{Im}\big(\langle f_i | f_j \rangle\big) = 0$. Ainsi $\langle f_i | f_j \rangle = 0$ et (f_i) forment une base orthonormée.
- (iv) $\implies$ (v) Soit (e_i) la base canonique, alors les $f_i = Ae_i$ sont les vecteurs colonnes de A. Comme (e_i) est une base orthonormale, alors (f_i) l'est aussi.
- (v) $\implies$ (i) Notons $M = AA^* - I$. Notons (e_i) la base canonique et $(f_i) = (Ae_i)$ les vecteurs colonnes de A.

$$\langle Me_i | e_j \rangle = \langle AA^* e_i - e_i | e_j \rangle = \langle AA^* e_i | e_j \rangle - \langle e_i | e_j \rangle = \langle Ae_i | Ae_j \rangle - \delta_{i,j} = \langle f_i | f_j \rangle - \delta_{i,j} = \delta_{i,j} - \delta_{i,j} = 0.$$

  Fixons i, comme $\langle Me_i | e_j \rangle = 0$ (scalaire nul) pour tout vecteur e_j de la base, alors $Me_i = 0$ (vecteur nul). Maintenant comme $Me_i = 0$ pour tout vecteur e_i de la base, alors $M = 0$ (matrice nulle). Ainsi $AA^* = I$ donc A est unitaire.

□

3.3. Porte quantique

Nous avons vu différentes portes quantiques, voici maintenant la définition générale :

Définition.
Une ***porte quantique*** est la transformation $|\psi\rangle \mapsto A|\psi\rangle$ où A est une matrice unitaire.

$$|\psi\rangle \longrightarrow \boxed{A} \longrightarrow A|\psi\rangle$$

Si l'entrée $|\psi\rangle$ est un n-qubit, alors A une matrice de taille 2^n (donc $A \in U_{2^n}$), la sortie est un n-qubit.
Comme la matrice A est unitaire alors en particulier la transformation est inversible. C'est une différence majeure par rapport à une porte de l'informatique classique (par exemple une porte AND n'est pas inversible).

3.4. Théorèmes de réalisation

Même si une porte quantique est donnée par une matrice unitaire A quelconque, cette porte quantique peut être réalisée de façon équivalente par un circuit composé de portes biens connues. Nous allons voir plusieurs résultats de réalisations que nous énonçons sans démonstration.

Théorème 2.
Toute porte quantique à n-qubits peut être réalisée de façon équivalente par un circuit ne comportant que des portes $CNOT$ et des portes à 1-qubit.

Ainsi l'étude de n'importe quel circuit quantique se ramène à l'étude de deux types de portes et à leur composition. Le défaut de ce résultat, c'est que la réalisation se fait à l'aide de portes parmi une infinité de possibilités. En effet, une porte à 1-qubit est définie par une matrice unitaire $A \in M_2(\mathbb{C})$, et il y a une infinité de telles matrices.

Le résultat suivant construit des circuits avec seulement trois types de portes, la contrepartie c'est que l'on n'obtient pas exactement le circuit voulu, mais une approximation.

Théorème 3.
Toute porte quantique à n-qubits peut être approchée d'aussi près que l'on veut par un circuit ne comportant que des portes H de Hadamard, des portes T (dite « porte $\frac{\pi}{8}$ ») et des portes $CNOT$.

On rappelle qu'une porte H de Hadamard est définie par la matrice :

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

La porte $\frac{\pi}{8}$ est définie par la matrice unitaire :

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$$

qui tient son nom de son écriture sous la forme :

$$T = e^{i\frac{\pi}{8}}\begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}.$$

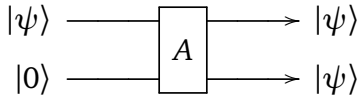
Le théorème de Solovay–Kitaev est une version améliorée du théorème précédent et affirme de plus qu'on peut réaliser le circuit en utilisant assez peu de portes.

4. Théorème de non-clonage quantique

Un ordinateur classique est modélisé par une machine de Turing et est capable de lire une série de bits et de les dupliquer à un autre endroit. Nous allons voir que ce n'est pas le cas pour un ordinateur quantique. En fait on peut copier un qubit, mais en créant la copie on perd l'original. On parle ainsi de « non-clonage quantique ».

4.1. Non-clonage des 1-qubits

Théorème 4.
Il n'existe pas de porte quantique qui réalise le clonage des 1*-qubits, c'est-à-dire telle que pour tout* 1*-qubit* $|\psi\rangle$ *on ait :*



Démonstration. Raisonnons par l'absurde et supposons que le clonage quantique soit possible. Cela signifie qu'il existe une porte quantique qui réalise ce clonage, c'est-à-dire qu'il existe une matrice $A \in M_4(\mathbb{C})$ unitaire telle que :

$$A|\psi.0\rangle = |\psi.\psi\rangle \qquad \text{pour tout 1-qubit } |\psi\rangle .$$

Comme cette égalité est vraie pour tous les 1-qubits, c'est également le cas :

- pour $|\psi_0\rangle = |0\rangle$, donc $A|0.0\rangle = |0.0\rangle$,
- pour $|\psi_1\rangle = |1\rangle$, donc $A|1.0\rangle = |1.1\rangle$,
- et pour $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Nous allons détailler ce que cela implique pour $|\psi_2\rangle$.

- D'une part comme $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle + |\psi_1\rangle)$.

$$\begin{aligned} A|\psi_2.0\rangle &= A\Big(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle).|0\rangle\Big) \\ &= \tfrac{1}{\sqrt{2}}A|0.0\rangle + \tfrac{1}{\sqrt{2}}A|1.0\rangle \\ &= \tfrac{1}{\sqrt{2}}|0.0\rangle + \tfrac{1}{\sqrt{2}}|1.1\rangle \end{aligned}$$

  On retient que :

$$A|\psi_2.0\rangle = \tfrac{1}{\sqrt{2}}(|0.0\rangle + |1.1\rangle). \tag{1}$$

- D'autre part par le clonage de $|\psi_2\rangle$:

$$\begin{aligned} A|\psi_2.0\rangle &= |\psi_2.\psi_2\rangle \\ &= \tfrac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= \tfrac{1}{2}(|0.0\rangle + |0.1\rangle + |1.0\rangle + |1.1\rangle) \end{aligned}$$

  On a prouvé :

$$A|\psi_2.0\rangle = \tfrac{1}{2}(|0.0\rangle + |0.1\rangle + |1.0\rangle + |1.1\rangle). \tag{2}$$

Nous pouvons maintenant conclure à partir des équations (1) et (2) :

$$\tfrac{1}{\sqrt{2}}(|0.0\rangle + |1.1\rangle) = \tfrac{1}{2}(|0.0\rangle + |0.1\rangle + |1.0\rangle + |1.1\rangle)$$

donc

$$\left(\tfrac{1}{2} - \tfrac{1}{\sqrt{2}}\right)|0.0\rangle + \tfrac{1}{2}|0.1\rangle + \tfrac{1}{2}|1.0\rangle + \left(\tfrac{1}{2} - \frac{1}{\sqrt{2}}\right)|1.1\rangle = 0. \tag{3}$$

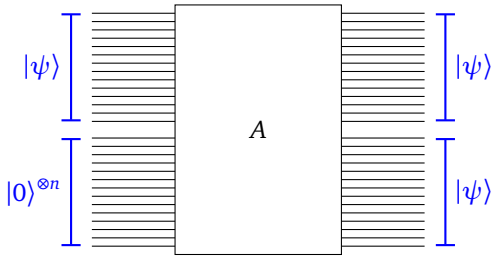
Souvenons-nous que $(|0.0\rangle, |0.1\rangle, |1.0\rangle, |1.1\rangle)$ est une base de $\mathbb{C}^4$, donc

$$\text{si } \alpha|0.0\rangle + \beta|0.1\rangle + \gamma|1.0\rangle + \delta|1.1\rangle = 0 \quad \text{alors} \quad \alpha = 0, \beta = 0, \gamma = 0, \delta = 0.$$

Dans notre cas cela implique que les coefficients de l'équation (3) sont tous nuls, et donc par exemple $\frac{1}{2} = 0$ ce qui fournit une contradiction.
Conclusion : une telle matrice A qui réalise le clonage ne peut exister. □

4.2. Cas général

Théorème 5.
Il n'existe pas de porte quantique qui réalise le clonage d'un n-qubit, c'est-à-dire telle que pour tout n-qubit $|\psi\rangle$ on ait :



La preuve pour le cas général des n-qubits est le même calcul que pour le cas des 1-qubits. On note $|e_0\rangle$, $|e_1\rangle$,…,$|e_{2^n-1}\rangle$ les vecteurs de la base canonique des n-qubits. On raisonne par l'absurde en supposant qu'il existe une matrice unitaire A telle que $A\left|\psi.0^{\otimes n}\right\rangle = |\psi.\psi\rangle$ quel que soit le n-qubit $|\psi\rangle$ (ici $|0\rangle^{\otimes n} = |0.0\ldots0\rangle$).
Ensuite on pose :

- pour $|\psi_0\rangle = |e_0\rangle$, donc $A\left|e_0.0^{\otimes n}\right\rangle = |e_0.e_0\rangle$,
- pour $|\psi_1\rangle = |e_1\rangle$, donc $A\left|e_1.0^{\otimes n}\right\rangle = |e_1.e_1\rangle$,
- Pour $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|e_0\rangle + |e_1\rangle)$, on obtient une contradiction en écrivant d'une part

$$A\left|\psi_2.0^{\otimes n}\right\rangle = \frac{1}{\sqrt{2}}\left(A\left|0.0^{\otimes n}\right\rangle + A\left|e_1.0^{\otimes n}\right\rangle\right)$$

et d'autre part

$$A\left|\psi_2.0^{\otimes n}\right\rangle = |\psi_2.\psi_2\rangle\,.$$