Méthodes mathématiques de la théorie quantique - 2022

Bases de l'Information quantique - Day 3

Nana Engo

Department of Physics
Faculty of Science
University of Yaounde I

https://github.com/NanaEngo/Memaquan2022

Porto-Novo - 11-15 Juillet 2022

Sommaire - Day 3 - 13 Juillet 2022

1. Généralités et notion de calculateur
2. Portes single-qubit
3. Portes de contrôle
4. Portes quantiques universelles

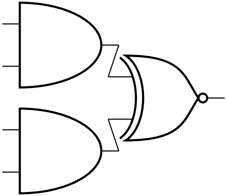
Definition (Calculateur classique)

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 $i \in [0, 2^n - 1]$, correspondant à 2^n configurations, décrit en notation binaire par

$$i = i_{n-1}2^{n-1} + \cdots + i_1 2^1 + i_0 2^0 = \sum_{m=0}^{n-1} i_m 2^m \qquad i_m \in [0, 1]$$

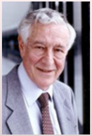
Exemple : 3 bits physiques $\Rightarrow$ $2^3 = 8$ configurations différentes (0 à 7 en binaire)

$000 \equiv 0 \quad 001 \equiv 1 \quad 010 \equiv 2 \quad 011 \equiv 3 \quad 100 \equiv 4 \quad 101 \equiv 5 \quad 110 \equiv 6 \quad 111 \equiv 7$



Exemple de circuit logique classique (2 portes AND et 1 porte XNOR)

Principe de Landauer (dissipation de la chaleur)



Chaque fois qu'un bit d'information est effacé, son entropie augmente d'au moins $k_B \ln 2$ et la quantité d'énergie dissipée dans l'environnement (circuit) vaut au moins $k_B T \ln 2$, T étant la température absolue de l'environnement.

Theorem (Théorème de Margolus-Levitin)

La vitesse ou le nombre d'opérations effectuées dans un temps donné, à laquelle toute machine ou tout autre procédé réalisable permettant de calculer, et utilisant une quantité d'énergie E donnée, ne peut pas être supérieur à 6×10^{33} opérations par seconde par joule d'énergie.

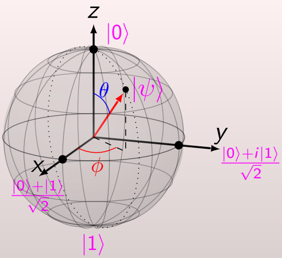
- Le Théorème de Margolus-Levitin, tout comme le Principe de Landauer, constitue une limite fondamentale à la loi de Koomey selon laquelle le nombre de calculs, pour une quantité d'énergie dépensée donnée, double tous les 18 mois

Definition (Bit quantique ou qubit)

Le qubit est l'unité de traitement de l'information quantique.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \alpha, \beta \in \mathbb{C} \qquad |\alpha|^2 + |\beta|^2 = 1$$

Qubit sur la sphere de Bloch



- Pour $0 \leq \theta \leq \pi$ et $0 \leq \phi < 2\pi$, $|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle$
- Pour $\theta = 0$ et ϕ, $|\psi\rangle = |0\rangle$
- Pour $\theta = \pi$ et ϕ, $|\psi\rangle = |1\rangle$
- Pour $\theta = \frac{\pi}{2}$ et $\phi = 0$, $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$
- Pour $\theta = \frac{\pi}{2}$ et $\phi = \frac{\pi}{2}$, $|\psi\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$

Definition (Calculateur quantique)

Un calculateur quantique est une collection de n qubits qui représente un registre quantique de taille n

$$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle = \sum_{i_{n-1}=0}^{1} \cdots \sum_{i_1=0}^{1} \sum_{i_0=0}^{1} c_{i_{n-1},\cdots i_1,i_0} |i_{n-1}\rangle \otimes \cdots \otimes |i_1\rangle \otimes |i_0\rangle$$

$$= \sum_{i_{n-1},\cdots i_1,i_0=0}^{1} c_{i_{n-1},\cdots i_1,i_0} |i_{n-1} \cdots i_1 i_0\rangle \qquad \sum_{i=0}^{2^n-1} |c_i|^2 = 1$$

- Parallélisme quantique. Grâce à la superposition d'états, un registre quantique de n qubits peut stocker 2^n nombres et effectuer en parallèle un grand nombre d'opérations simultanément
- Exemple : Pour $n = 2$, un état générique de 2-qubits s'écrit

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + c_3 |3\rangle = c_{00} |00\rangle + c_{01} |01\rangle + c_{10} |10\rangle + c_{11} |11\rangle$$

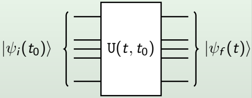
Généralités et notion de calculateur

Principe du calcul quantique

- $i \in \{0,1\}^n$ est une chaîne binaire de taille n $\Rightarrow |i\rangle \in \mathcal{H}^{\otimes n}$ (2^n dim)

Principe d'un calcul quantique

1. Préparation de n qubits dans l'état $|\psi_i(t_0)\rangle$
2. Implémentation de la transformation unitaire désirée ou souhaitée $\mathtt{U}(t, t_0)$, $|\psi_f(t)\rangle = \mathtt{U}(t, t_0)\,|\psi_i(t_0)\rangle$
3. Mesure sur les n qubits afin d'obtenir $|\psi_f(t)\rangle$



- L'évolution unitaire $\mathtt{U}(t, t_0)$ est réversible : connaissant le vecteur d'état au temps t, on peut remonter à celui au temps t_0 par $\mathtt{U}^{-1}(t, t_0) = \mathtt{U}(t_0, t)$

Calcul quantique $\equiv$ évolution quantique réversible $\Rightarrow$ ~~dissipation de chaleur~~

Généralités et notion de calculateur

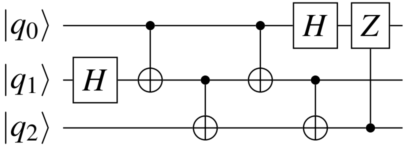
Éléments d'un circuit quantique

- Porte logique quantique : dispositif qui réalise une opération unitaire fixe sur un qubit donné, pendant une période de temps donnée

- Réseau ou circuit quantique : dispositif constitué de portes logiques quantiques dont les séquences de calculs sont synchronisées dans le temps

- Taille du circuit : nombre de portes logiques quantiques du réseau

- Largeur du circuit : nombre de fils du réseau



Circuit quantique de 7 portes logiques et de taille 3

Portes single-qubit

Portes unitaires single-qubit les plus usuelles

Porte	**Diagramme**	**Matrice dans** $\{\|0\rangle, \|1\rangle\}$
`Pauli X`	$\|k\rangle \;—\boxed{\mathtt{X}}—\; \|1-k\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
`Pauli Y`	$\|k\rangle \;—\boxed{\mathtt{Y}}—\; i(-1)^k \|1-k\rangle$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
`Pauli Z`	$\|k\rangle \;—\boxed{\mathtt{Z}}—\; (-1)^k \|k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
`Walsh-Hadamard W`	$\|k\rangle \;—\boxed{\mathtt{W}}—\; \frac{1}{\sqrt{2}}[(-1)^k \|k\rangle + \|1-k\rangle]$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
`Phase-Shift`	$\|k\rangle \;—\overset{\delta}{\bullet}—\; e^{ik\delta} \|k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}$
`Phase`	$\|k\rangle \;—\boxed{\mathtt{S}}—\; (i)^k \|k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\frac{\pi}{8}$	$\|k\rangle \;—\boxed{\mathtt{T}}—\; e^{ik\pi/4} \|k\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
`square root NOT`	$\|k\rangle \;—\boxed{\sqrt{\mathtt{X}}}—\; \frac{1+i}{2}[\|k\rangle - i\|1-k\rangle]$	$\frac{1+i}{2}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$

Portes single-qubit I

Porte Walsh-Hadamard W

Definition (Porte de `Walsh-Hadamard W`)

La porte de `Walsh-Hadamard` définie par la matrice

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

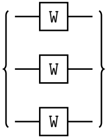
permet de transformer les états de base $\{|0\rangle, |1\rangle\}$ en état superposés

$$\mathtt{W}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \mathtt{W}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\mathtt{W}|k\rangle = \frac{1}{\sqrt{2}}((-1)^k |k\rangle + |1-k\rangle)$$

$$|k\rangle \;—\boxed{\mathtt{W}}—\; \frac{1}{\sqrt{2}}((-1)^k |k\rangle + |1-k\rangle)$$

- La porte `W` permet d'implémenter le parallélisme quantique à l'origine de l'accélération exponentielle d'un calcul quantique pour la résolution de certains problèmes

$|0\rangle^{\otimes 3}$  $\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)^{\otimes 3} = \frac{1}{\sqrt{2^3}}(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle)$

- Si initialement on a un registre de taille n dans un état $y \in \{0,1\}^n$, alors

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

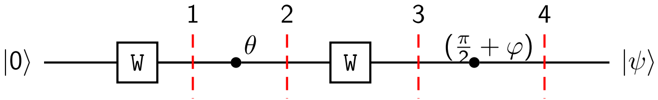
où le produit de $y = (y_{n-1}y_{n-2}\cdots y_1y_0)$ et de $x = (x_{n-1}x_{n-2}\cdots x_1x_0)$ est fait bit par bit

$$yx = (y_{n-1}x_{n-1} + y_{n-2}x_{n-2} + \cdots + y_1x_1 + y_0x_0)$$

Portes single-qubit I

Implémentation du 1-qubit générique

Les portes W et P(δ) suffisent pour construire toute opération unitaire sur un 1-qubit



- Il est à noter que le diagramme se lit de gauche à droite alors que le produit d'opérateurs se lit de droite à gauche

- Ce circuit quantique s'écrit vectoriellement sous la forme

$$
\begin{aligned}
|\psi\rangle &= \underbrace{\mathtt{P}(\frac{\pi}{2}+\varphi)}_{\mathbf{4}}\underbrace{\mathtt{W}}_{\mathbf{3}}\underbrace{\mathtt{P}(\theta)}_{\mathbf{2}}\underbrace{\mathtt{W}\,|0\rangle}_{\mathbf{1}} \\
&\overset{\mathbf{1}}{=} \underbrace{\mathtt{P}(\frac{\pi}{2}+\varphi)}_{\mathbf{4}}\underbrace{\mathtt{W}}_{\mathbf{3}}\underbrace{\mathtt{P}(\theta)}_{\mathbf{2}}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \\
&\overset{\mathbf{2}}{=} \underbrace{\mathtt{P}(\frac{\pi}{2}+\varphi)}_{\mathbf{4}}\underbrace{\mathtt{W}}_{\mathbf{3}}\frac{1}{\sqrt{2}}(|0\rangle+e^{\boldsymbol{i}\theta}\,|1\rangle) = \underbrace{\mathtt{P}(\frac{\pi}{2}+\varphi)}_{\mathbf{4}}\underbrace{\mathtt{W}}_{\mathbf{3}}\frac{e^{\boldsymbol{i}\frac{\theta}{2}}}{\sqrt{2}}(e^{-\boldsymbol{i}\frac{\theta}{2}}\,|0\rangle+e^{\boldsymbol{i}\frac{\theta}{2}}\,|1\rangle) \\
&\overset{\mathbf{3}}{=} \underbrace{\mathtt{P}(\frac{\pi}{2}+\varphi)}_{\mathbf{4}}\frac{e^{\boldsymbol{i}\frac{\theta}{2}}}{\sqrt{2}}(e^{-\boldsymbol{i}\frac{\theta}{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)+e^{\boldsymbol{i}\frac{\theta}{2}}\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right) \\
&= \underbrace{\mathtt{P}(\frac{\pi}{2}+\varphi)}_{\mathbf{4}}e^{\boldsymbol{i}\frac{\theta}{2}}\left(\cos\frac{\theta}{2}\,|0\rangle-i\sin\frac{\theta}{2}\,|1\rangle\right) \\
&\overset{\mathbf{4}}{=} e^{\boldsymbol{i}\frac{\theta}{2}}\left(\cos\frac{\theta}{2}\,|0\rangle+e^{\boldsymbol{i}\varphi}\sin\frac{\theta}{2}\,|1\rangle\right) \equiv \cos\frac{\theta}{2}\,|0\rangle+e^{\boldsymbol{i}\varphi}\sin\frac{\theta}{2}\,|1\rangle
\end{aligned}
$$

Portes de contrôle I

Porte `Controlled-U` ou `CU`

- Les portes CU sont des portes de contrôle $\mathtt{U}$ qui traduisent quantiquement `if ( x ) then` $y \leftarrow \mathtt{U}^x y$ par

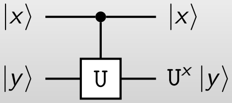
$$|x\rangle\,|y\rangle \mapsto |x\rangle\,\mathtt{U}^x\,|y\rangle$$

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

$$|0\rangle\,|0\rangle \to |0\rangle\,|0\rangle \qquad |0\rangle\,|1\rangle \to |0\rangle\,|1\rangle \qquad |1\rangle\,|0\rangle \to |1\rangle\,\mathtt{U}\,|0\rangle \qquad |1\rangle\,|1\rangle \to |1\rangle\,\mathtt{U}\,|1\rangle$$

Dans la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, où $\mathbb{I}$, $\mathbb{O}$ et $\mathtt{U}$ sont des matrices 2×2

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



Portes de contrôle II

Porte `Controlled-U` ou `CU`

- Le 1er bit $|x\rangle$ agit comme contrôle et sa valeur reste inchangée à la sortie. Le 2e bit $|y\rangle$ est appelé cible. Sur le diagramme, le contrôle est représenté le point noir

Une porte CU applique

- la transformation identité $\mathbb{I}$ au bit cible lorsque le bit de contrôle est dans l'état $|0\rangle$
- la transformation U au bit cible lorsque le bit de contrôle est dans l'état $|1\rangle$

- Puisque pour $x \in \{0, 1\}$, $\mathtt{U}^{2x} = \mathbb{I}$ et les opérateurs CU sont unitaires
- Pour une transformation unitaire quelconque $\mathtt{U}: \ (x, y) \rightarrow (x, y \oplus f(x))$, on a

$$|\psi\rangle = \mathtt{CU}(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle = \alpha\,|0f(0)\rangle + \beta\,|1f(1)\rangle$$

qui contient à la fois l'information sur $f(0)$ et sur $f(1)$

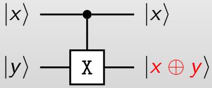
Definition (Porte `CNOT`)

`CNOT` ou `CX` est la plus populaire des portes CU

$$\mathtt{CX} = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \mathtt{X} = \begin{pmatrix} \mathbb{I} & \mathbb{O} \\ \mathbb{O} & \mathtt{X} \end{pmatrix} = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

qui inverse le bit cible $|y\rangle$ lorsque le bit de contrôle $|x\rangle \equiv |1\rangle$

$$\mathtt{CX}\,|x\rangle\,|y\rangle = |x\rangle\,|x \oplus y\rangle$$



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

Portes de contrôle II

- On note sur la table de vérité que lorsque la cible $|y\rangle \equiv |0\rangle$ la porte CX devient la porte COPY (clonage de $|x\rangle$) : $|x\rangle |0\rangle \mapsto |x\rangle |x\rangle \,, \ x \in \{0, 1\}$

$$\mathtt{CX}(\alpha |0\rangle + \beta |1\rangle) |0\rangle = \alpha |00\rangle + \beta |11\rangle$$

qui est non factorisable pour $\alpha, \beta \neq 0$.

La porte CNOT génère des états intriqués

Theorem

Toute opération unitaire sur $\mathcal{H}^{\otimes n}$ peut se décomposer en produit d'opérations unitaires single qubit (1-qubit) et de CNOT.

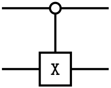
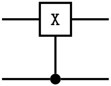
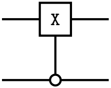
- Nous utiliserons la notation abrégée $\mathtt{CU}_{[ij]}$ pour indiquer que le qubits i est le contrôle et le qubits j la cible. Par exemple,

$$\mathtt{CX}_{[12]} |xy\rangle = \mathtt{CX} |xy\rangle = |x\rangle |x \oplus y\rangle \qquad \mathtt{CX}_{[21]} |xy\rangle = |x \oplus y\rangle |y\rangle$$

Portes de contrôle III

Porte CNOT

- Ainsi, les trois autres matrices CNOT sont, pour $P_0 = |0\rangle\langle 0|$ et $P_1 = |1\rangle\langle 1|$

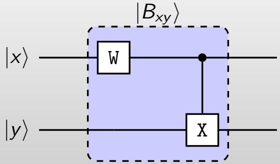
$\mathtt{CX}^{-}_{[12]} = P_0 \otimes \mathtt{X} + P_1 \otimes \mathbb{I}$	$\mathtt{CX}_{[21]} = \mathtt{X} \otimes P_1 + \mathbb{I} \otimes P_0$	$\mathtt{CX}^{-}_{[21]} = \mathbb{I} \otimes P_1 + \mathtt{X} \otimes P_0$
$\left(\begin{array}{cc\|cc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$	$\left(\begin{array}{cc\|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right)$	$\left(\begin{array}{cc\|cc} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$
		
$\mathtt{CX}^{-}_{[12]}$ inverse le 2e qubit lorsque le 1er est dans l'état $\|0\rangle$	$\mathtt{CX}_{[21]}$ inverse le 1er qubit lorsque le 2e est dans l'état $\|1\rangle$	$\mathtt{CX}^{-1}_{[21]}$ inverse le 1er qubit lorsque le 2e est dans l'état $\|0\rangle$

- cercle noir= opération de contrôle positif ou qubit cible inversé lorsque le contrôle est $|1\rangle$
- cercle vide= opération de contrôle négatif ou qubit cible inversé lorsque le contrôle est $|0\rangle$

Portes de contrôle

Génération des états de Bell - États maximalement intriqués

- Circuit générant les états intriqués de Bell



$$
\begin{aligned}
|B_{xy}\rangle &= \mathtt{CX}(\mathtt{W} \otimes \mathbb{I})\,|xy\rangle \quad x, y \in \{0, 1\} \\
&= \frac{1}{\sqrt{2}}(|0y\rangle + (-1)^x\,|1(1-y)\rangle)
\end{aligned}
$$

- Ainsi,

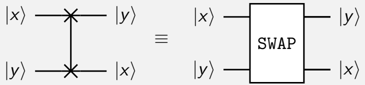
$$
|00\rangle \to |B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |10\rangle \to |B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)
$$

$$
|01\rangle \to |B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |11\rangle \to |B_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
$$

Definition (Porte SWAP)

La porte SWAP permute ou intervertit deux qubits

$$\mathrm{SWAP} = \mathrm{CXCX}_{[21]}\mathrm{CX} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



- Par exemple, pour $|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)$ et $|\phi\rangle = (\delta|0\rangle + \gamma|1\rangle)$ on a

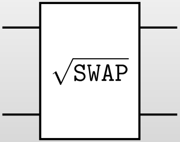
$$\begin{aligned}
\mathrm{CXCX}_{[21]}\mathrm{CX}\,|\psi\rangle|\phi\rangle &= \mathrm{CXCX}_{[21]}\mathrm{CX}(\alpha|0\rangle + \beta|1\rangle)(\delta|0\rangle + \gamma|1\rangle) \\
&= \mathrm{CXCX}_{[21]}(\alpha\delta|00\rangle + \alpha\gamma|01\rangle + \beta\delta|11\rangle + \beta\gamma|10\rangle) \\
&= \mathrm{CX}(\alpha\delta|00\rangle + \alpha\gamma|11\rangle + \beta\delta|01\rangle + \beta\gamma|10\rangle) \\
&= (\alpha\delta|00\rangle + \alpha\gamma|10\rangle + \beta\delta|01\rangle + \beta\gamma|11\rangle) \\
&= \delta|0\rangle(\alpha|0\rangle + \beta|1\rangle) + \gamma|1\rangle(\alpha|0\rangle + \beta|1\rangle) \\
&= |\phi\rangle|\psi\rangle
\end{aligned}$$

Portes quantiques universelles

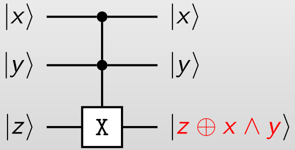
Porte $\sqrt{\texttt{SWAP}}$

- Les portes universelles facilitent l'intégration à partir de portes pré-caractérisées
- Comme n'importe quelle fonction peut être synthétisée à l'aide des $\texttt{CNOT}$ et 1-qubits $\texttt{W}$, $\texttt{P}(\delta)$: ($\texttt{CNOT}$, $\texttt{W}$, $\texttt{P}(\delta)$) forme un ensemble infini de portes quantiques universelles
- La porte $\sqrt{\texttt{SWAP}}$ qui effectue la moitié des chemins de deux qubits swap est universelle : n'importe quelle porte logique quantique peut être construite à partir de seulement la porte $\sqrt{\texttt{SWAP}}$, et des portes 1-qubit

$$\sqrt{\texttt{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



La porte TOFFOLI ou porte Controlled-Controlled-NOT (CCNOT, C^2NOT) est une porte à trois bits d'entrée et de sortie



z est inversé lorsque x=y=1

N°	x	y	z	x	y	$z \oplus x \wedge y$
1	0	0	0	0	0	0
2	0	0	1	0	0	1
3	0	1	0	0	1	0
4	0	1	1	0	1	1
5	1	0	0	1	0	0
6	1	0	1	1	0	1
7	1	1	0	1	1	1
8	1	1	1	1	1	0

La porte CCNOT nous donne la connectivité logique nécessaire à l'arithmétique

- Lorsque le qubit cible $|z\rangle$ est dans l'état $|0\rangle$ (lignes 1, 3, 5, 7), la porte de CCNOT effectue l'opération AND

$$\mathtt{CCNOT}\,|x\rangle\,|y\rangle\,|0\rangle = |x\rangle\,|y\rangle\,|x \wedge y\rangle$$

Portes quantiques universelles II

Porte de TOFFOLI

- Lorsque le qubit cible $|z\rangle$ est dans l'état $|1\rangle$ (lignes 2, 4, 6, 7), la porte de CCNOT effectue l'opération NAND

$$\mathtt{CCNOT}\,|x\rangle\,|y\rangle\,|1\rangle = |x\rangle\,|y\rangle\,|x \barwedge y\rangle$$

- Lorsque le premier qubit de contrôle $|x\rangle$ est dans l'état $|1\rangle$ (lignes 5-8), la porte de CCNOT effectue l'opération CNOT

$$\mathtt{CCNOT}\,|1\rangle\,|y\rangle\,|z\rangle = |1\rangle\,|y\rangle\,|z \oplus y\rangle$$

- Lorsque le premier qubit de contrôle $|x\rangle$ est dans l'état $|1\rangle$ et le qubit cible $|z\rangle$ est dans l'état $|0\rangle$ (lignes 5 et 7), la porte de CCNOT effectue l'opération COPY

$$\mathtt{CCNOT}\,|1\rangle\,|y\rangle\,|0\rangle = |1\rangle\,|y\rangle\,|y\rangle$$

La porte de CCNOT, avec l'initialisation de valeur constante, est une porte universelle pour toutes les opérations réversibles de la logique booléenne.