Notes de cours
Semaine 2

Cours Turing+

1 Trois qubits et plus

L'état d'un système de n qubits est décrit par un vecteur unité dans $\mathbb{R}^{2^n}$. Ainsi, pour trois qubits, l'espace vectoriel est $\mathbb{R}^8$ (et non $\mathbb{R}^6$!) et les vecteurs de base de cet espace à 8 dimensions sont

$$|0,0,0\rangle = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix} \quad |0,0,1\rangle = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix} \quad |0,1,0\rangle = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix} \quad |0,1,1\rangle = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}$$

et

$$|1,0,0\rangle = \begin{pmatrix}0\\0\\0\\0\\1\\0\\0\\0\end{pmatrix} \quad |1,0,1\rangle = \begin{pmatrix}0\\0\\0\\0\\0\\1\\0\\0\end{pmatrix} \quad |1,1,0\rangle = \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix} \quad |1,1,1\rangle = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix}$$

Remarquez également que les trois bits à gauche de l'égalité représentent en binaire la position du 1 dans le vecteur colonne à droite de l'égalité (avec des positions numérotées de 0 à 7).

L'état général de trois qubits s'écrit donc sous la forme

$$|\varphi\rangle = \sum_{x_1,x_2,x_3\in\{0,1\}} \alpha_{x_1,x_2,x_3} |x_1,x_2,x_3\rangle \quad \text{avec} \quad \sum_{x_1,x_2,x_3\in\{0,1\}} \alpha^2_{x_1,x_2,x_3} = 1$$

Introduisons également la notation plus compacte :

$$|\varphi\rangle = \sum_{0\leq x\leq 7} \alpha_x |x\rangle \quad \text{avec} \quad \sum_{0\leq x\leq 7} \alpha_x^2 = 1$$

où le nombre $0 \leq x \leq 7$ remplace ici sa représentation binaire x_1, x_2, x_3. L'état d'un ensemble de trois qubits peut être "encore plus" intriqué que les états à deux qubits, comme par exemple l'état baptisé "état GHZ" (pour Greenberger-Horne-Zeilinger[1]) défini par :

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0,0,0\rangle + |1,1,1\rangle)$$

Voici finalement la généralisation à n qubits. Un état s'écrit :

$$|\varphi\rangle = \sum_{x_1,\ldots,x_n \in \{0,1\}} \alpha_{x_1,\ldots,x_n} |x_1,\ldots,x_n\rangle \quad \text{avec} \quad \sum_{x_1,\ldots,x_n \in \{0,1\}} \alpha^2_{x_1,\ldots,x_n} = 1$$

ou encore en notation plus compacte :

$$|\varphi\rangle = \sum_{0 \leq x \leq 2^n-1} \alpha_x |x\rangle \quad \text{avec} \quad \sum_{0 \leq x \leq 2^n-1} \alpha^2_x = 1$$

2 Portes quantiques

Nous avons déjà vu trois portes qui peuvent être utilisées dans des circuits quantiques : les portes NOT, CNOT et CCNOT (ou Toffoli). Comme mentionné précédemment, ces portes ont la propriété d'être réversibles (une double application de chacune permettant de revenir à l'état de départ), ce qui les rend utilisables dans un circuit quantique. Mais avant d'aller plus loin, il importe d'abord d'expliquer plus en détail l'action que peut avoir une porte quantique sur un ou des qubits (ce qui nous donnera aussi l'occasion de comprendre pourquoi il faut que celles-ci soient réversibles).

Une porte quantique (ou plus généralement un circuit quantique) peut toujours être vue comme une transformation linéaire agissant sur l'espace vectoriel dans lequel "vivent" les qubits concernés. Et toute transformation linéaire peut toujours être représentée par une matrice de mêmes dimensions que l'espace sur lequel elle agit. Ainsi, une porte quantique agissant sur un qubit peut être représentée par une matrice 2×2, une porte agissant sur deux qubits par une matrice 4×4, une porte agissant sur trois qubits par une matrice 8×8, etc.

Et c'est là qu'intervient une contrainte importante : vu que l'état $|\varphi\rangle$ d'un système quantique est toujours représenté par un vecteur *unité*, la transformation linéaire représentant une porte quantique (qu'on note en général par une lettre majuscule, disons U) doit toujours être *unitaire*, ce qui veut dire mathématiquement que $UU^T = U^TU = I$, où U^T désigne la transposée de la matrice U, et I la matrice identité. Ceci veut dire en particulier qu'il est toujours possible, après le passage par une porte quantique U, d'appliquer potentiellement une autre transformation U^T (en fait, la même transformation si U est une matrice *symétrique* : $U^T = U$) pour revenir à l'état initial ; en d'autres mots, la transformation U est réversible.

[1] lauréat du Prix Nobel 2022 avec Alain Aspect, mentionné la semaine dernière

Remarque préliminaire : Attention à ne pas confondre dans ce qui va suivre :

- l'addition "simple" de deux vecteurs dans $\mathbb{R}^2$ (ou $\mathbb{R}^4$ ou ...) : $|\varphi_1\rangle + |\varphi_2\rangle$

- le produit tensoriel de deux bits quantiques $|\varphi_1\rangle \otimes |\varphi_2\rangle$

- l'addition modulo 2 (XOR) de deux bits classiques $x \oplus y$

La porte NOT (aussi notée X)

Symbole : $|x\rangle$ —[X]— $|\overline{x}\rangle$

Commençons par la porte quantique la plus simple: la porte NOT (aussi notée X parfois). Celle-ci agit sur un qubit (donc $\mathbb{R}^2$). Pour décrire son effet, le plus simple est de décrire celui-ci sur les états de base $|0\rangle$ et $|1\rangle$:

$$\mathrm{NOT}\,|0\rangle = |1\rangle \quad \text{et} \quad \mathrm{NOT}\,|1\rangle = |0\rangle$$

donc $\mathrm{NOT}\,|x\rangle = |\overline{x}\rangle$ pour $x \in \{0,1\}$. Vu qu'il s'agit d'une transformation linéaire, on déduit que pour un état superposé $|\varphi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$,

$$\mathrm{NOT}\,|\varphi\rangle = \alpha_0\,\mathrm{NOT}\,|0\rangle + \alpha_1\,\mathrm{NOT}\,|1\rangle = \alpha_0\,|1\rangle + \alpha_1\,|0\rangle$$

On déduit aussi que

$$\langle 0|\,\mathrm{NOT}\,|0\rangle = \langle 0|1\rangle = 0 \qquad \langle 0|\,\mathrm{NOT}\,|1\rangle = \langle 0|0\rangle = 1$$
$$\langle 1|\,\mathrm{NOT}\,|0\rangle = \langle 1|1\rangle = 1 \qquad \langle 1|\,\mathrm{NOT}\,|1\rangle = \langle 1|0\rangle = 0$$

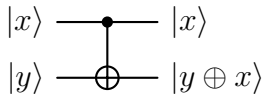
d'où la représentation matricielle $\mathrm{NOT} = \mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Cette matrice est clairement symétrique et aussi unitaire, car

$$XX^T = X^T X = X^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Exercice : Calculez $\mathrm{NOT}\,|+\rangle$ et $\mathrm{NOT}\,|-\rangle$.

La porte CNOT

Symbole :



Celle-ci agit sur deux qubits (donc $\mathbb{R}^4$). Son action sur les états de base est la suivante :

$$\mathrm{CNOT}\,|x,y\rangle = |x, y \oplus x\rangle \quad x,y \in \{0,1\}$$
(ce qui pourrait aussi s'écrire : $\mathrm{CNOT}\,(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus x\rangle$)

et son action sur un état superposé est donc, par linéarité :

$$\mathrm{CNOT}\,(\alpha_{0,0}\,|0,0\rangle + \alpha_{0,1}\,|0,1\rangle + \alpha_{1,0}\,|1,0\rangle + \alpha_{1,1}\,|1,1\rangle) = \alpha_{0,0}\,|0,0\rangle + \alpha_{0,1}\,|0,1\rangle + \alpha_{1,0}\,|1,1\rangle + \alpha_{1,1}\,|1,0\rangle$$

Exercice : Calculez la représentation matricielle de la porte CNOT et vérifiez également que c'est une transformation (symétrique et) unitaire.

Remarque importante : Même s'il a été dit dans la cas classique que la porte CNOT peut être utilisée pour émuler une porte COPY (en choisissant 0 pour la valeur de y en entrée), ce n'est pas vrai dans le cas quantique ! Voyez plutôt : supposons que le premier qubit en entrée soit dans l'état superposé $|\varphi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$. Alors

$$\mathrm{CNOT}\left(|\varphi\rangle \otimes |0\rangle\right) = \mathrm{CNOT}\left(\alpha_0 |0\rangle \otimes |0\rangle + \alpha_1 |1\rangle \otimes |0\rangle\right) = \alpha_0 |0\rangle \otimes |0\rangle + \alpha_1 |1\rangle \otimes |1\rangle = \alpha_0 |0,0\rangle + \alpha_1 |1,1\rangle$$

et cette sortie n'est clairement pas égale à

$$|\varphi\rangle \otimes |\varphi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) = \alpha_0^2 |0,0\rangle + \alpha_0\alpha_1(|0,1\rangle + |1,0\rangle) + \alpha_1^2 |1,1\rangle$$

En fait, il existe un théorème plus profond qui dit qu'en général, on ne peut jamais copier (ou "cloner") un état quantique !

La porte CNOT quantique permet également de réaliser des choses amusantes... Par exemple, si le second qubit en entrée est dans l'état $|-\rangle$, qui pour rappel vaut $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, alors nous avons d'une part :

$$\mathrm{CNOT}\left(|0\rangle \otimes |-\rangle\right) = \mathrm{CNOT}\left(\frac{1}{\sqrt{2}} |0,0\rangle - \frac{1}{\sqrt{2}} |0,1\rangle\right) = \frac{1}{\sqrt{2}} |0,0\rangle - \frac{1}{\sqrt{2}} |0,1\rangle = |0\rangle \otimes |-\rangle$$

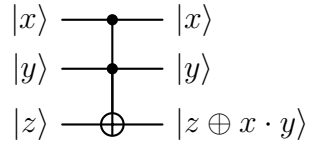
et d'autre part :

$$\mathrm{CNOT}\left(|1\rangle \otimes |-\rangle\right) = \mathrm{CNOT}\left(\frac{1}{\sqrt{2}} |1,0\rangle - \frac{1}{\sqrt{2}} |1,1\rangle\right) = \frac{1}{\sqrt{2}} |1,1\rangle - \frac{1}{\sqrt{2}} |1,0\rangle = -|1\rangle \otimes |-\rangle$$

Ainsi donc, $\mathrm{CNOT}\left(|x\rangle \otimes |-\rangle\right) = (-1)^x |x\rangle \otimes |-\rangle$ pour $x \in \{0,1\}$: l'état global des deux qubits ne change pas, fondamentalement : il est juste mutiplié par -1 lorsque x vaut 1 (et bizarrement, l'état du second qubit ne semble pas le moins du monde affecté, alors que dans le cas classique, la porte CNOT n'agit *que* sur le second qubit !).

La porte de Toffoli (ou CCNOT)

Symbole :



Cette porte agit sur trois qubits (donc sur $\mathbb{R}^8$). Son action sur les états de base $|x,y,z\rangle$ ainsi que sa représentation matricielle sont obtenues de manière similaire à la porte CNOT et sont laissées en exercice.

3 Autres portes quantiques

La richesse du monde quantique permet de construire de nouvelles portes qui n'ont tout simplement pas d'équivalent dans le monde classique. Voyons-en quelques-unes.

3.1 Portes à un qubit

La porte de Hadamard (aussi notée H)

Cette porte va nous être très utile pour le calcul quantique ! Elle permet de créer des états superposés à partir des états de base. Son action est la suivante:

$$\mathrm{H}\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle \quad \text{et} \quad \mathrm{H}\,|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle$$

donc si $|\varphi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$, alors

$$\mathrm{H}\,|\varphi\rangle = \frac{\alpha_0 + \alpha_1}{\sqrt{2}}\,|0\rangle + \frac{\alpha_0 - \alpha_1}{\sqrt{2}}\,|1\rangle$$

Sa représentation matricielle est ainsi donnée par $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Exercice : Vérifiez ce dernier point et aussi le fait que H est unitaire.

La porte Z

La porte Z est quant à elle définie par

$$\mathrm{Z}\,|0\rangle = |0\rangle \quad \text{et} \quad \mathrm{Z}\,|1\rangle = -\,|1\rangle$$

Ainsi, pour $|\varphi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$, on obtient $\mathrm{Z}\,|\varphi\rangle = \alpha_0\,|0\rangle - \alpha_1\,|1\rangle$ et sa représentation matricielle est donnée par $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, qui est clairement une transformation unitaire.

Exercice : Calculez $\mathrm{Z}\,|+\rangle$ et $\mathrm{Z}\,|-\rangle$.

Les portes S et T

Nous n'utiliserons pas ces portes quantiques dans le présent cours, mais il est important de les mentionner malgré tout. Celles-ci sont définies respectivement par

$$\mathrm{S}\,|0\rangle = |0\rangle\,, \quad \mathrm{S}\,|1\rangle = e^{i\pi/2}\,|1\rangle \quad \text{et} \quad \mathrm{T}\,|0\rangle = |0\rangle\,, \quad \mathrm{T}\,|1\rangle = e^{i\pi/4}\,|1\rangle$$

et il importe donc de travailler dans un l'espace vectoriel complexe $\mathbb{C}^2$ (et non plus $\mathbb{R}^2$) pour les définir correctement. L'utilité de ces portes est multiple :

- on peut montrer tout d'abord que toute porte unitaire U agissant sur un qubit (donc sur $\mathbb{C}^2$) peut être approximée par un ensemble de portes H, S et T ;

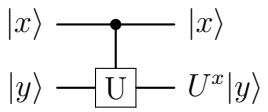
- les portes S et T sont utilisées dans l'algorithme de Shor ;

- on peut montrer en général (mais c'est un peu théorique) que sans la porte T, un circuit quantique n'est pas capable de résoudre un problème de manière exponentiellement plus efficace que ne le ferait un circuit classique (théorème de Gottesman-Knill).

3.2 Portes à deux qubits

La porte "Controlled-U" (CU)

Symbole :



Cette porte est une généralisation de la porte CNOT : U est ici une porte à un qubit (agissant donc sur $\mathbb{R}^2$) qui agit sur le second qubit $|y\rangle$ seulement lorsque le premier qubit $|x\rangle$ est dans l'état $|1\rangle$. Concrètement, ceci veut dire que pour $y \in \{0,1\}$:

$$\mathrm{CU}\left(|0\rangle \otimes |y\rangle\right) = |0\rangle \otimes |y\rangle \quad \text{et} \quad \mathrm{CU}\left(|1\rangle \otimes |y\rangle\right) = |1\rangle \otimes U\,|y\rangle$$

ce qu'on peut résumer par

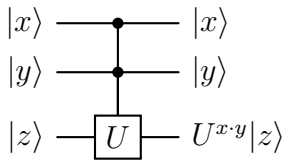
$$\mathrm{CU}\left(|x\rangle \otimes |y\rangle\right) = |x\rangle \otimes U^x\,|y\rangle \quad \text{pour } x, y \in \{0,1\}$$

L'action de la porte CU est ensuite étendue par linéarité à tout état $|\varphi\rangle \in \mathbb{R}^4$.

3.3 Portes à trois qubits et plus

La porte "Controlled-Controlled-U" (CCU)

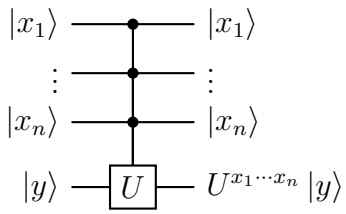
Symbole :



Cette porte (agissant sur trois qubits) est une généralisation de la porte de Toffoli : pour que la porte U agisse sur le dernier qubit $|z\rangle$, il faut que les qubits $|x\rangle$ et $|y\rangle$ soient tous deux dans l'état $|1\rangle$.

La porte "Multicontrolled-U"

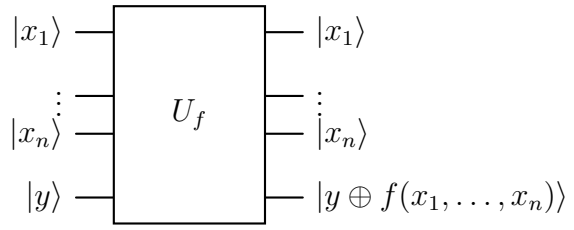
Symbole :



Cette porte (agissant sur $n+1$ qubits) est encore une généralisation de la précécente : pour que la porte U agisse sur le dernier qubit $|y\rangle$, il faut que *tous* les n premiers qubits $|x_1\rangle, \ldots, |x_n\rangle$ soient dans l'état $|1\rangle$.

La porte "oracle" U_f

Symbole :



Pour finir, voici une porte qui sera d'importance capitale pour la suite de ce cours !

En effet, il n'est en général pas possible d'évaluer directement une fonction booléenne $f : \{0,1\}^n \to \{0,1\}^m$ au moyen un circuit quantique, pour la bonne raison que si $n \neq m$, alors un circuit avec n entrées et m sorties ne peut être réversible (il y aurait une possibilité lorsque $n = m$, mais il faudrait alors que la fonction f soit bijective, ce qui constitue une limitation trop sévère).

Pour autant, il est toujours possible de construire une porte quantique réversible pour évaluer la fonction f. Pour simplifier, supposons ici que la dimension de l'ensemble d'arrivée vaut $m = 1$, ce qui sera le cas pour le reste du cours (mais notez bien que la généralisation à $m > 1$ n'est pas difficile). La porte U_f est une porte à $n+1$ qubits dont l'action sur les états de base est la suivante:

$$U_f \, |x_1, \ldots, x_n, y\rangle = |x_1, \ldots, x_n, y \oplus f(x_1, \ldots, x_n)\rangle$$

Elle ressemble ainsi quelque peu à la porte multi-contrôlée vue plus haut, à la différence près que le contrôle est ici dépendant de la valeur de $f(x_1, \ldots, x_n)$: si cette valeur vaut 0, alors la porte ne fait rien ; tandis que si cette valeur vaut 1, alors la valeur du $(n+1)^e$ qubit y est inversée.

Vous noterez que quelle que soit la fonction f, cette porte est réversible, car une double application de celle-ci nous ramène à l'état de départ. Nous avons ainsi trouvé un moyen d'évaluer la fonction f dans un circuit quantique !