Informatique Quantique: Devoir 1

Jean-Baptiste Bertrand

27 septembre 2022

I : Concurrence

Pour un état à deux qubits quelconque, écrit

$$|\psi\rangle = \psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle$$

, la concurrence d'un tel état s'écrit

$$C = 2|\psi_{00}\psi_{11} - \psi_{01}\psi_{10}|$$

. Cette dernière est nulle si et seulement si les deux qubits ne sont pas intriqués.

($\Longleftarrow$)
Si l'état est non intriqué, on peut l'écrire comme

$$|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = \begin{pmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{10} \\ \psi_{11} \end{pmatrix}$$

$$\implies C = 2|ac \cdot bd - ad \cdot bc| = 0$$

$\blacksquare$

($\implies$)

La condition de factorisabilité mentionné plus haut donne quatre équation qui contraignes les valeurs de coefficient φ_{ij}. On peut réécrire celles-ci comme

$$\begin{cases} ac = \psi_{00} \\ ad = \psi_{01} \\ bc = \psi_{10} \\ db = \psi_{11} \end{cases} \overset{*}{\iff} \begin{cases} \frac{a\cancel{c}}{b\cancel{c}} = \frac{\psi_{00}}{\psi_{10}} \\ \frac{a\cancel{d}}{\cancel{d}b} = \frac{\psi_{01}}{\psi_{11}} \\ abcd = \psi_{10}\psi_{01} \\ abcd = \psi_{11}\psi_{00} \end{cases} \iff \begin{cases} \frac{\psi_{01}}{\psi_{11}} = \frac{\psi_{00}}{\psi_{10}} \\ \psi_{11}\psi_{00} = \psi_{10}\psi_{01} \end{cases} \iff \psi_{11}\psi_{00} = \psi_{10}\psi_{01}$$

$$C = 0 \implies \psi_{00}\psi_{11} = \psi_{01}\psi_{10} \quad \therefore C = 0 \implies \text{les états sont factorisables (non-intriqués)}$$

* La double implication surmontée d'une étoile suggère qu'il n'y a pas de division par 0 ($b \neq 0$). Cela peut sembler problématique mais on peut toujours faire la supposition que $b \neq 0$ car il existe toujours un base ou cela sera la cas. De plus l'intrication ne dépend évidement pas de la base choisi, on est donc libre de faire ce choix.

$\blacksquare$

II : Échange d'intrication

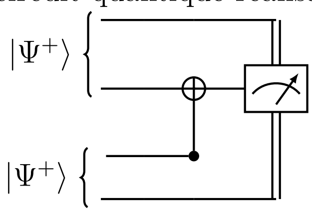
Les paires de qubits peuvent s'écrirent ainsi :

$$\frac{1}{\sqrt{2}}\left(|01\rangle_A + |10\rangle_B\right)\otimes\frac{1}{\sqrt{2}}\left(|01\rangle_A + |10\rangle_B\right) = \frac{1}{2}\left(|0\rangle_A|10\rangle_C|1\rangle_B + |1\rangle_A|00\rangle_C|1\rangle_B + |0\rangle_A|11\rangle_C|0\rangle_B + |1\rangle_A|01\rangle_C|0\rangle_B\right)$$

Les deux qubits *centraux* on été séparer des autres afin de bien voir ceux auquel charlies à accès. On remarque que si Charlie mesure $Z_1 \oplus Z_2$ il obtiens 1 ou 0 et effondre les deux qubits restant dans une paire de Bell

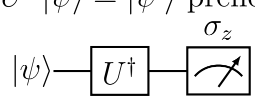
$$\begin{cases} Z \oplus Z = 0 & |1\rangle_A|1\rangle_B + |0\rangle_A|0\rangle_B \\ Z \oplus Z = 1 & |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B \end{cases}$$

Donc, dans les deux cas, on obtiens une paire de Bell partagé entre Alice et Bob. Charlie peut ensuite transmettre un bit classique à Alice et Bob pour leur dire quel état de Bell ils ont (Le résultat de $Z \oplus Z$). Alice et Bob peuvent alors manipuler la paire pour avoir exactement l'état de Bell qu'ils veulent. Le circuit quantique réalisant un telle chose ressemblerait à :



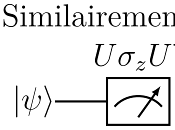
III : Circuit quantique et mesure

A Dans le cadre de l'informatique quantique, que deux mesures soient pareilles signifie que la valeur moyenne est la même pour n'importe quel état. Le cricuit $|\psi\rangle$—$\boxed{U^\dagger}$— est équvalent à l'expression $U^\dagger|\psi\rangle = |\psi'\rangle$ prendre une mesure de σ_z s'écris donc



$= \langle\psi'|\sigma_z|\psi'\rangle = \langle\psi|U\sigma_z U^\dagger|\psi\rangle$

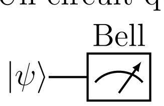
Similairement, le circuit qui mesure $U\sigma_z U^\dagger$ est

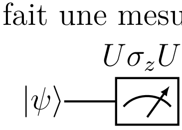


$= \langle\psi|U\sigma_z U^\dagger|\psi\rangle$

Les deux mesures sont donc parfaitement équivalentes

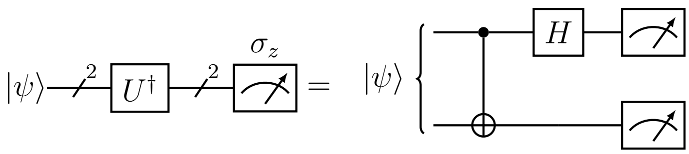
B Un circuit qui fait une mesure dans la base de Bell serait



$=$


$= \langle\psi|U\sigma_z U^\dagger|\psi\rangle = \langle\psi|\,\mathrm{cNOT}(H\mathbb{1})\sigma_z(H\mathbb{1})\mathrm{cNOT}\,|\psi\rangle$

avec U l'opérateur qui nous envoie dans la base de Bell soit $(H\mathbb{1})$cNOT . Le circuit qui réalise une telle mesure en se fiant au A, est alors



C Le circuit s'écrit comme

$$
\begin{aligned}
&(H\mathbb{1})CU(H\mathbb{1})\,|\psi_t\rangle \\
=&(H\mathbb{1})CU(H\mathbb{1})\,(|0\rangle \otimes |\psi\rangle) \\
=&\frac{1}{\sqrt{2}}(H\mathbb{1})CU\,\Big(\,|0\rangle\,|\psi\rangle + |1\rangle\,|\psi\rangle\Big) \\
=&\frac{1}{\sqrt{2}}(H\mathbb{1})\,\Big(\,|0\rangle\,|\psi\rangle + |1\rangle\,U\,|\psi\rangle\Big) \\
=&\frac{1}{2}\,\Big([|0\rangle + |1\rangle]\,|\psi\rangle + [|0\rangle - |1\rangle]U\,|\psi\rangle\Big) \\
=&\frac{1}{2}\,\Big([|0\rangle + |1\rangle]\,|\psi\rangle + [|0\rangle - |1\rangle]U\,|\psi\rangle\Big) \\
=&\frac{1}{2}\,\Big(\,|0\rangle\,(|\psi\rangle + U\,|\psi\rangle) + |1\rangle\,(|\psi\rangle - U\,|\psi\rangle)\Big) \\
=&\frac{1}{2}\,\Big(\,|0\rangle\,(\mathbb{1} + U) + |1\rangle\,(\mathbb{1} - U)\Big)\,|\psi\rangle
\end{aligned}
$$

$$
U = |u_+\rangle\!\langle u_+| - |u_-\rangle\!\langle u_-| \qquad \mathbb{1} = |u_+\rangle\!\langle u_+| + |u_-\rangle\!\langle u_-|
$$

$$
\implies \mathbb{1} + U = 2\,|u_+\rangle\!\langle u_+| \qquad \mathbb{1} - u = 2\,|u_i\rangle\!\langle u_i|
$$

$$
\begin{aligned}
&= |0\rangle\,|u_+\rangle\!\langle u_+|\,|\psi\rangle + |1\rangle\,|u_-\rangle\!\langle u_-|\,|\psi\rangle \\
&=\psi_{u_+}\,|0\rangle\,|u_+\rangle + \psi_{u_-}\,|1\rangle\,|u_-\rangle
\end{aligned}
$$

Les probabilité d'obtenir 0 ou 1 sont les même que d'obtenir u_+ ou u_-, respectivement. Aussi, l'effondrement de la fonction d'onde sur $|0\rangle$ ou $|1\rangle$ amène également l'effondrement de la fonction d'onde sur $|u_+\rangle$ ou $|u_-\rangle$, respectivement. Mesurer σ_z sur le premier qubit est donc une mesure de U sur le deuxième.

IV : Exponentielle de chaînes de Pauli

A D'abord, on peut montrer que $U\left(\hat{O}_1\right)^n U^\dagger = \left(\hat{O}_2\right)^n$ par récurrence. Premièrement

$$U\hat{O}_1U^\dagger = \hat{O}_2 \implies U\hat{O}_1 = \hat{O}_2 U$$

Ensuite, si on assume que

$$U\left(\hat{O}_1\right)^{n-1} U^\dagger = \left(\hat{O}_2\right)^{n-1}$$

alors

$$U\left(\hat{O}_1\right)^n U^\dagger = U\hat{O}_1\left(\hat{O}_1\right)^{n-1} U^\dagger = \hat{O}_2 U\left(\hat{O}_1\right)^{n-1} U^\dagger = \hat{O}_2\left(\hat{O}_2\right)^{n-1} = \left(\hat{O}_2\right)^n$$

Comme on sait que c'est vrai pour $n = 1$, c'est alors vrai $\forall n \geq 1$. On peut donc dire

$$Ue^{i\theta\hat{O}_1}U^\dagger = U\left(\sum_{n=1}^{\infty}\frac{1}{n!}(i\theta\hat{O}_1)^n\right)U^\dagger = \sum_{n=1}^{\infty}\frac{1}{n!}(i\theta)^n U(\hat{O}_1)^n U^\dagger = \sum_{n=1}^{\infty}\frac{1}{n!}(i\theta)^n(\hat{O}_2)^n = e^{i\theta\hat{O}_2}$$

$\blacksquare$

B

$$\text{cNOT}R_z(\theta)\text{cNOT} = \text{cNOT}e^{i\theta Z}\text{cNOT}$$

On a vu en classe que

$$\text{cNOT}\mathbb{1}Z_2\text{cNOT} = Z_1Z_2$$

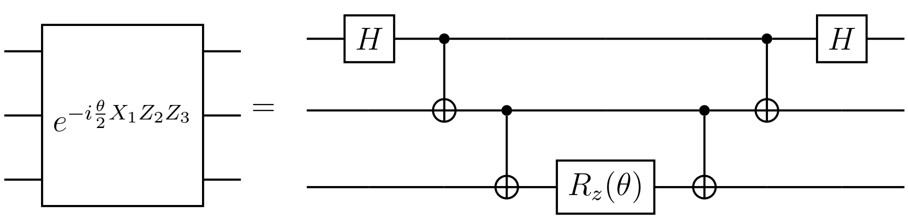
Donc, puisque cNOT est unitaire, par la propriété démontré en A, on a que

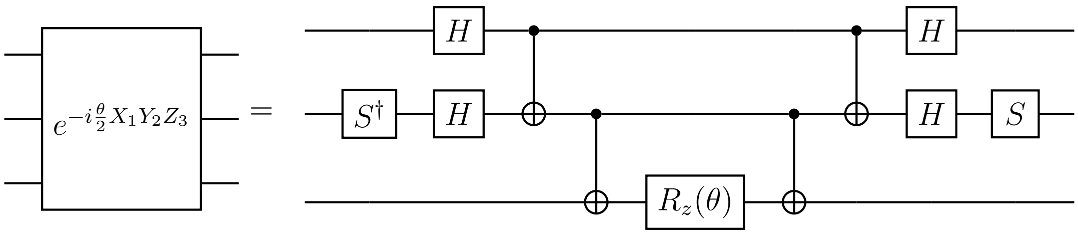
$$\text{cNOT}R_z(\theta)\text{cNOT} = \text{cNOT}e^{-i\theta/2Z}\text{cNOT} = e^{-i\theta/2\text{cNOT}\mathbb{1}Z\text{cNOT}} = e^{-i\theta/2Z_1Z_2}$$

De la même manière, pour le circuit à 3 qubits, on a

$$\begin{aligned}
&\text{cNOT}_{12}\text{cNOT}_{23}R_{z(\theta)}\text{cNOT}_{23}\text{cNOT}_{12}\\
=&\text{cNOT}_{12}\text{cNOT}_{23}e^{-i\theta/2\mathbb{1}\mathbb{1}Z_3}\text{cNOT}_{23}\text{cNOT}_{12}\\
=&\exp(-i\theta/2\text{cNOT}_{12}\text{cNOT}_{23}\mathbb{1}\mathbb{1}Z_3\text{cNOT}_{23}\text{cNOT}_{12})\\
=&\exp(-i\theta/2\text{cNOT}_{12}\mathbb{1}Z_2Z_3\text{cNOT}_{12})\\
=&e^{-i\theta/2Z_1Z_2Z_3}
\end{aligned}$$

C On a que $HZH = X$ et $SXS^\dagger = Y$ par conséquent, on peut générer transformer les Z obtenus précédemment en X et Y :





En effet, on a que

$$H_1 e^{-i\theta/2 Z_1 Z_2 Z_3} H_1 = e^{-i\theta/2 H_1 Z_1 H_1 Z_2 Z_3} = e^{-i\theta/2 X_1 Z_2 Z_3}$$

et que

$$S_2 H_2 e^{-i\theta/2 X_1 Z_2 Z_3} H_2 S_2^\dagger = e^{-i\theta/2 X_1 S_2 H_2 Z_2 H_2 S_2^\dagger Z_3} = e^{-i\theta/2 X_1 S X_2 S^\dagger Z_3} = e^{-i\frac{\theta}{2} X_1 Y_2 Z_3}$$