Informatique Quantique

Simon Perdrix [1]

Pépites Algorithmiques
simon.perdrix@loria.fr

Ecole des Mines de Nancy - 1 mars 2016

1. CNRS, équipe CARTE, LORIA

Une Information Quantique

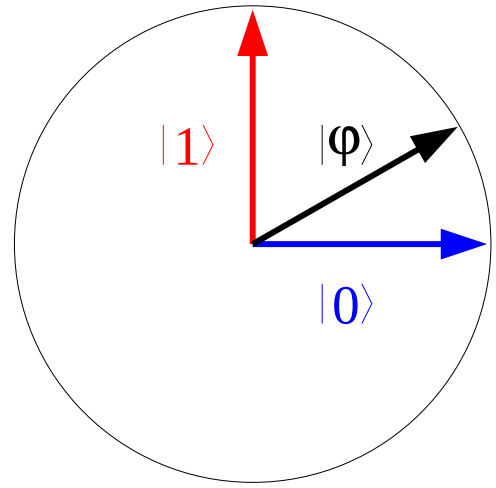
- Brique de base de l'information :

$$\mathbf{0}, \mathbf{1}$$

- Nous vivons dans un monde quantique :

$$\alpha \left|\mathbf{0}\right\rangle + \beta \left|\mathbf{1}\right\rangle$$

avec $\alpha, \beta \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 = 1$



Exemples :

$$\left|0\right\rangle$$

$$\frac{1}{\sqrt{2}}(\left|0\right\rangle + i \left|1\right\rangle)$$

Definition

L'état d'un registre quantique de taille n est un vecteur unité de $\mathbb{C}^{\{0,1\}^n}$:

$$\mathbf{\Phi} = \sum_{x \in \{0,1\}^n} \alpha_x \left|x\right\rangle \quad \text{avec} \quad ||\mathbf{\Phi}||^2 = \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$

Exemples :

$$\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$

$$\frac{1}{\sqrt{3}}(|00\rangle + i\,|01\rangle + |11\rangle)$$

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Système composé

Soit $\mathbf{\Phi}_1$ l'état d'un registre de n qubits et $\mathbf{\Phi}_2$ celui d'un registre de m qubits, l'état du registre composé de $(n+m)$ qubits est

$$\mathbf{\Phi} = \mathbf{\Phi}_1 \otimes \mathbf{\Phi}_2$$

avec $\cdot \otimes \cdot$ bilinéaire et $\forall x \in \{0,1\}^n, \forall y \in \{0,1\}^m, |x\rangle \otimes |y\rangle = |xy\rangle$

Exemples :

1. $|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$
2. $\frac{|0\rangle + i|1\rangle}{\sqrt{2}} \otimes \frac{|00\rangle - i|10\rangle}{\sqrt{2}} =$
3. $\frac{|01\rangle + |11\rangle}{\sqrt{2}} = ? \otimes ?$
4. $\frac{|00\rangle - |11\rangle}{\sqrt{2}} = ? \otimes ?$

Intrication

Definition

Un état $\mathbf{\Phi}$ est intriqué si pour tout $\mathbf{\Phi_1}, \mathbf{\Phi_2}$,

$$\mathbf{\Phi} \neq \mathbf{\Phi_1} \otimes \mathbf{\Phi_2}$$

Exemple :

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Mesurer, c'est Transformer

$$\alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{|\alpha|^2} |0\rangle \text{ on mesure } 0$$

$$\alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{|\beta|^2} |1\rangle \text{ on mesure } 1$$

La mesure est **probabiliste** et **irréversible**.

$$\text{Mesure} \implies \text{Interaction} \implies \text{Transformation}$$

Système fermé : une évolution unitaire

Un système fermé évolue

- de façon linéaire, i.e. $U(\alpha\mathbf{\Phi} + \beta\mathbf{\Psi}) = \alpha U(\mathbf{\Phi}) + \beta U(\mathbf{\Psi})$;
- en préservant la condition de normalisation, i.e. $||U(\mathbf{\Phi})|| = ||\mathbf{\Phi}||$.

Exemples d'évolutions unitaires

$$X \;:\; \begin{array}{lcl} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{array}$$

$$Z \;:\; \begin{array}{lcl} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{array}$$

$$H \;:\; \begin{array}{lcl} |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

$$R_z(\theta) \;:\; \begin{array}{lcl} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & e^{i\theta}|1\rangle \end{array}$$

$$CNot \;:\; \begin{array}{lcl} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$$

Exemples : $\begin{array}{ll} HH|0\rangle & = \\ HH|1\rangle & = \end{array}$

Composition de transformations unitaires

Si une partie d'un registre évolue selon U et le reste du registre selon V alors l'évolution globale du registre est $U \otimes V$ avec :

$$(U \otimes V)(\mathbf{\Phi} \otimes \mathbf{\Psi}) = (U\mathbf{\Phi}) \otimes (V\mathbf{\Psi})$$

Exemples :

$(H \otimes H)\,|01\rangle =$

$(H\,|0\rangle) \otimes (H\,|1\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2}$

Quand l'état est intriqué, utiliser la linéarité :

$$(U \otimes V)\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{(U\otimes V)|00\rangle+(U\otimes V)|11\rangle}{\sqrt{2}}$$

$$= \frac{(U|0\rangle)\otimes(V|0\rangle)+(U|1\rangle)\otimes(V|1\rangle)}{\sqrt{2}}$$

Exemples d'évolutions unitaires

$$X \quad : \quad \begin{array}{lcl} |0\rangle & \mapsto & |1\rangle \\ |1\rangle & \mapsto & |0\rangle \end{array}$$

$$Z \quad : \quad \begin{array}{lcl} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{array}$$

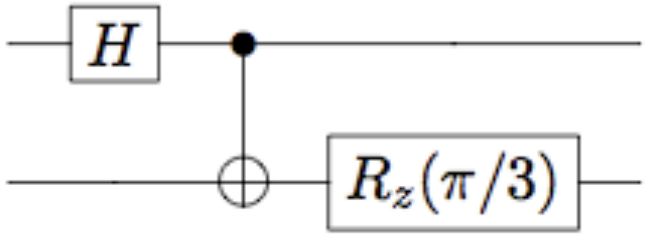
$$H \quad : \quad \begin{array}{lcl} |0\rangle & \mapsto & \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |1\rangle & \mapsto & \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{array}$$

$$R_z(\theta) \quad : \quad \begin{array}{lcl} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & e^{i\theta}|1\rangle \end{array}$$

$$CNot \quad : \quad \begin{array}{lcl} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$$

Exemple :
$CNot \circ (H \otimes I)(|00\rangle) =$

Circuits quantiques



$$(I \otimes R_z(\pi/3)) \circ CNot \circ (H \otimes I)$$

- $\{H, CNot, R_z(\theta), \theta \in [0, 2\pi)\}$ est une famille universelle de transformations unitaires.

- Toute transformation unitaire est *réversible*.

Circuits Classiques / Quantiques

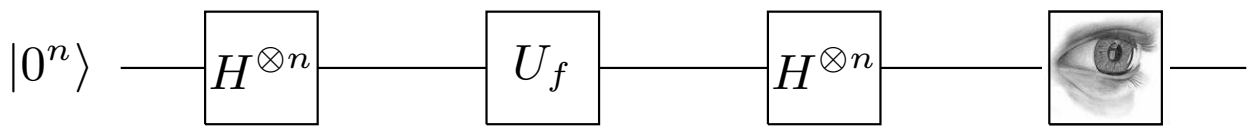
Lemme : Si $f : \{0,1\}^n \to \{0,1\}$ est calculée par un circuit classique de taille t alors son extension quantique $U_f : |x\rangle \mapsto (-1)^{f(x)} |x\rangle$ est calculée par un circuit quantique de taille $O(t)$.

Preuve : voir exercices 4 & 5.

Un 1er algorithme quantique

Umesh veut identifier les fausses pièces parmi un ensemble de n pièces. Il sait qu'une vraie pièce a une masse de 8g contre 7.5g pour une fausse. Umesh possède une balance dont l'écran défectueux n'indique que le chiffre après la virgule : 0 pour $8g$, 5 pour $22.5g$ etc. Ainsi Umesh ne peut connaître que la parité du nombre de fausses pièces posées sur le plateau de la balance. Combien de pesées Umesh doit effectuer pour identifier l'ensemble des fausses pièces ?

Donnée : $f : \{0,1\}^n \to \{0,1\}$ t.q. $\exists a \in \{0,1\}^n, f(x) = x \bullet a = \sum_{i=1}^{n} x_i a_i \bmod 2$.
Problème : Trouver $a \in \{0,1\}^n$.
Algorithme classique : n appels à f sont nécessaires et suffisants.
Algorithme quantique : 1 appel à U_f.



$$
\begin{aligned}
H^{\otimes n} U_f H^{\otimes n} \left|0^n\right\rangle &= \frac{1}{\sqrt{2^n}} H^{\otimes n} U_f \sum_{x \in \{0,1\}^n} \left|x\right\rangle && (1)\\
&= \frac{1}{\sqrt{2^n}} H^{\otimes n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \left|x\right\rangle && (2)\\
&= \frac{1}{\sqrt{2^n}} H^{\otimes n} \sum_{x \in \{0,1\}^n} (-1)^{x \bullet a} \left|x\right\rangle && (3)\\
&= H^{\otimes n} H^{\otimes n} \left|a\right\rangle && (4)\\
&= \left|a\right\rangle && (5)
\end{aligned}
$$