Découverte de l'informatique quantique

Vidéo ■ partie 1.1. Un qubit
Vidéo ■ partie 1.2. Portes quantiques
Vidéo ■ partie 1.3. Les 2-qubits (partie 1)
Vidéo ■ partie 1.3. Les 2-qubits (partie 2)
Vidéo ■ partie 1.4. Plus de qubits
Vidéo ■ partie 1.5. Communication par codage super-dense

Plongeons directement au cœur de l'informatique quantique en abordant la notion de qubit et les circuits quantiques fondamentaux.
Ce chapitre donne un aperçu des calculs avec les qubits et est une introduction détaillée des chapitres suivants dans lesquels plusieurs notions seront revues : nombres complexes, vecteurs, matrices, portes logiques, physique quantique. Ce chapitre se termine par une application assez difficile : le codage super-dense.

1. Un qubit

Pour un ordinateur classique l'unité d'information est le ***bit*** représenté soit par 0, soit par 1. Avec plusieurs bits on peut coder un entier, par exemple 19 est codé en binaire par 1.0.0.1.1 ; on peut aussi coder des caractères, par exemple le code ASCII de « A » est 1.0.0.0.0.0.1.

1.1. Un qubit est un vecteur

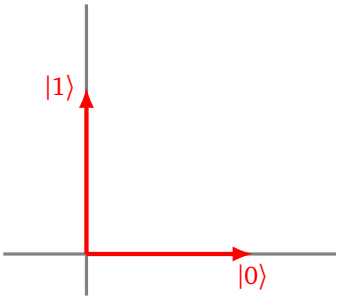
En informatique quantique on part aussi de deux ***états quantiques de base*** :

$$|0\rangle \qquad \text{et} \qquad |1\rangle\,.$$

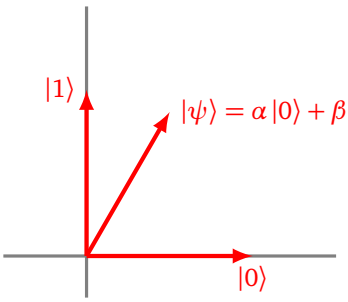
La notation est un peu bizarre (elle sera justifiée ultérieurement). En fait $|0\rangle$ et $|1\rangle$ sont deux vecteurs :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{et} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Ces deux vecteurs forment une base orthonormée du plan.



États quantiques de base



Un état quantique $|\psi\rangle$

Ce qui est nouveau et fondamental est que l'on peut ***superposer*** ces deux états $|0\rangle$ et $|1\rangle$. Un ***qubit*** est un ***état quantique*** obtenu par combinaison linéaire :

$$\boxed{|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle}$$

Ainsi, un qubit est représenté par un vecteur :

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}.$$

En effet :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}.$$

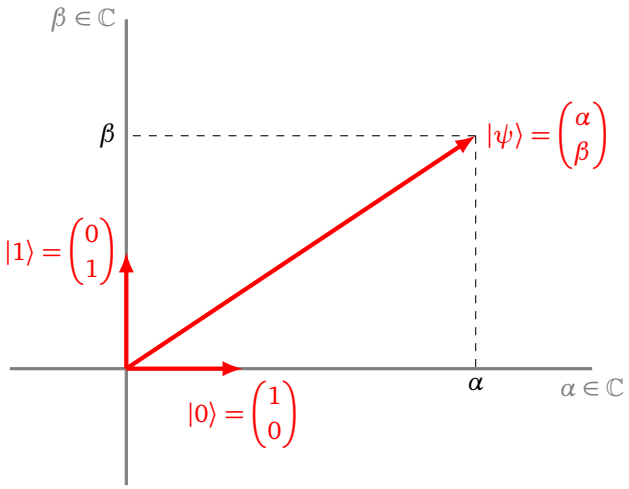
Vocabulaire.

- Les états $|0\rangle$ et $|1\rangle$ se lisent « ket zéro » et « ket un » (« ket » se prononce comme le mot « quête »).
- ψ est la lettre grecque « psi », ainsi $|\psi\rangle$ se lit « ket psi ».

Là où cela se complique un peu, c'est que les coefficients α et β ne sont pas des nombres réels mais des nombres complexes :

$$\boxed{\alpha \in \mathbb{C} \quad \text{et} \quad \beta \in \mathbb{C}}$$

Ainsi $|\psi\rangle$ est un vecteur de $\mathbb{C}^2$, défini par ses deux coordonnées complexes α et β.



Sur la figure ci-dessus, on a représenté un vecteur à coordonnées complexes comme un vecteur du plan. Cette figure aide à la compréhension mais ne correspond pas tout à fait à la réalité. Comme chacun des axes correspond à une coordonnée complexe (de dimension 2), un dessin réaliste nécessiterait quatre dimensions.
‘

Exemple.

- $|\psi\rangle = (3+4\mathrm{i})\,|0\rangle + (2-8\mathrm{i})\,|1\rangle$. On rappelle que i est le nombre complexe tel que $\mathrm{i}^2 = -1$.
- $|\psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{\mathrm{i}}{\sqrt{2}}\,|1\rangle$.
- On peut superposer des états par addition, par exemple :

  $$\big(2\,|0\rangle + (1+\mathrm{i})\,|1\rangle\big) + \big(\mathrm{i}\,|0\rangle + (2-3\mathrm{i})\,|1\rangle\big) = (2+\mathrm{i})\,|0\rangle + (3-2\mathrm{i})\,|1\rangle\,,$$

  ce qui correspond à additionner deux vecteurs :

  $$\begin{pmatrix}2\\1+\mathrm{i}\end{pmatrix} + \begin{pmatrix}\mathrm{i}\\2-3\mathrm{i}\end{pmatrix} = \begin{pmatrix}2+\mathrm{i}\\3-2\mathrm{i}\end{pmatrix}.$$

Remarque.

- Si on souhaitait définir $|\psi\rangle$ uniquement avec des nombres réels, alors on pourrait écrire $\alpha = \alpha_1 + i\alpha_2$, $\beta = \beta_1 + i\beta_2$ et dire qu'un état quantique est défini par 4 nombres réels α_1, α_2, β_1, β_2. Cependant ce n'est pas le bon état d'esprit pour la suite.
- Attention $|0\rangle$ n'est pas le vecteur nul $\binom{0}{0}$, mais bien le vecteur $\binom{1}{0}$.

1.2. Norme

États de norme 1. On va principalement considérer les états $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ dont la ***norme est égale à 1***, c'est-à-dire :

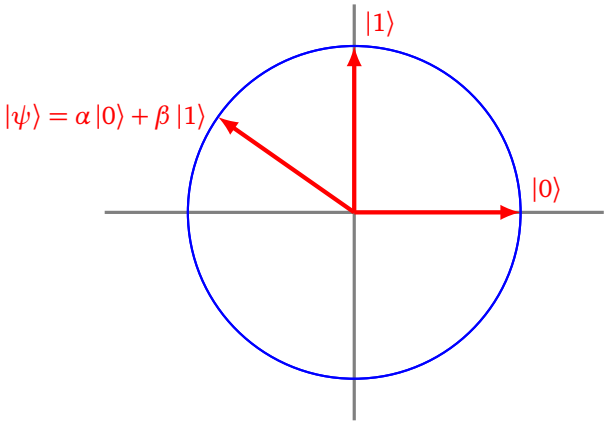
$$\boxed{|\alpha|^2 + |\beta|^2 = 1}$$

où $|\alpha|$ et $|\beta|$ sont les modules des coefficients complexes. On rappelle que si $z = a + ib$ est un nombre complexe (avec $a, b \in \mathbb{R}$), alors son ***module*** $|z|$ est le nombre réel positif défini par $|z|^2 = a^2 + b^2$.

Exemple.

- $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.
  Alors
  $$|\alpha|^2 + |\beta|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = 1.$$
  Ainsi cet état $|\psi\rangle$ est bien de norme 1.
- $|\psi\rangle = (3+4i)|0\rangle + (2-8i)|1\rangle$.
  $$|\alpha|^2 + |\beta|^2 = |3+4i|^2 + |2-8i|^2 = 25 + 68 = 93.$$
  Ainsi la norme de $|\psi\rangle$ est $\sqrt{|\alpha|^2 + |\beta|^2} = \sqrt{93}$ et n'est pas égale à 1. En divisant par la norme, on transforme facilement $|\psi\rangle$ en un état $|\psi'\rangle$ de norme 1 :
  $$|\psi'\rangle = \frac{3+4i}{\sqrt{93}}|0\rangle + \frac{2-8i}{\sqrt{93}}|1\rangle.$$

Remarque.
On peut schématiser de façon imparfaite les états de norme 1 par le dessin du cercle ci-dessous.



Cependant ceci est un dessin où l'on considère que les coefficients α et β sont des nombres réels, ce qui n'est pas le cas en général. La « sphère de Bloch » fournira une représentation plus fidèle, voir le chapitre « Nombres complexes ».

1.3. Mesure et probabilités

Un des aspects fondamentaux mais troublants de la physique quantique est que l'on ne peut pas mesurer les coefficients α et β de l'état quantique $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Partons d'un état quantique de norme 1 :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{avec} \quad |\alpha|^2 + |\beta|^2 = 1.$$

La ***mesure*** de l'état quantique $|\psi\rangle$ va renvoyer l'un des bits classiques 0 ou 1 :

- 0 avec une probabilité $|\alpha|^2$
- 1 avec une probabilité $|\beta|^2$

Noter que, comme nous sommes partis d'un état de norme 1, nous avons bien la somme des probabilités $|\alpha|^2 + |\beta|^2$ qui vaut 1.

Exemple.
Considérons l'état quantique :

$$|\psi\rangle = \frac{1-\mathrm{i}}{\sqrt{3}}|0\rangle + \frac{1+2\mathrm{i}}{\sqrt{15}}|1\rangle.$$

Alors

$$|\alpha|^2 = \left|\frac{1-\mathrm{i}}{\sqrt{3}}\right|^2 = \frac{2}{3}$$

et

$$|\beta|^2 = \left|\frac{1+2\mathrm{i}}{\sqrt{15}}\right|^2 = \frac{5}{15} = \frac{1}{3}.$$

On a bien $|\alpha|^2 + |\beta|^2 = 1$. Si on mesure $|\psi\rangle$ alors on obtient 0 avec une probabilité $\frac{2}{3}$ et 1 avec une probabilité $\frac{1}{3}$.
Autrement dit, si je peux répéter 100 fois l'expérience « je prépare l'état initial $|\psi\rangle$, puis je le mesure », alors pour environ 66 cas sur 100 j'obtiendrai pour mesure 0 et pour environ 33 cas sur 100 j'obtiendrai 1.

La mesure d'un état quantique $|\psi\rangle$ le perturbe de façon irrémédiable. C'est un phénomène physique appelé « réduction du paquet d'onde ». Si la mesure a donné le bit 0, alors l'état $|\psi\rangle$ est devenu $|0\rangle$, si la mesure a donné le bit 1 alors $|\psi\rangle$ est devenu $|1\rangle$. Autrement dit, une fois qu'il est mesuré, un qubit ne sert plus à grand chose !

Remarque.
Bien évidemment la mesure de $|0\rangle$ donne 0 avec une probabilité 1 (l'événement est presque sûr). De même la mesure de $|1\rangle$ donne 1 avec une probabilité 1. Dans ce cours nous faisons le choix qu'une mesure renvoie un bit classique 0 ou 1. Une autre convention serait de décider qu'une mesure renvoie un des états de base $|0\rangle$ ou $|1\rangle$.

Bilan. On retient qu'à partir d'un état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec $\alpha, \beta \in \mathbb{C}$ tels que $|\alpha|^2 + |\beta|^2 = 1$:

- on ne peut pas mesurer les coefficients α et β ;
- la mesure de $|\psi\rangle$ renvoie soit 0 avec une probabilité $|\alpha|^2$, soit 1 avec une probabilité $|\beta|^2$;
- la mesure transforme le qubit $|\psi\rangle$ en $|0\rangle$ ou en $|1\rangle$, les coefficients α et β ont disparu après mesure.

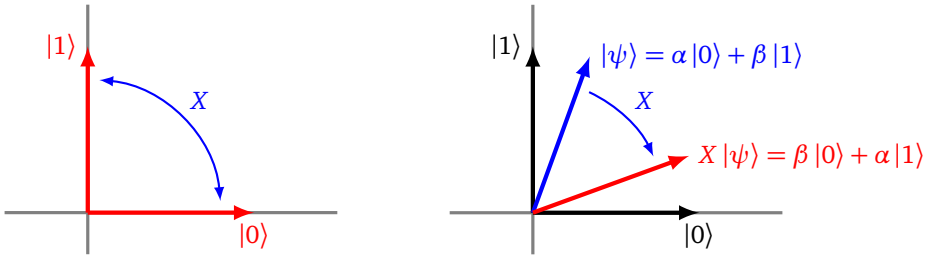
2. Porte avec une entrée

Un ordinateur quantique produit des qubits et leur applique des transformations, qui dans un circuit s'appellent des « portes ». Nous commençons par transformer un seul qubit.

2.1. Porte X

La porte X s'appelle aussi porte NON (ou NOT) et est la transformation qui échange les deux états quantiques de base :

$$|0\rangle \xmapsto{X} |1\rangle \quad \text{et} \quad |1\rangle \xmapsto{X} |0\rangle$$



Porte X

La transformation est de plus linéaire, ce qui fait que la porte X échange les deux coefficients d'un état quantique :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xmapsto{X} \beta|0\rangle + \alpha|1\rangle\,.$$

Par exemple l'état $|\psi\rangle = 2|0\rangle + (1-\mathrm{i})|1\rangle$ est transformé par la porte X en l'état $X(|\psi\rangle) = (1-\mathrm{i})|0\rangle + 2|1\rangle$.
En termes de vecteurs cette transformation s'écrit :

$$\begin{pmatrix}1\\0\end{pmatrix} \xmapsto{X} \begin{pmatrix}0\\1\end{pmatrix} \qquad \begin{pmatrix}0\\1\end{pmatrix} \xmapsto{X} \begin{pmatrix}1\\0\end{pmatrix} \qquad \begin{pmatrix}\alpha\\\beta\end{pmatrix} \xmapsto{X} \begin{pmatrix}\beta\\\alpha\end{pmatrix}$$

La matrice de la porte X est donc :

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

car

$$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\beta\\\alpha\end{pmatrix}.$$

Note. La notion de matrice n'est pas indispensable pour ce premier chapitre, elle sera développée dans le chapitre « Vecteurs et matrices ».

2.2. Porte H de Hadamard

La porte H de Hadamard est la transformation linéaire définie par :

$$|0\rangle \xmapsto{H} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \qquad \text{et} \qquad |1\rangle \xmapsto{H} \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

Ainsi, si $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ alors

$$H(|\psi\rangle) = \alpha\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) + \beta\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big).$$

On regroupe les coefficients selon les termes $|0\rangle$ et $|1\rangle$, pour obtenir :

$$H(|\psi\rangle) = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle\,.$$

Par exemple l'état $|\psi\rangle = \mathrm{i}|0\rangle + (2+\mathrm{i})|1\rangle$ est transformé en $H(|\psi\rangle) = \frac{2+2\mathrm{i}}{\sqrt{2}}|0\rangle - \frac{2}{\sqrt{2}}|1\rangle$.

En termes de vecteurs cette transformation s'écrit sur les vecteurs de base :

$$\begin{pmatrix}1\\0\end{pmatrix} \xmapsto{H} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad \begin{pmatrix}0\\1\end{pmatrix} \xmapsto{H} \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

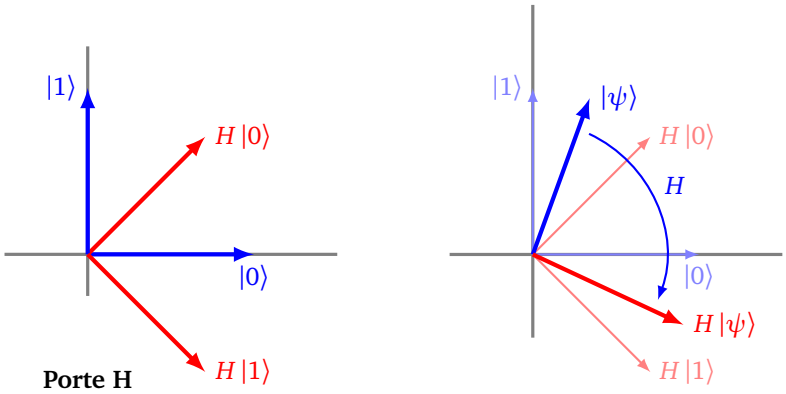
La matrice de la porte H est donc :

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

car la multiplication

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

redonne bien le vecteur correspondant à $H(|\psi\rangle)$.
Géométriquement la base $(|0\rangle, |1\rangle)$ est transformée en une autre base orthonormée $(H(|0\rangle), H(|1\rangle))$.



Porte H

Remarque. Il est fréquent de rencontrer les notations suivantes :

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

même si nous éviterons de les utiliser ici.

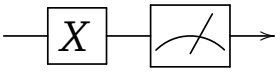
2.3. Mesure

C'est un élément fondamental d'un circuit quantique. C'est le seul moment où l'on peut obtenir une information sur un état quantique $|\psi\rangle$, mais c'est aussi la fin du qubit, car la mesure ne renvoie que 0 ou 1 et perturbe irrémédiablement l'état quantique.

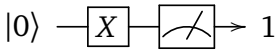
2.4. Exemples de circuit

Un ***circuit*** est composé d'une succession de portes. Il se lit de gauche à droite.

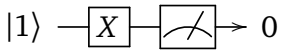
Exemple.
Voici un circuit composé d'une porte X (c'est-à-dire une porte NON) suivie d'une porte mesure symbolisée par un petit cadran.



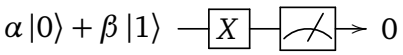
- Si l'entrée est $|0\rangle$, alors $X(|0\rangle) = |1\rangle$, la sortie mesurée vaut donc 1 (avec une probabilité 1) :



- Par contre si l'entrée est $|1\rangle$, alors $X(|1\rangle) = |0\rangle$ et la sortie mesurée vaut 0 :

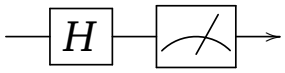


- Si l'entrée est l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (avec $|\alpha|^2 + |\beta|^2 = 1$), alors $X(|\psi\rangle) = \beta|0\rangle + \alpha|1\rangle$. La mesure donne donc 0 avec une probabilité $|\beta|^2$ et 1 avec une probabilité $|\alpha|^2$.



Exemple.

Ce circuit est formé d'une porte H de Hadamard, suivi d'une mesure :



- Si l'entrée est $|0\rangle$, alors $H(|0\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, la mesure donne donc le bit 0 avec une probabilité $\frac{1}{2}$ et le bit 1 avec une probabilité $\frac{1}{2}$.
- Si l'entrée est $|1\rangle$, alors $H(|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ et les mesures conduisent aux mêmes résultats que précédemment.
- Par contre si l'entrée est $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, alors :

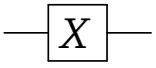
$$\begin{aligned} H(|\psi\rangle) &= H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}H(|0\rangle) + \frac{1}{\sqrt{2}}H(|1\rangle) \\ &= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{2}|0\rangle + \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle - \frac{1}{2}|1\rangle \\ &= |0\rangle \end{aligned}$$

  Ainsi pour cette entrée, le circuit renvoie, après mesure, 0 avec une quasi-certitude.
- Exercice : trouver $|\psi\rangle$ tel que la mesure donne 1 avec une quasi-certitude.

2.5. Portes X, Y et Z de Pauli

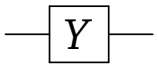
Nous avons déjà rencontré la porte X (dite aussi porte NOT), qui fait partie d'une famille de trois portes, dites ***portes de Pauli***. Les voici définies par leur action sur les états quantiques de base $|0\rangle$ et $|1\rangle$, et également par leur matrice.

Porte X



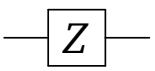
$$\begin{cases} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{cases} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Porte Y



$$\begin{cases} |0\rangle \mapsto \mathrm{i}|1\rangle \\ |1\rangle \mapsto -\mathrm{i}|0\rangle \end{cases} \qquad Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$$

Porte Z



$$\begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{cases} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Exercice.
On considère la porte $\sqrt{NOT}$ définie par

$$\left\{\begin{array}{l} |0\rangle \mapsto \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \\ |1\rangle \mapsto \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \end{array}\right. \quad \text{c'est-à-dire} \quad M = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

1. Pour l'entrée $|0\rangle$, que donne une mesure après la porte $\sqrt{NOT}$? Même question avec $|1\rangle$.

$$|0\rangle \text{ — } \boxed{\sqrt{NOT}} \text{ — } \nearrow \text{ ?} \qquad |1\rangle \text{ — } \boxed{\sqrt{NOT}} \text{ — } \nearrow \text{ ?}$$

2. Pour l'entrée $|\psi\rangle = \frac{1}{2}|0\rangle + i\frac{\sqrt{3}}{2}|1\rangle$, que donne la sortie après la porte $\sqrt{NOT}$? Que donne ensuite une mesure ?

$$|\psi\rangle \text{ — } \boxed{\sqrt{NOT}} \text{ ?} \qquad |\psi\rangle \text{ — } \boxed{\sqrt{NOT}} \text{ — } \nearrow \text{ ?}$$

3. Montrer que le circuit suivant, qui consiste à enchaîner deux portes $\sqrt{NOT}$, équivaut à une seule porte NOT (notée aussi porte X).

$$\text{— } \boxed{\sqrt{NOT}} \text{ — } \boxed{\sqrt{NOT}} \text{ — } \quad = \quad \text{— } \boxed{NOT} \text{ —}$$

Autrement dit, il s'agit de montrer que :

$$\sqrt{NOT}\big(\sqrt{NOT}(|\psi\rangle)\big) = NOT(|\psi\rangle)$$

Indication. On peut faire les calculs avec un qubit général $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Mais on peut aussi seulement vérifier que cette affirmation est vraie pour les deux états de bases $|0\rangle$ et $|1\rangle$, ce qui est suffisant par linéarité. Une autre technique serait d'utiliser les matrices.

3. Les 2-qubits

Nous allons maintenant réunir deux qubits pour obtenir un 2-qubit. C'est la version quantique de l'union de deux bits.

3.1. Superposition

Deux qubits réunis sont dans un état quantique $|\psi\rangle$, appelé *2-qubit*, défini par la superposition :

$$\boxed{|\psi\rangle = \alpha|0.0\rangle + \beta|0.1\rangle + \gamma|1.0\rangle + \delta|1.1\rangle}$$

où $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, avec souvent la convention de normalisation :

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

La mesure d'un 2-qubit, donne deux bits classiques :

- 0.0 avec probabilité $|\alpha|^2$,
- 0.1 avec probabilité $|\beta|^2$,
- 1.0 avec probabilité $|\gamma|^2$,
- 1.1 avec probabilité $|\delta|^2$.

Notons déjà la différence remarquable avec l'informatique classique : avec deux bits classiques, on encode un seul des quatre états 0.0, 0.1, 1.0 ou 1.1, mais avec un 2-qubit on encode en quelque sorte les quatre états en même temps !
Que représentent $|0.0\rangle$, $|0.1\rangle$,… ? Il s'agit de nouveaux vecteurs d'une base mais cette fois en dimension 4 :

$$|0.0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |0.1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad |1.0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |1.1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Ainsi $|\psi\rangle$ est un vecteur de $\mathbb{C}^4$:

$$|\psi\rangle = \alpha \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \delta \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}.$$

Exemple.

$$|\psi\rangle = \frac{1}{\sqrt{6}}|0.0\rangle + \frac{\mathrm{i}}{\sqrt{6}}|1.0\rangle + \frac{1+\mathrm{i}}{\sqrt{3}}|1.1\rangle$$

est un 2-qubit de norme 1. Sa mesure donne :

- 0.0 avec probabilité $1/6$,
- 0.1 avec probabilité 0,
- 1.0 avec probabilité $1/6$,
- 1.1 avec probabilité $2/3$.

On peut aussi noter les états de base par des formules de multiplications :

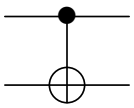
$$|0.0\rangle = |0\rangle \cdot |0\rangle \qquad |0.1\rangle = |0\rangle \cdot |1\rangle \qquad |1.0\rangle = |1\rangle \cdot |0\rangle \qquad |1.1\rangle = |1\rangle \cdot |1\rangle$$

On note aussi ce produit par le symbole $\otimes$:

$$|0.1\rangle = |0\rangle \otimes |1\rangle = \begin{matrix} |0\rangle \\ \otimes \\ |1\rangle \end{matrix}$$

3.2. Porte CNOT

La porte $CNOT$ est une porte qui prend en entrée deux qubits et renvoie deux qubits en sortie.



Voici la règle sur les quatre états quantiques de bases :

Autrement dit le premier qubit reste inchangé. C'est différent pour le second qubit :

- si le premier qubit est $|0\rangle$ alors le second qubit est inchangé,
- si le premier qubit est $|1\rangle$ alors le second qubit est changé selon la règle d'une porte X : $|0\rangle \mapsto |1\rangle$ et $|1\rangle \mapsto |0\rangle$.

On peut interpréter cette porte comme une instruction « si …, sinon … » : si le premier qubit est $|0\rangle$ faire ceci, sinon faire cela.

Voici la règle reformulée avec la notation des 2-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 cette même règle présentée à l'aide de vecteurs :

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

La matrice de la transformation de $CNOT$ est donc la matrice 4×4 :

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

La porte $CNOT$ transforme un vecteur représentant un 2-qubit par multiplication par cette matrice M :

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} \longmapsto^{CNOT} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{pmatrix}.$$

3.3. L'état de Bell

À l'aide de la porte $CNOT$ nous allons obtenir un des états les plus importants pour deux qubits : l'***état de Bell*** :

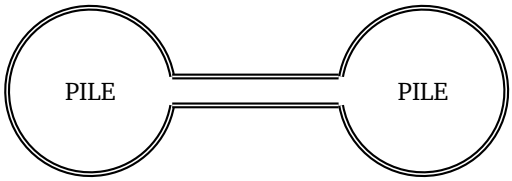
$$\boxed{\left|\Phi^+\right\rangle = \tfrac{1}{\sqrt{2}}\left|0.0\right\rangle + \tfrac{1}{\sqrt{2}}\left|1.1\right\rangle}$$

Une mesure de cet état conduit à :

- 0.0 avec une probabilité $\frac{1}{2}$,
- 1.1 avec une probabilité $\frac{1}{2}$,
- les deux autres sorties 0.1 et 1.0 ayant une probabilité nulle.

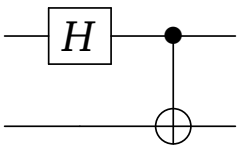
Remarque.
En physique quantique il est toujours aventureux de faire des analogies avec le monde tel qu'on le connaît. Permettons-nous un petit écart :

- Un qubit, c'est un peu comme une pièce de monnaie lancée en l'air. Tant que la pièce tourne dans l'air, « pile » et « face » ont les mêmes chances de se produire. Ce n'est que lorsque la pièce est retombée que l'on peut lire le résultat (c'est la partie « mesure ») et ensuite le résultat est définitivement figé à « pile » ou bien à « face ».
- Un 2-qubit, c'est-à-dire la réunion de deux qubits, c'est comme deux pièces de monnaie en train d'être lancées en l'air en même temps. Les quatre résultats « pile/pile », « pile/face », « face/pile » ou encore « face/face » sont possibles.
- L'état de Bell, c'est comme deux pièces liées entre elles lancées en l'air. Le résultat ne peut être que « pile/pile » ou bien « face/face ». Ce phénomène s'appelle « l'intrication quantique ».



Obtention de l'état de Bell.

Considérons le circuit suivant, composé d'une porte de Hadamard, suivie d'une porte $CNOT$:



Alors, à partir de l'entrée $|0.0\rangle$, l'état de Bell $\left|\Phi^+\right\rangle$ est obtenu en sortie.

$$\begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix} \quad \text{—}H\text{—}\bullet\text{—}\oplus\text{—} \quad \frac{1}{\sqrt{2}}\begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix} + \frac{1}{\sqrt{2}}\begin{matrix}|1\rangle\\ \otimes\\ |1\rangle\end{matrix}$$

Reprenons le calcul en détails (en adoptant la notation verticale) à partir de l'entrée

$$|0.0\rangle = \begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix}$$

Tout d'abord le premier qubit (celui du haut) passe par une porte H, le second qubit reste inchangé :

$$\begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix} \xmapsto{H} \begin{matrix}H(|0\rangle)\\ \otimes\\ |0\rangle\end{matrix} = \begin{matrix}\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\\ \otimes\\ |0\rangle\end{matrix} = \frac{1}{\sqrt{2}}\begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix} + \frac{1}{\sqrt{2}}\begin{matrix}|1\rangle\\ \otimes\\ |0\rangle\end{matrix}$$

Ensuite ce résultat intermédiaire passe par la porte $CNOT$. On regarde d'abord indépendamment les deux termes de la somme obtenue :

$$\begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix} \xmapsto{CNOT} \begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix} \quad \text{et} \quad \begin{matrix}|1\rangle\\ \otimes\\ |0\rangle\end{matrix} \xmapsto{CNOT} \begin{matrix}|1\rangle\\ \otimes\\ |1\rangle\end{matrix}$$

Ainsi par linéarité, la porte $CNOT$ a pour action :

$$\begin{matrix}H(|0\rangle)\\ \otimes\\ |0\rangle\end{matrix} \xmapsto{CNOT} \frac{1}{\sqrt{2}}\begin{matrix}|0\rangle\\ \otimes\\ |0\rangle\end{matrix} + \frac{1}{\sqrt{2}}\begin{matrix}|1\rangle\\ \otimes\\ |1\rangle\end{matrix}$$

qui est bien l'état de Bell $\left|\Phi^+\right\rangle$.

Exercice.
Reprenons le même circuit :

$$\text{—}H\text{—}\bullet\text{—}\oplus\text{—}$$

1. Quelle est la sortie produite pour l'entrée $|1.0\rangle$?
2. Trouver où insérer une porte X dans le circuit, de sorte que l'entrée $|0.0\rangle$ conduise à la sortie $\frac{1}{\sqrt{2}}|0.1\rangle + \frac{1}{\sqrt{2}}|1.0\rangle$.

3.4. Calculs algébriques avec un ou deux qubits

Il faut savoir faire des calculs algébriques avec les qubits, même si pour vraiment comprendre ces opérations il faudra attendre le produit tensoriel qui sera expliqué dans le chapitre « Vecteurs et matrices ».

Addition.
L'addition se fait coefficient par coefficient et ne pose pas de problème, par exemple si

$$|\phi\rangle = (1+3\mathrm{i})|0\rangle + 2\mathrm{i}\,|1\rangle \qquad \text{et} \qquad |\psi\rangle = 3\,|0\rangle + (1-\mathrm{i})\,|1\rangle$$

alors

$$|\phi\rangle + |\psi\rangle = (4+3\mathrm{i})\,|0\rangle + (1+\mathrm{i})\,|1\rangle\,.$$

Ou encore pour des 2-qubits :

$$\big(|1.0\rangle + |0.1\rangle\big) + \big(|1.0\rangle - |0.1\rangle\big) = 2\,|1.0\rangle\,.$$

Multiplication.
On peut multiplier deux 1-qubits pour obtenir un 2-qubit. Les calculs se font comme des calculs algébriques à l'aide des règles de bases $|0\rangle \cdot |0\rangle = |0.0\rangle$, $|0\rangle \cdot |1\rangle = |0.1\rangle$,…

Par exemple :

$$\begin{aligned}\big(3\,|0\rangle + 2\mathrm{i}\,|1\rangle\big)\cdot\big((1+\mathrm{i})\,|0\rangle - |1\rangle\big) = \;& 3(1+\mathrm{i})\,|0\rangle\cdot|0\rangle \;-\; 3\,|0\rangle\cdot|1\rangle \;+\; 2\mathrm{i}(1+\mathrm{i})\,|1\rangle\cdot|0\rangle \;-\; 2\mathrm{i}\,|1\rangle\cdot|1\rangle \\ = \;& (3+3\mathrm{i})\,|0.0\rangle \;-\; 3\,|0.1\rangle \;+\; (-2+2\mathrm{i})\,|1.0\rangle \;-\; 2\mathrm{i}\,|1.1\rangle\,.\end{aligned}$$

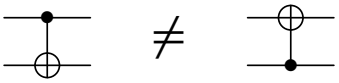
On a utilisé l'identité $\mathrm{i}^2 = -1$ et fait attention que la multiplication des « ket » n'est pas commutative : $|0\rangle\cdot|1\rangle \neq |1\rangle\cdot|0\rangle$. En particulier on a la relation $(k\,|a\rangle)\cdot|b\rangle = |a\rangle\cdot(k\,|b\rangle) = k\,|a.b\rangle$ pour $k\in\mathbb{C}$. Cette relation a été utilisée précédemment sans le dire pour la porte $CNOT$: $\left(\frac{1}{\sqrt{2}}\,|0\rangle\right)\cdot|0\rangle = \frac{1}{\sqrt{2}}\,|0.0\rangle$.
On a aussi la relation de développement/factorisation $|(a+b).c\rangle = |a.c\rangle + |b.c\rangle$. Par exemple : $|(0+1).1\rangle = |0.0\rangle + |0.1\rangle$.

Norme.

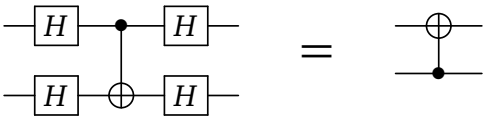
- Pour un nombre réel x, $|x|$ est sa valeur absolue.
- Pour un nombre complexe $z = a+\mathrm{i}b$, $|z| = \sqrt{a^2+b^2}$ est son module.
- Pour un qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, $\||\psi\|| = \sqrt{|\alpha|^2+|\beta|^2}$ est sa norme.
- Pour un 2-qubit $|\psi\rangle = \alpha\,|0.0\rangle + \beta\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle$, sa norme est $\||\psi\|| = \sqrt{|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2}$.
- La normalisation d'un qubit $|\psi\rangle$ est $\frac{|\psi\rangle}{\||\psi\|\|}$ qui est un qubit de norme 1.

Exercice.
Soit $|\phi\rangle = \frac{1}{\sqrt{3}}\,|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}\mathrm{i}\,|1\rangle$ et $|\psi\rangle = \frac{2+\mathrm{i}}{\sqrt{10}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle$. Calculer la norme de $|\phi\rangle$, $|\psi\rangle$, $|\phi\rangle + |\psi\rangle$ et $|\phi\rangle\cdot|\psi\rangle$.
Conclusion : on note que la somme de deux qubits de norme 1 n'est pas nécessairement de norme 1, par contre le produit de deux qubits de norme 1 est encore un qubit de norme 1.

Exercice.
Dans une porte $CNOT$ les deux entrées ne jouent pas des rôles symétriques.



Sur la figure à droite, est dessinée une porte $CNOT$ renversée pour laquelle c'est le premier qubit qui change (ou non) en fonction du second qubit.
Cependant on peut construire la porte $CNOT$ renversée à partir de la porte $CNOT$ classique et de quatre portes H de Hadamard.
Montrer que les circuits suivants sont équivalents :

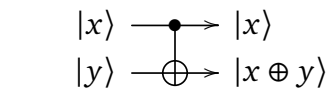


Indication. Il suffit de vérifier que l'affirmation est vraie pour les quatre états de base $|0.0\rangle$, $|0.1\rangle$, $|1.0\rangle$, $|1.1\rangle$.

La porte $CNOT$. Revisitons la porte $CNOT$ d'une manière un peu plus abstraite. La transformation associée à cette porte s'écrit aussi :

$$|x.y\rangle \xmapsto{\;CNOT\;} |x.y\oplus x\rangle$$

c'est-à-dire :



où x et y ont pour valeurs 0 ou 1 et où « $\oplus$ » représente l'addition usuelle sur un bit (comme une porte XOR) :

$$0\oplus 0 = 0 \qquad 1\oplus 0 = 1 \qquad 0\oplus 1 = 1 \quad \text{et} \quad 1\oplus 1 = 0.$$

Par exemple :

$$CNOT(|1.1\rangle) = |1.(1\oplus 1)\rangle = |1.0\rangle\,.$$

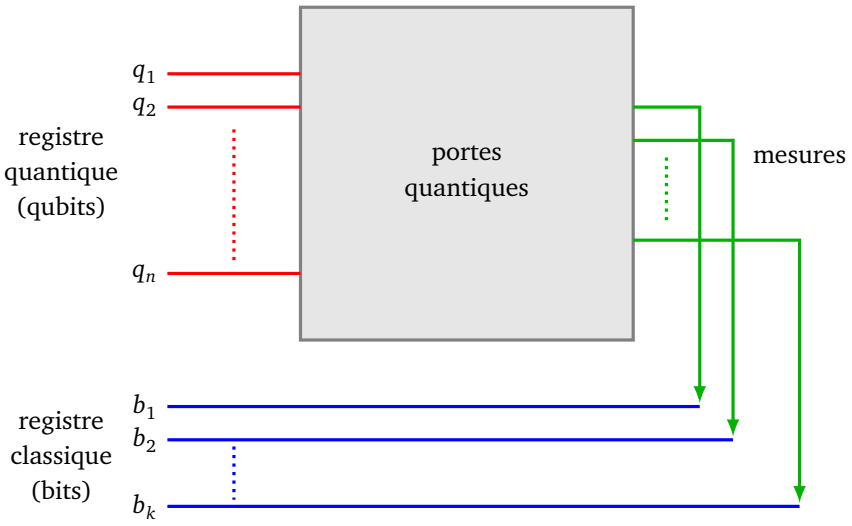
4. Plus de qubits

4.1. Circuit quantique

D'une façon générale, le regroupement de plusieurs qubits conduit à un « n-qubit ». Voici le schéma de principe d'un circuit quantique :

- en entrée : n qubits dont la superposition représente un n-qubit ;
- une succession de portes quantiques, chacune agissant sur un ou plusieurs qubits ;
- le circuit est terminé par un certain nombre de mesures, qui renvoient des bits classiques.

Circuit quantique



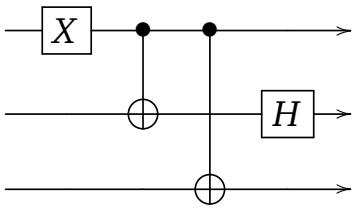
4.2. Les n-qubits

Un *n-qubit* est un état quantique :

$$|\psi\rangle = \alpha_0 |0.0\ldots0.0\rangle + \alpha_1 |0.0\ldots0.1\rangle + \cdots + \alpha_{2^n-1} |1.1\ldots1.1\rangle .$$

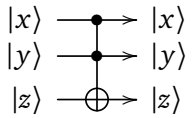
- Un n-qubit possède donc 2^n coefficients. C'est toute la puissance de l'informatique quantique : la réunion de n qubits conduit à la superposition de 2^n états de base. Travailler avec un n-qubit correspond à travailler sur tous les 2^n n-bits classiques $0.0\ldots0.0$, $0.0\ldots0.1$, …, $1.1\ldots1.1$ en même temps, alors que l'informatique classique ne s'occupe que d'un seul n-bit à la fois.
  Par exemple, l'écriture d'un 3-qubit est la superposition de 8-états de base :
  $$|\psi\rangle = \alpha_0 |0.0.0\rangle + \alpha_1 |0.0.1\rangle + \alpha_2 |0.1.0\rangle + \alpha_3 |0.1.1\rangle + \alpha_4 |1.0.0\rangle + \alpha_5 |1.0.1\rangle + \alpha_6 |1.1.0\rangle + \alpha_7 |1.1.1\rangle .$$
- Un n-qubit correspond donc au vecteur :
  $$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^n-1} \end{pmatrix} \in \mathbb{C}^{2^n}$$
- On impose souvent la condition de normalisation $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$.
- La mesure d'un n-qubit de norme 1 produit un n-bit classique : $0.0\ldots0.0$ avec la probabilité $|\alpha_0|^2$, $0.0\ldots0.1$ avec la probabilité $|\alpha_1|^2$,…, $1.1\ldots1.1$ avec la probabilité $|\alpha_{2^n-1}|^2$.

Exercice.
Voici un exemple de circuit avec 3 qubits en entrée.

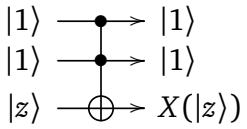


Pour chacune des entrées, correspondant à un état de base $|0.0.0\rangle$, $|0.0.1\rangle$,…,$|1.1.1\rangle$, calculer la sortie produite.
Exemple. Pour $|0.0.0\rangle$ la sortie est $\frac{1}{\sqrt{2}}|1.0.1\rangle - \frac{1}{\sqrt{2}}|1.1.1\rangle$.

Exercice.
La ***porte de Toffoli*** est un exemple de porte qui nécessite 3 qubits en entrée. Si l'état des deux premiers qubits est $|1\rangle$ alors la porte échange $|0\rangle$ et $|1\rangle$ pour le troisième qubit, sinon elle conserve le troisième qubit. C'est une généralisation de la porte $CNOT$ qui se note aussi $CCNOT$. Autrement dit, si $(x, y) \neq (1, 1)$ alors :



Mais pour le cas particulier $x = 1$ et $y = 1$:



On suppose que les qubits en entrée sont :

- $|\psi_1\rangle = |0\rangle + |1\rangle$
- $|\psi_2\rangle = |0\rangle + 2i\,|1\rangle$
- $|\psi_3\rangle = 2\,|0\rangle - 3\,|1\rangle$

Calculer les trois qubits de sortie.
Indication. On pourra commencer en développant $|\psi_1\rangle \cdot |\psi_2\rangle \cdot |\psi_3\rangle$ (voir la section 3.4).
Note. La matrice associée à la porte de Toffoli est la matrice 8×8 suivante :

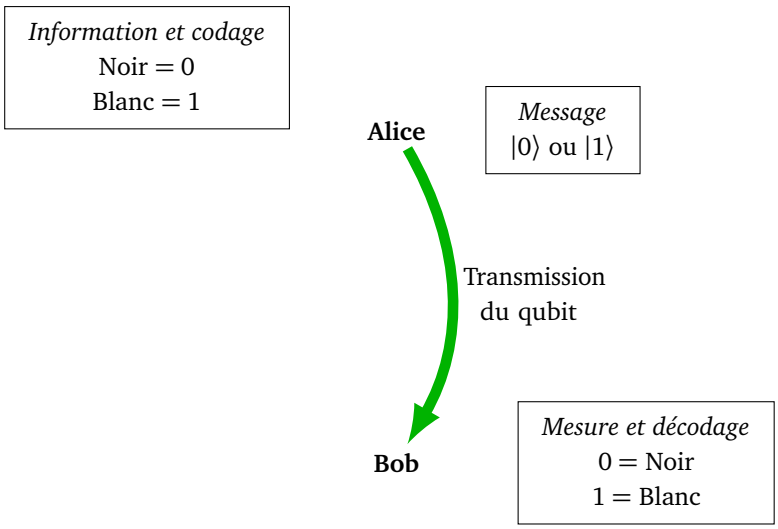
$$M = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0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

5. Communication par codage super-dense

Le codage super-dense est un protocole quantique permettant à deux personnes d'échanger de l'information.

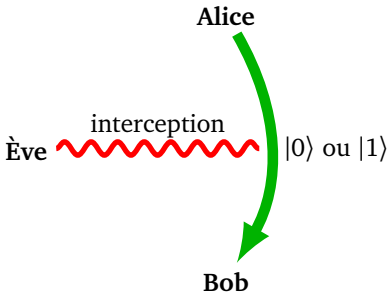
5.1. Motivation

On commence par une situation très simple.
Transmission. Alice souhaite envoyer un message à Bob, par exemple « Noir » codé par 0 ou « Blanc » codé par 1. Elle peut envoyer le qubit $|0\rangle$ à Bob qui le mesure, obtient 0 et sait donc que le message est « Noir ». Si Alice envoie le qubit $|1\rangle$ à Bob, sa mesure donne 1 et le message est « Blanc ».

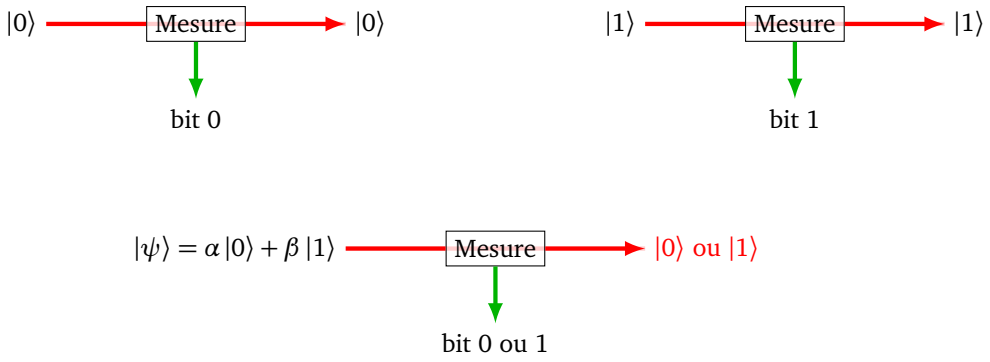


Avec cette technique, un seul bit classique d'information est transmis pour chaque qubit envoyé. Ne pourrait-on pas mieux faire ?

Interception. De plus cette technique n'est pas sûre, si l'espionne Ève intercepte le qubit transmis, alors elle peut mesurer le qubit sans changer son état. Elle récupère l'information et Bob ne s'aperçoit de rien !



En effet, mesurer le qubit $|0\rangle$ donne 0 mais ne change pas son état, idem pour le qubit $|1\rangle$. Ce ne serait pas le cas pour les autres états. Lorsque, par exemple, le qubit $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ est mesuré en 0 ou 1 (une chance sur deux), il change d'état en $|0\rangle$ ou en $|1\rangle$.

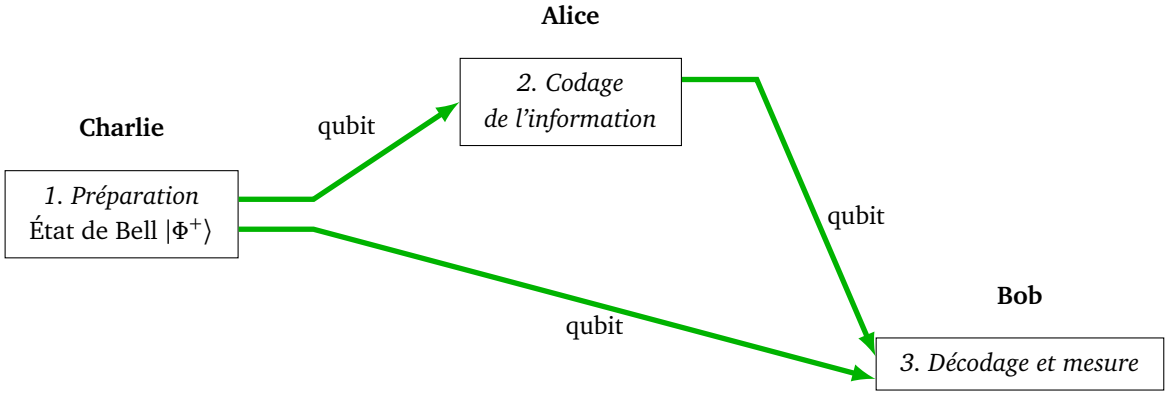


Note. Alice, Bob et Ève (pour *eavesdropper*, espionne) sont les noms habituels utilisés en cryptographie !

5.2. Schéma général du protocole

Le reste de la section est consacré au protocole appelé « codage super-dense ». Alice souhaite transmettre de façon sécurisée à Bob une information constituée de deux bits classiques, en envoyant un seul qubit.
Voici les trois étapes de ce protocole :

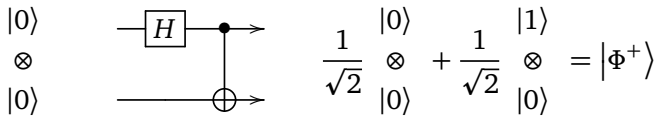
1. préparation de l'état de Bell,
2. codage de l'information par Alice,
3. décodage par Bob.



5.3. Préparation de l'état de Bell

Le protocole commence par un travail de préparation externe : une troisième personne, Charlie, prépare l'état de Bell.
C'est très facile : partant de l'état quantique $|0.0\rangle$, l'action d'une porte H suivi d'une porte $CNOT$ conduit à l'état de Bell :

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}|0.0\rangle + \frac{1}{\sqrt{2}}|1.1\rangle\,.$$



Les calculs ont été expliqués dans la section 3.3, les voici refaits rapidement :

$$|0.0\rangle \xmapsto{H} \left|\tfrac{1}{\sqrt{2}}(0+1).0\right\rangle = \tfrac{1}{\sqrt{2}}(|0.0\rangle + |1.0\rangle) \xmapsto{CNOT} \tfrac{1}{\sqrt{2}}(|0.0\rangle + |1.1\rangle)$$

Pour clarifier l'exposé et distinguer ce qui est à destination d'Alice et ce qui est à destination de Bob, on note l'état de Bell sous la forme :

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}|0_A.0_B\rangle + \frac{1}{\sqrt{2}}|1_A.1_B\rangle\,.$$

Ensuite Charlie envoie :

- un premier qubit $|\psi_A\rangle = \frac{1}{\sqrt{2}}|0_A\rangle + \frac{1}{\sqrt{2}}|1_A\rangle$ à Alice,
- un second qubit $|\psi_B\rangle = \frac{1}{\sqrt{2}}|0_B\rangle + \frac{1}{\sqrt{2}}|1_B\rangle$ à Bob.

Intrication quantique. Attention ces deux qubits $|\psi_A\rangle$ et $|\psi_B\rangle$ sont ***intriqués***, c'est-à-dire liés entre eux, même une fois séparés. Si on mesure $|\psi_A\rangle$ et que l'on obtient 0, alors la mesure de $|\psi_B\rangle$ donne aussi 0 et, bien entendu, si la mesure de $|\psi_A\rangle$ donne 1 alors la mesure de $|\psi_B\rangle$ donne aussi 1.
Cela s'explique par le fait que ces deux qubits sont issus de l'état de Bell, qui lors de sa mesure ne peut conduire qu'à 0.0 ou 1.1. L'intrication quantique est un des aspects les plus troublants de la mécanique quantique. Deux particules intriquées, même distantes, continuent de partager des propriétés communes.

5.4. Transformation d'Alice

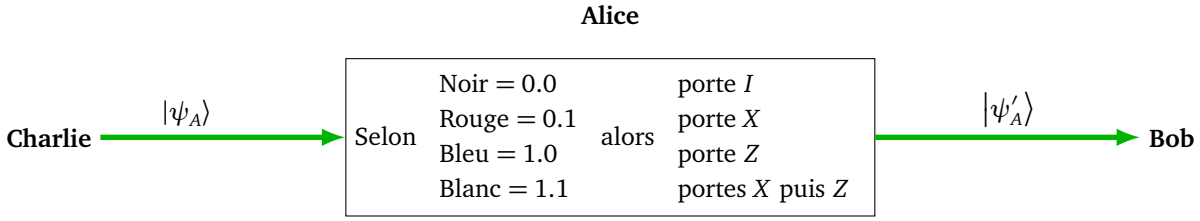
Alice souhaite envoyer un des quatre messages suivants à Bob, codés chacun par une couleur ou deux bits classiques.

- « Noir » ou 0.0,
- « Rouge » ou 0.1,
- « Bleu » ou 1.0,
- « Blanc » ou 1.1.

Elle reçoit de Charlie le qubit $|\psi_A\rangle = \frac{1}{\sqrt{2}}|0_A\rangle + \frac{1}{\sqrt{2}}|1_A\rangle$ et lui applique une des quatre transformations en fonction de l'information qu'elle souhaite transmettre :

- Si elle veut transmettre l'information « Noir/0.0 » elle applique l'identité I (elle ne fait rien et conserve $|\psi_A\rangle$).
- Si elle veut transmettre « Rouge/0.1 », elle applique la porte X à $|\psi_A\rangle$.
- Si elle veut transmettre « Bleu/1.0 », elle applique la porte Z à $|\psi_A\rangle$.
- Si elle veut transmettre « Blanc/1.1 », elle applique la porte X, suivie de la porte Z à $|\psi_A\rangle$.

Ensuite elle transmet le qubit transformé $|\psi'_A\rangle$ à Bob.

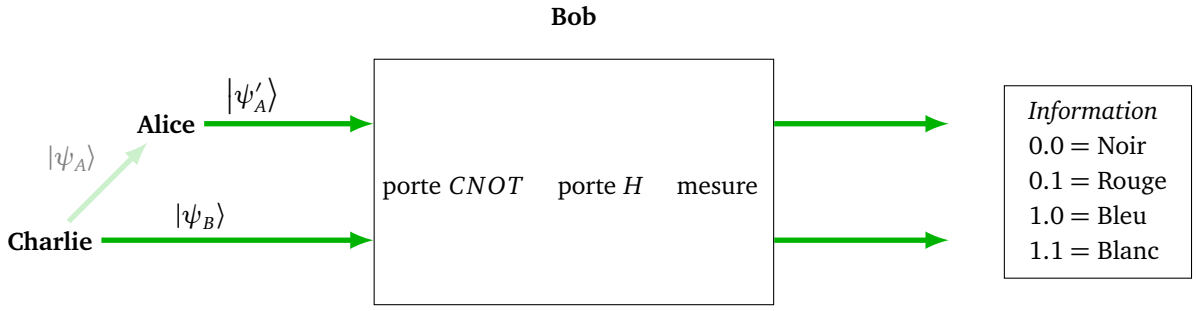


5.5. Décodage de Bob

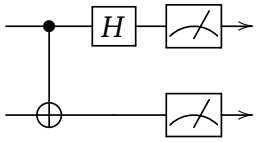
Bob reçoit deux qubits :

- le qubit transformé $|\psi'_A\rangle$ envoyé par Alice,
- le qubit $|\psi_B\rangle = \frac{1}{\sqrt{2}}|0_B\rangle + \frac{1}{\sqrt{2}}|1_B\rangle$ préparé par Charlie.

Mais attention, ces deux qubits sont toujours liés par intrication.
Bob a suffisamment d'informations pour retrouver le message d'Alice. Dans la pratique, il applique une porte $CNOT$ suivi d'une porte H (c'est l'opération inverse de la préparation de Charlie). Puis Bob mesure les deux qubits. Nous allons vérifier que la mesure redonne exactement l'information que voulait transmettre Alice : 0.0, 0.1, 1.0, 1.1 (pour Noir, Rouge, Bleu, Blanc).



Voici le circuit quantique du décodage de Bob :



On reprend pour chaque cas le codage d'Alice et le décodage de Bob. Ainsi Alice reçoit le qubit $|\psi_A\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$. Elle applique ensuite une transformation.

Cas de « Noir/0.0 ». Dans ce cas Alice ne fait rien (porte identité I sur le premier qubit), elle envoie donc directement $|\psi_A\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$ à Bob. Bob reçoit aussi $|\psi_B\rangle = \frac{1}{\sqrt{2}}(|0_B\rangle + |1_B\rangle)$ de Charlie. Mais n'oublions pas que ces deux qubits sont intriqués. Ainsi Bob a en main le 2-qubit $\frac{1}{\sqrt{2}}(|0_A.0_B\rangle + |1_A.1_B\rangle)$. Il applique ensuite une porte $CNOT$:

$$\frac{1}{\sqrt{2}}(|0_A.0_B\rangle + |1_A.1_B\rangle) \xmapsto{CNOT} CNOT(\tfrac{1}{\sqrt{2}}|0_A.0_B\rangle) + CNOT(\tfrac{1}{\sqrt{2}}|1_A.1_B\rangle) = \tfrac{1}{\sqrt{2}}|0_A.0_B\rangle + \tfrac{1}{\sqrt{2}}|1_A.0_B\rangle\,.$$

Bob continue et applique une porte H sur le premier qubit (indexé par A) :

$$\xmapsto{H_A} \frac{1}{\sqrt{2}}\left|\frac{1}{\sqrt{2}}(0_A + 1_A).0_B\right\rangle + \frac{1}{\sqrt{2}}\left|\frac{1}{\sqrt{2}}(0_A - 1_A).0_B\right\rangle = \frac{1}{2}(|0_A.0_B\rangle + |1_A.0_B\rangle + |0_A.0_B\rangle - |1_A.0_B\rangle) = |0_A.0_B\rangle\,.$$

Il ne reste plus que la mesure qui donne bien évidemment 0.0, ce qui est exactement le message d'Alice.

Cas de « Rouge/0.1 ». Alice applique la porte X au premier qubit de l'état de Bell, elle transforme son qubit $\frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$ en $\frac{1}{\sqrt{2}}(|1_A\rangle + |0_A\rangle)$. Mais pour l'état de Bell $\frac{1}{\sqrt{2}}(|0_A.0_B\rangle + |1_A.1_B\rangle)$ initial, cette transformation correspond au nouvel état $\frac{1}{\sqrt{2}}(|1_A.0_B\rangle + |0_A.1_B\rangle)$. Ainsi Bob reçoit le 2-qubit $|\psi\rangle = \frac{1}{\sqrt{2}}(|1_A.0_B\rangle + |0_A.1_B\rangle)$. Bob applique une porte $CNOT$, suivie d'une porte H sur le premier qubit :

$$\begin{aligned}\tfrac{1}{\sqrt{2}}(|1_A.0_B\rangle + \tfrac{1}{\sqrt{2}}|0_A.1_B\rangle) &\xmapsto{CNOT} \tfrac{1}{\sqrt{2}}|1_A.1_B\rangle + \tfrac{1}{\sqrt{2}}|0_A.1_B\rangle \\ &\xmapsto{H_A} \tfrac{1}{2}|(0_A - 1_A).1_B\rangle + \tfrac{1}{2}|(0_A + 1_A).1_B\rangle = |0_A.1_B\rangle\,.\end{aligned}$$

Ainsi Bob mesure 0.1 ce qui est le message d'Alice.

Cas de « Bleu/1.0 ». Alice applique la porte Z au premier qubit de l'état de Bell, Bob reçoit donc $|\psi\rangle = \frac{1}{\sqrt{2}}(|0_A.0_B\rangle - |1_A.1_B\rangle)$. Bob applique une porte $CNOT$, suivie d'une porte H sur le premier qubit :

$$\begin{aligned}\tfrac{1}{\sqrt{2}}(|0_A.0_B\rangle - |1_A.1_B\rangle) &\xmapsto{CNOT} \tfrac{1}{\sqrt{2}}|0_A.0_B\rangle - \tfrac{1}{\sqrt{2}}|1_A.0_B\rangle \\ &\xmapsto{H_A} \tfrac{1}{2}|(0_A + 1_A).0_B\rangle - \tfrac{1}{2}|(0_A - 1_A).0_B\rangle = |1_A.0_B\rangle\,.\end{aligned}$$

Ainsi Bob mesure 1.0 ce qui est le message d'Alice.

Cas de « Blanc/1.1 ». À partir de l'état de Bell, Alice applique la porte X sur le premier qubit, ce qui donne $\frac{1}{\sqrt{2}}(|1_A.0_B\rangle + |0_A.1_B\rangle)$, puis une porte Z sur le premier qubit. Ainsi Bob reçoit $|\psi\rangle = \frac{1}{\sqrt{2}}(-|1_A.0_B\rangle + |0_A.1_B\rangle)$. Bob applique une porte $CNOT$, suivie d'une porte H sur le premier qubit :

$$\begin{aligned}\tfrac{1}{\sqrt{2}}(-|1_A.0_B\rangle + |0_A.1_B\rangle) &\xmapsto{CNOT} -\tfrac{1}{\sqrt{2}}|1_A.1_B\rangle + \tfrac{1}{\sqrt{2}}|0_A.1_B\rangle \\ &\xmapsto{H_A} -\tfrac{1}{2}|(0_A - 1_A).1_B\rangle + \tfrac{1}{2}|(0_A + 1_A).1_B\rangle = |1_A.1_B\rangle\,.\end{aligned}$$

Ainsi Bob mesure 1.1 ce qui est le message d'Alice.

5.6. Bilan

Alice transmet une information composée de deux bits à Bob, mais elle ne lui a envoyé qu'un seul qubit (même si Bob reçoit globalement deux qubits). De plus c'est un protocole de transmission sécurisé. En effet, si Ève intercepte le qubit qu'Alice envoie à Bob alors elle ne peut en tirer aucune information car ce qubit est de la forme $\frac{1}{\sqrt{2}}(\pm|0\rangle \pm |1\rangle)$ et donc sa mesure donne 0 ou 1 et ne permet pas à Ève de conclure quoi que ce soit sur l'information que souhaitait transmettre Alice.