

Nombres complexes et l'informatique quantique

« Je crois pouvoir dire sans risque de me tromper que personne ne comprend la mécanique quantique. »

— Richard Feynman

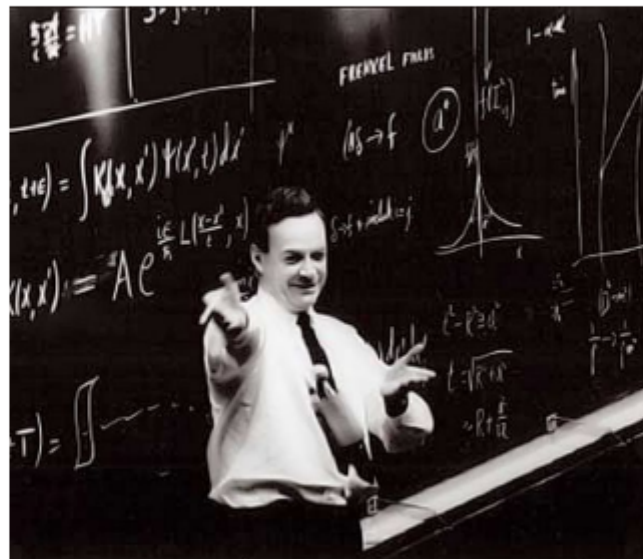


FIGURE 10.1 – Richard Feynman, ici en 1965 après avoir reçu son prix Nobel, est l'un des pères fondateurs de la théorie des ordinateurs quantiques (source © IOP, Cern).

1 Rappels sur les nombres complexes \mathbb{C}

Définition 1 : Écriture algébrique et opérations

- Un nombre complexe z est un couple $(a, b) \in \mathbb{R}^2$ que l'on notera $z = a + ib$. Le nombre complexe i vérifie l'équation : $i^2 = -1$. le nombre a est appelé **partie réelle** et on la note $a = \text{Re}(z)$. Le nombre b est appelé **partie imaginaire** et on la note $b = \text{Im}(z)$. Exemple avec $a = 2$ et $b = 3$: $z = 2 + 3i$.
- **Addition** : $(a + ib) + (a' + ib') = (a + a') + i(b + b')$
- **Multiplication** : $(a + ib) \times (a' + ib') = (aa' - bb') + i(ab' + ba')$. Ainsi on développe, en suivant les règles usuelles de la multiplication et en utilisant la règle $i^2 = -1$.

**Exemple 1 :**

Soit $z_1 = 2 + 3i$ et $z_2 = 5 - 4i$.

Alors

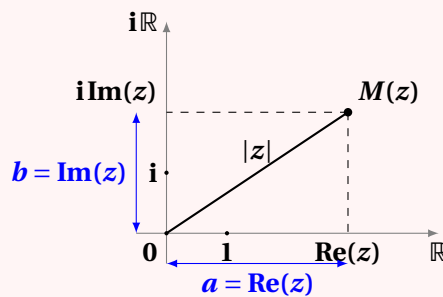
$$z_1 + z_2 = (2 + 3i) + (5 - 4i) = 7 - i.$$

Et

$$\begin{aligned} z_1 \times z_2 &= (2 + 3i) \times (5 - 4i) \\ &= 10 - 8i + 15i - 12i^2 \\ &= 10 - 8i + 15i + 12 \\ &= 22 + 7i. \end{aligned}$$

**Définition 2 : Représentation géométrique**

- A tout point M du plan de coordonnées $(a; b)$ est associé le complexe $z_M = a + ib$ appelé affixe du point M .
- Le **module** de $z = a + ib$ est le réel positif $OM = |z| = \sqrt{a^2 + b^2}$. Il mesure la distance du point (a, b) à l'origine $(0, 0)$.

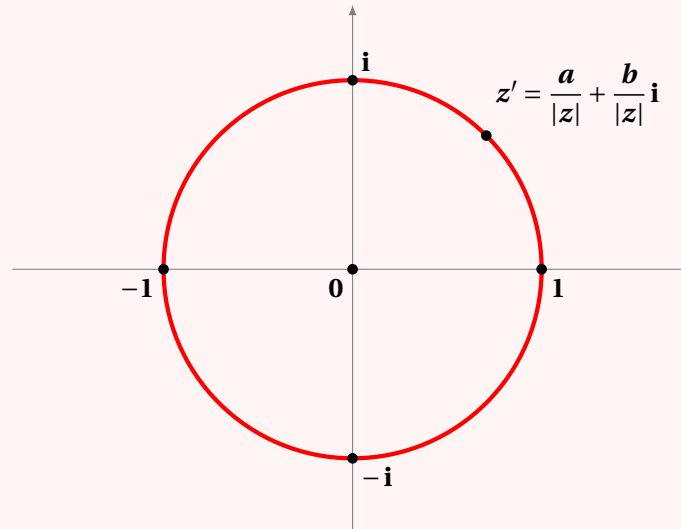


- **Propriétés du module :**

$$|zz'| = |z| \cdot |z'| \quad \text{et} \quad \left| \frac{z}{z'} \right| = \frac{|z|}{|z'|}$$


Définition 3 : Nombres complexes de module 1

On peut transformer un nombre complexe quelconque $z = a + ib$ (non nul) en un nombre complexe z' de module 1 en le divisant par son module $z' = \frac{z}{|z|} = \frac{a}{|z|} + \frac{b}{|z|}i$

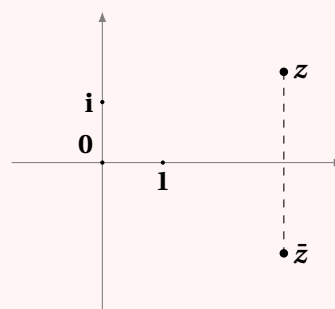


Par exemple, le nombre $z = 5 - 2i$ a pour module $|z| = \sqrt{29}$, donc $z' = \frac{z}{|z|} = \frac{5}{\sqrt{29}} - \frac{2}{\sqrt{29}}i$ est de module 1.


Définition 4 : Conjugué et inverse d'un complexe

- Le **conjugué** de $z = a + ib$ est $\bar{z} = a - ib$, autrement dit $\text{Re}(\bar{z}) = \text{Re}(z)$ et $\text{Im}(\bar{z}) = -\text{Im}(z)$.

Le point d'affixe \bar{z} est le symétrique du point d'affixe z par rapport à l'axe réel. Comme $z \times \bar{z} = (a + ib)(a - ib) = a^2 + b^2$ alors le module vaut aussi $|z| = \sqrt{z\bar{z}}$.



- Inverse** : Si $z \neq 0$, il existe un unique $z' \in \mathbb{C}$ tel que $zz' = 1$ (où $1 = 1 + i \times 0$).

$$z' = \frac{1}{z} = \frac{a - ib}{a^2 + b^2} = \frac{\bar{z}}{|z|^2}.$$

Exercice 1 :

Mettre sous forme algébrique les nombres complexes suivants :

$$\begin{array}{llll} z_1 = (2 + 5i) + (i + 3) & z_2 = 4(-2 + 3i) + 3(-5 - 8i) & z_3 = (2 - i)(3 + 8i) & z_4 = (1 - i)\overline{(1 + i)} \\ z_5 = i(1 - 3i)^2 & z_6 = \frac{1}{1+i} & z_7 = \frac{-4}{1+i\sqrt{3}} & z_8 = \frac{1-2i}{3+i} \end{array}$$

Correction

1. On regroupe simplement les parties réelles et les parties imaginaires. On trouve

$$z_1 = 5 + 6i$$

2. De la même façon,

$$z_2 = (-8 + 12i) + (-15 - 24i) = -23 - 12i$$

3. On développe, puis on regroupe pour trouver :

$$z_3 = 6 + 16i - 3i + 8 = 14 + 13i$$

4. On écrit

$$z_4 = (1 - i)(1 - i) = 1 - 2i - 1 = -2i$$

5. On commence par calculer $(1 - 3i)^2$

$$(1 - 3i)^2 = 1 - 2 \times 1 \times 3i + (3i)^2 = 1 - 6i - 9 = -8 - 6i$$

On multiplie ensuite par i

$$i(1 - 3i)^2 = -8i - 6i^2 = 6 - 8i$$

6. Le conjugué de $1 + i$ et $1 - i$ et donc on a

$$z_6 = \frac{1}{1+i} = \frac{1-i}{(1+i)(1-i)} = \frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i$$

7. Avec la même méthode, on trouve

$$z_7 = \frac{-4(1-i\sqrt{3})}{(1+i\sqrt{3})(1-i\sqrt{3})} = \frac{-4(1-i\sqrt{3})}{1+3} = -1 + i\sqrt{3}$$

8. On écrit

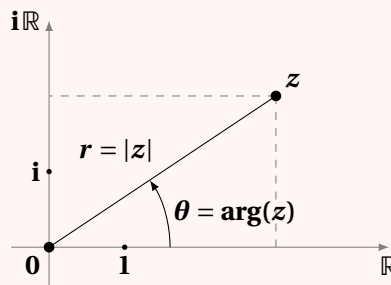
$$\frac{1-2i}{3+i} = \frac{(1-2i)(3-i)}{(3-i)(3+i)} = \frac{1-7i}{9+1} = \frac{1}{10} - \frac{7}{10}i$$



Définition 5 : Notation trigonométrique

Un nombre complexe $z \in \mathbb{C}$, admet l'écriture trigonométrique :

$$z = r(\cos \theta + i \sin \theta) \quad \text{avec } r \in \mathbb{R}_+ \text{ et } \theta \in \mathbb{R}$$



- r est en fait le module de z : $r = |z|$,
- θ est un **argument** de z , on le note $\arg(z)$, et tels que

$$\cos(\theta) = \frac{a}{r} \quad \text{et} \quad \sin(\theta) = \frac{b}{r}$$



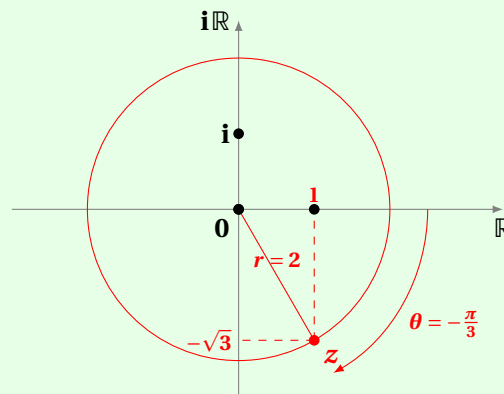
Exemple 2 :

- Soit $z = 1 - \sqrt{3}i$. Alors $r = |z| = 2$ et $\theta = -\frac{\pi}{3}$, car alors

$$r \cos \theta = 2 \cos\left(-\frac{\pi}{3}\right) = 2 \times \frac{1}{2} = 1 = \operatorname{Re}(z)$$

et

$$r \sin \theta = 2 \sin\left(-\frac{\pi}{3}\right) = -2 \times \frac{\sqrt{3}}{2} = -\sqrt{3} = \operatorname{Im}(z).$$



**Remarque 1 :**

L'argument n'est pas unique : si θ est un argument alors $\theta + 2k\pi$ ($k \in \mathbb{Z}$) aussi. On dira que $\arg(z)$ est **défini modulo 2π** et l'écriture $\theta \equiv \theta' \pmod{2\pi}$ signifie que $\theta = \theta' + 2k\pi$ pour un certain entier $k \in \mathbb{Z}$.

L'écriture module-argument facilite le calcul des multiplications. Les modules se multiplient, les arguments s'additionnent.

**Proposition 1 :**

Soient z et z' deux nombres complexes. Alors

$$\arg(zz') = \arg(z) + \arg(z') \pmod{2\pi} \quad \text{et} \quad \arg\left(\frac{z}{z'}\right) = \arg(z) - \arg(z') \pmod{2\pi}$$

Exercice 2 :

Soit les nombres complexes : $z_1 = \sqrt{2} + i\sqrt{6}$, $z_2 = 2 + 2i$ et $Z = \frac{z_1}{z_2}$.

1. Écrire Z sous forme algébrique.
2. Donner les modules et arguments de z_1 , z_2 et Z .
3. En déduire $\cos \frac{\pi}{12}$ et $\sin \frac{\pi}{12}$.

Correction

1. On a $Z = \frac{z_1}{z_2} = \frac{\sqrt{2} + i\sqrt{6}}{2 + 2i} = \frac{\sqrt{2}}{2} \cdot \frac{1 + i\sqrt{3}}{1 + i} = \frac{\sqrt{2}}{2} \cdot \frac{(1 + i\sqrt{3})(1 - i)}{(1 + i)(1 - i)} = \frac{\sqrt{2}}{4} [1 + \sqrt{3} + i(\sqrt{3} - 1)]$.

2. (a) $|z_1|^2 = 2 + 6 = 8 \Rightarrow |z_1| = 2\sqrt{2}$. On a donc $z_1 = 2\sqrt{2} \left(\frac{1}{2} + i\frac{\sqrt{3}}{2} \right)$. Donc $\arg(z_1) = \frac{\pi}{3} [2\pi]$.

(b) On a de même $|z_2| = 2\sqrt{2}$, puis $z_2 = 2\sqrt{2} \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \right)$. Donc $\arg(z_2) = \frac{\pi}{4} [2\pi]$.

(c) Aisi, $\arg(Z) = \arg\left(\frac{z_1}{z_2}\right) = \arg(z_1) - \arg(z_2) = \frac{\pi}{3} - \frac{\pi}{4} = \frac{\pi}{12} [2\pi]$, et $|Z| = \frac{|z_1|}{|z_2|} = 1$.

3. On en déduit que $Z = \cos\left(\frac{\pi}{12}\right) + i\sin\left(\frac{\pi}{12}\right)$ et par identification avec la forme algébrique du 1):

$$\cos\left(\frac{\pi}{12}\right) = \frac{\sqrt{2}}{4}(1 + \sqrt{3}) \quad \text{et} \quad \sin\left(\frac{\pi}{12}\right) = \frac{\sqrt{2}}{4}(\sqrt{3} - 1)$$


Définition 6 : Notation exponentielle

Nous définissons la **notation exponentielle** par

$$e^{i\theta} = \cos \theta + i \sin \theta$$

et donc tout nombre complexe s'écrit :

$$z = r e^{i\theta}$$

où $r = |z|$ est son module et $\theta = \arg(z)$ est un de ses arguments.


Remarque 2 :

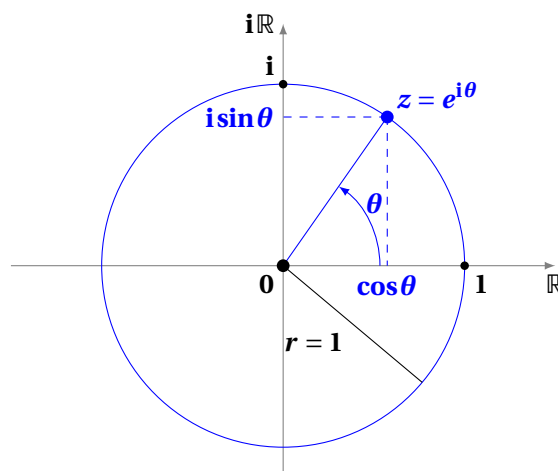
Avec la notation exponentielle, les calculs s'effectuent avec les lois habituelles pour les puissances. Par exemple : $(e^{i\theta})^n = e^{in\theta}$ Il s'agit en fait de la **formule de Moivre** qui s'écrit en version étendue :

$$(\cos \theta + i \sin \theta)^n = \cos(n\theta) + i \sin(n\theta).$$

De façon plus générale, pour $z = r e^{i\theta}$ et $z' = r' e^{i\theta'}$, on peut écrire :

- $zz' = r r' e^{i\theta} e^{i\theta'} = r r' e^{i(\theta+\theta')}$
- $z^n = (r e^{i\theta})^n = r^n (e^{i\theta})^n = r^n e^{in\theta}$
- $1/z = 1/(r e^{i\theta}) = \frac{1}{r} e^{-i\theta}$
- $\bar{z} = r e^{-i\theta}$

Tout nombre complexe de module 1 s'écrit sous la forme $z = e^{i\theta}$, autrement dit $z = \cos \theta + i \sin \theta$.



Exercice 3 :

Déterminer la forme algébrique des nombres complexes suivants :

$$z_1 = (2 + 2i)^6 \quad z_2 = \left(\frac{1 + i\sqrt{3}}{1 - i} \right)^{20}$$

Correction

La méthode la plus facile, ici, consiste à calculer d'abord la forme trigonométrique qui se comporte bien mieux vis à vis des puissances, puis à revenir à la forme algébrique.

1. On écrit : $2 + 2i = 2\sqrt{2} \left(\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2} \right) = 2\sqrt{2} e^{i\pi/4}$. D'où $z_1 = 2^9 e^{3i\pi/2} = -512i$.
2. On commence par passer par la forme exponentielle :

$$\frac{1 + i\sqrt{3}}{1 - i} = \frac{2 \left(\frac{1}{2} + i \frac{\sqrt{3}}{2} \right)}{\sqrt{2} \left(\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \right)} = \sqrt{2} \frac{e^{i\pi/3}}{e^{-i\pi/4}} = \sqrt{2} e^{i7\pi/12}$$

On en déduit que

$$z_2 = \left(\frac{1 + i\sqrt{3}}{1 - i} \right)^{20} = (\sqrt{2})^{20} e^{i \frac{140\pi}{12}} = 2^{10} e^{i \frac{35\pi}{3}}$$

2 Application à l'informatique quantique

2.1 1-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 la lettre **A** est **1.1.0.0.0.1**.

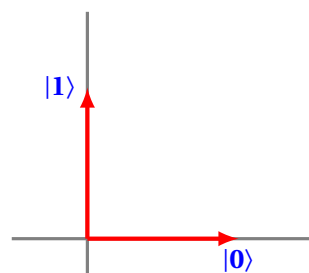
En informatique quantique on part aussi de deux **états quantiques de base** : $|0\rangle$ et $|1\rangle$



Remarque 3 :

Les états $|0\rangle$ et $|1\rangle$ se lisent **ket zéro** et **ket un** ("ket" se prononce comme le mot **quête**).

En fait $|0\rangle$ et $|1\rangle$ sont deux vecteurs : $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Ces deux vecteurs forment une base orthonormée du plan.



États quantiques de base

Ce qui est nouveau et fondamental est que l'on peut **superposer** ces deux états $|0\rangle$ et $|1\rangle$, d'où la définition suivante.



Définition 7 :

Un **1-qubit** $|\psi\rangle$, se lit **ket psi**, est un **état quantique** obtenu par combinaison linéaire de $|0\rangle$ et $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{avec } \alpha \in \mathbb{C} \quad \text{et} \quad \beta \in \mathbb{C}$$

avec souvent la condition de normalisation :

$$|\alpha|^2 + |\beta|^2 = 1$$

Un qubit est donc défini par deux nombres complexes, $\alpha = a_1 + i b_1$ et $\beta = a_2 + i b_2$. Il faut ainsi 4 nombres réels a_1, b_1, a_2, b_2 pour définir un qubit. Par exemple :

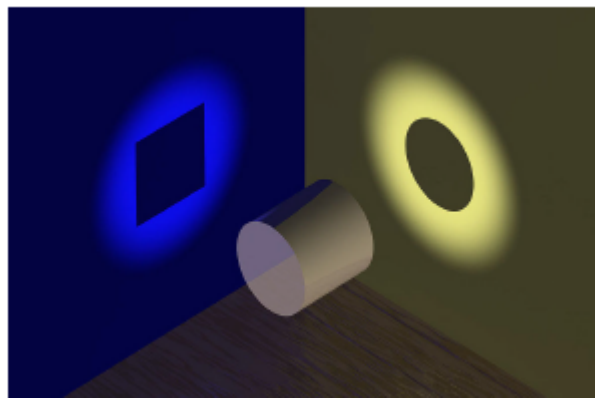
$$|\psi\rangle = (3 + 4i)|0\rangle + (2 - 8i)|1\rangle; \quad |\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$$

Remarque 4 :

La présence de nombres complexes pour décrire l'état d'un qubit $|\psi\rangle$ s'explique par la nature ondulatoire des particules quantiques. Chaque coefficient α ou β représente l'amplitude et la phase d'une onde qui est de manière générale un nombre complexe selon la théorie ondulatoire classique.

Remarque 5 :

Dans le monde physique, la superposition traduit la dualité onde-corpusculaire. Par exemple, la métaphore du cylindre est l'exemple d'un objet ayant des propriétés (comme être un cercle ou un carré) apparemment inconciliables. Mais une projection peut nous faire apparaître l'une ou l'autre de ces propriétés. Pour une particule dans un état quantique c'est la même chose : onde et particule sont deux facettes (observations) d'une même réalité mais pas la réalité elle-même.



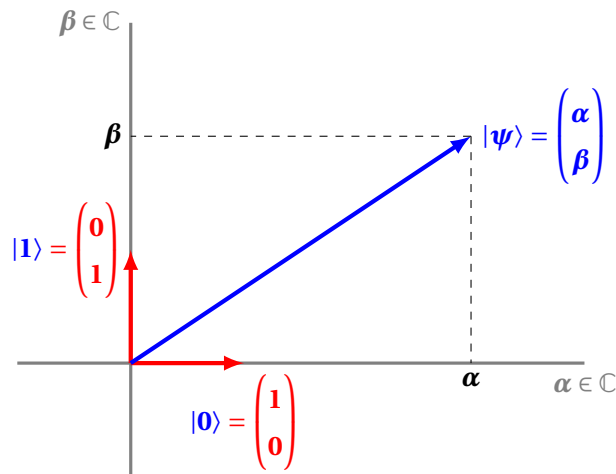
D'après la définition 7, un 1-qubit $|\psi\rangle$ est représenté par un vecteur :

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

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 :

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

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

**Remarque 6 :**

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.

3 Opérations sur les qubits

Addition : L'addition de deux qubits se fait coefficient par coefficient, il s'agit donc d'additionner des paires de nombres complexes. Par exemple si

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

alors

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

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

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

Pour les coefficients, on utilise la multiplication des nombres complexes, avec bien sûr toujours la relation $i^2 = -1$.

**Attention :**

| Notez en passant que ce produit n'est pas commutatif en général.

**Exemple 3 :**

Avec

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

on a

$$\begin{aligned} |\phi\rangle \cdot |\psi\rangle &= ((1 + 3i)|0\rangle + 2i|1\rangle) \times (3|0\rangle + (1 - i)|1\rangle) \\ &= (1 + 3i) \cdot 3 \cdot |0\rangle \cdot |0\rangle + (1 + 3i) \cdot (1 - i) \cdot |0\rangle \cdot |1\rangle + 2i \cdot 3 \cdot |1\rangle \cdot |0\rangle + 2i \cdot (1 - i) \cdot |1\rangle \cdot |1\rangle \\ &= (3 + 9i)|0.0\rangle + (4 + 2i)|0.1\rangle + 6i|1.0\rangle + (2 + 2i)|1.1\rangle \end{aligned}$$

où on a utilisé $(1 + 3i) \cdot (1 - i) = 1 - i + 3i - 3i^2 = 4 + 2i$ et $2i \cdot (1 - i) = 2i - 2i^2 = 2 + 2i$.

Norme : La norme d'un qubit est un nombre réel notée $\|\psi\|$.

- Pour un 1-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 1-qubit $|\psi\rangle$ est $\frac{|\psi\rangle}{\|\psi\|}$, qui est un 1-qubit de norme 1.

**Exemple 4 :**

Pour $|\psi\rangle = (3 + 4i)|0\rangle + (2 - i)|1\rangle$ alors la norme au carré vaut :

$$\begin{aligned} \|\psi\|^2 &= |3 + 4i|^2 + |2 - i|^2 \\ &= (3^2 + 4^2) + (2^2 + (-1)^2) \\ &= 30. \end{aligned}$$

Donc $\|\psi\| = \sqrt{30}$. et la normalisation de $|\psi\rangle$ est

$$|\psi\rangle_{\text{norm}} = \frac{1}{\|\psi\|} \left((3 + 4i)|0\rangle + (2 - i)|1\rangle \right)$$

Exercice 4 : Addition de deux qubits (superposition d'états)

Soient les qubits $|q_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$ et $|q_2\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. Calculez la superposition $|q\rangle = |q_1\rangle + |q_2\rangle$ et normalisez l'état résultant.

Correction :

– Addition des qubits :

$$|q\rangle = |q_1\rangle + |q_2\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right) + \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)$$

Regroupons les termes :

$$|q\rangle = \left(\frac{1}{\sqrt{2}} + \frac{1}{2}\right)|0\rangle + \left(\frac{\sqrt{3}}{2} + \frac{i}{\sqrt{2}}\right)|1\rangle$$

– Simplification des coefficients :

Pour $|0\rangle$:

$$\frac{1}{\sqrt{2}} + \frac{1}{2} = \frac{\sqrt{2}}{2} + \frac{1}{2} = \frac{\sqrt{2}+1}{2}$$

Pour $|1\rangle$:

$$\frac{\sqrt{3}}{2} + \frac{i}{\sqrt{2}}$$

L'état non normalisé est donc :

$$|q\rangle = \frac{\sqrt{2}+1}{2}|0\rangle + \left(\frac{\sqrt{3}}{2} + \frac{i}{\sqrt{2}}\right)|1\rangle$$

– Norme de $|q\rangle$:

La norme est donnée par :

$$\|q\| = \sqrt{\left|\frac{\sqrt{2}+1}{2}\right|^2 + \left|\frac{i}{\sqrt{2}} + \frac{\sqrt{3}}{2}\right|^2}$$

Calculons chaque terme séparément :

$$\left|\frac{\sqrt{2}+1}{2}\right|^2 = \frac{(\sqrt{2}+1)^2}{4} = \frac{2+2\sqrt{2}+1}{4} = \frac{3+2\sqrt{2}}{4}$$

$$\left|\frac{i}{\sqrt{2}} + \frac{\sqrt{3}}{2}\right|^2 = \frac{1}{2} + \frac{3}{4} = \frac{5}{4}$$

Donc :

$$\|q\| = \sqrt{\frac{3+2\sqrt{2}}{4} + \frac{5}{4}} = \sqrt{\frac{8+2\sqrt{2}}{4}} = \sqrt{2 + \frac{\sqrt{2}}{2}}$$

– **État normalisé :**

L'état normalisé est :

$$|q_{\text{norm}}\rangle = \frac{1}{\|q\|} \left(\frac{\sqrt{2}+1}{2} |0\rangle + \left(\frac{i}{\sqrt{2}} + \frac{\sqrt{3}}{2} \right) |1\rangle \right)$$

Exercice 5 : Multiplication de deux qubits

Soient $|q_1\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle$ et $|q_2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. Calculez le produit $|q_1\rangle \cdot |q_2\rangle$.

Correction :

Le produit est donné par :

$$|q_1\rangle \cdot |q_2\rangle = \left(\frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle \right) \cdot \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right).$$

En développant :

$$|q_1\rangle \cdot |q_2\rangle = \frac{1}{\sqrt{3}} \frac{1}{\sqrt{2}} |0\rangle|0\rangle - \frac{1}{\sqrt{3}} \frac{1}{\sqrt{2}} |0\rangle|1\rangle + \frac{\sqrt{2}}{\sqrt{3}} \frac{1}{\sqrt{2}} |1\rangle|0\rangle - \frac{\sqrt{2}}{\sqrt{3}} \frac{1}{\sqrt{2}} |1\rangle|1\rangle.$$

– **Simplification des coefficients :**

$$|q_1\rangle \cdot |q_2\rangle = \frac{1}{\sqrt{6}} |0.0\rangle - \frac{1}{\sqrt{6}} |0.1\rangle + \frac{1}{\sqrt{3}} |1.0\rangle - \frac{1}{\sqrt{3}} |1.1\rangle.$$

4 Écriture exponentielle d'un 1-qubit

À l'aide des notations exponentielles de α et β , un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ peut aussi s'écrire :

$$|\psi\rangle = r e^{i\theta} |0\rangle + r' e^{i\theta'} |1\rangle.$$

Un tel qubit est normalisé si $r^2 + r'^2 = 1$.

Certains utilisent un vocabulaire issu de la physique :

- θ est la **phase** associée à $|0\rangle$,
- θ' est la phase associée à $|1\rangle$.

L'écriture algébrique est adaptée à un calcul de somme tandis que la notation exponentielle rend le calcul d'une multiplication plus facile.

**Exemple 5 :**

Si $|\phi\rangle = 2e^{i\frac{\pi}{3}}|0\rangle + 3e^{i\frac{\pi}{4}}|1\rangle$ et $|\psi\rangle = 4e^{i\frac{\pi}{5}}|0\rangle + 5e^{i\frac{\pi}{6}}|1\rangle$. Alors :

$$\begin{aligned} |\phi\rangle \cdot |\psi\rangle &= \left(2e^{i\frac{\pi}{3}}|0\rangle + 3e^{i\frac{\pi}{4}}|1\rangle\right) \times \left(4e^{i\frac{\pi}{5}}|0\rangle + 5e^{i\frac{\pi}{6}}|1\rangle\right) \\ &= 2e^{i\frac{\pi}{3}} \cdot 4e^{i\frac{\pi}{5}}|0.0\rangle + 2e^{i\frac{\pi}{3}} \cdot 5e^{i\frac{\pi}{6}}|0.1\rangle + 3e^{i\frac{\pi}{4}} \cdot 4e^{i\frac{\pi}{5}}|1.0\rangle + 3e^{i\frac{\pi}{4}} \cdot 5e^{i\frac{\pi}{6}}|1.1\rangle \\ &= 8e^{i(\frac{\pi}{3}+\frac{\pi}{5})}|0.0\rangle + 10e^{i(\frac{\pi}{3}+\frac{\pi}{6})}|0.1\rangle + 12e^{i(\frac{\pi}{4}+\frac{\pi}{5})}|1.0\rangle + 15e^{i(\frac{\pi}{4}+\frac{\pi}{6})}|1.1\rangle. \end{aligned}$$

5 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 :

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

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 6 :**

Une particule quantique comme un électron peut être décrite par un état quantique qui associe à chaque point de l'espace un nombre complexe. L'expérience réalisée pour localiser l'électron ne peut pas dire avec certitude où l'électron se trouvera.

**Exemple 7 :**

Considérons l'état quantique :

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

Alors

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

et

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

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**¹. 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 7 :**

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**.

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.

¹La réduction du paquet d'onde est un concept de la mécanique quantique selon lequel, après une mesure, un système physique voit son état entièrement réduit à celui qui a été mesuré.

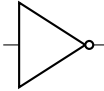
6 Circuit dans un ordinateur quantique

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.

6.1 Porte avec une entrée X, Y, Z de Pauli

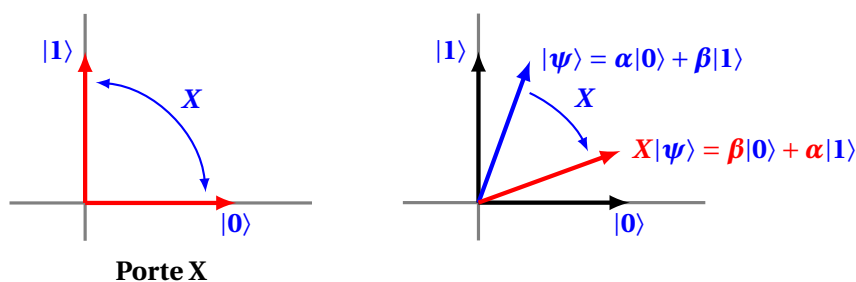
Porte X :

$$\text{Input} \longrightarrow \boxed{X} \longrightarrow \text{Output}$$

Équivalent en ordinateur classique 

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

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



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

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

Par exemple l'état $|\psi\rangle = 2|0\rangle + (1-i)|1\rangle$ est transformé par la porte X en l'état $X(|\psi\rangle) = (1-i)|0\rangle + 2|1\rangle$.

En termes de vecteurs cette transformation s'écrit :

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \xrightarrow{X} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \xrightarrow{X} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \xrightarrow{X} \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

La matrice de la porte X est donc :

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

car

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

Porte Y et Z :

$$\begin{array}{lcl}
 \text{---} \boxed{Y} \text{---} & \left\{ \begin{array}{l} |0\rangle \mapsto i|1\rangle \\ |1\rangle \mapsto -i|0\rangle \end{array} \right. & Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\
 \text{---} \boxed{Z} \text{---} & \left\{ \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{array} \right. & Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
 \end{array}$$

Porte H de Hadamard

$$\text{Input} \text{---} \boxed{H} \text{---} \text{Output}$$

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

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{et} \quad |1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

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

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

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 $|\psi\rangle = i|0\rangle + (2 + i)|1\rangle$ est transformé en $H(|\psi\rangle) = \frac{2+2i}{\sqrt{2}}|0\rangle - \frac{2}{\sqrt{2}}|1\rangle$.

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

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

La matrice de la porte **H** est donc :

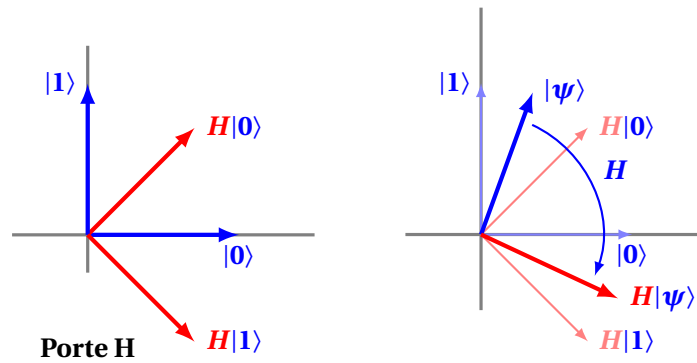
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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 $(H(|0\rangle), H(|1\rangle))$.



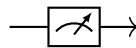
Remarque. Il est fréquent de rencontrer les notations suivantes :

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

même si nous éviterons de les utiliser ici.

Porte de mesure

La porte de mesure est symbolisée par un petit cadran.



Attention :

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.

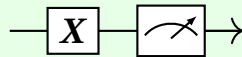
6.2 Exemples de circuit quantique

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

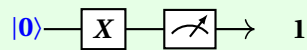


Exemple 8 :

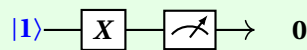
Voici un circuit composé d'une porte X (c'est-à-dire une porte **NON**) suivie d'une porte de mesure :



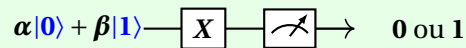
- Si l'entrée est $|0\rangle$, alors $X(|0\rangle) = |1\rangle$, la sortie mesurée vaut donc **1** (avec une probabilité **1**)



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

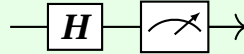


- Si l'entrée est l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (avec $|\alpha|^2 + |\beta|^2 = 1$), alors $X(|\psi\rangle) = \beta|0\rangle + \alpha|1\rangle$. La mesure donne donc **0** avec une probabilité $|\beta|^2$ et **1** avec une probabilité $|\alpha|^2$.



**Exemple 9 :**

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 :

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

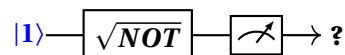
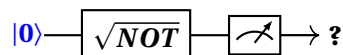
Ainsi, pour cette entrée, le circuit renvoie, après mesure, 0 avec une quasi-certitude.

Exercice 6 :

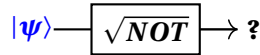
On considère la porte \sqrt{NOT} définie par

$$\begin{array}{c} \text{---} \boxed{\sqrt{NOT}} \text{---} \end{array} \quad \left\{ \begin{array}{l} |0\rangle \mapsto \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \\ |1\rangle \mapsto \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \end{array} \right. \quad \text{c'est-à-dire} \quad M = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

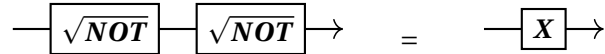
1. Pour l'entrée $|0\rangle$, que donne une mesure après la porte \sqrt{NOT} ? Même question avec $|1\rangle$.



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 ?



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



Autrement dit, il s'agit de montrer que :

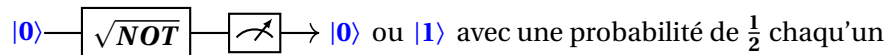
$$\sqrt{\text{NOT}}(\sqrt{\text{NOT}}(|\psi\rangle)) = \text{NOT}(|\psi\rangle)$$

Correction :

1. On a $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, d'où

$$\sqrt{\text{NOT}}(|0\rangle) = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+i \\ 1-i \end{pmatrix} = \frac{1}{2} ((1+i)|0\rangle + (1-i)|1\rangle)$$

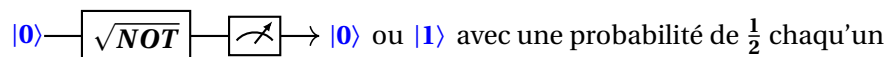
Par conséquent, une mesure de $\sqrt{\text{NOT}}(|0\rangle)$ donne $|0\rangle$ avec une probabilité de $\frac{1}{2}$ et $|1\rangle$ avec une probabilité de $\frac{1}{2}$. Ainsi,



De même

$$\sqrt{\text{NOT}}(|1\rangle) = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1-i \\ 1+i \end{pmatrix} = \frac{1}{2} ((1-i)|0\rangle + (1+i)|1\rangle)$$

Ainsi,



7 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.

7.1 Superposition

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

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

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 $|0.0\rangle, |0.1\rangle, \dots$? Il s'agit de nouveaux vecteurs d'une base mais cette fois en dimension 4 :

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

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 10 :**

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

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 :

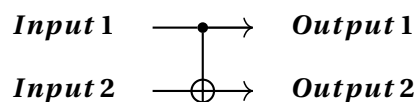
$$|0.0\rangle = |0\rangle \cdot |0\rangle \quad |0.1\rangle = |0\rangle \cdot |1\rangle \quad |1.0\rangle = |1\rangle \cdot |0\rangle \quad |1.1\rangle = |1\rangle \cdot |1\rangle$$

On note aussi ce produit par le symbole \otimes :

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

7.2 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 :

$$|0.0\rangle \xrightarrow{CNOT} |0.0\rangle \quad |0.1\rangle \xrightarrow{CNOT} |0.1\rangle \quad |1.0\rangle \xrightarrow{CNOT} |1.1\rangle \quad |1.1\rangle \xrightarrow{CNOT} |1.0\rangle$$

Voici cette même règle présentée à l'aide de vecteurs :

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

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** :

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



Exemple 11 :

Calculons la sortie d'une porte **CNOT** lorsque l'entrée est formée des deux qubits

$$|\psi_1\rangle = |0\rangle - 2|1\rangle \quad \text{et} \quad |\psi_2\rangle = 3|0\rangle + 5|1\rangle$$

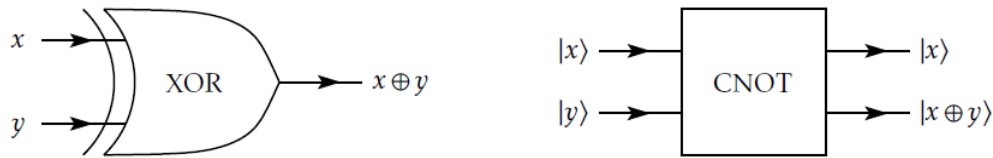
$$\begin{array}{ccc} |0\rangle - 2|1\rangle & \xrightarrow{\bullet} & ? \\ 3|0\rangle + 5|1\rangle & \xrightarrow{\oplus} & ? \end{array}$$

On sépare l'état $|\psi_1\rangle$ en $|0\rangle$ et $-2|1\rangle$ et on regarde séparément leur action, :

$$\begin{array}{ccc} |0\rangle & \xrightarrow{\bullet} & |0\rangle \\ 3|0\rangle + 5|1\rangle & \xrightarrow{\oplus} & 3|0\rangle + 5|1\rangle \end{array}$$

$$\begin{array}{ccc} -2|1\rangle & \xrightarrow{\bullet} & -2|1\rangle \\ 3|0\rangle + 5|1\rangle & \xrightarrow{\oplus} & 5|0\rangle + 3|1\rangle \end{array}$$

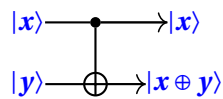
7.3 La porte **CNOT** \equiv **XOR**



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

$$|x, y\rangle \xrightarrow{\text{CNOT}} |x, y \oplus x\rangle$$

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**) :

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

Par exemple :

$$\text{CNOT}(|\mathbf{1,1}\rangle) = |\mathbf{1, (1 \oplus 1)}\rangle = |\mathbf{1,0}\rangle.$$

7.4 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** :

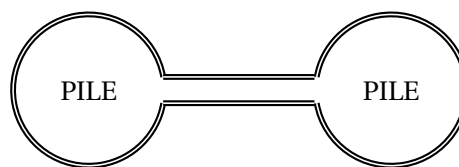
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|0,0\rangle + \frac{1}{\sqrt{2}}|1,1\rangle$$

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 8 :

- 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**, c-à-d si $|\psi_A\rangle$ et $|\psi_B\rangle$ sont **intriqués**, ils seront 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**.



Attention :

L'intrication quantique est un des aspects les plus troublants de la mécanique quantique. Deux photons intriqués, même distantes, continuent de partager des propriétés communes.

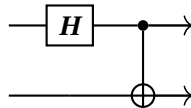
Métaphore : On peut voir l'intrication quantique comme la télépathie que décrivent parfois des jumeaux ou des frères : un frère arriverait ainsi à percevoir ou à ressentir des émotions fortes ressenties par son jumeau, sans être avec lui ni lui parler, c'est l'intrication.

Cependant, l'intrication ne consisterait, pour l'un des frères, qu'à faire savoir à son autre frère que quelque chose se passe. Il ne sait ni quoi exactement, ni si c'est en bien ou en mal. Pour avoir plus d'information, il leur faudra toujours passer par une voie classique comme le téléphone.

- L'intrication permet aux ordinateurs quantiques de manipuler de nombreux qubits en une seule opération, au lieu de manipuler chaque qubit individuellement, comme dans l'informatique classique.

7.4.1 Obtention de l'état de Bell

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



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

$$\begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} \xrightarrow{\text{Circuit}} \frac{1}{\sqrt{2}} \begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} + \frac{1}{\sqrt{2}} \begin{array}{c} |1\rangle \\ \otimes \\ |1\rangle \end{array}$$

En effet, reprenons le calcul en détails (en adoptant la notation verticale) à partir de l'entrée

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

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

$$\begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} \xrightarrow{H} \begin{array}{c} H(|0\rangle) \\ \otimes \\ |0\rangle \end{array} = \begin{array}{c} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ \otimes \\ |0\rangle \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} + \frac{1}{\sqrt{2}} \begin{array}{c} |1\rangle \\ \otimes \\ |0\rangle \end{array}$$

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

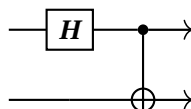
$$\begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} \xrightarrow{CNOT} \begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} \quad \text{et} \quad \begin{array}{c} |1\rangle \\ \otimes \\ |0\rangle \end{array} \xrightarrow{CNOT} \begin{array}{c} |1\rangle \\ \otimes \\ |1\rangle \end{array}$$

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

$$\begin{array}{c} H(|0\rangle) \\ \otimes \\ |0\rangle \end{array} \xrightarrow{CNOT} \frac{1}{\sqrt{2}} \begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} + \frac{1}{\sqrt{2}} \begin{array}{c} |1\rangle \\ \otimes \\ |1\rangle \end{array} = \frac{1}{\sqrt{2}} |0.0\rangle + \frac{1}{\sqrt{2}} |1.1\rangle$$

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

Exercice 7 :



Quelle est la sortie produite pour l'entrée $|1.0\rangle$?

Correction

Adoptant la notation verticale à partir de l'entrée

$$|1.0\rangle = \begin{array}{c} |1\rangle \\ \otimes \\ |0\rangle \end{array}$$

Le premier qubit (celui du haut) passe par une porte H , le second qubit reste inchangé :

$$\begin{array}{c} |1\rangle \\ \otimes \\ |0\rangle \end{array} \xrightarrow{H} \begin{array}{c} H(|1\rangle) \\ \otimes \\ |0\rangle \end{array} = \begin{array}{c} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \\ \otimes \\ |0\rangle \end{array} = \frac{1}{\sqrt{2}} \begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} - \frac{1}{\sqrt{2}} \begin{array}{c} |1\rangle \\ \otimes \\ |0\rangle \end{array}$$

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

$$\begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} \xrightarrow{CNOT} \begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} \quad \text{et} \quad \begin{array}{c} |1\rangle \\ \otimes \\ |0\rangle \end{array} \xrightarrow{CNOT} \begin{array}{c} |1\rangle \\ \otimes \\ |1\rangle \end{array}$$

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

$$\begin{array}{c} H(|0\rangle) \\ \otimes \\ |0\rangle \end{array} \xrightarrow{CNOT} \frac{1}{\sqrt{2}} \begin{array}{c} |0\rangle \\ \otimes \\ |0\rangle \end{array} - \frac{1}{\sqrt{2}} \begin{array}{c} |1\rangle \\ \otimes \\ |1\rangle \end{array} = \frac{1}{\sqrt{2}} |0.0\rangle - \frac{1}{\sqrt{2}} |1.1\rangle$$

8 Théorème de non-clonage quantique

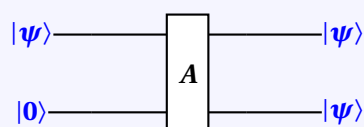
Un ordinateur classique est modélisé par une machine de Turing et est capable de lire une série de bits et de les dupliquer à un autre endroit. Nous allons voir que ce n'est pas le cas pour un ordinateur quantique. En fait on peut copier un qubit, mais en créant la copie on perd l'original. On parle ainsi de **non-clonage quantique**.

8.1 Non-clonage des 1-qubits



Théorème 1 :

Il n'existe pas de porte quantique qui réalise le clonage des 1-qubits, c'est-à-dire telle que pour tout 1-qubit $|\psi\rangle$ on ait :

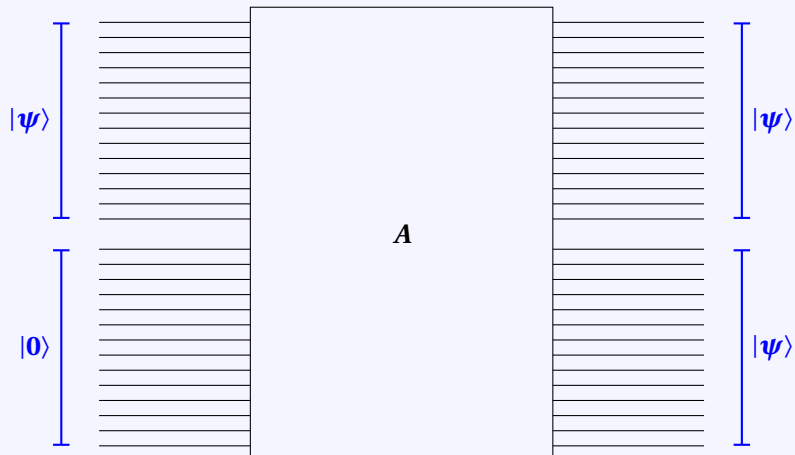


8.2 Cas général



Théorème 2 :

Il n'existe pas de porte quantique qui réalise le clonage d'un n -qubit, c'est-à-dire telle que pour tout n -qubit $|\psi\rangle$ on ait:



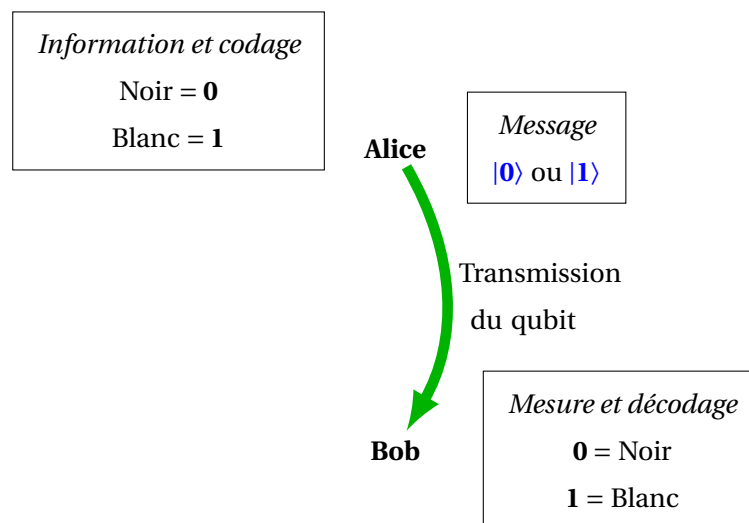
9 Application : Communication par codage super-dense sécurisé

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

9.1 Motivation

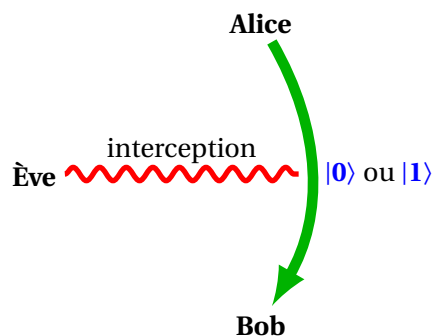
On commence par une situation très simple.

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**.

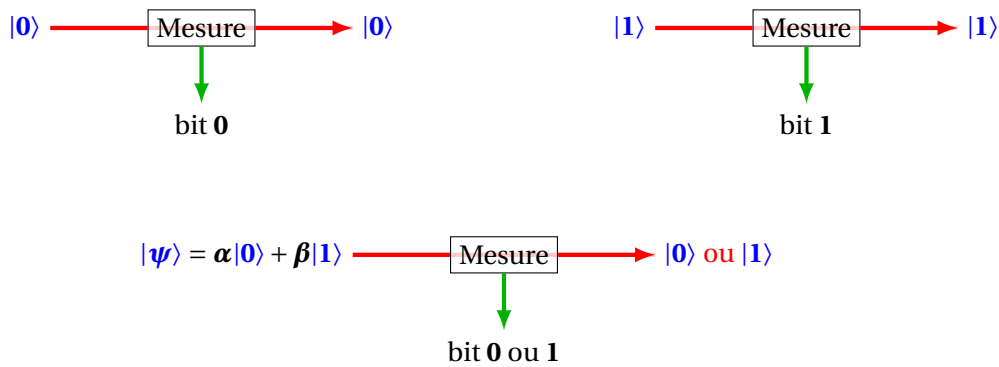


Avec cette technique, un seul bit classique d'information est transmis pour chaque qubit envoyé. Ne pourrait-on pas mieux faire ?

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 $|1\rangle$.

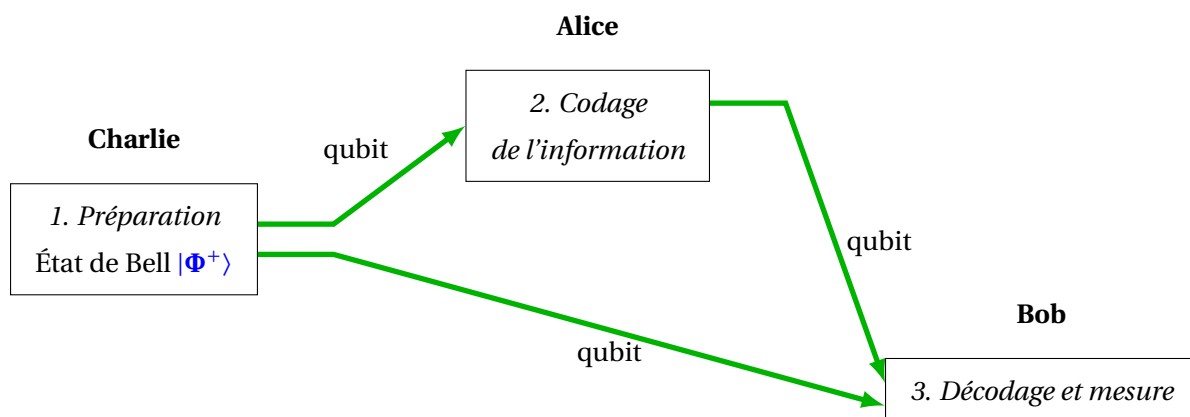


9.2 Schéma général du protocole du codage super-dense sécurisé

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 par Charlie,
2. codage de l'information par Alice,
3. décodage par Bob.



Etape 1: 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 : (Les calculs ont été expliqués plus haut)

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

$$\begin{aligned} & \frac{1}{\sqrt{2}} \begin{matrix} |0\rangle \\ \otimes \\ |0\rangle \end{matrix} + \frac{1}{\sqrt{2}} \begin{matrix} |1\rangle \\ \otimes \\ |1\rangle \end{matrix} = \frac{1}{\sqrt{2}}|0,0\rangle + \frac{1}{\sqrt{2}}|1,1\rangle = |\Phi^+\rangle \end{aligned}$$

**Remarque 9 :**

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 :

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

Etape 2: Charlie envoie

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

**Attention : 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**.

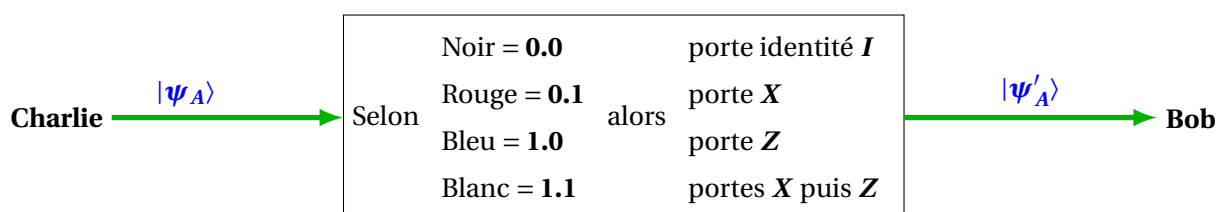
Etape 3: Transformation de $|\psi_A\rangle$ par d'Alice

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

Alice



- Si elle veut transmettre l'information **Noir/0.0** elle applique l'identité **I** au premier qubit de l'état de Bell $|\psi_A\rangle$, (elle ne fait rien et conserve $|\psi_A\rangle = |\psi'_A\rangle$). Ensuite elle transmet le qubit transformé $|\psi'_A\rangle = \frac{1}{\sqrt{2}}|0_A\rangle + \frac{1}{\sqrt{2}}|1_A\rangle$ à Bob.

- Si elle veut transmettre **Rouge/0.1**, elle applique la porte X au premier qubit de l'état de Bell, $|\psi_A\rangle$, c-à-d, elle transforme son qubit $\frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$ en $|\psi'_A\rangle = \frac{1}{\sqrt{2}}(|1_A\rangle + |0_A\rangle)$. Ensuite elle transmet le qubit transformé $|\psi'_A\rangle$ à Bob.
- Si elle veut transmettre **Bleu/1.0**, elle applique la porte Z au premier qubit de l'état de Bell, $|\psi_A\rangle$, c-à-d elle transforme son qubit $\frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$ en $|\psi'_A\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle - |1_A\rangle)$. Ensuite elle transmet le qubit transformé $|\psi'_A\rangle$ à Bob.
- Si elle veut transmettre **Blanc/1.1**, elle applique la porte X à $|\psi_A\rangle$ ce qui donne $\frac{1}{\sqrt{2}}(|1_A\rangle + |0_A\rangle)$, suivie de la porte Z ce qui donne $|\psi'_A\rangle = \frac{1}{\sqrt{2}}(-|1_A\rangle + |0_A\rangle)$. Ensuite elle transmet le qubit transformé $|\psi'_A\rangle$ à Bob.

Etape 3: Décodage de Bob

Bob reçoit deux qubits :

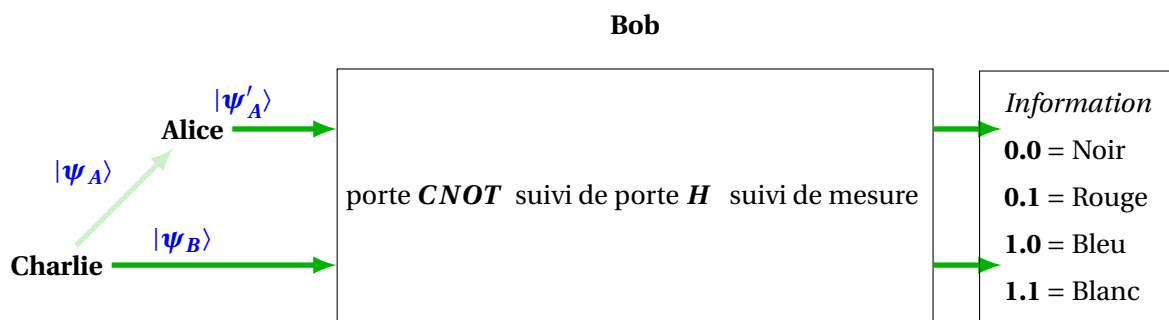
- le qubit transformé $|\psi'_A\rangle$ envoyé par Alice,
- le qubit $|\psi_B\rangle = \frac{1}{\sqrt{2}}|0_B\rangle + \frac{1}{\sqrt{2}}|1_B\rangle$ préparé par Charlie.



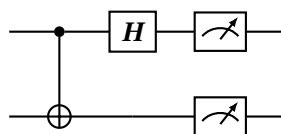
Attention :

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** ou **1.1** (pour Noir, Rouge, Bleu, Blanc).



Voici le circuit quantique du décodage de Bob :



Cas de Noir/0.0 : Bob reçoit $|\psi'_A\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$. Mais n'oublions pas que les deux qubits $|\psi_A\rangle$ et $|\psi_B\rangle$ sont intriqués. Ainsi Bob a en main le 2-qubit

$$\frac{1}{\sqrt{2}}(|0_A \cdot 0_B\rangle + |1_A \cdot 1_B\rangle)$$

Il applique ensuite une porte **CNOT** :

$$\frac{1}{\sqrt{2}}(|0_A \cdot 0_B\rangle + |1_A \cdot 1_B\rangle) \xrightarrow{\text{CNOT}} \text{CNOT}\left(\frac{1}{\sqrt{2}}|0_A \cdot 0_B\rangle\right) + \text{CNOT}\left(\frac{1}{\sqrt{2}}|1_A \cdot 1_B\rangle\right) = \frac{1}{\sqrt{2}}|0_A \cdot 0_B\rangle + \frac{1}{\sqrt{2}}|1_A \cdot 0_B\rangle.$$

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

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

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 : Bob reçoit $\frac{1}{\sqrt{2}}(|1_A\rangle + |0_A\rangle)$. Mais pour l'état de Bell $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A \cdot 0_B\rangle + |1_A \cdot 1_B\rangle)$ initial, cette transformation correspond au nouvel état

$$\frac{1}{\sqrt{2}}(|1_A \cdot 0_B\rangle + |0_A \cdot 1_B\rangle)$$

Il applique ensuite une porte **CNOT**, suivie d'une porte **H** sur le premier qubit (indexé par *A*) :

$$\begin{aligned} \frac{1}{\sqrt{2}}(|1_A \cdot 0_B\rangle + |0_A \cdot 1_B\rangle) &\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}|1_A \cdot 1_B\rangle + \frac{1}{\sqrt{2}}|0_A \cdot 1_B\rangle \\ &\xrightarrow{H_A} \frac{1}{2}(|0_A - 1_A\rangle \cdot 1_B) + \frac{1}{2}(|0_A + 1_A\rangle \cdot 1_B) = |0_A \cdot 1_B\rangle. \end{aligned}$$

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

Cas de Bleu/0.1 : Bob reçoit $\frac{1}{\sqrt{2}}(|0_A\rangle - |1_A\rangle)$. Mais pour l'état de Bell $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A \cdot 0_B\rangle + |1_A \cdot 1_B\rangle)$ initial, cette transformation correspond au nouvel état

$$\frac{1}{\sqrt{2}}(|0_A \cdot 0_B\rangle - |1_A \cdot 1_B\rangle)$$

Il applique ensuite une porte **CNOT**, suivie d'une porte **H** sur le premier qubit (indexé par *A*) :

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0_A \cdot 0_B\rangle - |1_A \cdot 1_B\rangle) &\xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}}|0_A \cdot 0_B\rangle - \frac{1}{\sqrt{2}}|1_A \cdot 0_B\rangle \\ &\xrightarrow{H_A} \frac{1}{2}(|0_A + 1_A\rangle \cdot 0_B) - \frac{1}{2}(|0_A - 1_A\rangle \cdot 0_B) = |1_A \cdot 0_B\rangle. \end{aligned}$$

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

Cas de Blanc/1.1 : Bob reçoit $|\psi'_A\rangle = \frac{1}{\sqrt{2}}(-|1_A\rangle + |0_A\rangle)$. Mais pour l'état de Bell $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$ initial, cette transformation correspond au nouvel état

$$\frac{1}{\sqrt{2}}(-|1_A 0_B\rangle - |0_A 1_B\rangle)$$

Il applique ensuite une porte **CNOT**, suivie d'une porte **H** sur le premier qubit (indexé par **A**) :

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

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

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.