Chapitre 1 : Bases de l'informatique quantique

ENSIIE - Informatique quantique pour la recherche opérationnelle

Dimitri Watel (dimitri.watel@ensiie.fr)

2022

Plan

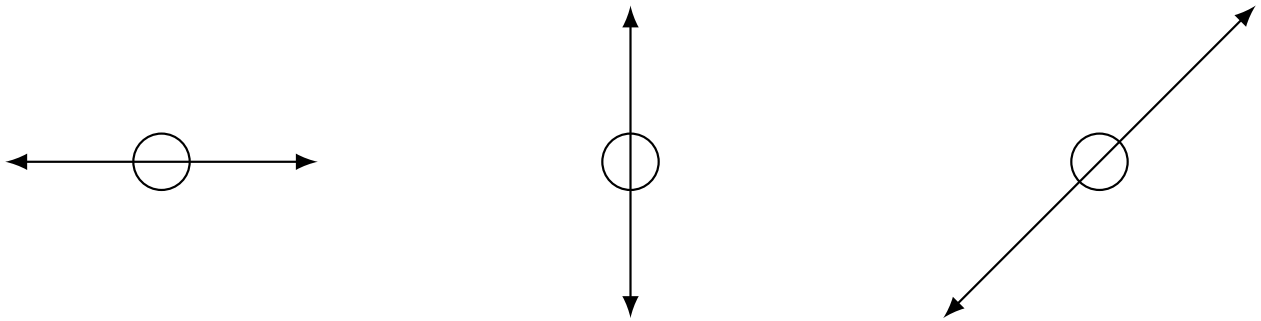
1 Introduction

2 Qbits et algèbre linéaire

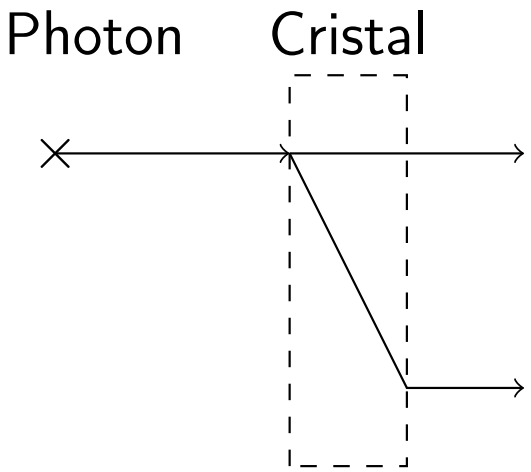
Quelques concepts de mécanique quantique

Spin

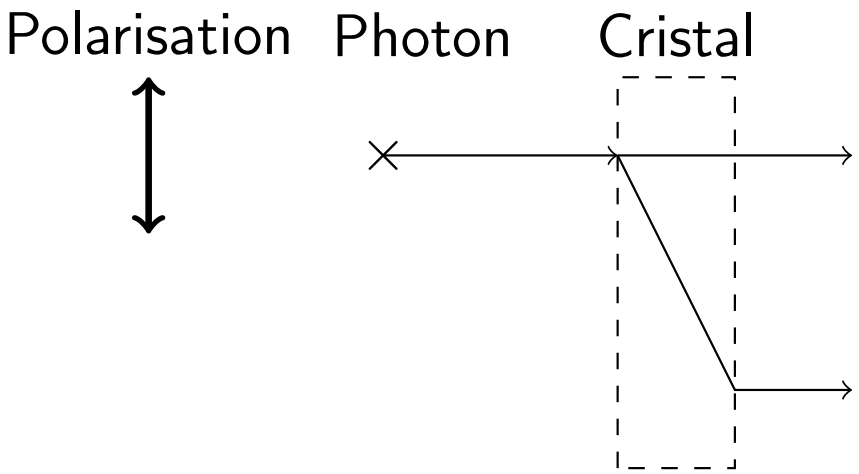
Une particule possède une orientation naturelle représentée par un angle.



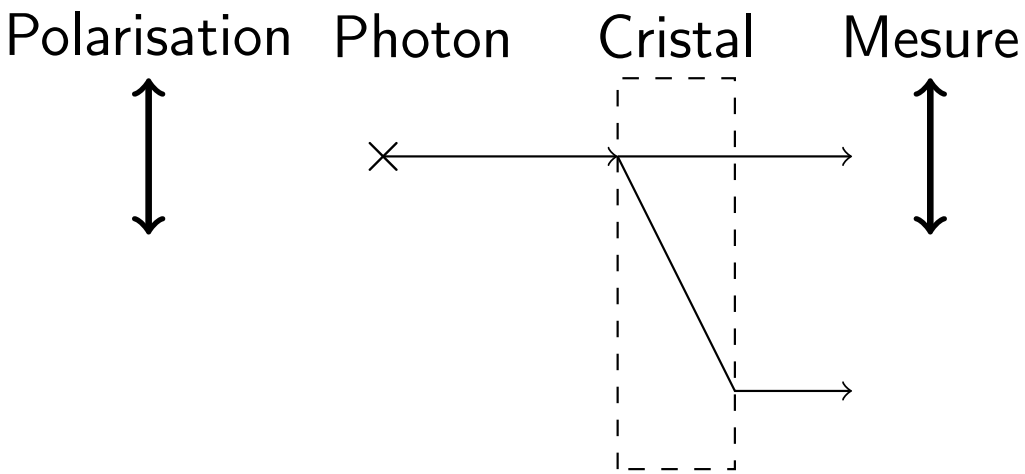
Cristal de calcite



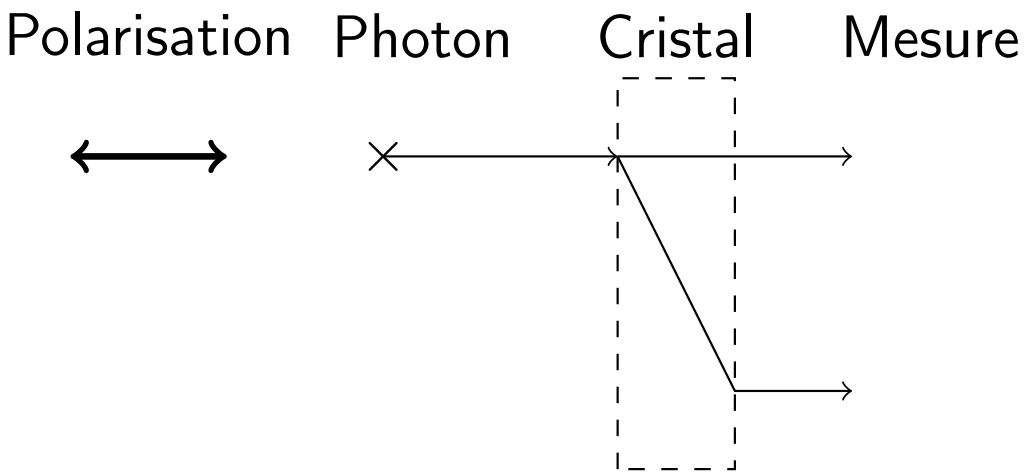
Cristal de calcite



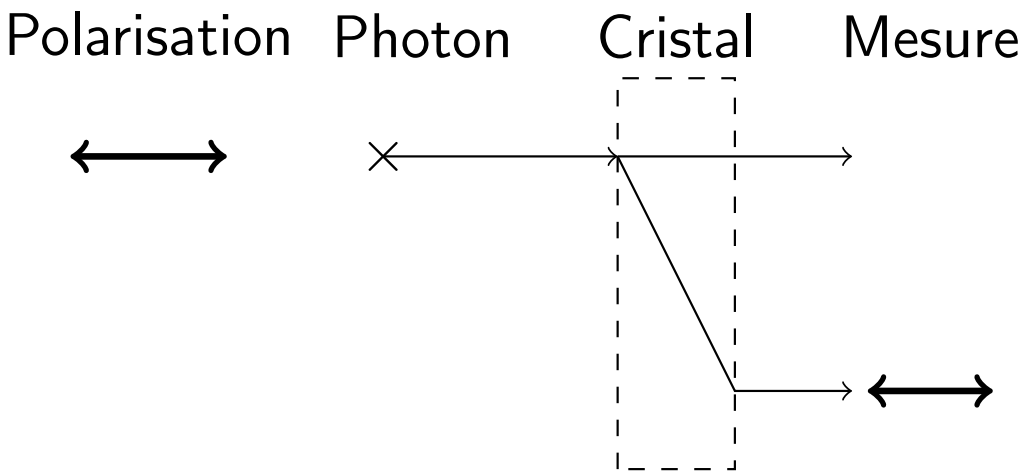
Cristal de calcite



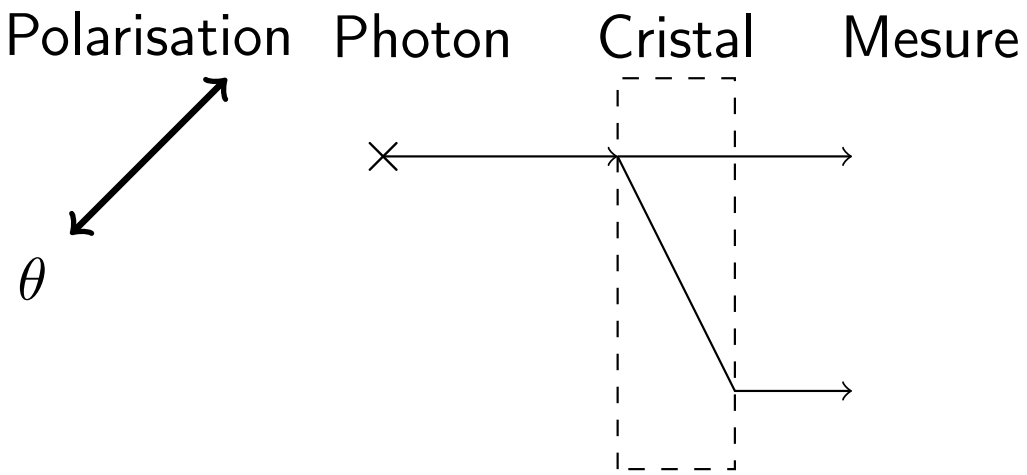
Cristal de calcite



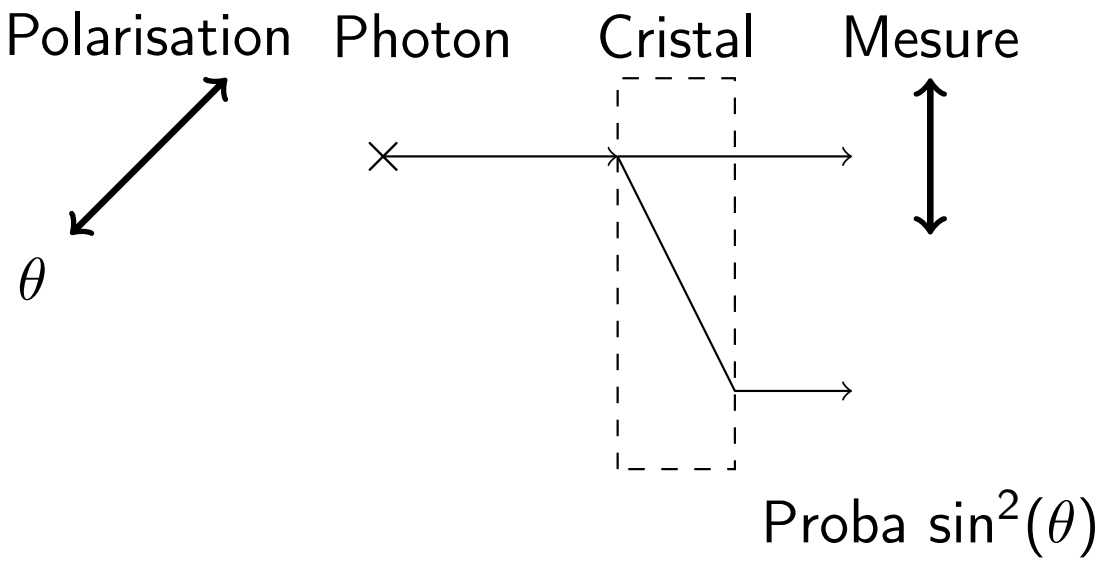
Cristal de calcite



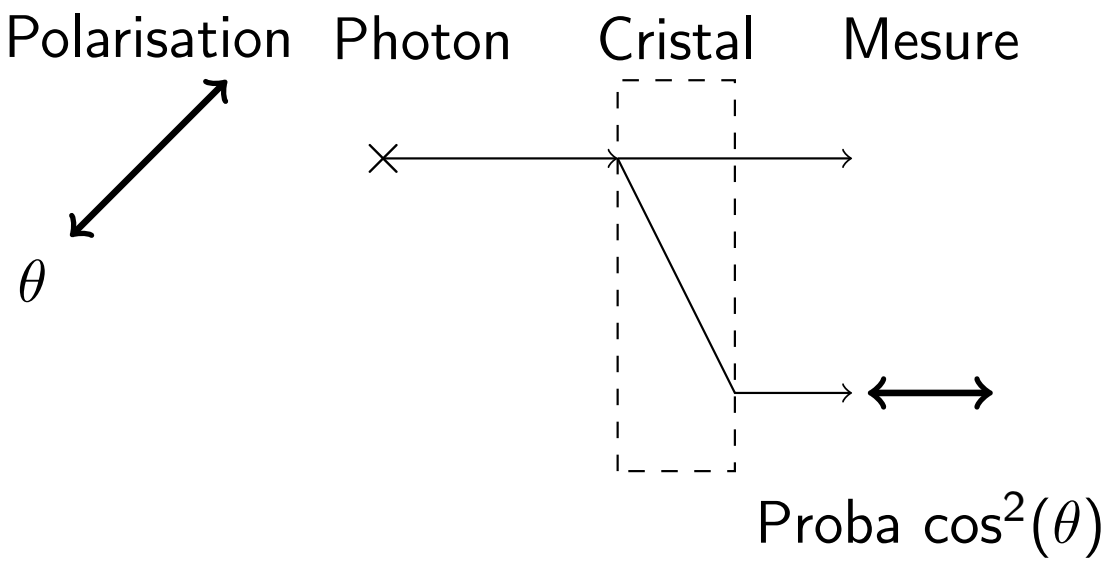
Cristal de calcite



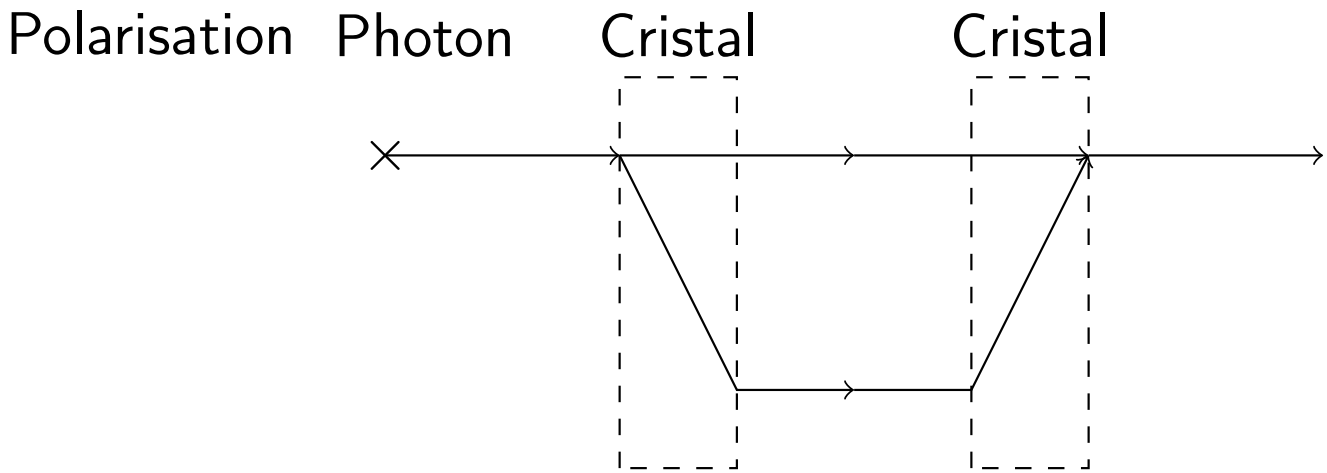
Cristal de calcite



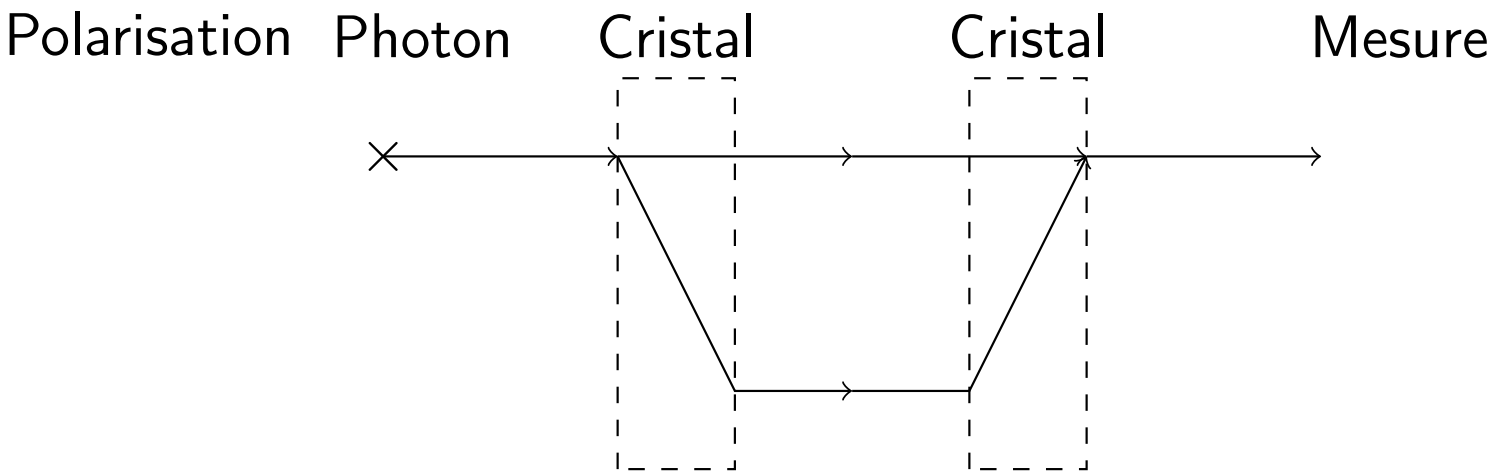
Cristal de calcite



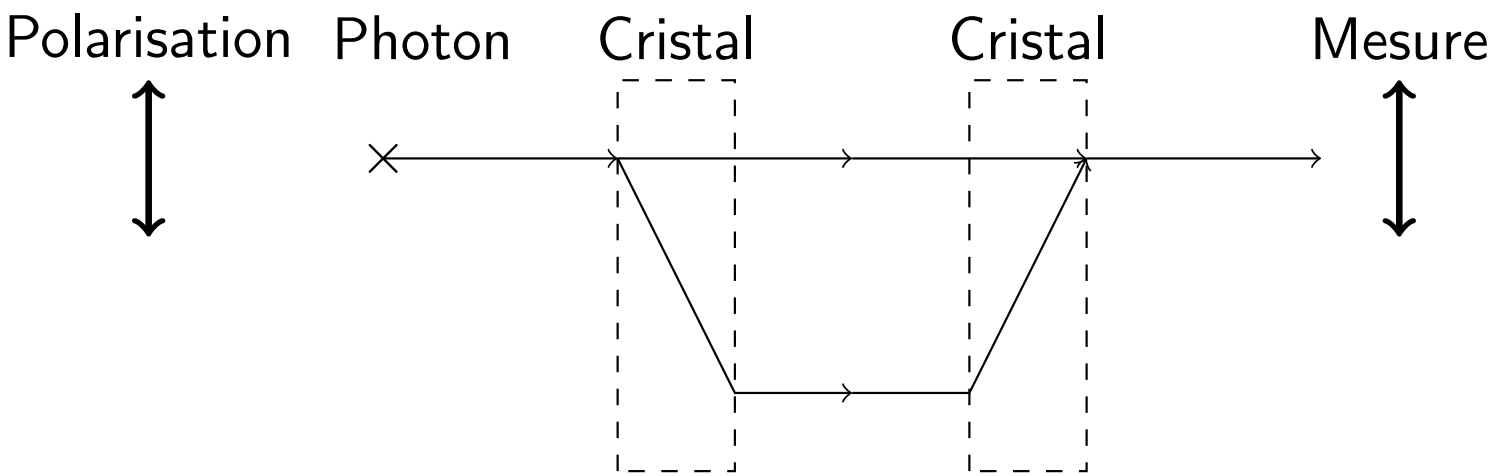
Cristal de calcite



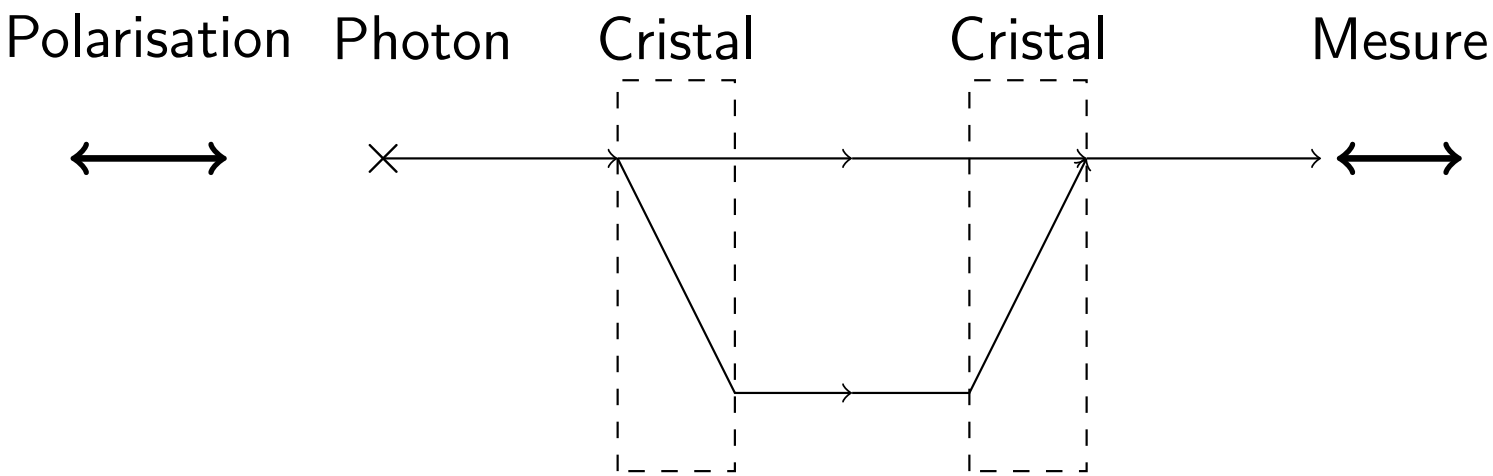
Cristal de calcite



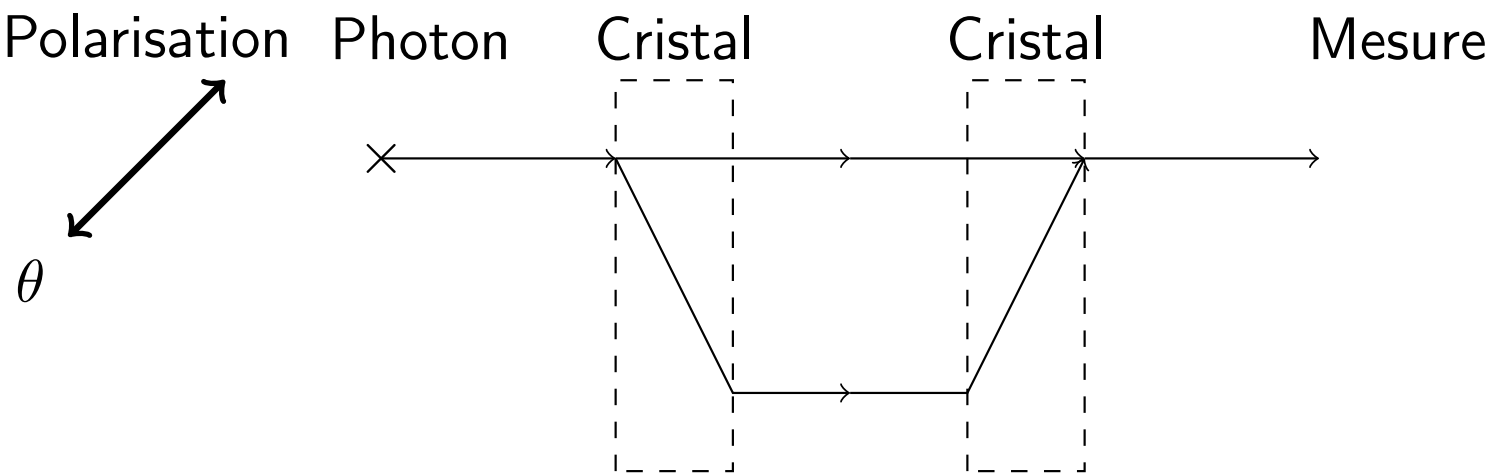
Cristal de calcite



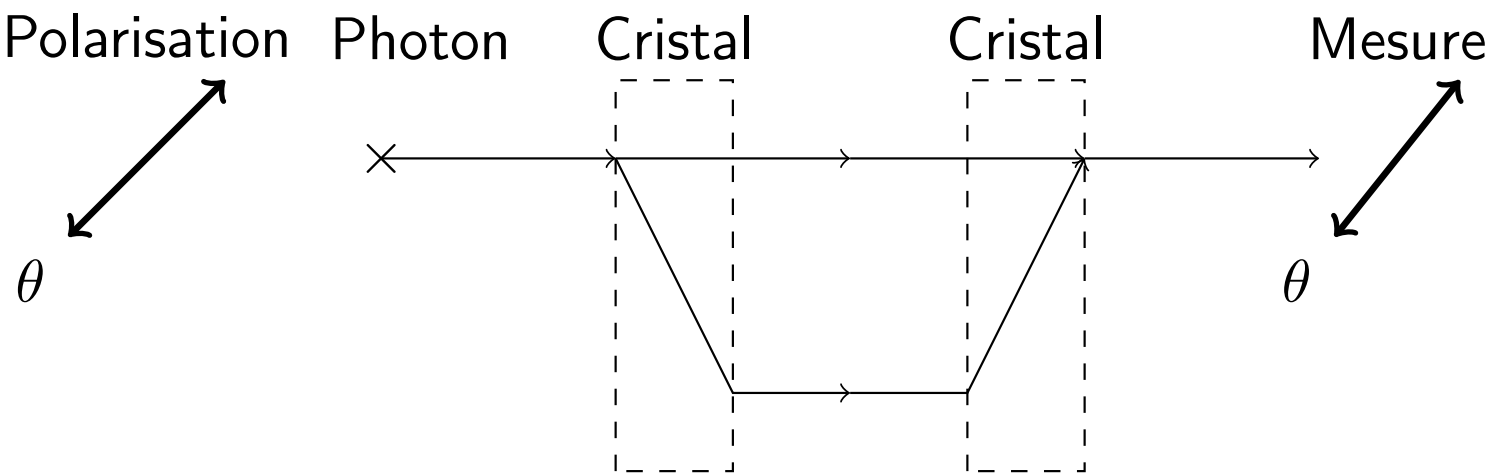
Cristal de calcite



Cristal de calcite



Cristal de calcite



Paradoxe : où est passé le photon ?

Un qbit

Définition

Un *qbit* $|\varphi\rangle$ est une superposition de deux états, les états $|0\rangle$ et $|1\rangle$. Il existe $\alpha, \beta \in \mathbb{C}$ tels que

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

Par exemple

$$\alpha = 1 \text{ et } \beta = 0 \qquad |\varphi\rangle = |0\rangle$$

$$\alpha = 0 \text{ et } \beta = -2i \qquad |\varphi\rangle = -2i\,|1\rangle$$

$$\alpha = \frac{2}{\sqrt{2}} \text{ et } \beta = \frac{-2i}{\sqrt{2}} \qquad |\varphi\rangle = \frac{2}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$$

Un qbit : norme

Définition

La *norme* d'un qbit $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ est

$$\||\varphi\rangle\| = \sqrt{|\alpha|^2 + |\beta|^2}$$

Par exemple

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

Un ordinateur quantique manipule des qbits de norme 1.

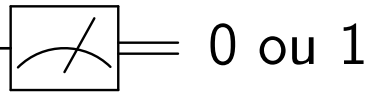
Propriétés des qbits : mesure

Mesure et effondrement

On peut *mesurer* un qbit $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ tel que $\||\varphi\rangle\| = 1$. On obtient alors

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

$|\varphi\rangle$ s'effondre alors sur $|0\rangle$ ou $|1\rangle$ selon le cas, une seconde mesure donnera toujours le même résultat que la première.

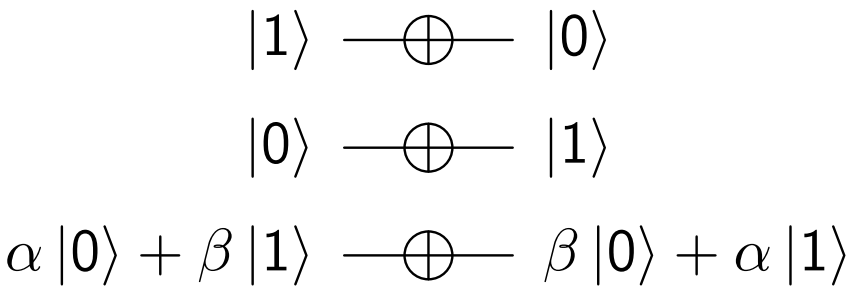
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  0 ou 1 avec une proba $\frac{1}{2}$

Porte quantique

Definition

Une *porte quantique* est un opérateur qui transforme un qbit en un autre qbit tel que . . . *(on verra plus tard)*

Exemples :
Porte X (ou NOT)



Porte quantique

Definition

Une *porte quantique* est un opérateur qui transforme un qbit en un autre qbit tel que . . . *(on verra plus tard)*

Exemples :

Porte de Hadamard

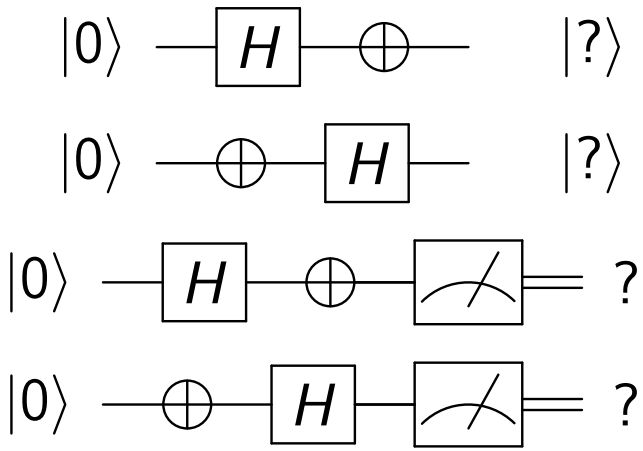
$$|0\rangle \;\text{—}\boxed{H}\text{—}\; \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \;\text{—}\boxed{H}\text{—}\; \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \;\text{—}\boxed{H}\text{—}\; |0\rangle$$

Exemple de circuit quantique

Définition

Un *circuit quantique* est une succession de portes quantiques.

Que renvoient les 4 circuits suivants ?



Un 2-qbit

Définition

Un *2-qbit* $|\varphi\rangle$ est une superposition de quatre états, $|00\rangle$, $|01\rangle$, $|10\rangle$ et $|11\rangle$.
Il existe $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ tels que

$$|\varphi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

$$\||\varphi\rangle\| = \sqrt{|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2}$$

On peut mesurer ce qbit si $\||\varphi\rangle\| = 1$. On obtient alors

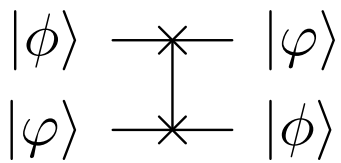
- 00 avec une probabilité $|\alpha|^2$
- 01 avec une probabilité $|\beta|^2$
- 10 avec une probabilité $|\gamma|^2$
- 11 avec une probabilité $|\delta|^2$

Porte quantique

Definition

Certaines portes quantiques agissent sur des 2-qbits.

Exemples :
Porte SWAP

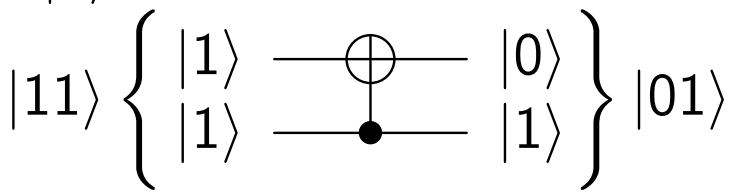


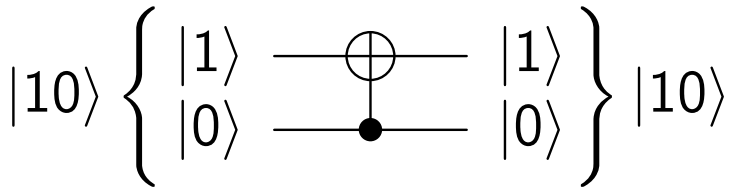
Porte quantique

Definition

Certaines portes quantiques agissent sur des 2-qbits.

Exemples :
Porte Controlled-NOT (CNOT ou CX) : inverse le qbit marqué $\oplus$ si le qbit marqué $\bullet$ est $|1\rangle$.





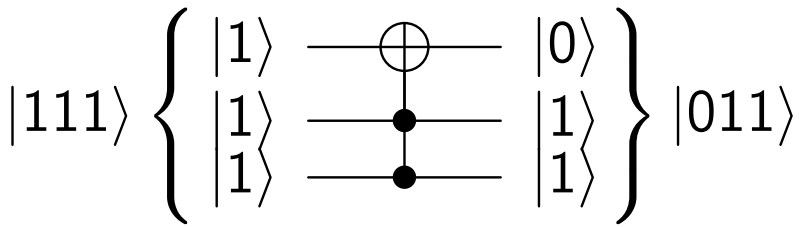
Porte quantique

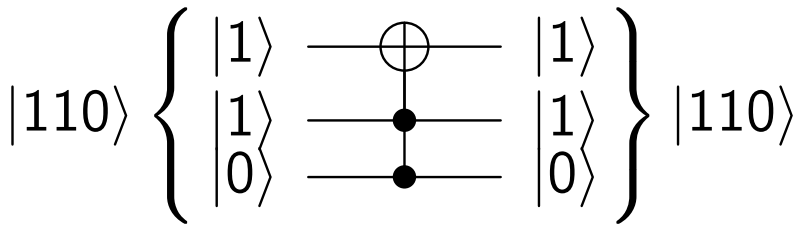
Definition

Certaines portes quantiques agissent sur des 3-qbits.

Exemples :

Porte de Toffoli (ou CCNOT ou CCX) : inverse le qbit marqué $\oplus$ si les qbits marqués $\bullet$ sont $|1\rangle$ tous les deux.



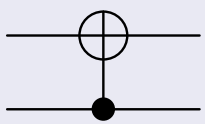


Un avantage indéniable au quantique

Plusieurs calculs en une seule opération élémentaire

Le circuit suivant effectue les deux calculs de la porte CNOT en une seule fois.

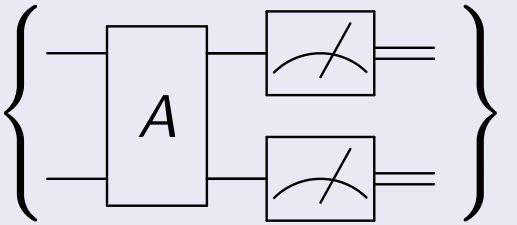
$$\frac{1}{\sqrt{2}}(|11\rangle + |10\rangle) \left\{ \quad \right\} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$



Un désavantage indéniable au quantique

Mesure d'un seul résultat à la fois

Imaginons le circuit suivant :

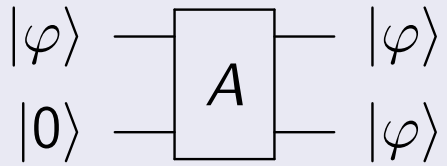
$$\frac{1}{\sqrt{2}}(|11\rangle + |10\rangle)$$  01 ou 10 avec proba $\frac{1}{2}$

- On peut observer expérimentalement les sorties : on voit que A envoie parfois 01 et parfois 10 (avec une proba proche de 1/2)
- **Impossible**, sans plus d'information, de déterminer le qbit renvoyé par A :
  $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ ou $\frac{-i}{\sqrt{2}}(|01\rangle + |10\rangle)$ ou $\frac{1}{\sqrt{2}}|01\rangle + \frac{1+i}{2}|10\rangle$?

Un (autre) désavantage indéniable au quantique

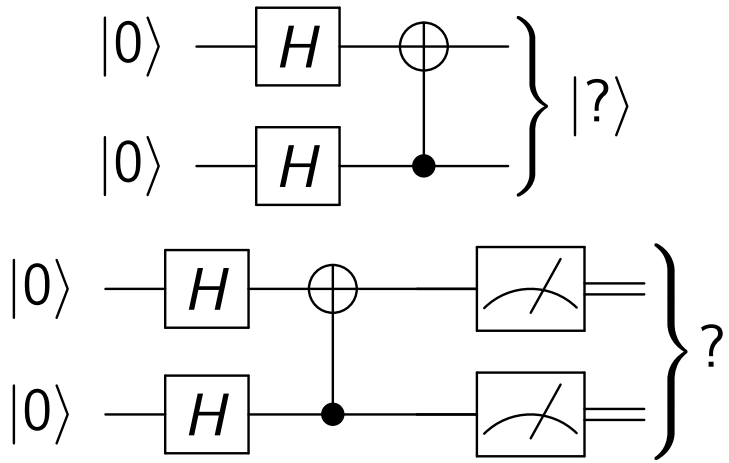
Impossible de cloner un qbit

Il n'existe pas de porte A dont le résultat serait le suivant quel que soit $|\varphi\rangle$:



Exemple de circuit

Que renvoient les circuits suivants ?



qbits équivalents

Définition expérimentale

Deux qbits sont dits équivalents si une mesure physique ne peut les distinguer.

Par exemple

- $|0\rangle$ et $i \cdot |0\rangle$
- $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et $\frac{-1}{\sqrt{2}}|00\rangle + \frac{1+i}{2}|11\rangle)$

qbits équivalents

Définition formelle

Deux qbits $|\varphi\rangle$ et $|\varphi'\rangle$ sont dits équivalents si $|\varphi\rangle = e^{i\theta} |\varphi'\rangle$

Théorème

Pout tout qbit $|\varphi\rangle$, il existe θ et ϕ tels que $|\varphi\rangle$ est équivalent $\cos(\frac{\theta}{2}) |0\rangle + \sin(\frac{\theta}{2}) \cdot e^{i\phi} |1\rangle$.

Approcher θ et φ

$|\varphi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ est équivalent $\cos(\frac{\theta}{2})\,|0\rangle + \sin(\frac{\theta}{2}) \cdot e^{i\phi}\,|1\rangle$

Approcher θ

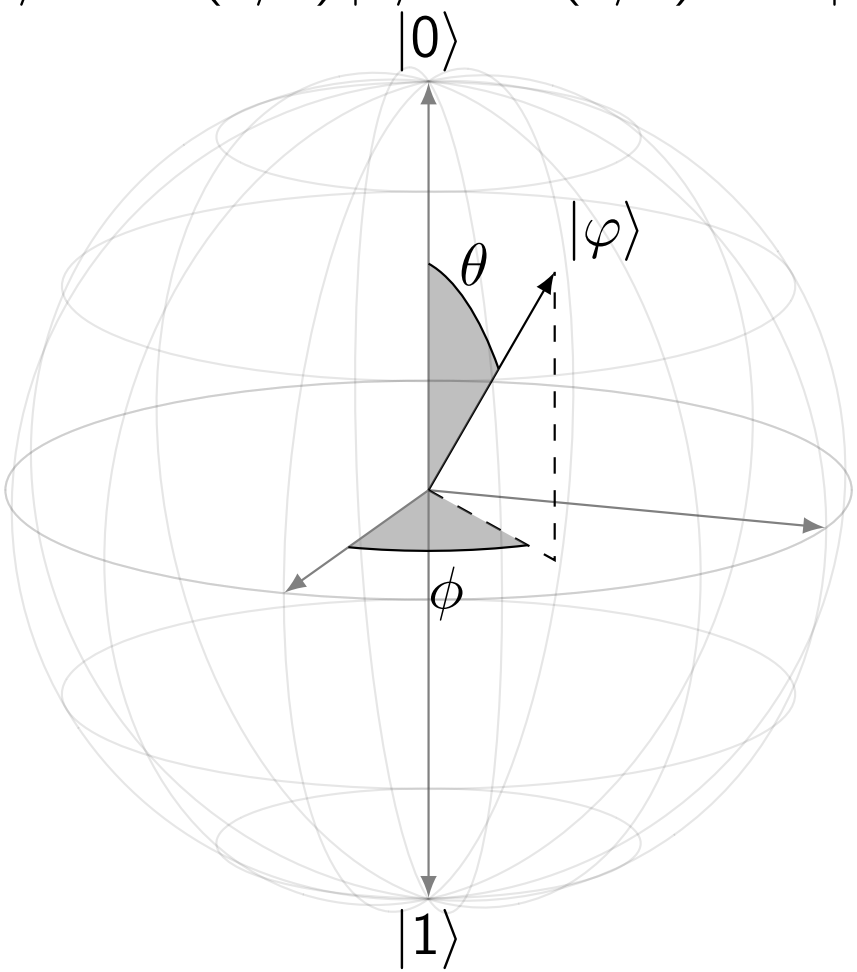
Mesurer $|\varphi\rangle$ de nombreuses fois donne une approximation statistique de $|\alpha|^2$ et $|\beta|^2$ dont on déduit $\cos(\frac{\theta}{2})$ et $\sin(\frac{\theta}{2})$.

Approcher ϕ

? ? ?

Sphère de bloch

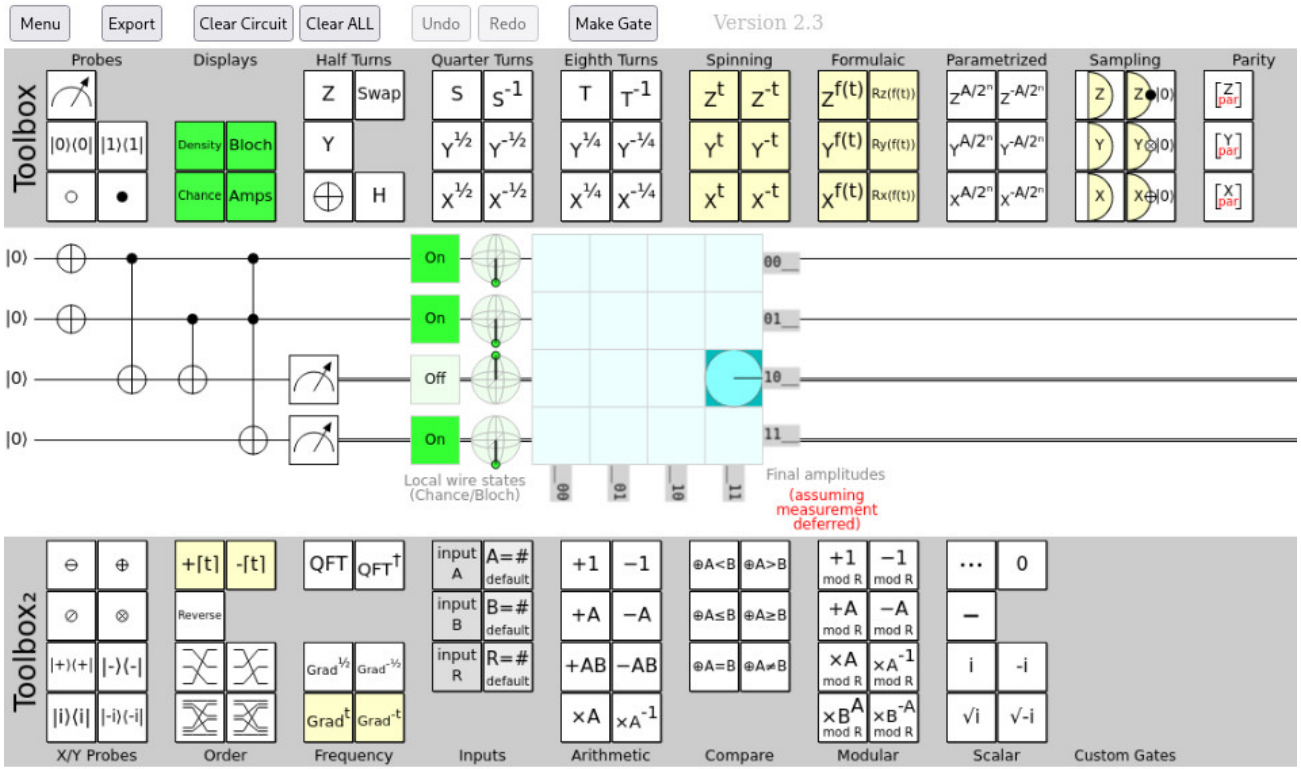
$$|\varphi\rangle \simeq \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\cdot e^{i\phi}\,|1\rangle$$



Manipulation graphique de circuits

Quirk

Quirk est un outil graphique fonctionnant en local dans le navigateur.



Plan

1 Introduction

2 Qbits et algèbre linéaire

Un qbit : notation vectorielle

Définition alternative

Un qbit $|\varphi\rangle$ est un vecteur de $\mathbb{C}^2$.
Il existe $\alpha, \beta \in \mathbb{C}$ tels que

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

Par exemple

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

$$-2i\,|1\rangle = \begin{pmatrix} 0 \\ -2i \end{pmatrix}$$

$$\frac{2}{\sqrt{2}}(|0\rangle - i\,|1\rangle) = \begin{pmatrix} 2/\sqrt{2} \\ -2i/\sqrt{2} \end{pmatrix}$$

Propriétés des qbits : linéarité

Linéarité

On peut additionner des qbits :

- $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- $|\varphi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$
- $a, b \in \mathbb{C}$

$$a \cdot |\phi\rangle + b \cdot |\varphi\rangle = (a \cdot \alpha + b \cdot \gamma)\,|0\rangle + (a \cdot \beta + b \cdot \delta)\,|1\rangle$$

L'ensemble des qbits est l'espace vectoriel $(\mathbb{C}^2, +, \cdot)$.

Produit scalaire de qbits

Définition

Le produit scalaire des qbits :

- $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- $|\varphi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$

est

$$\langle\phi|\varphi\rangle = \alpha^*\gamma + \beta^*\delta$$

où x^* est le conjugé de x.

On peut aussi noter le vecteur $\langle\phi| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix} = \begin{pmatrix}\alpha^* \\ \beta^*\end{pmatrix}^t = |\phi\rangle^\dagger$.

$\langle\phi|\varphi\rangle$ est alors le produit matriciel de $\langle\phi|$ et $|\varphi\rangle$.
On peut noter que $\||\phi\rangle\| = \sqrt{\langle\phi|\phi\rangle}$.

n-qbits

Définition

Un n-qbit est une superposition de 2^n états, les états $|0\ldots000\rangle$, $|0\ldots001\rangle$, $|0\ldots010\rangle$, $|0\ldots011\rangle$, ..., et $|1\ldots111\rangle$. Il existe $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1} \in \mathbb{C}$ tels que

$$|\varphi\rangle = \alpha_0 \cdot |0\ldots000\rangle + \alpha_1 \cdot |0\ldots001\rangle + \cdots + \alpha_{2^n-1} \cdot |1\ldots111\rangle$$

On peut aussi noter

$$|\varphi\rangle = \alpha_0 \cdot |\underline{0}\rangle + \alpha_1 \cdot |\underline{1}\rangle + \cdots + \alpha_{2^n-1} \cdot |\underline{2^n-1}\rangle$$

avec $\underline{i}$ la représentation binaire de i avec n bits.

Par exemple

$$|\varphi\rangle = |0\ldots100\rangle$$

$$|\varphi\rangle = i\,|0\ldots000\rangle + \frac{1+i}{\sqrt{2}}\,|0\ldots010\rangle \qquad |\varphi\rangle = \sum_{i=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \cdot |\underline{i}\rangle$$

n-qbits

Définition

Un n-qbit est une superposition de 2^n états, les états $|0\ldots000\rangle$, $|0\ldots001\rangle$, $|0\ldots010\rangle$, $|0\ldots011\rangle$, ..., et $|1\ldots111\rangle$. Il existe $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1} \in \mathbb{C}$ tels que

$$|\varphi\rangle = \alpha_0 \cdot |0\ldots000\rangle + \alpha_1 \cdot |0\ldots001\rangle + \cdots + \alpha_{2^n-1} \cdot |1\ldots111\rangle$$

On peut aussi noter

$$|\varphi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \cdots \\ \alpha_{2^n-1} \end{pmatrix}$$

Par exemple

$$|\varphi\rangle = |0\ldots100\rangle$$

$$|\varphi\rangle = i\,|0\ldots000\rangle + \frac{1+i}{\sqrt{2}}\,|0\ldots010\rangle \qquad |\varphi\rangle = \sum_{i=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \cdot |\underline{i}\rangle$$

Un n-qbit : norme

Définition

La norme d'un n-qbit $|\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot |\underline{i}\rangle$ est

$$\||\varphi\rangle\| = \sqrt{\sum_{i=0}^{2^n-1} |\alpha_i|^2}$$

Par exemple

$$\left\| \sum_{i=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \cdot |\underline{i}\rangle \right\| = 1 \qquad \|-2i\,|0\ldots100\rangle\| = 2$$

$$\|(|00\rangle - i\,|10\rangle + 4\,|11\rangle)\| = \sqrt{18}$$

Un ordinateur quantique manipule des n-qbits de norme 1.

Propriétés des n-qbits : linéarité

Linéarité

On peut additionner des n-qbits :

- $|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot |\underline{i}\rangle$
- $|\varphi\rangle = \sum_{i=0}^{2^n-1} \beta_i \cdot |\underline{i}\rangle$
- $a, b \in \mathbb{C}$

$$a \cdot |\phi\rangle + b \cdot |\varphi\rangle = \sum_{i=0}^{2^n-1} (a \cdot \alpha_i + b \cdot \beta_i) \cdot |\underline{i}\rangle$$

L'ensemble des n-qbits est l'espace vectoriel $(\mathbb{C}^{2^n}, +, \cdot)$.

Produit scalaire de n-qbits

Définition

Le produit scalaire des n-qbits :

- $|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot |\underline{i}\rangle$
- $|\varphi\rangle = \sum_{i=0}^{2^n-1} \beta_i \cdot |\underline{i}\rangle$

est

$$\langle\phi|\varphi\rangle = \langle\phi| \cdot |\varphi\rangle = |\phi\rangle^\dagger \cdot |\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i^* \beta_i$$

On peut noter que $\||\phi\rangle\| = \sqrt{\langle\phi|\phi\rangle}$.

Porte quantique : matrice associée

Définition

Une porte quantique de taille n est un opérateur linéaire qui transforme un n-qbit en un autre n-qbit de même norme.
$\Rightarrow$ Porte = **matrice unitaire** de taille $2^n \times 2^n$.

Définition

Soit $A \in \mathcal{M}_{2^n}(\mathbb{C})$, on note $A^\dagger$ la matrice adjointe (conjuguée de la transposée).

A est unitaire si et seulement si $A^\dagger A = I$.

Exemple :

$$A = \frac{1}{2}\begin{pmatrix} 2i & 0 & 0 \\ 0 & 1+i & 1-i \\ 0 & 1-i & 1+i \end{pmatrix} \quad A^\dagger = \frac{1}{2}\begin{pmatrix} -2i & 0 & 0 \\ 0 & 1-i & 1+i \\ 0 & 1+i & 1-i \end{pmatrix} \quad A^\dagger A = I_3$$

Appliquer une porte quantique

- $|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$
- $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, une porte quantique

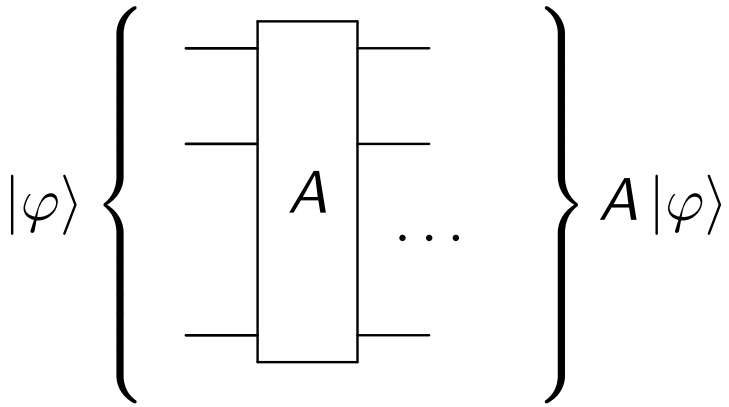
$$|\varphi\rangle \; \boxed{A} \; A|\varphi\rangle$$

$$A|\varphi\rangle = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \cdot a_1 + \beta \cdot a_2 \\ \alpha \cdot a_3 + \beta \cdot a_4 \end{pmatrix}$$
$$= (\alpha \cdot a_1 + \beta \cdot a_2)|0\rangle + (\alpha \cdot a_3 + \beta \cdot a_4)|1\rangle$$

$$|0\rangle \; \boxed{A} \; A|0\rangle = a_1|0\rangle + a_3|1\rangle$$
$$|1\rangle \; \boxed{A} \; A|1\rangle = a_2|0\rangle + a_4|1\rangle$$
$$|\varphi\rangle \; \boxed{A} \; \alpha A|0\rangle + \beta A|1\rangle$$

Appliquer une porte quantique

- $|\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot |\underline{i}\rangle$
- A, une porte quantique de taille $2^n \times 2^n$

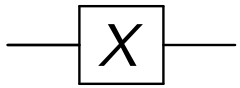
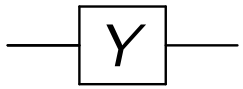


$$A|\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot A|\underline{i}\rangle$$

Porte quantique : exemples

-  $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ Porte de Hadamard

Portes de Pauli

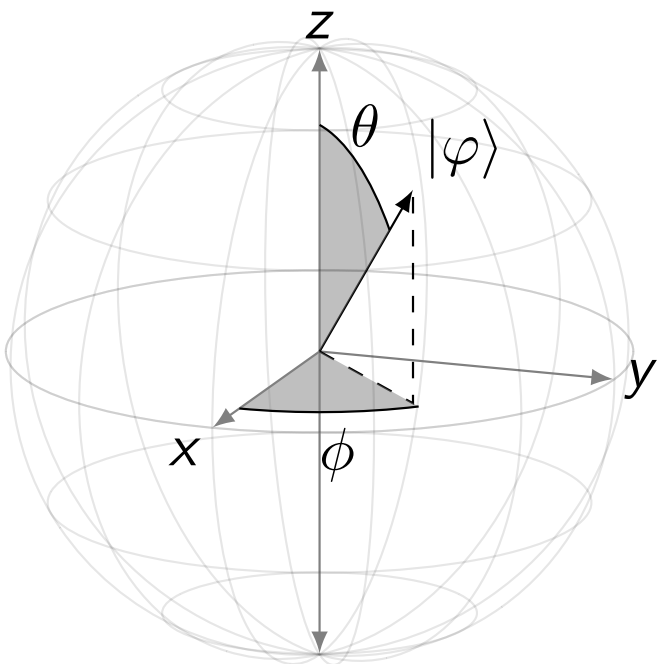
-  $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ Porte X
-  $\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$ Porte Y
-  $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$ Porte Z

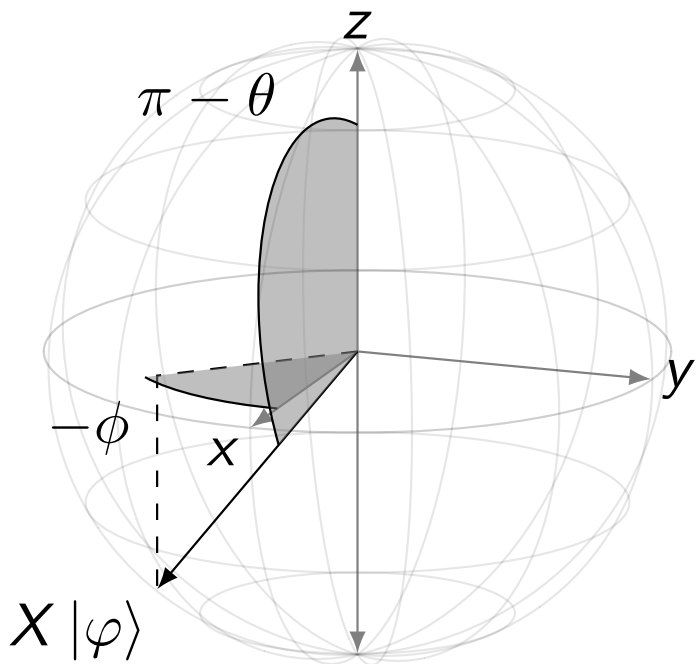
Apparté : effet des portes de Pauli sur la sphère de Bloch

$$|\varphi\rangle \simeq \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\cdot e^{i\phi}\,|1\rangle$$

$$X\,|\varphi\rangle \simeq \sin(\theta/2)\cdot e^{i\phi}\,|0\rangle + \cos(\theta/2)\,|1\rangle$$

$$X\,|\varphi\rangle \simeq \cos(\pi/2-\theta/2)\,|0\rangle + \sin(\pi/2-\theta/2)\cdot e^{-i\phi}\,|1\rangle$$



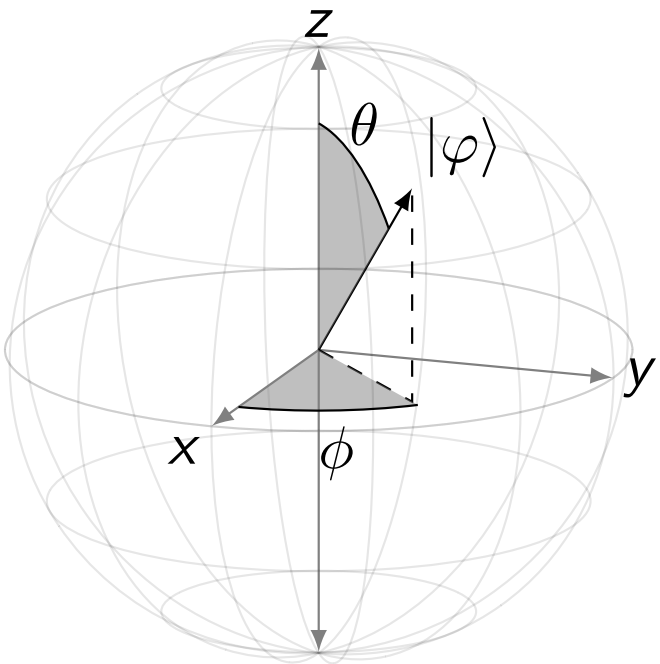


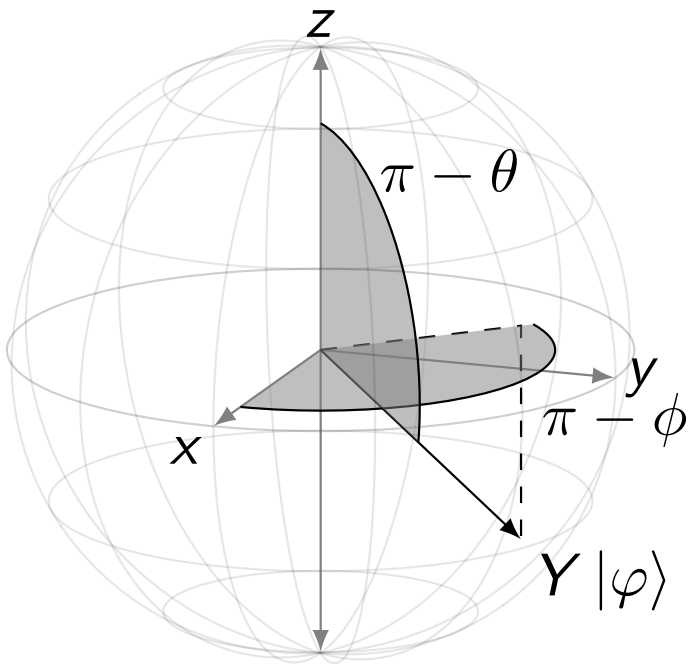
Apparté : effet des portes de Pauli sur la sphère de Bloch

$$|\varphi\rangle \simeq \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\cdot e^{i\phi}\,|1\rangle$$

$$Y\,|\varphi\rangle \simeq i\sin(\theta/2)\cdot e^{i\phi}\,|0\rangle + -i\cos(\theta/2)\,|1\rangle$$

$$Y\,|\varphi\rangle \simeq \cos(\pi/2-\theta/2)\,|0\rangle + \cos(\pi/2-\theta/2)\cdot e^{i\cdot(\pi-\phi)}\,|0\rangle$$



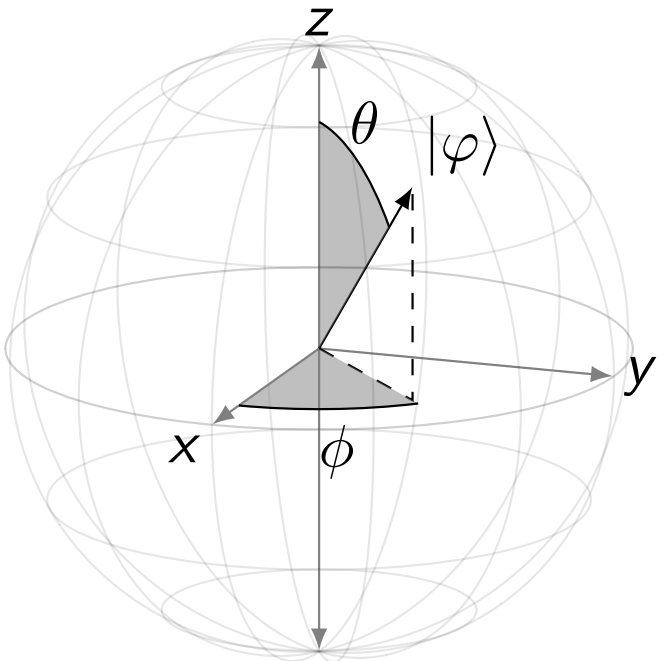


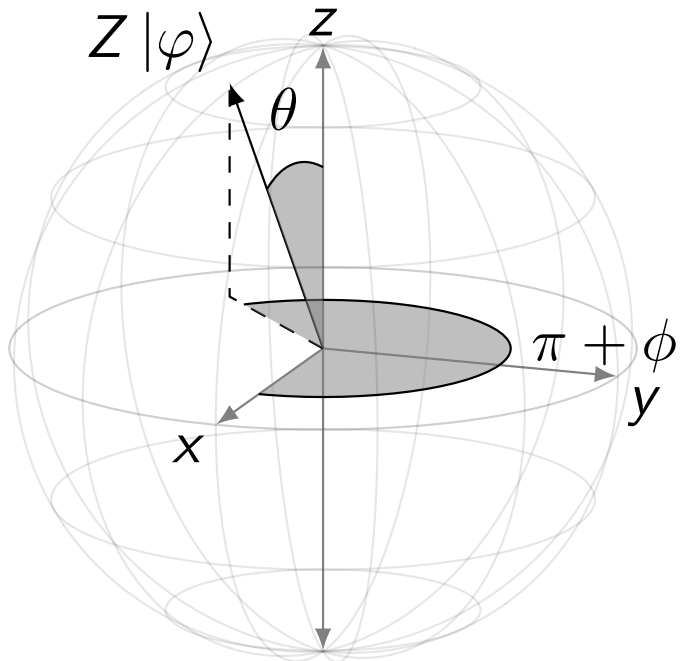
Apparté : effet des portes de Pauli sur la sphère de Bloch

$$|\varphi\rangle \simeq \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\cdot e^{i\phi}\,|1\rangle$$

$$Z\,|\varphi\rangle \simeq \cos(\theta/2)\,|0\rangle - \sin(\theta/2)\cdot e^{i\phi}\,|1\rangle$$

$$Z\,|\varphi\rangle \simeq \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\cdot e^{\pi+i\phi}\,|1\rangle$$





Exercice

Montrez, en calculant les angles θ et ϕ de $H|\varphi\rangle$, que H est équivalent à une rotation selon l'axe Y de $\frac{\pi}{2}$ puis une rotation selon l'axe X de π.

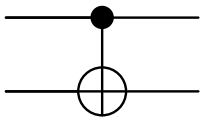
Propriété utile des portes quantiques

Propriétés

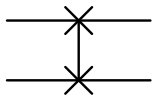
Une matrice unitaire préserve le produit scalaire de deux qbits.

Porte quantique : exemples

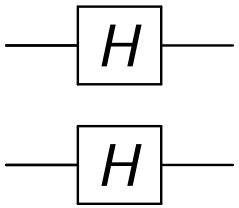
- Porte CNOT : $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$



- Porte SWAP : $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$



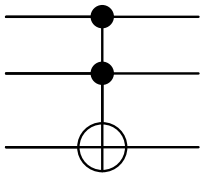
- Porte $H^{\otimes 2}$: $\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$



Porte quantique : exemples

- Porte de Toffoli :

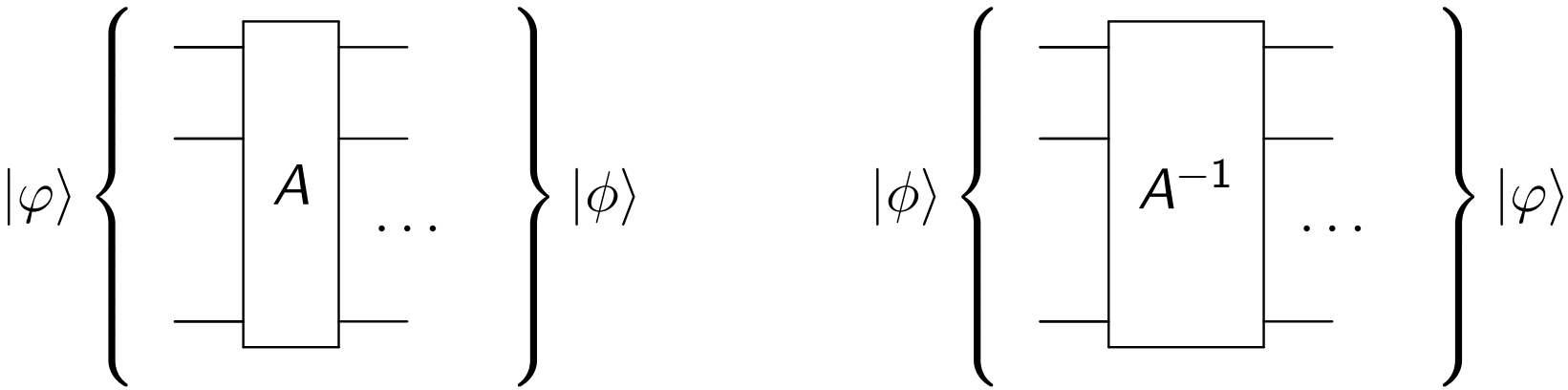
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$



Réversibilité des circuits quantiques

Soit

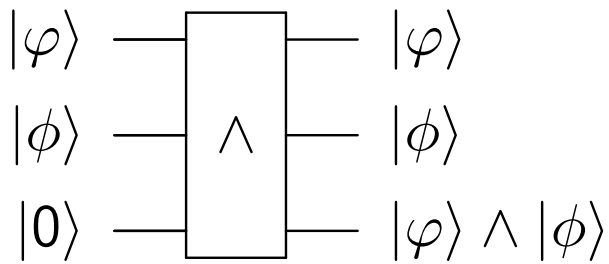
- A, une porte quantique de taille $2^n \times 2^n$
- telle que $A|\varphi\rangle = |\phi\rangle$



Tout circuit est réversible.

Conséquence de la réversibilité

La porte ET classique n'est pas réversible. Donc une porte ET quantique doit envoyer plus d'information en sortie que le résultat. Par exemple



(Cette porte est exactement la porte de Toffoli.)

Propriétés des qbits : produit de qbits

Produit tensoriel

On peut multiplier des qbits :

- $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- $|\varphi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$

$$|\phi\rangle \otimes |\varphi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \otimes \begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \begin{pmatrix}\alpha\cdot\gamma\\ \alpha\cdot\delta\\ \beta\cdot\gamma\\ \beta\cdot\delta\end{pmatrix}$$

$$= \alpha\cdot\gamma\cdot|00\rangle + \alpha\cdot\delta\cdot|01\rangle + \beta\cdot\gamma\cdot|10\rangle + \beta\cdot\delta\cdot|11\rangle$$

Un produit de qbits donne un 2-qbit.

Propriétés des qbits : produit de qbits

Voir le produit tensoriel sous forme de produit terme à terme

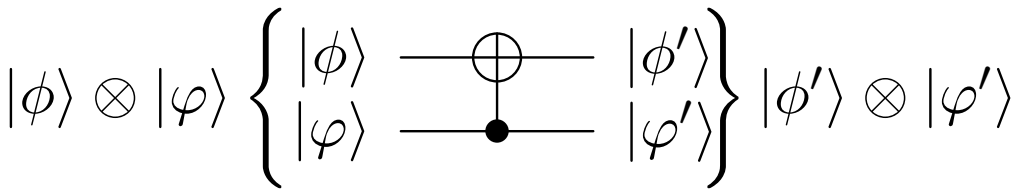
$$|0\rangle \otimes |0\rangle = |00\rangle$$
$$|0\rangle \otimes |1\rangle = |01\rangle$$
$$|1\rangle \otimes |0\rangle = |10\rangle$$
$$|1\rangle \otimes |1\rangle = |11\rangle$$

Donc

$$\begin{aligned}|\phi\rangle \otimes |\varphi\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \\ &= \alpha \cdot \gamma \cdot |0\rangle \otimes |0\rangle + \alpha \cdot \delta \cdot |0\rangle \otimes |1\rangle \\ &+ \beta \cdot \gamma \cdot |1\rangle \otimes |0\rangle + \beta \cdot \delta \cdot |1\rangle \otimes |1\rangle \\ &= \alpha \cdot \gamma \cdot |00\rangle + \alpha \cdot \delta \cdot |01\rangle + \beta \cdot \gamma \cdot |10\rangle + \beta \cdot \delta \cdot |11\rangle\end{aligned}$$

Propriétés des qbits : dessin d'un produit

Les circuits à 2 lignes représentent **souvent** un produits de 2 qbits.
(mais pas tout le temps, on y reviendra)



Propriétés des n-qbits : produit de qbits

Produit tensoriel

On peut multiplier un n-qbit et un m-qbit :

- $|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot |\underline{i}\rangle$
- $|\varphi\rangle = \sum_{i=0}^{2^m-1} \beta_i \cdot |\underline{i}\rangle$

$$|\phi\rangle \otimes |\varphi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \dots \\ \alpha_{2^n-1} \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \\ \dots \\ \beta_{2^m-1} \end{pmatrix} = \begin{pmatrix} \alpha_0 \cdot \beta_0 \\ \alpha_0 \cdot \beta_1 \\ \dots \\ \alpha_{2^n-1} \cdot \beta_{2^m-2} \\ \alpha_{2^n-1} \cdot \beta_{2^m-1} \end{pmatrix}$$

$$= \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^m-1} \alpha_i \cdot \beta_j \cdot |\underline{i}\rangle \otimes |\underline{j}\rangle$$

Avec $|\underline{i}\rangle \otimes |\underline{j}\rangle = |\underline{i * 2^m + j}\rangle$

qbits intriqués

Certains n-qbits ne sont pas le produit d'autres qbits. On dit que les qbits qui le composent sont intriqués.

Définition : intrication

Soit $|\varphi\rangle$, un n-qbit, alors $|\varphi\rangle$ est intriqué si et seulement si pour tout

- $n_1, n_2 \in \mathbb{N}^*$ tels que $n_1 + n_2 = n$
- $|\varphi_1\rangle$ un n_1-qbit
- $|\varphi_2\rangle$ un n_2-qbit

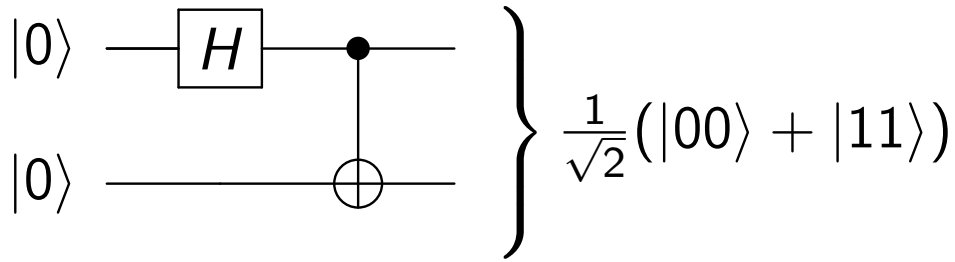
on a

$$|\varphi\rangle \neq |\varphi_1\rangle \otimes |\varphi_2\rangle$$

Par exemple
$|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ est intriqué (preuve plus loin).

Fabriquer un qbit intriqué

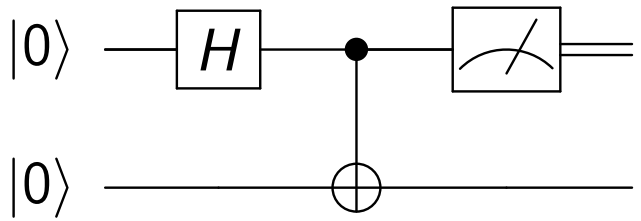
Le circuit suivant forme un qbit intriqué.



qbits intriqués

Intérêt de l'intrication

Si un n-qbit est intriqué, mesurer une partie du qbit donne des information sur le reste du qbit.

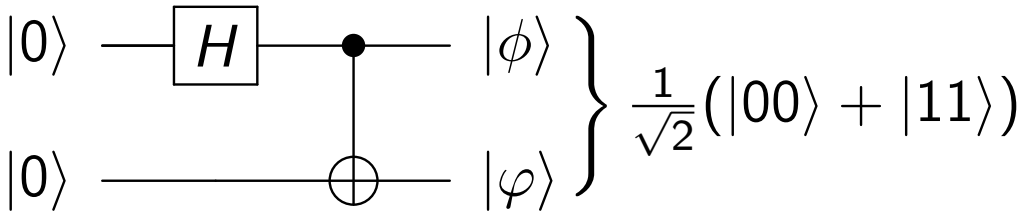


$$\Big\} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Si la mesure donne 0, alors le deuxième qbit est dans l'état $|0\rangle$ sinon il est dans l'état $|1\rangle$.

Remarque !

ATTENTION !



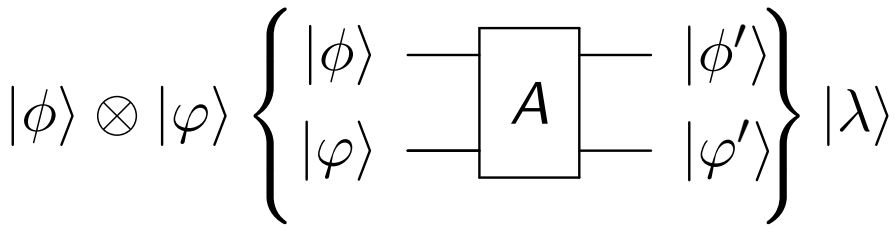
Ici, ce dessin ne signifie pas que $|\phi\rangle \otimes |\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$!

Il signifique que :

- si on mesure $|\phi\rangle$ et qu'on obtient 0 alors $|\varphi\rangle = |0\rangle$
- si on mesure $|\phi\rangle$ et qu'on obtient 1 alors $|\varphi\rangle = |1\rangle$

Propriétés des qbits : dessin d'un produit

Les circuits à 2 lignes représentent parfois un produit de 2 qbits si les 2 qbits ne sont pas intriqués.



$|\lambda\rangle = |\phi'\rangle \otimes |\varphi'\rangle$ si les qbits sont indépendants.

L'état de Bell est intriqué

Théorème

$|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ est intriqué.

Preuve :

Sinon, il existe $\alpha, \beta, \gamma, \delta$ tels que

$$|\varphi\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \cdot \gamma \\ \alpha \cdot \delta \\ \beta \cdot \gamma \\ \beta \cdot \delta \end{pmatrix}.$$

$\alpha\gamma = 1$, $\alpha\delta = 0$, $\beta\gamma = 0$, $\beta\delta = 1$

Donc $\beta = 0$ ou $\gamma = 0$ (3e égalité)

Et $\gamma \neq 0$ (1e égalité)

Et $\beta \neq 0$ (4e égalité)

Produit de portes

Définition : produit tensoriel de portes

On peut multiplier les portes. Soient deux portes $A \in \mathcal{M}_{2^n}(\mathbb{C})$ et $B \in \mathcal{M}_{2^m}(\mathbb{C})$

$$A \otimes B = \begin{pmatrix} a_{00} \cdot B & a_{01} \cdot B & \cdots & a_{02^n-1} \cdot B \\ a_{10} \cdot B & a_{11} \cdot B & \cdots & a_{12^n-1} \cdot B \\ \vdots & \vdots & \ddots & \vdots \\ a_{2^n-10} \cdot B & a_{2^n-11} \cdot B & \cdots & a_{2^n-12^n-1} \cdot B \end{pmatrix}$$

$$= \begin{pmatrix} a_{00} \cdot b_{00} & a_{00} \cdot b_{01} & \cdots & a_{02^n-1} \cdot b_{02^m-1} \\ a_{00} \cdot b_{10} & a_{00} \cdot b_{11} & \cdots & a_{02^n-1} \cdot b_{12^m-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{2^n-10} \cdot b_{2^m-10} & a_{2^n-10} \cdot b_{2^m-11} & \cdots & a_{2^n-12^n-1} \cdot b_{2^m-12^m-1} \end{pmatrix}$$

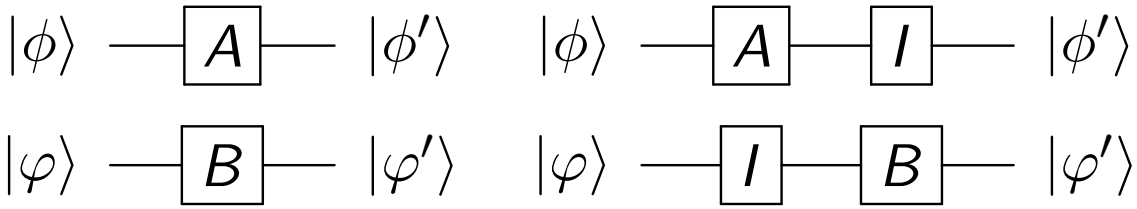
Produit de portes : exemples

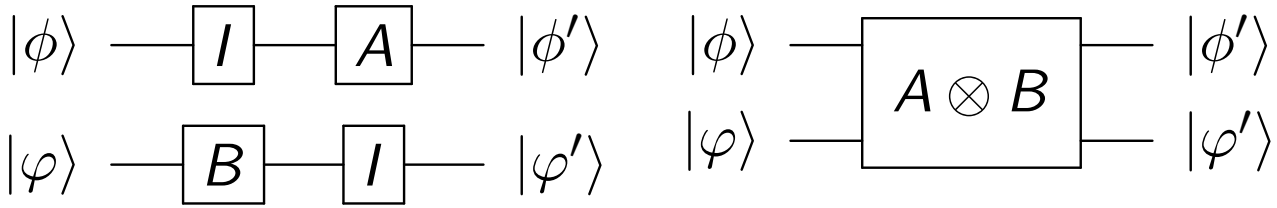
$$H \otimes I_3 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}$$

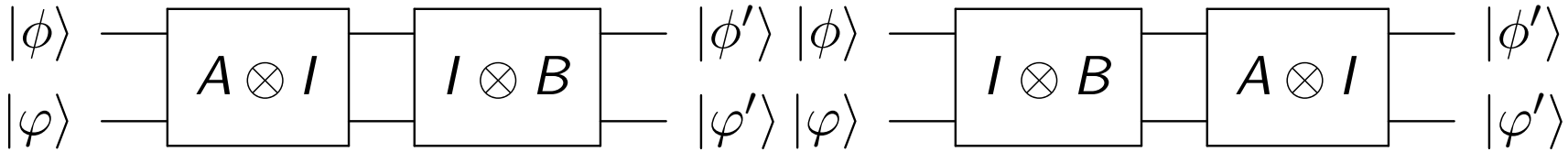
$$I_3 \otimes H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

Portes parallèles

Les circuits suivants sont équivalents (I = Identité).

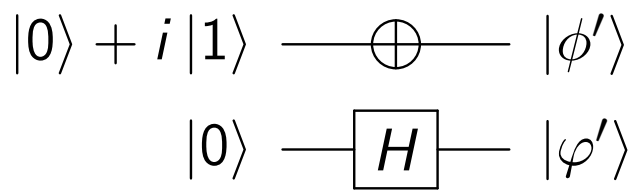


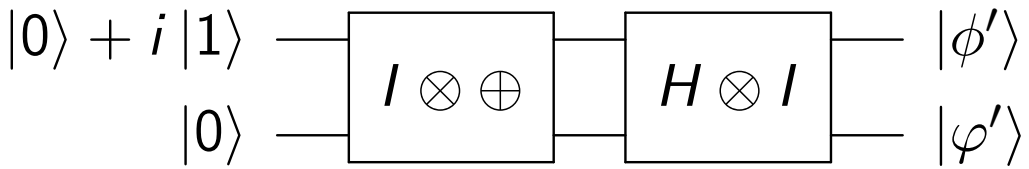




Portes parallèles : exemples

Montrez que les circuits suivants sont équivalents.

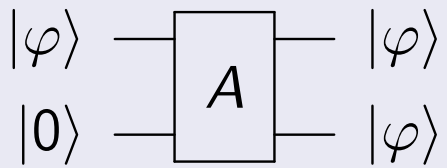




Non clonage

Impossible de cloner un qbit

Il n'existe pas de porte A dont le résultat serait le suivant quel que soit $|\varphi\rangle$:



Preuve : si cela est vrai pour tout φ, c'est en particulier vrai pour $|0\rangle$ et $|1\rangle$, donc

- $A \cdot (|0\rangle \otimes |0\rangle) = |00\rangle$
- $A \cdot (|1\rangle \otimes |0\rangle) = |11\rangle$

Par linéarité :

$A \cdot ((\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle) = \alpha |00\rangle + \beta |11\rangle$

Cependant, par définition de A :

$A \cdot ((\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle) = (\alpha |0\rangle + \beta |1\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle)$

Base

Définition

Une *base de n-qbits* est un ensemble de 2^n n-qbits linéairement indépendants.

Il s'agit simplement d'une base de l'espace vectoriel $(\mathbb{C}^{2^n}, +, \cdot)$.
Par définition, $(|0\rangle, |1\rangle)$ est une base des 1-qbits.
Par définition, $(|\underline{0}\rangle, |\underline{1}\rangle, \ldots, |\underline{2^n - 1}\rangle)$ est une base des n-qbits.

Définition

Une *base de n-qbits* est *orthonormale* si, pour tout vecteur $|\varphi\rangle$ de la base, $\||\varphi\rangle\| = 1$ et pour tout couple $|\phi\rangle$ et $|\varphi\rangle$ de vecteurs de la base, $\langle\phi|\varphi\rangle = 0$.

Les bases ci-dessus sont orthonormales.

Base : propriété

Théorème

Connaissant une base $(|\varphi_0\rangle, |\varphi_1\rangle, \ldots, |\varphi_{2^n-1}\rangle)$ de n-qbits et une porte quantique A, alors $(A|\phi_0\rangle, A|\varphi_1\rangle, \ldots, A|\varphi_{2^n-1}\rangle)$ est aussi une base de n-qbits.

Preuve : A est unitaire donc inversible. Elle transforme donc une base en une autre base.

Théorème

Connaissant une base orthonormale $(|\varphi_0\rangle, |\varphi_1\rangle, \ldots, |\varphi_{2^n-1}\rangle)$ de n-qbits et une porte quantique A, alors $(A|\phi_0\rangle, A|\varphi_1\rangle, \ldots, A|\varphi_{2^n-1}\rangle)$ est aussi une base orthonormale de n-qbits.

Preuve : A est unitaire donc préserve les produits scalaires.

Base : propriété

Théorème

Connaissant deux bases

- une base orthonormale $(|\phi_i\rangle, i \in [\![0; 2^n - 1]\!])$ de n-qbits
- une base orthonormale $(|\varphi_i\rangle, i \in [\![0; 2^m - 1]\!])$ de m-qbits

alors

$$(|\phi_i\rangle \otimes |\varphi_j\rangle, i \in [\![0; 2^n - 1]\!], j \in [\![0; 2^m - 1]\!])$$

est une base de orthonormale $(n + m)$-qbits.

Bases classiques

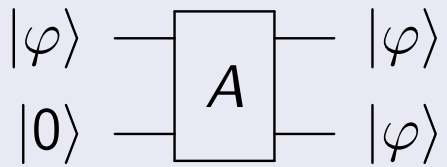
- $|0\rangle$ et $|1\rangle$
- Base de Hadamard :
  - $|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Base de Bell (obtenue avec $(H \otimes I_2) \cdot CNOT$) :
  - $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
  - $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
  - $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

Presque clonage

Clonage des états de bases

Pour toute base de 1-qbits ($|e_0\rangle$, $|e_1\rangle$) orthonormale, il existe un circuit qui

- clone les états de la base
- ne clone pas les autres



seulement si $\varphi = |e_0\rangle$ ou $|e_1\rangle$.

Preuve : il suffit de trouver A pour la base ($|0\rangle, |1\rangle$), de trouver la matrice de passage B entre les deux bases et de mettre les portes B et B^{-1} au bon endroit dans le circuit.