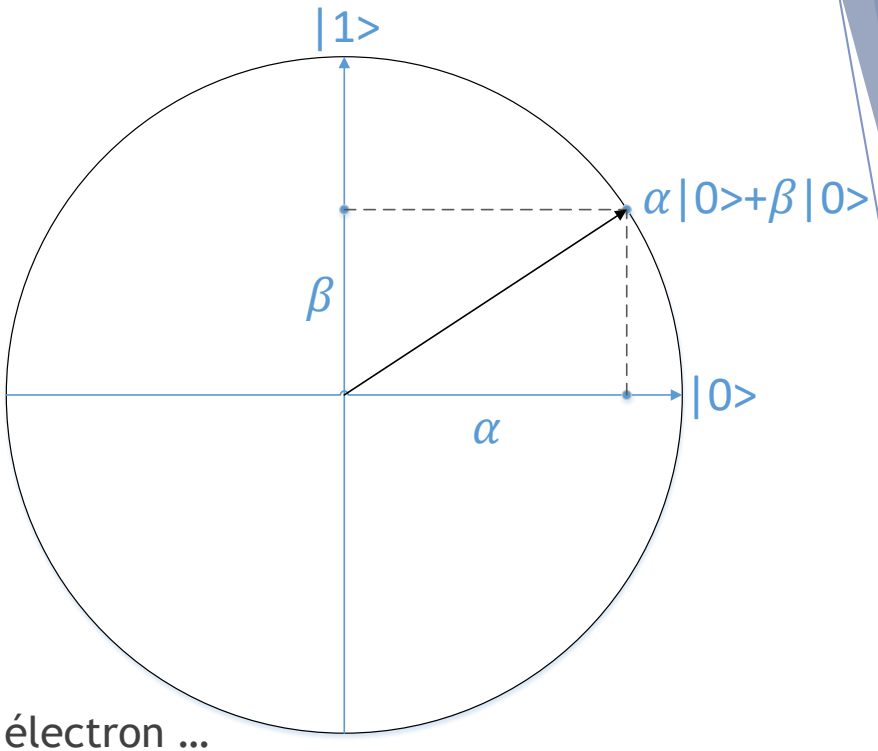
Informatique quantique

Les qbits



- Les états basiques :

(computational basis)

  - |0>
  - |1>
- Leur réalisation :
  - atome, molécule, électron …
- L'état quantique :
  - C'est une combinaison linéaire normalisée des états basiques

$$(\alpha, \beta) \in \mathbb{C}^2, \alpha|0> + \beta|1>$$
$$\alpha^2 + \beta^2 = 1$$

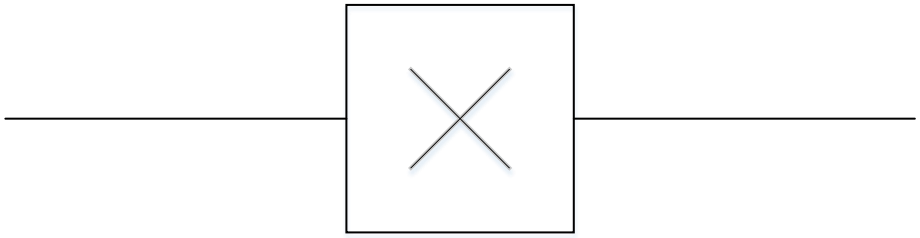
  - Superposition :

$$\alpha \neq 0, \beta \neq 0$$

Notation et porte non (not gate)

- $|\varphi> = \alpha|0> + \beta|1> = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$
- Not gate :

$$\alpha|0> + \beta|1> \rightarrow \alpha|1> + \beta|0>$$

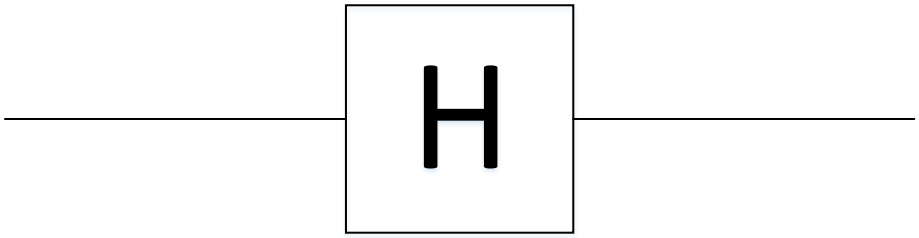


$$X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

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

Porte Hadamard

- $|0> \rightarrow \frac{|0>+|1>}{\sqrt{2}}$
- $|1> \rightarrow \frac{|0>-|1>}{\sqrt{2}}$

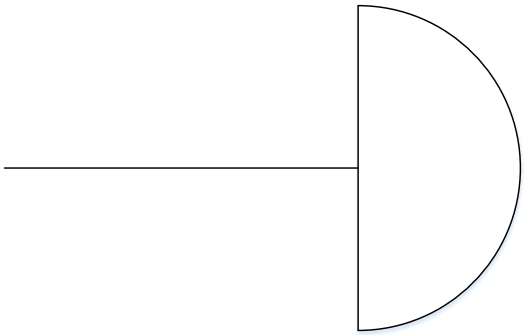


- $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Note : $H^2 = I$

La mesure

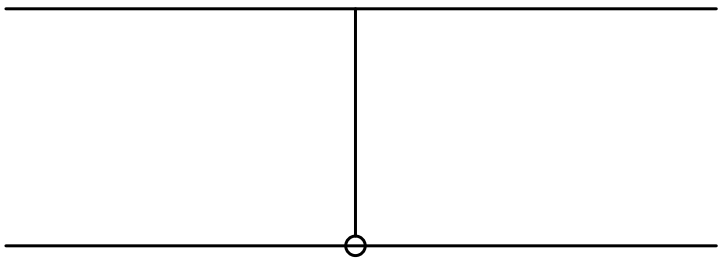
- On ne peut mesurer que |0> ou |1>
  - L'état $\alpha|0> + \beta|1>$ donnera donc que |0> ou |1>
    - |0> avec la probabilité $|\alpha|^2$
    - |1> avec la probabilité $|\beta|^2$
- La mesure est destructive
  - Lire |0> implique que l'état actuel du système est |0>
  - Lire |1> implique que l'état actuel du système est |1>



Portes quantiques à un qbit

- Matrice unitaire U:
  - Notation : matrice adjointe $U^\dagger = (U^T)^*$
  - $U \in M_{2,2}(\mathbb{C}), U^\dagger U = I$
- H et X en sont
- Pourquoi unitaires ?
  - Unitaire préserve la norme, c'est une condition nécessaire et suffisante pour passer d'un état quantique à l'autre (démonstration un peu longue)

La porte « non contrôlé » (cNOT)



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

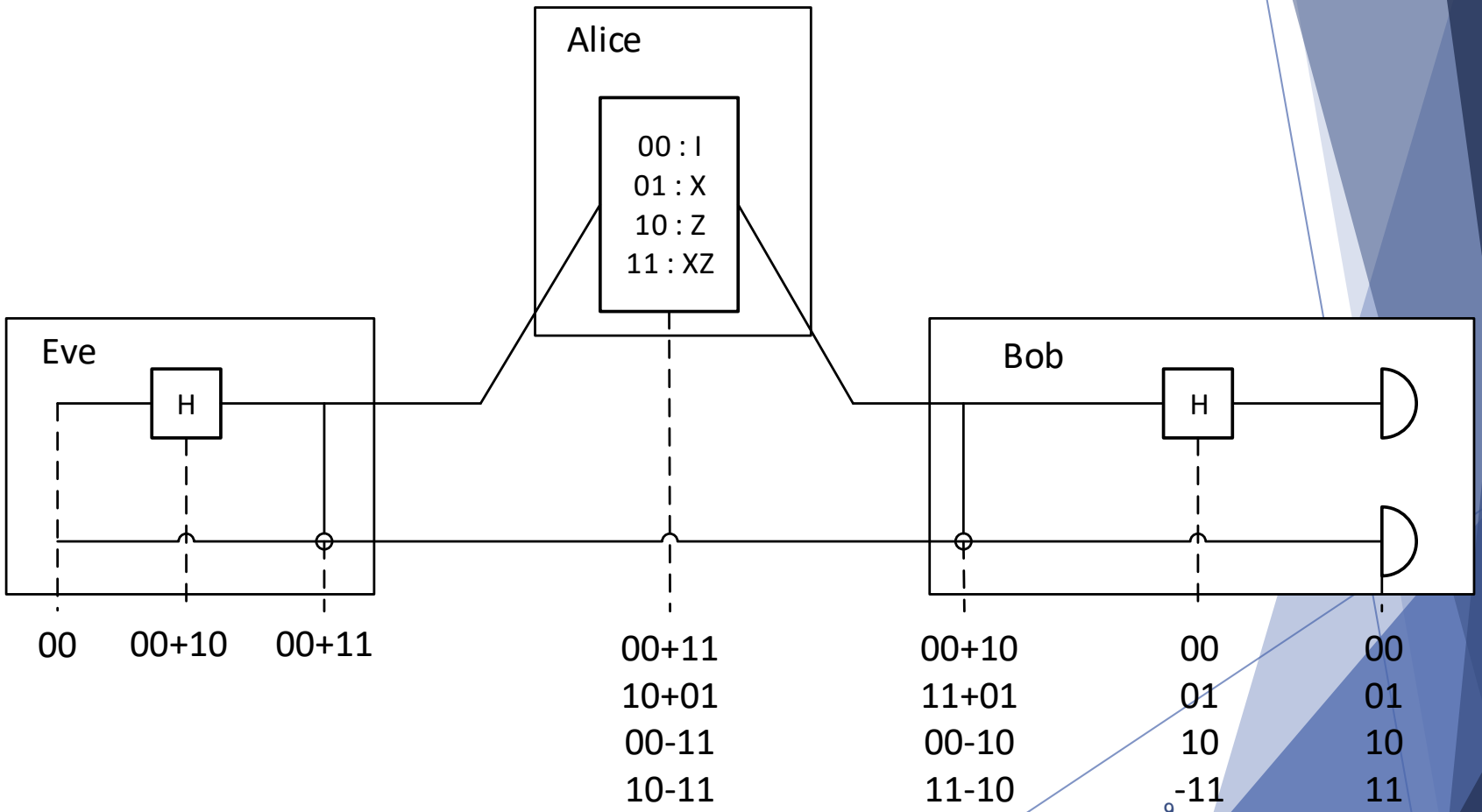
- Table de vérités
  - $|00> \rightarrow |00>$
  - $|01> \rightarrow |01>$
  - $|10> \rightarrow |11>$
  - $|11> \rightarrow |10>$
- Équivalent en informatique classique
  - $q_2 \cdot \overline{q_1} + \overline{q_2} \cdot q_1$
- Formule dans Z/2Z
  - $|x, y> \rightarrow |x, y \oplus x>$

Portes universelles

- Informatique classique:
  - And, not
- Informatique quantique
  - cNOT et l'ensemble des portes à un qbit

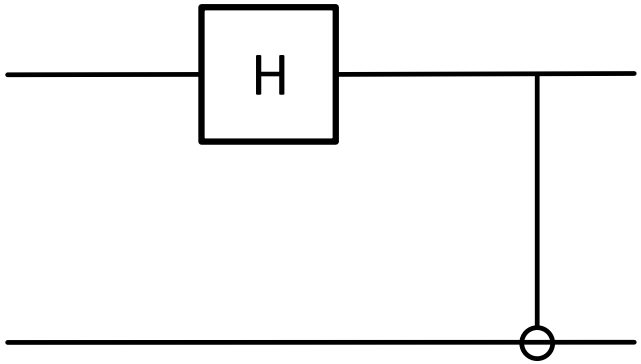
- À ce point, nous avons un modèle, on considèrera en plus une manière d'avoir les inputs/outputs :
  - $|x, 0> \rightarrow |x, f(x)>$
  - Quelques points suplémentaire:
    - Ce n'est pas le seul modèle possible
    - On ne prend pas en compte ici les bits de computation
    - Il a été démontré que toute fonction programmable en info classique l'était en en info quantique (avec un nombre de portes similaire)

Première application : encodage super dense



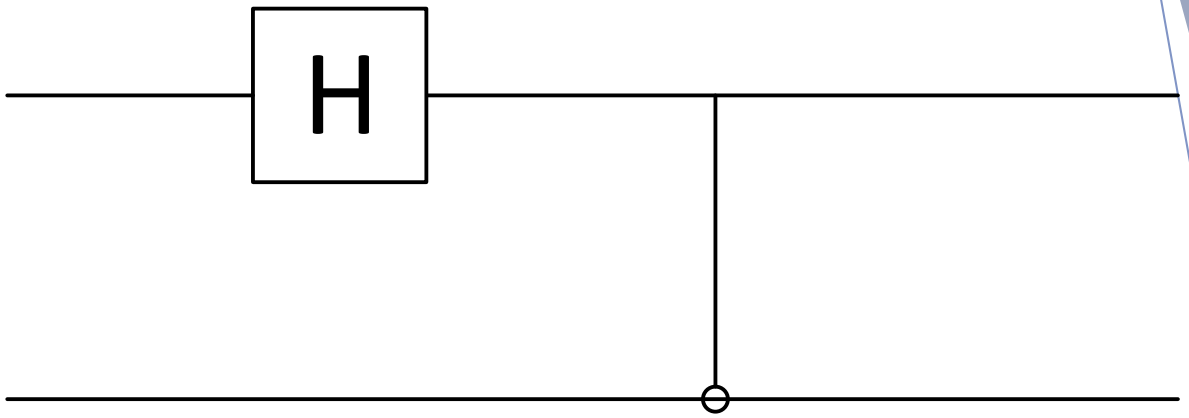
L’état de Bell

- $\frac{|00> + |11>}{\sqrt{2}}$



- De manière plus générale, pour tout $|\varphi>, |\theta>$
  $\exists U\ unitaire, \mathrm{U}|\varphi> = |\theta>$
  - En l’occurrence $\mathrm{U}|00> = |Bell>$
  - C’est un théorème d’algèbre indépendant des propriétés quantiques d’un système

État d'intrication quantique



- $|00> \rightarrow \frac{|00> + |10>}{\sqrt{2}} \rightarrow \frac{|00> + |11>}{\sqrt{2}}$
- Qu'est ce qui est spécial ?
  - Inaccessible en préparant les bits séparément
    - $\frac{|00> + |11>}{\sqrt{2}} \neq (\alpha|0> + \beta|1>)(\gamma|0> + \delta|1>) = \alpha\gamma|00> + \alpha\delta|01> + \beta\gamma|10> + \beta\delta|11>$
  - Leur état ne peut être décrit qu'en donnant l'ensemble des qbits
  - Intuitivement : $|\varphi> = \varphi_{00\dots00}|00\dots00> + \dots + \varphi_{11\dots11}|11\dots11>$
    - 2^n amplitudes pour n qbits ⇒ 2^n interactions possibles

Téléportation d'un état quantique