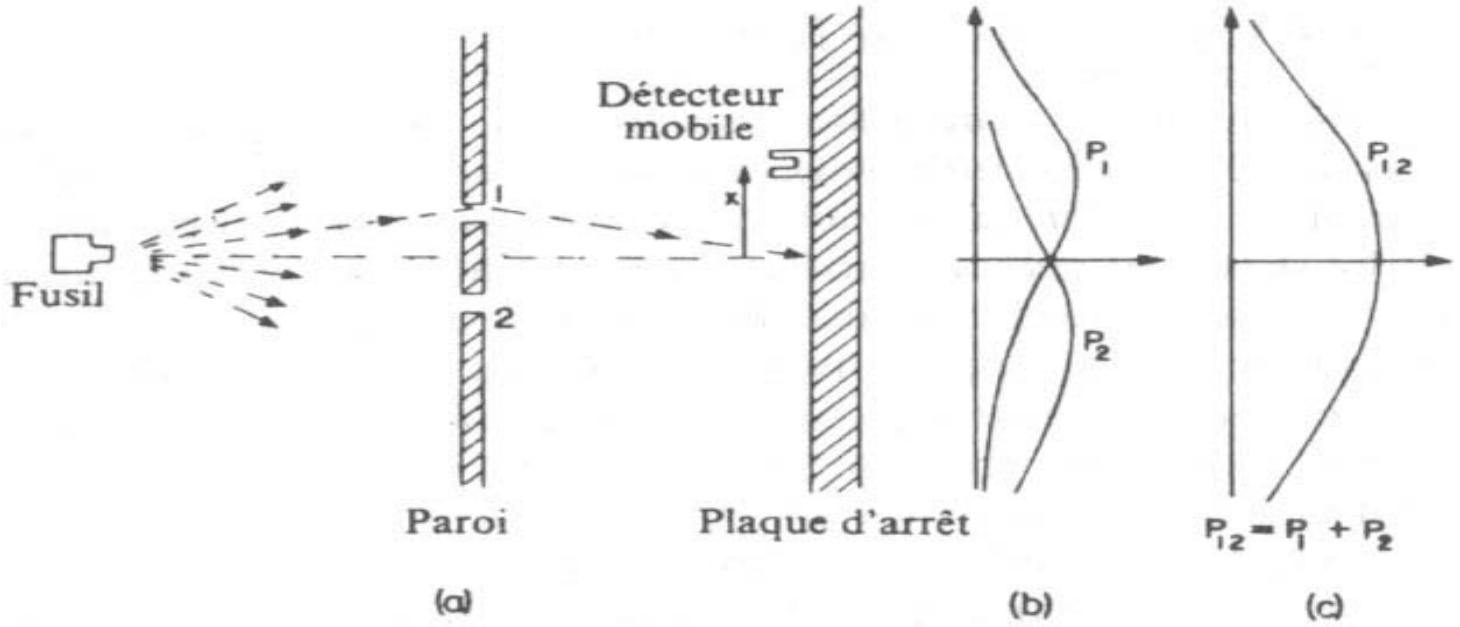
Un peu de calcul quantique

- Quelques expériences simples
- L'expérience de Stern et Gerlacht
- La notion de qubit
- Portes quantiques élémentaires
- Algorithmes élémentaires

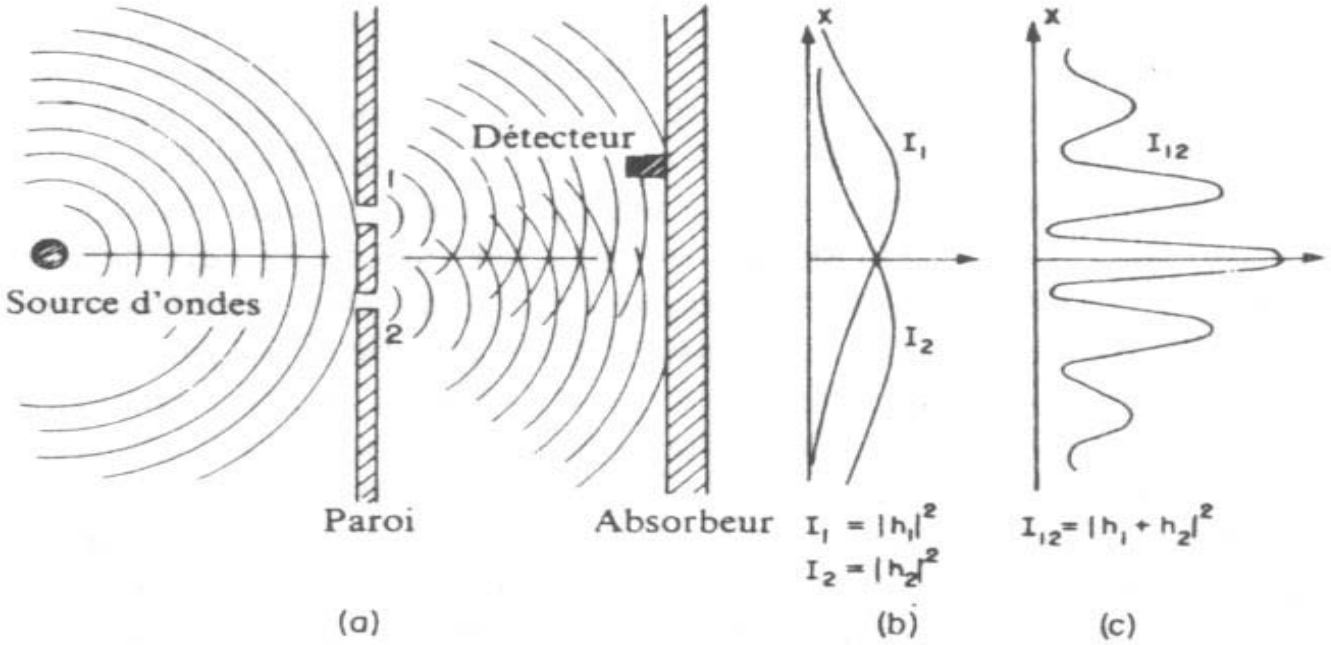
L'expérience des balles de fusil

- On tire avec un fusil sur une plaque percée de deux trous et on observe les impacts sur un écran



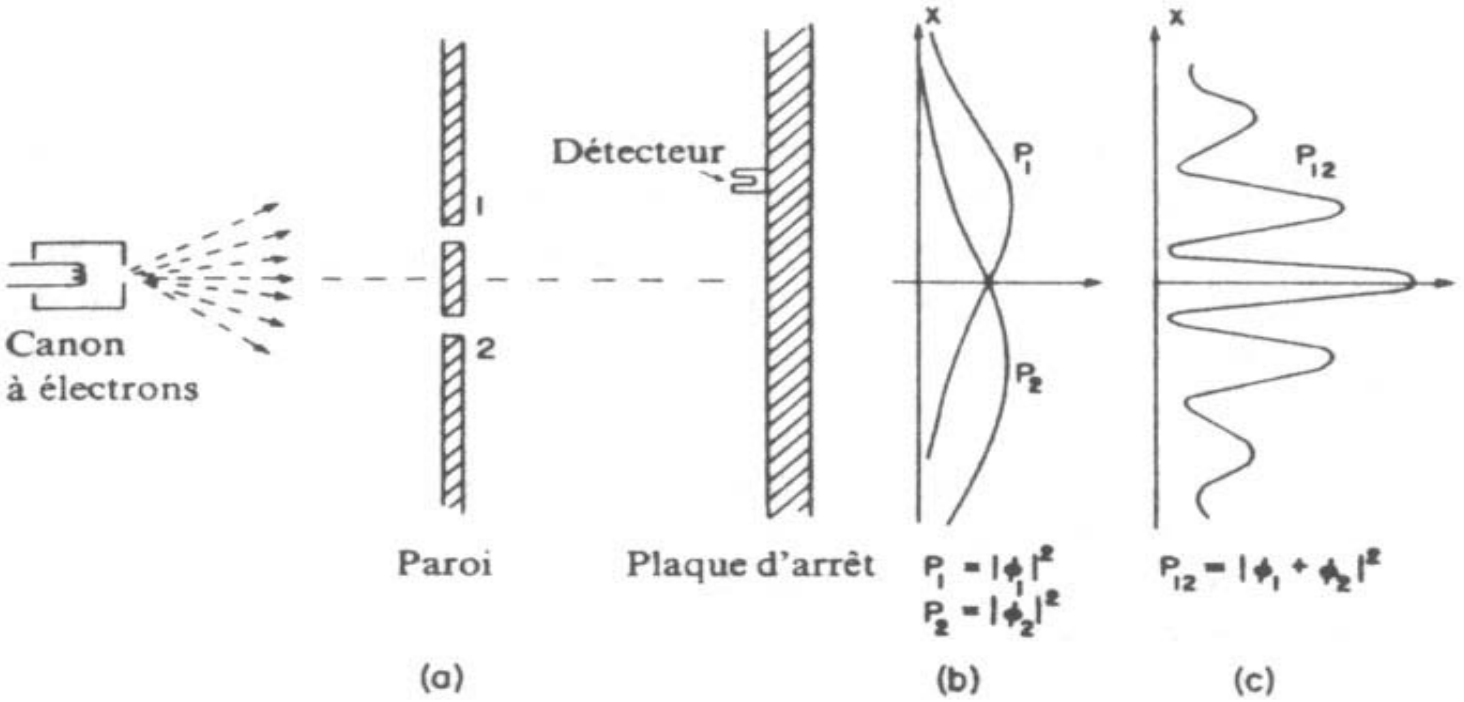
L 'expérience des vagues

- On crée un onde que l'on filtre à travers deux trous et on observe l'amplitude



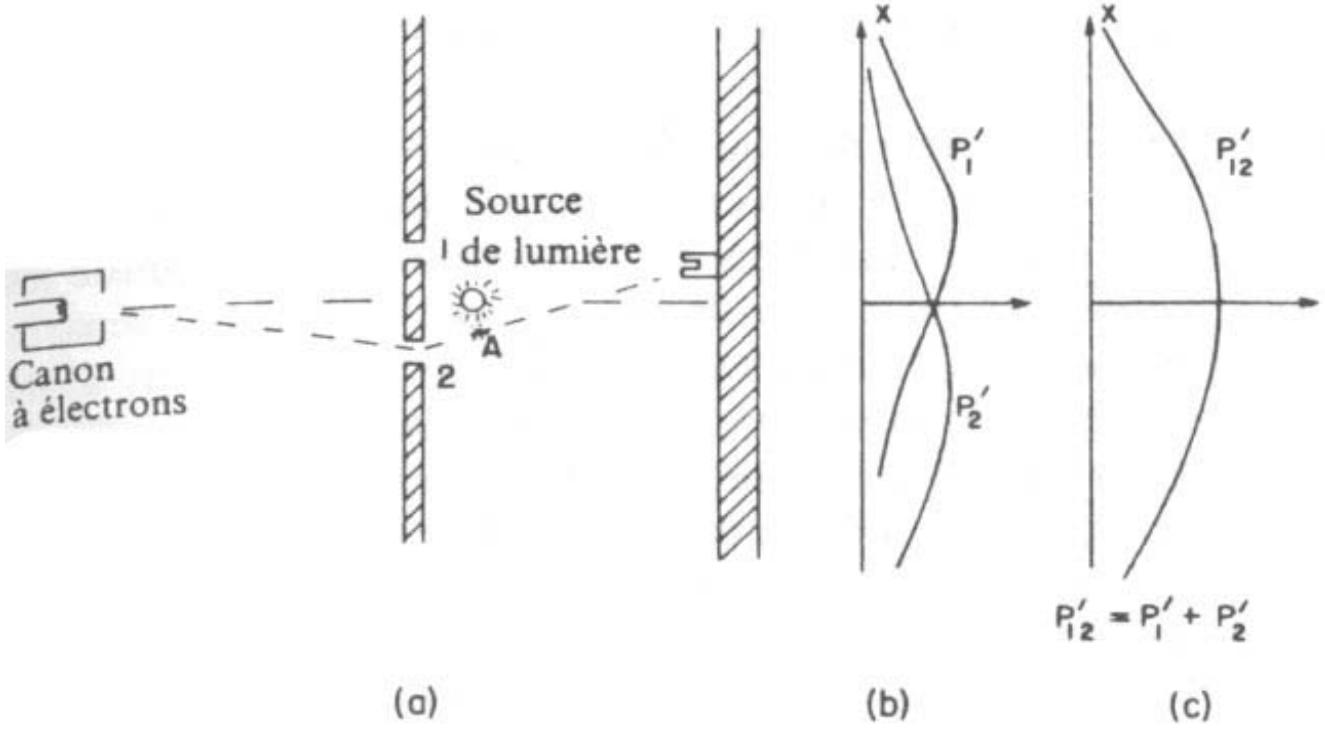
Un tir au canon à électrons

- On bombarde une plaque avec des électrons



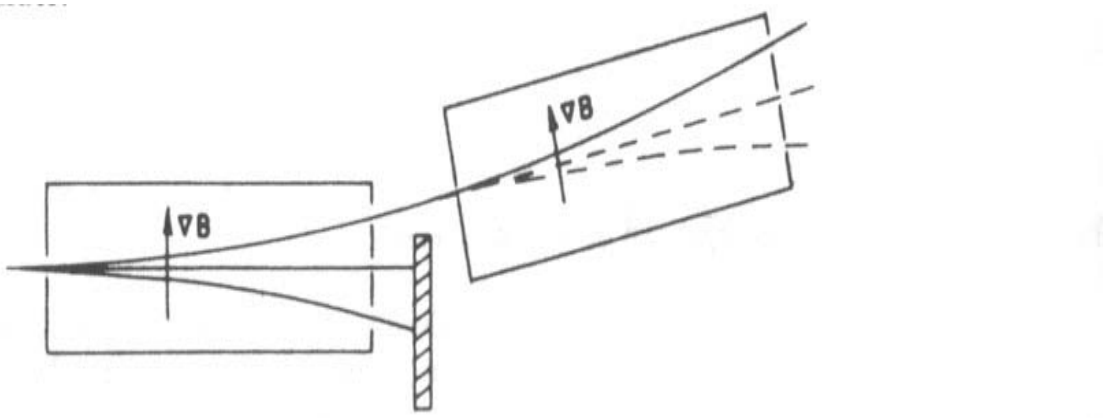
Observons les électrons

- On place une source lumineuse pour savoir où passent les électrons



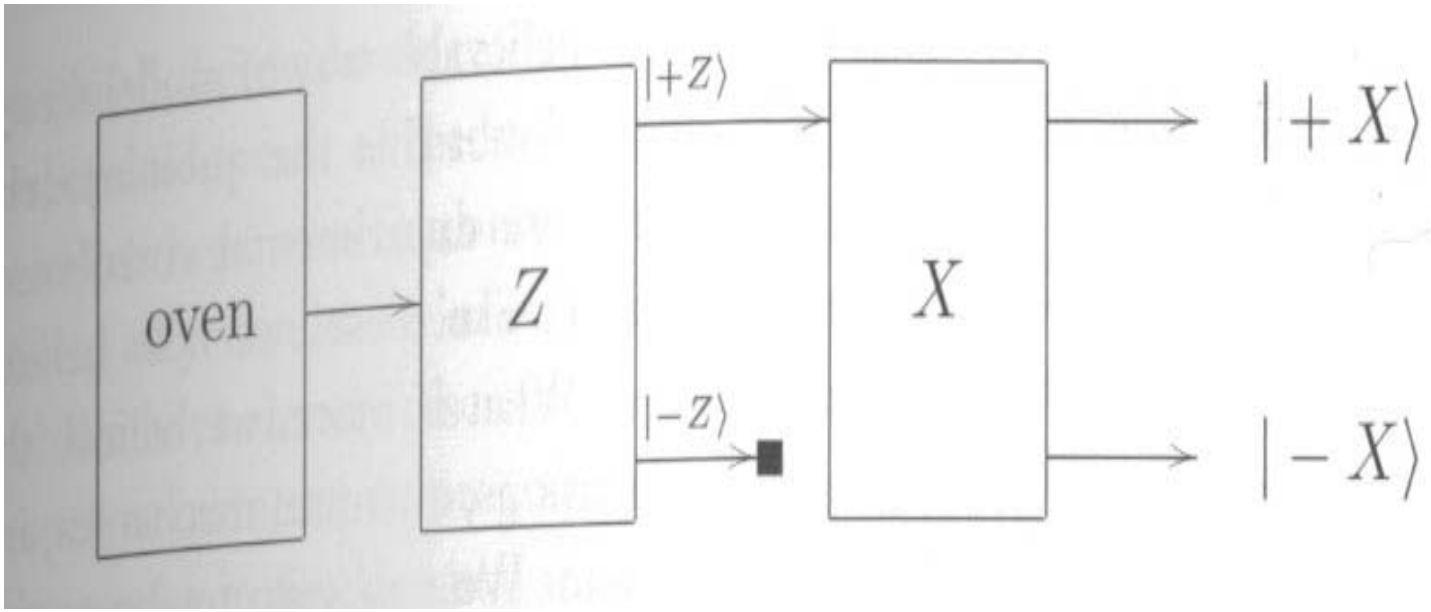
L'expérience de Stern et Gerlacht

- On sépare un faisceau d'atomes d'hydrogène avec un aimant
- On obtient un faisceau purifié et quantifié



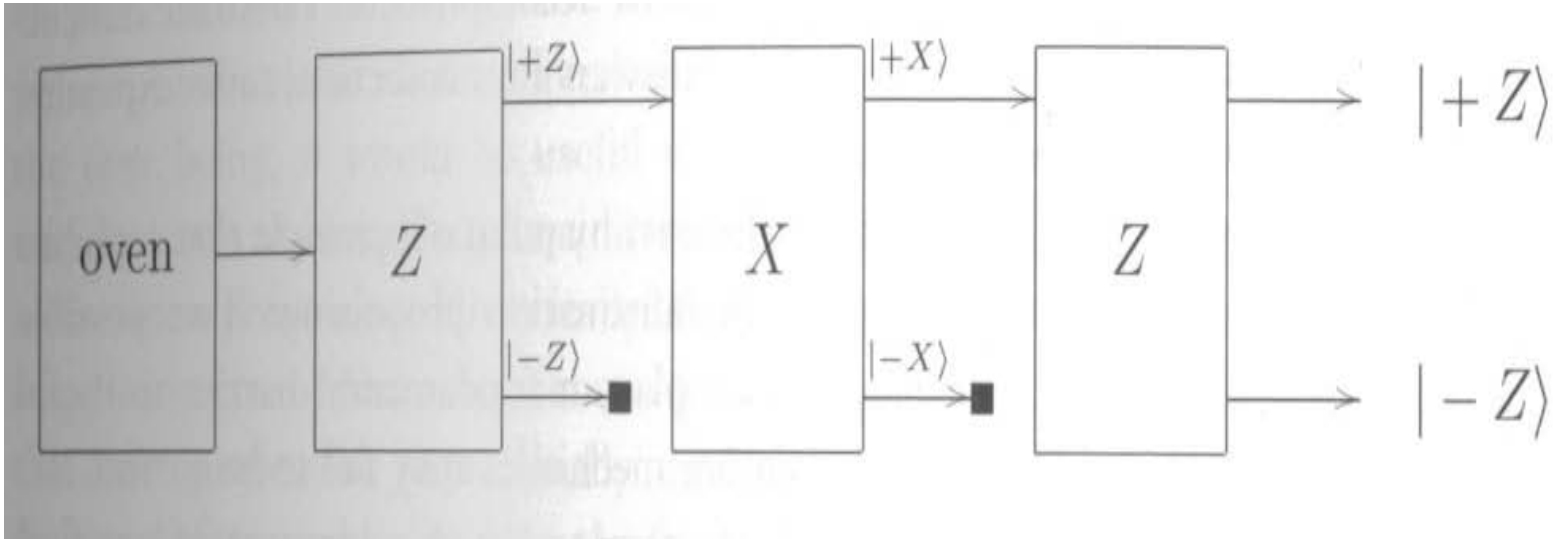
Stern et Gerlacht 2

- On cascade deux aimants: un suivant l'axe Z et l'autre suivant l'axe X



Stern et Gerlacht 3

- On enchaine 3 filtres: un en Z, un en X et un nouveau en Z
- Les résultats sont inexplicables classiquement



La mécanique quantique

- Apparaît lorsque lors s'intéresse aux propriétés des « très petites » choses
- Dit que tout objet à des propriétes corpusculaires et ondulatoires
- Le principe d'incertitude est un élément central
- Admet plusieurs formalismes qui se rejoignent tous

Le formalisme du qubit

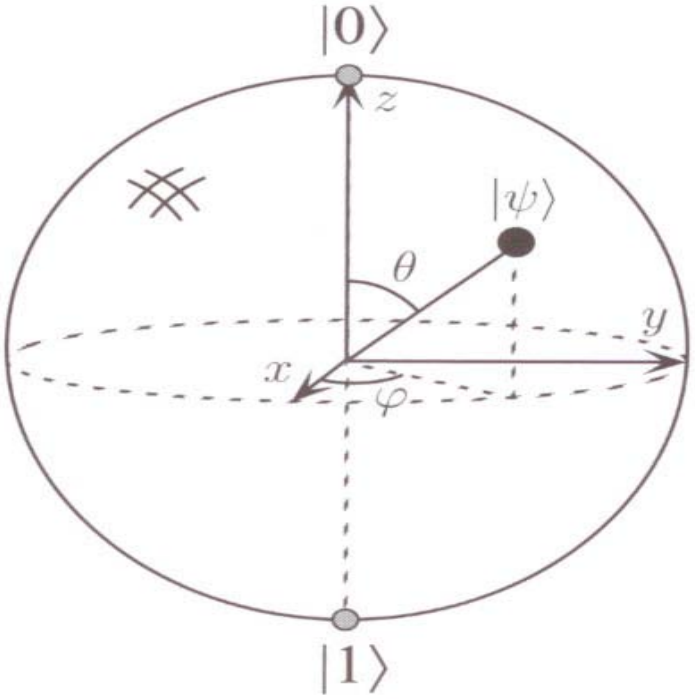
- $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle$ avec a et b complexes et $|a|^2+|b|^2=1$
- Lorsque l'on mesure $|\Psi\rangle$, on a une probabilité $|a|^2$ de trouver $|0\rangle$ et une probabilité $|b|^2$ de trouver $|1\rangle$
- Si l'on a mesuré $|0\rangle$, alors $|\Psi\rangle = |0\rangle$ après la mesure: c'est l'*effondrement* de la fonction d'onde

Le formalisme du qubit

- |0> et |1> sont simplement une base d'un espace vectoriel complexe de dimension 2. Ils correspondent à une mesure possible (par exemple le spin suivant l'axe Z)
- On peut choisir n'importe quelle autre base de mesure, par exemple:
  - $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$ $|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$
- La notion de *base* et d'*effondrement* de la fonction d'onde explique Stern/Gerlacht

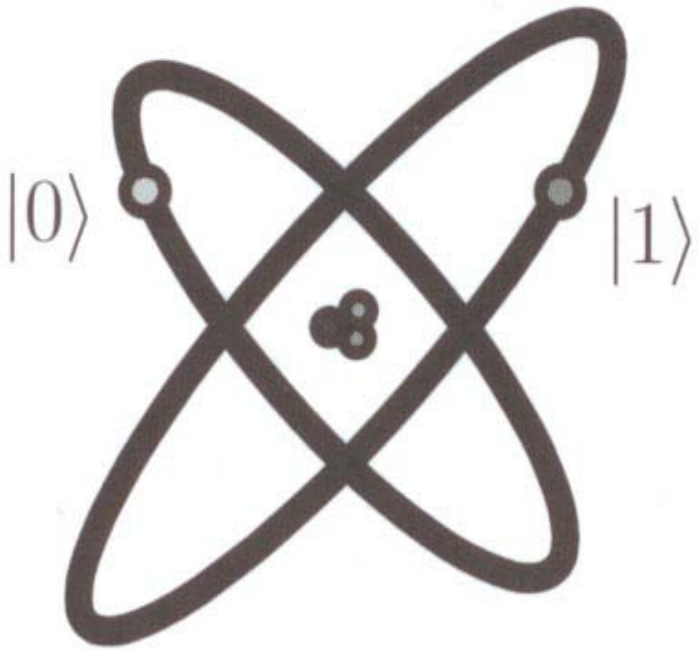
Sphère de Bloch

- $|\Psi\rangle = a|0\rangle + b|1\rangle$
  - $= \exp(i\,\omega)(\cos(\Theta/2)|0\rangle + \exp(i\varphi)\sin(\Theta/2)|1\rangle)$
  - Sphère de Bloch
  - Φ quelconque
  - -> infinité d'informations?



Comment faire un qubit

- Excitation d'un électron par un laser
  - Suivant l'énergie dispensée:
  - |0> => |1>
  - |0> => a|0>+b|1>



Plusieurs qubits

- Deux qubits:
  - $|\psi\rangle = a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle$
  - $|a|^2+|b|^2+|c|^2+|d|^2=1$
  - Base de 4 éléments
- Si on mesure 0 sur le bit 1 alors
  - $|\psi\rangle = (a|00\rangle+b|01\rangle)/\sqrt{(|a|^2+|b|^2)}$
- Avec *n* qubits -> base de 2^n éléments
  - 500 qubits représente 2^{500} amplitudes!

Deux qubits

- Soient deux qubits
  - $|\psi\rangle = a|0\rangle + b|1\rangle$
  - $|\varphi\rangle = c|0\rangle + d|1\rangle$
- On écrit le système composé:
  - $|\Psi\rangle|\varphi\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$
  - La probabilité de mesurer le premier qubit à 0 est bien: $|ac|^2 + |ad|^2 = |a|^2(|c|^2 + |d|^2) = |a|^2$

Les paires EPR

- $|\psi\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$
- La mesure sur le premier qubit donne ½ de fixer la paire dans l'état $|00\rangle$ et ½ de la fixer dans l'état $|11\rangle$
- Lorsque la mesure du premier qubit est connu, celle du second est fixé
  - Transport d'information instantané? Non.
  - Théorie des variables cachées? Non.

Porte logique à 1 qubit

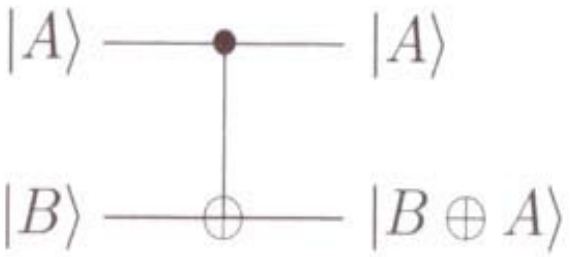
- Une porte logique quantique transforme un qubit en un autre qubit de façon linéaire. On peut les représenter sous la forme de matrices complexes U 2x2
- La condition de normalisation des coefficients impose: $U^t U = I$

Exemples de porte

- La porte quantique NOT: $X = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$
- La porte de Hadamard: $H = 1/\sqrt{2} \begin{matrix} 1 & 1 \\ 1 & -1 \end{matrix}$
- $|\psi\rangle = a|0\rangle + b|1\rangle$
- $X|\psi\rangle = b|0\rangle + a|1\rangle$
- $H|\psi\rangle = 1/\sqrt{2}\,((a+b)|0\rangle + (a-b)|1\rangle)$

Porte à deux qubits

- Exemple: la porte CNOT
- Transformation unitaire
- Transformation ***réversible***
- ***FANOUT interdit***



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

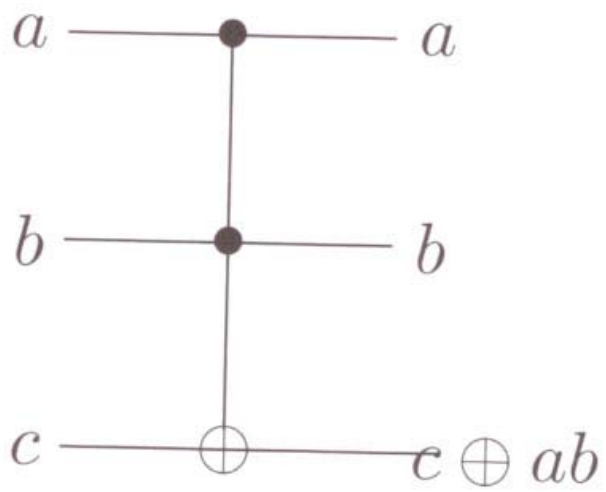
Le théorème « NO-COPY »

- Il est impossible de copier un qubit dans son intégralité
- Immense différence avec la logique classique
- La copie d'un bit « classique » reste bien sûr possible

La porte de Toffoli

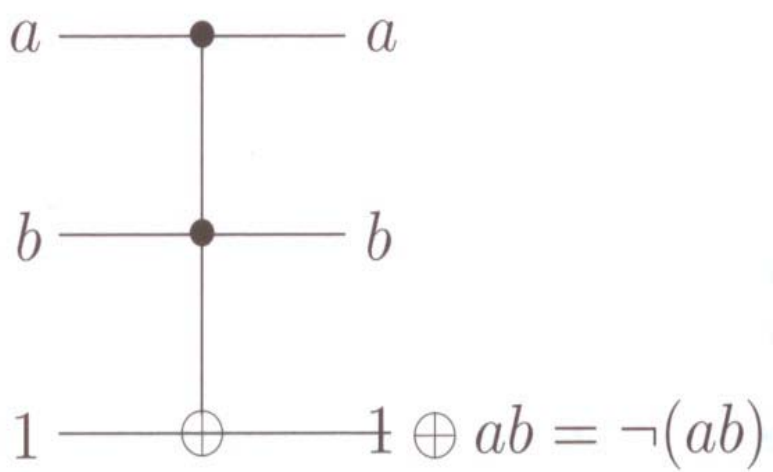
- Porte classique réversible permettant de simuler la porte NAND et le FANOUT

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

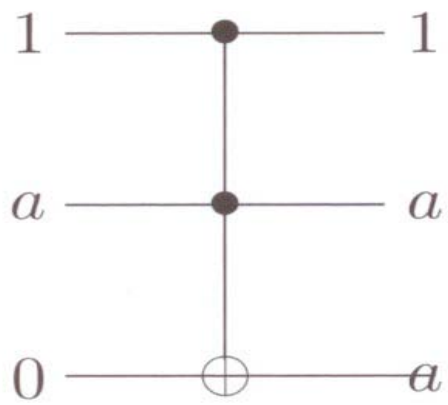


Porte de Toffoli

- NAND



- FANOUT

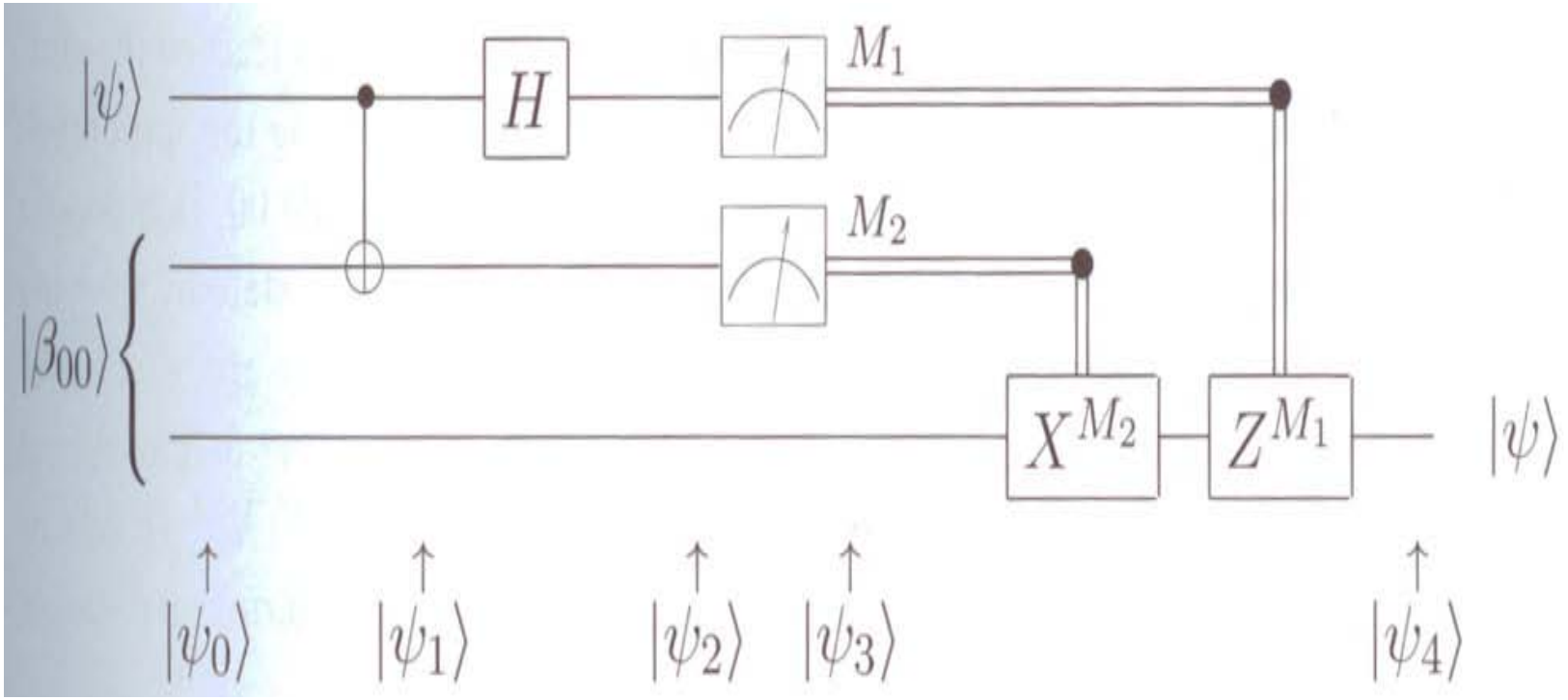


Propriétés

- Un circuit quantique peut émuler tout circuit classique
- En revanche, l'émulation par un circuit classique d'un système quantique à 50 qubits demanderait de stocker plusieurs milliers de terabytes de données

« Téléportation » quantique

- Alice et Bob partagent deux qubits EPR
- Alice doit transmettre un qubit |ψ> à Bob

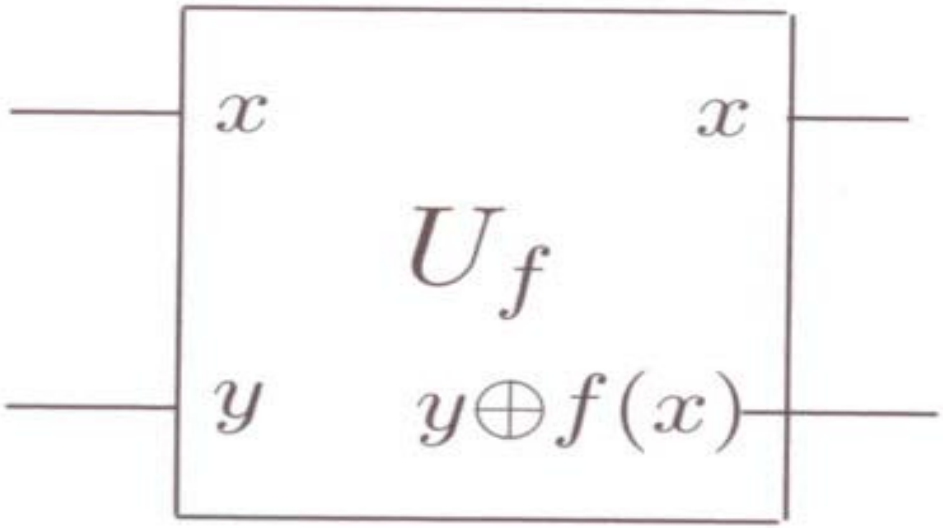


Téléportation quantique

- Copie d'un qubit?
  - Non, le qubit d'Alice est perdu dans l'opération.
- Transport d'information non relativiste?
  - Non, il faut transmettre une information classique via un canal classique

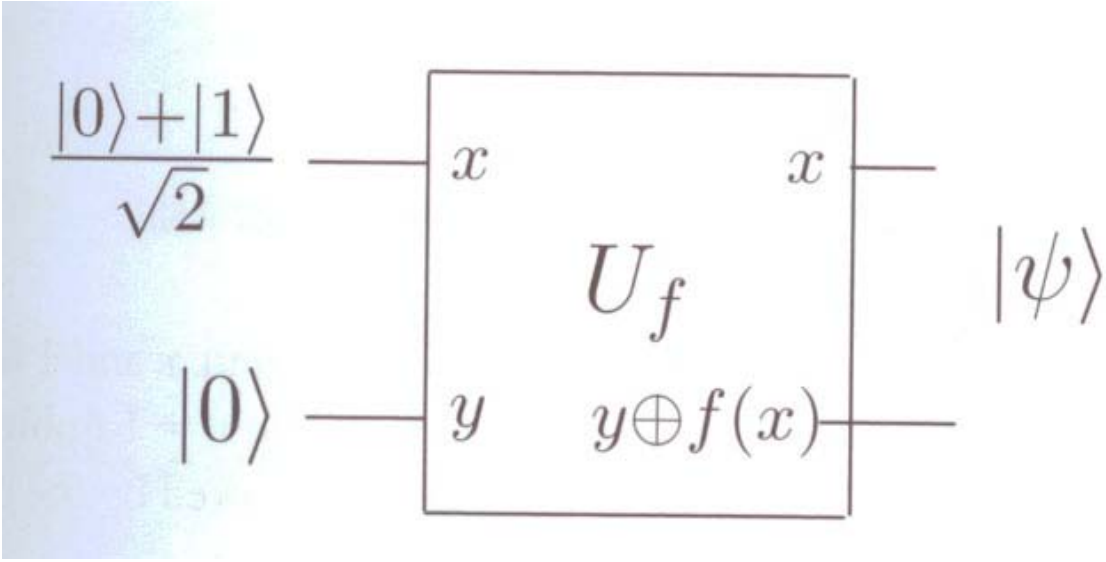
Parallélisme quantique

- Porte U_f opérant sur deux qubits |x,y> et calculant |x,(y *xor* f(x))>



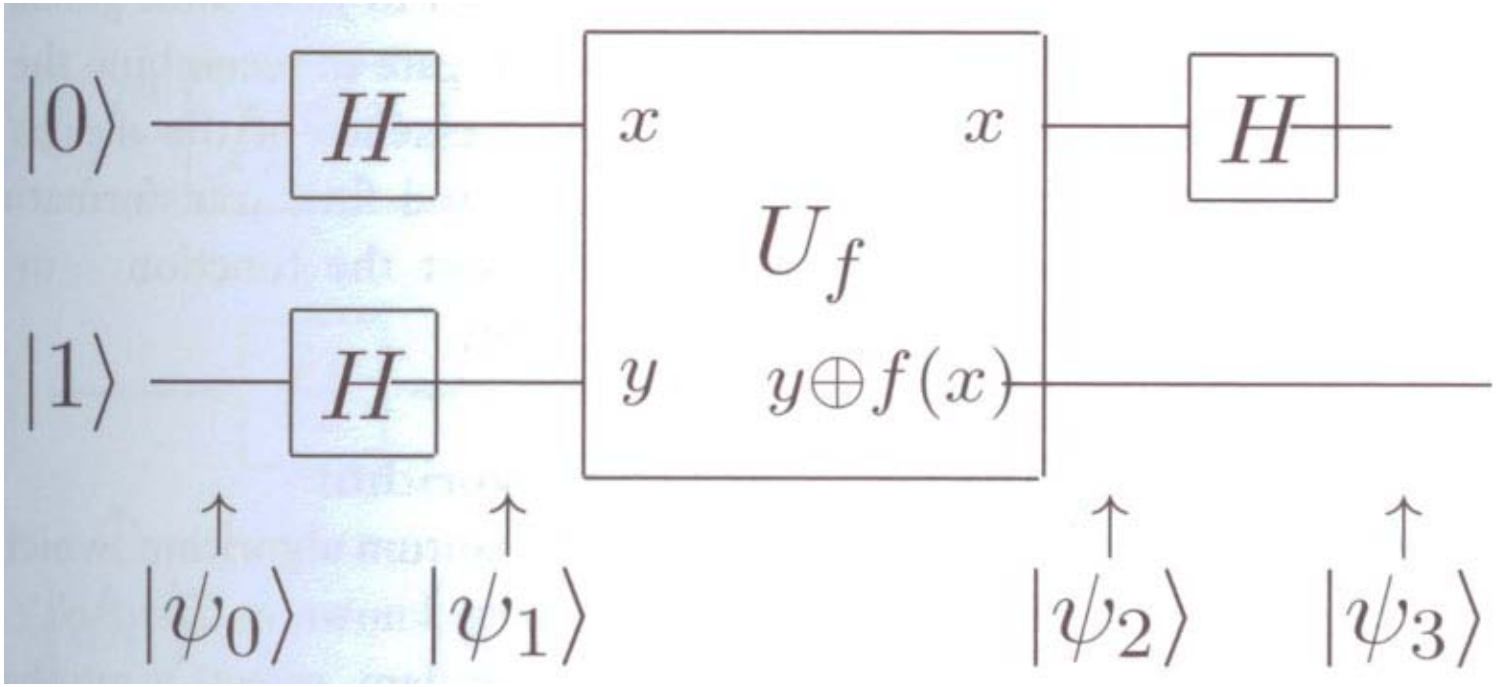
Parallélisme quantique

- Pour x=(|0>+|1>)/√2 et y = |0>
- Sortie: (|0,f(0)>+|1,f(1)>)/√2
- Un seul circuit calcule f(0) et f(1)



Algorithme de Deutsch

- $|\psi_3\rangle = |f(0) \text{ xor } f(1)\rangle \; (|0\rangle - |1\rangle)/\sqrt{2}$



Algorithme de Deutsch

- Calcule f(0) *xor* f(1) en une seule évaluation
- Montre bien la différence entre un système classique calculant aléatoirement f(0) ou f(1) et un système quantique qui calcule effectivement les deux, même s'ils ne sont pas simultanément accessibles

Transformée de Fourier

- Transformée de Fourier discrète

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} x_j$$

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle$$

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi i j k/2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle$$

Transformée de Fourier

- Temps nécessaire pour $N=2^n$ nombres:
  - Calculateur classique: $N \log(N) = 2^n n$
  - Calculateur quantique: n^2
- Attention! L'information n'est pas disponible directement. La mesure d'un coefficient effondre la fonction d'onde.
- Il est cependant possible d'exploiter les informations de la fonction d'onde

Algorithmes quantiques

- Algorithmes dérivant de la transformée de Fourier:
  - Algorithme de factorisation de nombres premiers
  - Calcul de logarithmes discrets: $a^x = b$ [p]
  - Importants en théorie de la cryptographie
- Algorithmes de recherche:
  - Passage de *n* à *log(n)*