iCoSys

Institute of Complex Systems

Hes·SO FRIBOURG FREIBURG

Haute Ecole Spécialisée de Suisse occidentale

Fachhochschule Westschweiz

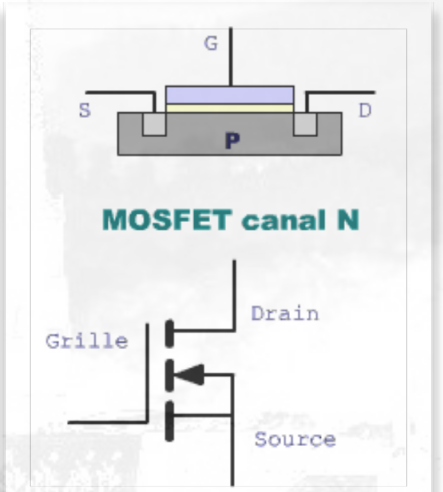
Introduction à l'informatique quantique

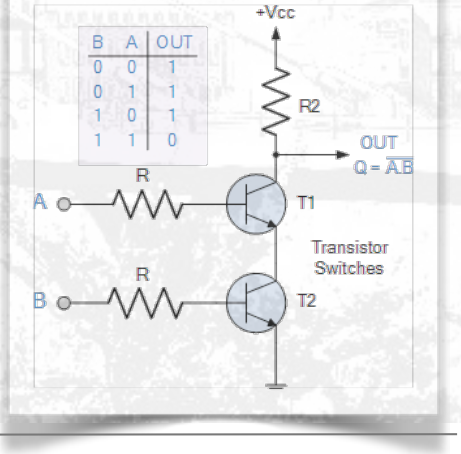
Le futur des ordinateurs ?

Pierre Kuonen : pierre.kuonen@hefr.ch

Petit récapitulatif

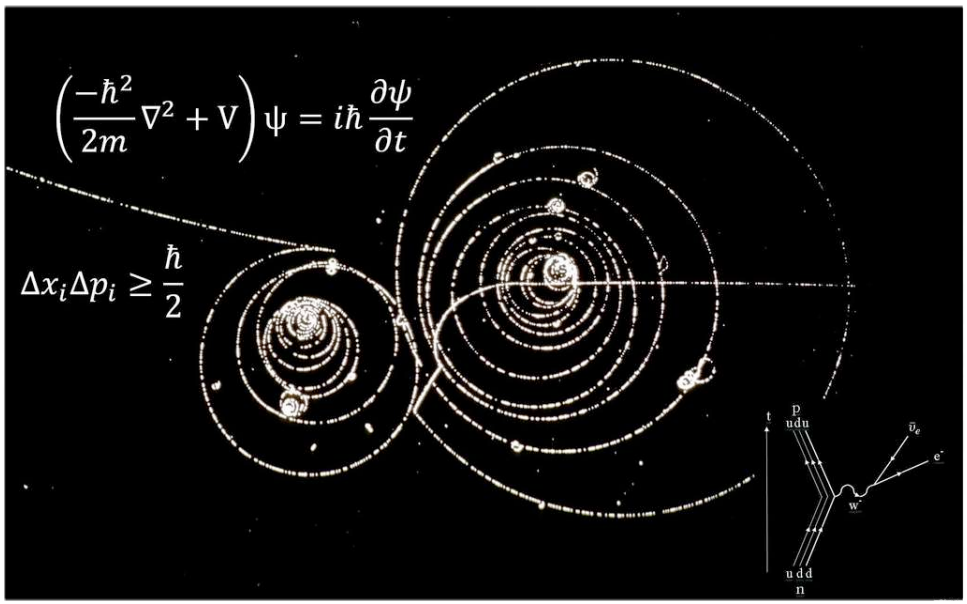
- Pourquoi est-on capable de fabriquer des ordinateurs ?
  - On dispose d'une technologie permettant de fabriquer physiquement des dispositifs qui calculent des fonctions logiques booléennes élémentaires
    - Fonction logiques: ET, OU, NON, etc…
    - Dispositif physique: le transistor
  - On dispose d'une théorie mathématique permettant de faire des calculs complexes à partir de ces fonctions logiques élémentaires
    - L'algèbre de Boole
  - On dispose de techniques permettant de synthétiser des circuits complexes à partir de circuits élémentaires pour réaliser des calculs complexes ainsi que de la mémoire 〈
    - Les techniques de synthèse des circuits combinatoires et séquentiels





C’est quoi un ordinateur quantique ?

- Il s’agit non seulement d’une nouvelle technologie pour construire des circuits mais également d’une manière radicalement différente d’effectuer les calculs et d’écrire les programmes/algorithmes
- L’idée de base est d’exploiter les propriétés de la physique quantique pour faire des calculs
  - On va utiliser plus particulièrement deux principes de la physique quantique
    - La superposition quantique
    - L’intrication quantique



Le principe de superposition quantique

- Le **principe de superposition quantique** dit qu'un objet quantique (échelle de l'atome) peut être dans *plusieurs états en même temps*
  - Exemple de valeurs quantiques: spin, position, quantité de mouvement, …
  - Ce principe n'a d'interprétation *que dans le monde quantique* car c'est une pure conséquence du modèle mathématique sur lequel est basé la physique quantique
    - Ce modèle mathématique utilise des calculs de probabilité pour connaître l'état d'un objet quantique, chaque état étant associée à un coefficient de probabilité
- Si l'on utilise une valeur quantique, par exemple le spin d'un électron, pour implémenter un bit alors ce bit peut être à la fois à zéro et à un ..!
  - On appelle cela un **qubit** (pour *quantum bit*, parfois aussi noté *qbit*)

La décohérence quantique

- La **décohérence quantique** permet d'effectuer le passage entre le monde quantique et le monde physique classique.
  - Les objets physiques classiques que nous observons et manipulons chaque jour, sont constitués de particules élémentaire (atomes,…) qui sont régis par la physique quantique
  - Par contre les phénomènes quantiques, tel que la superposition, ne s'observent pas à l'échelle macroscopique
    - Une tasse ne peut pas être à deux endroits à la fois
- Les lois de la physique quantique sont valables pour un système quantique isolé
  - Un système quantique peut difficilement être complètement isolé car il est en interaction avec un *environnement*. Ces interactions provoquent la disparition rapide des états superposés, c'est la *décohérence quantique*.
  - En particulier, pour **observer** un état quantique on est contraint d'interagir avec l'objet quantique ce qui provoque sa décohérence et donc sa projection dans un état déterminé.

Les états d'un système physique

- En mécanique *classique*, l'état d'un système est représenté par un ensemble de grandeurs physiques à partir duquel on peut déterminer toutes les propriétés du système concerné
  - Par exemple dans le cas d'un point matériel, l'état est complètement décrit par la donnée du vecteur position et de la quantité de mouvement
- En mécanique *quantique*, il n'est pas possible de supposer que les grandeurs physiques aient une valeur définie que l'on puisse mesurer sans perturber le système
  - L'état quantique doit donc être vu comme représentant toute l'information disponible sur le système : une description de l'histoire du système permettant de calculer les probabilités de mesure
    - Il faut comprendre que le système est dans un état quantique unique, mais que les mesures peuvent donner plusieurs résultats différents, chaque résultat étant associé à sa probabilité d'apparaître lors de la mesure.

Les états quantiques

- Pour résoudre ce problème les physiciens/mathématiciens ont élaboré une théorie dans laquelle les états d'un système quantique sont représentés par un vecteur dans un espace vectoriel complexe de Hilbert
  - Un espace vectoriel complexe est un espace vectoriel dans lequel les cordonnées des vecteurs $\in \mathbb{C}$
  - Un espace de Hilbert est un espace vectoriel muni d'un *produit scalaire* euclidien ou hermitien
  - Lorsque l'on associe deux systèmes V_1 et V_2 pour en faire un plus gros, l'espace des états de ce gros système est le *produit tensoriel* des espaces des états associés aux deux sous-systèmes V_1 et V_2.

Produit tensoriel

- Soit deux espaces vectoriels de dimension finie munis de leur base canonique : $\mathcal{E}$ de dimension m et $\mathcal{F}$ de dimension n.
- Soit deux vecteurs : $x \in \mathcal{E}$, de composantes $(x_1, x_2, \ldots, x_m)$, et y $\in \mathcal{F}$, de composantes $(y_1, y_2, \ldots, y_n)$.
- Alors le produit tensoriel x ⊗ y de ces deux vecteurs est la matrice de dimension m × n :

$$x \otimes y = \begin{pmatrix} x_1 y_1 & x_1 y_2 & \cdots & x_1 y_n \\ x_2 y_1 & x_2 y_2 & \cdots & x_2 y_n \\ \vdots & \vdots & & \vdots \\ x_m y_1 & x_m y_2 & \cdots & x_m y_n \end{pmatrix}$$

Exemple:

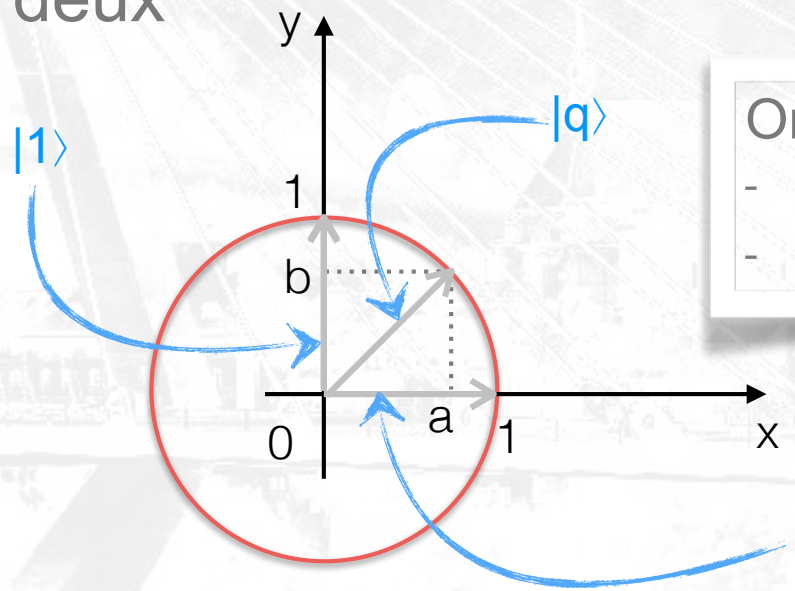
$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Les états quantiques: Notation “bra-ket”

- En logique classique un bit peut prendre deux états que nous notons 0 et 1
  - L’état d’un bit peut être représenté par une variable: *q*
- En logique quantique comme les états sont des vecteurs d’un espace vectoriel de Hilbert, on utilise la notation de Dirac (dite “bra-ket”, 1939). On note les états quantiques *zéro* et *un* de la manière suivante: $|0\rangle$ et $|1\rangle$
  - L’état d’un *qubit* sera noté par la variable : $|q\rangle$ *(aussi dite “ket”)*
  - En toute généralité on a: $\mathbf{|q\rangle = a|0\rangle + b|1\rangle}$
    avec $|a|^2 + |b|^2 = 1$ où *a* et *b* sont des nombres complexes
    ($|q\rangle$ est un vecteur unité dans l’espace vectoriel complexe de dimension 1)
  - $\mathbf{|a|^2}$ est la *probabilité* d’observer le qubit dans l’état $|0\rangle$ et $\mathbf{|b|^2}$ est la *probabilité* d’observer le qubit dans l’état $|1\rangle$

Exemple: Représentation matricielle dans $\mathbb{R}$

- Si on utilise la représentation matricielle habituelle
  - $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $|q\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$
- On peut représenter cela dans un espace vectoriel euclidien de dimension deux



On remarque que:
- $|q\rangle$, $|0\rangle$ et $|1\rangle$ sont des vecteurs
- $|0\rangle$ et $|1\rangle$ forme une base

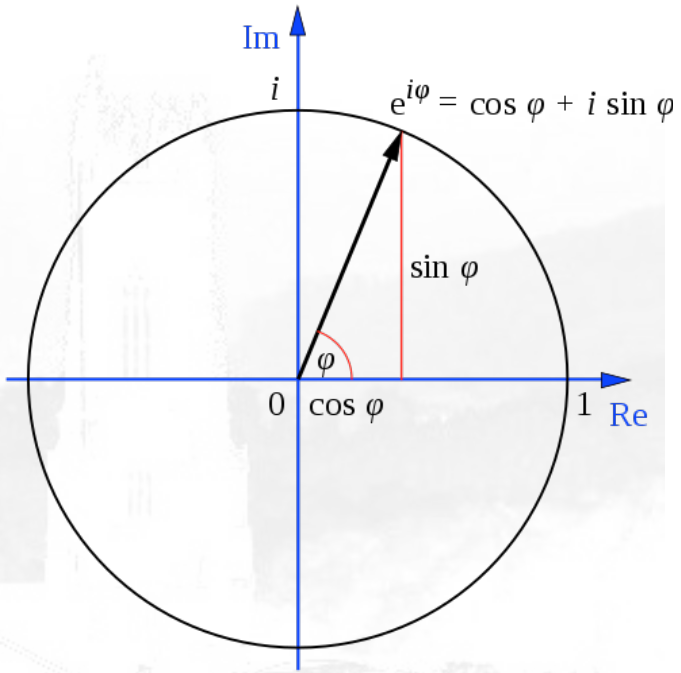
  - Comme $|a|^2 + |b|^2 = 1$, les valeurs possibles pour un qubit se situent sur le cercle de rayon unité centré à l'origine *(en rouge sur le schéma)*

Produit scalaire hermitien

- Dans un espace vectoriel à deux dimensions on définit ainsi un *produit scalaire* hermitien (ou plus simplement "*produit scalaire*"):
  - produit scalaire de $|q\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ par $|q'\rangle = \begin{pmatrix} a' \\ b' \end{pmatrix} = (a,b) \begin{pmatrix} a' \\ b' \end{pmatrix} = \langle q||q'\rangle = a \cdot a' + b \cdot b'$
- Par convention on note ce produit scalaire
  - $\langle q|q'\rangle$ et non ~~$\langle q||q'\rangle$~~
- On voit ici apparaitre la notation $\langle q| = (a,b)$ *(aussi dite "bra")*
  - (a,b) est une *forme linéaire* (ou plus simplement *forme*) noté: $\langle q|$
  - $\begin{pmatrix} a \\ b \end{pmatrix}$ est un *vecteur* noté: $|q\rangle$, c'est le *dual* de la forme $\langle q|$ (et réciproquement)
- On a les propriétés suivantes *(je vous laisse faire la vérification)*
  - $\langle 0|1\rangle = \langle 1|0\rangle = 0$ et $\langle 0|0\rangle = \langle 1|1\rangle = 1$
  - si $q = \begin{pmatrix} a \\ b \end{pmatrix}$ alors $\langle q|0\rangle = a$ et $\langle q|1\rangle = b$

La formule d'Euler: $e^{ix} = \cos(x) + i \sin(x)$

- Elle permet d'écrire: $a+ib = \rho \cdot e^{i\varphi}$
  - Avec: $a=\cos(\varphi)$ et $b=\sin(\varphi)$



- Cette formule peut être interprétée de la façon suivante:
  - la fonction $\varphi \mapsto e^{i\varphi}$, (appelée fonction **cis**), décrit le cercle unité dans le plan complexe lorsque φ varie dans l'ensemble des nombres réels
  - φ représente la mesure de l'angle orienté que fait la demi-droite d'extrémité l'origine et passant par un point du cercle unité avec la demi-droite des réels positifs.
    - La formule n'est valable que si *sin* et *cos* ont des arguments exprimés en radians et non en degrés

  - Cette formule a de nombreuses applications que nous ne détaillerons pas ici

La formule d'Euler: démonstration

Le développement en série de la fonction exp de la variable réelle t peut s'écrire :

$$\mathrm{e}^t = \frac{t^0}{0\,!} + \frac{t^1}{1\,!} + \frac{t^2}{2\,!} + \frac{t^3}{3\,!} + \frac{t^4}{4\,!} + \cdots = \sum_{n=0}^{\infty} \frac{t^n}{n\,!}$$

et s'étend à tout nombre complexe t : le développement en série de Taylor reste absolument convergent et définit l'exponentielle complexe.

En particulier pour $t = \mathrm{i}x$ avec x réel :

$$\mathrm{e}^{\mathrm{i}\,x} = \sum_{n=0}^{\infty} \frac{(\mathrm{i}\,x)^n}{n\,!} = \sum_{n=0}^{\infty} \frac{\mathrm{i}^{\,n} x^n}{n\,!}.$$

Cette série, séparée en deux, devient, en utilisant le fait que $\mathrm{i}^{\,2k} = (\mathrm{i}^{\,2})^k = (-1)^k$:

$$\mathrm{e}^{\mathrm{i}\,x} = \sum_{k=0}^{\infty} \frac{\mathrm{i}^{\,2k} x^{2k}}{(2k)\,!} + \sum_{k=0}^{\infty} \frac{\mathrm{i}^{\,2k+1} x^{2k+1}}{(2k+1)\,!} = \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)\,!} + \mathrm{i} \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)\,!}.$$

On voit *ainsi* apparaître les développements en série de Taylor des fonctions cosinus et sinus

$$\cos(x) = 1 - \frac{x^2}{2\,!} + \frac{x^4}{4\,!} - \frac{x^6}{6\,!} + \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)\,!}$$

$$\sin(x) = x - \frac{x^3}{3\,!} + \frac{x^5}{5\,!} - \frac{x^7}{7\,!} + \cdots = \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)\,!}$$

ce qui, en remplaçant dans l'expression précédente de $\mathrm{e}^{\mathrm{i}x}$, donne bien :

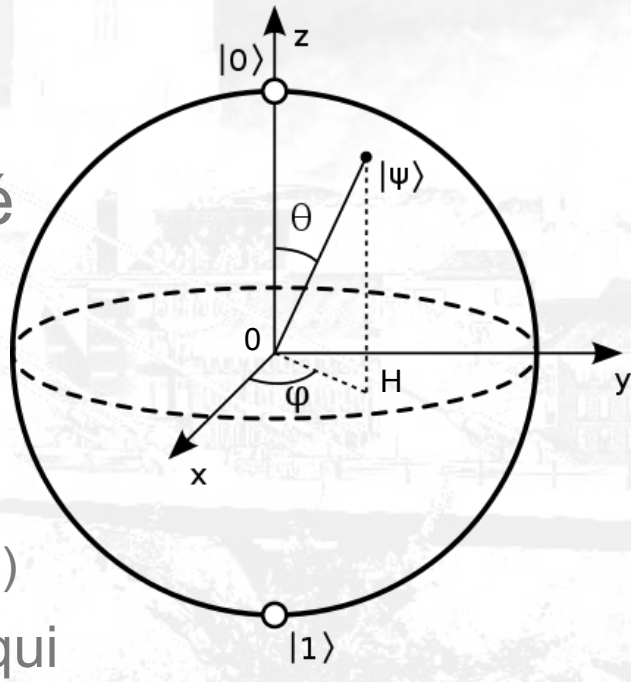
$$\mathrm{e}^{\mathrm{i}\,x} = \cos(x) + \mathrm{i}\,\sin(x).$$

Dimension de l'espace vectoriel des qubits

- Avec ce que nous avons vu, un qubit $|\psi\rangle$ est représenté par un vecteur dans le plan complexe $\mathbb{C}^2$
  - $|\psi\rangle = a|0\rangle + b|1\rangle = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}$ avec $a, b \in \mathbb{C}$ et $|a|^2+|b|^2=1$
    - On dit que $|\psi\rangle$ est une vecteur normalisé
- L'espace des qubits est donc de dimension 3
  - Si on écrit: $a=x_0+iy_0$ et $b=x_1+iy_1$ on peut vérifier que le quadruplet (x_0,y_0,x_1,y_1) est sur la sphère unité de dimension 3 dans l'espace réel euclidien de dimension 4
- Cependant, il est possible de ne considérer qu'un espace de dimension 2 en se restreignant aux qubits dits *purs*.
  - Pour cela il faut considérer comme équivalent des qubits ψ et ψ' s'ils sont proportionnels entre eux, c'est à dire: $|\psi'\rangle = z|\psi\rangle = \begin{pmatrix}za\\zb\end{pmatrix}$ avec $z \in \mathbb{C}$
    - Il est à noter que z est forcément de module 1.

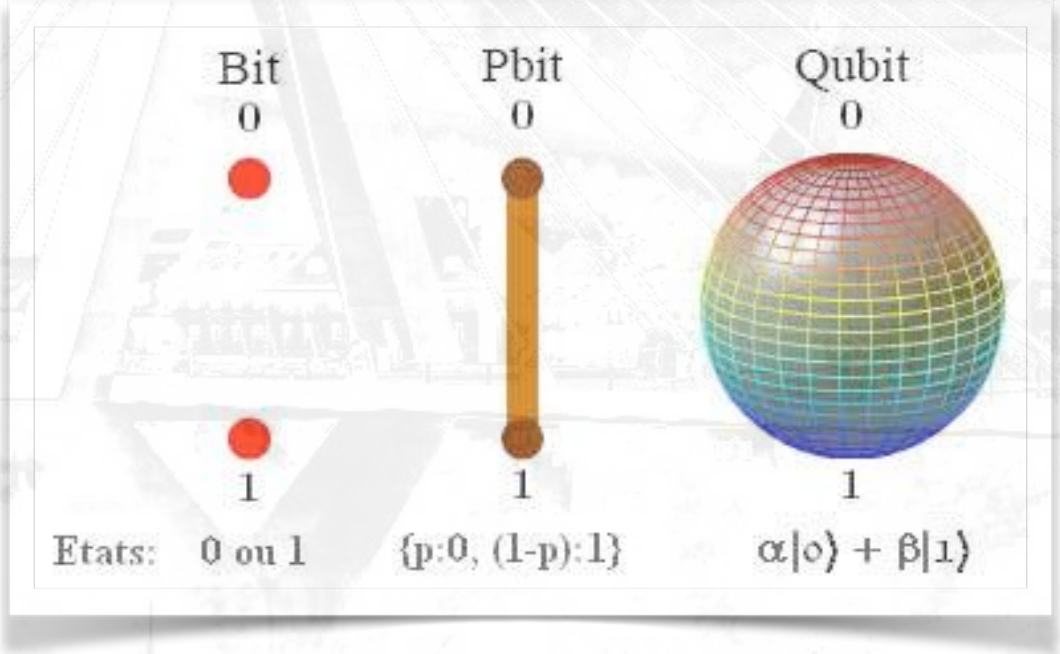
Sphère de Bloch

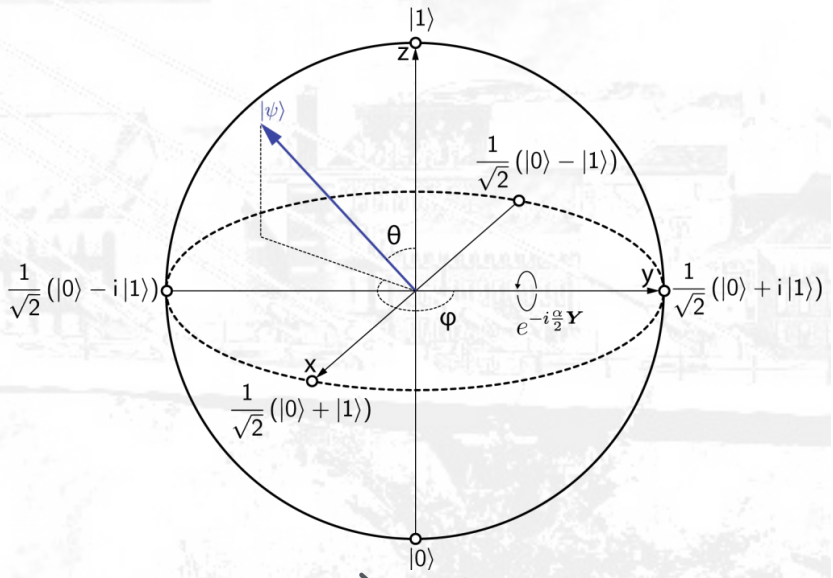
- Il n'existe qu'un seul angle $\theta \in [0,\pi]$ tel que:
  - $|a|=\cos(\theta/2)$ et $|b|=\sin(\theta/2)$
- Les physiciens disent:
  - "puisque les facteurs de phase n'affectent pas l'état physique d'un système, nous pouvons sans perte de généralité supposer a réel positif, et réécrire" *(???)*
    - $|\psi\rangle=\cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle$ avec $0\leq\theta\leq\pi$, $0\leq\varphi< 2\pi$
- Cette représentation décrit ψ sans ambiguïté
  - Les paramètres φ et θ spécifient de manière unique un point sur la sphère unité de $\mathbb{R}^3$ ayant pour coordonnées cartésiennes:
    - **x**=sin θ × cos φ, **y**=sin θ × sin φ et **z**=cos θ
    - Dans cette représentation: $|0\rangle \cong (0, 0, 1)$ et $|1\rangle \cong (0, 0, -1)$
  - L'espace des qubits purs est donc de dimension 2 qui peut être représentée par cette sphère, appelée *sphère de Bloch*



Le qubit: synthèse

- A gauche un bit ordinaire est caractérisé par deux états, 0 ou 1.
- Au centre un *pbit* ou "bit probabiliste". Il représente la distribution des probabilités d'un bit. L'expression indiquée signifie que le *pbit* a une probabilité p d'être dans l'état 0 et 1-p d'être dans l'état 1. C'est l'exemple typique de la pièce de monnaie que l'on jette en l'air : elle a 1 chance sur 2 de tomber sur pile, 1 chance sur 2 de tomber sur face.
- A droite, le *qubit* opère dans un univers multidimensionnel, ses états propres correspondant à la surface d'une sphère dite de Bloch tandis que ses états logiques correspondent aux pôles de cette sphère.





La sphère de Bloch

Opération logiques sur un qubit

- Notre objectif est de définir des “portes logiques quantiques”
  - Pour des raisons liées à la théorie de la physique quantique on ne peut réaliser que des portes logiques quantiques ***réversibles***
    - A partir de la sortie de la porte on peut retrouver l’entrée de cette dernière
  - Exemple
    - La porte NOT : 0->1, 1->0 est réversible
    - La porte RESET : 0->0, 1->0 n’est pas réversible
  - Il existe un théorème en mécanique quantique appelé le théorème de non-clonage *(en 1982 par Wootters, Zurek, et Dieks)*
    - Il est impossible de copier à l'identique un état quantique inconnu et arbitraire
  - En logique classique il existe un théorème qui dit que toute fonction logique peut être construite à partir de l’opération NAND, qui est irréversible, et de l’opération COPY de copie.
    - Les ordinateurs classiques sont construits avec ce principe

Porte logiques quantiques

- Il faut donc trouver des portes logiques quantiques
  - qui soient réversibles
  - n'impliquent pas de copie
  - à partir desquels on puisse réaliser n'importe quelle fonction logique
  - dont les valeurs $\in \mathbb{C}$
- Il a été démontré que tout algorithme irréversible peut être transformé en algorithme réversible à l'aide d'un ensemble universel fini de trois portes réversibles, sans changer la classe de complexité de l'algorithme.
  - La porte de ***Hadamard*** (notée H) à un qubit
    - $H(a|0\rangle+b|1\rangle) = 1/\sqrt{2}((a+b)|0\rangle + (a-b)|1\rangle)$
  - La porte $S(\frac{\pi}{4})$ (notée ***T***) à un qubit
    - $T(a|0\rangle+b|1\rangle) =(a|0\rangle + b\, e^{i\frac{\pi}{4}}|1\rangle)$ [Rappel: $e^{i\frac{\pi}{4}}$ est un nombre complexe]
  - La porte *controlled NOT* (noté ***cNOT***) à deux qubits
    - $cNOT(x, y) = (x, x \oplus y)$ [Note: $\oplus$ est a fonction logique *ou exclusif*]

L’intrication quantique

- Avec tout ce que nous venons de voir il n’est toujours pas possible de réaliser des algorithmes complexes (des calculs) avec le modèle quantique
  - Nous allons exploiter un phénomène quantique supplémentaire appelé l’**intrication quantique**
- L'intrication quantique est un phénomène dans lequel plusieurs objets quantiques ont des états quantiques dépendant les uns des autres quelle que soit la distance qui les sépare
  - Un tel état est dit «intriqué» parce qu'il existe des corrélations entre les propriétés physiques observées de ces différents objets quantiques

L'intrication quantique

- Nous allons définir les états du système à deux qubits
  - On peut ensuite le généraliser à un système à n qubits
- On part des états
  - $|0_A\rangle$ et $|1_A\rangle$ pour le qubit A
  - $|0_B\rangle$ et $|1_B\rangle$ pour le qubit B
- On suppose que chaque qubit se trouve dans un état de superposition
  - qubitA : $|q_A\rangle=\alpha|0_A\rangle+\beta|1_A\rangle$
  - qubitB : $|q_B\rangle=\gamma|0_B\rangle+\delta|1_B\rangle$
- L'état du système global est obtenu par le produit tensoriel
  - $|q_A\rangle|q_B\rangle=\alpha\gamma|0_A\rangle|0_B\rangle+\alpha\delta|0_A\rangle|1_B\rangle+\beta\gamma|1_A\rangle|0_B\rangle+\beta\delta|1_A\rangle|1_B\rangle$
    - Avec la contrainte : $|\alpha\gamma|^2+|\alpha\delta|^2+|\beta\gamma|^2+|\beta\delta|^2=1$

Système quantique à deux qubits

- On a vu que l'état du système est donné par
  - $|q_A\rangle|q_B\rangle = \alpha\gamma|0_A\rangle|0_B\rangle + \alpha\delta|0_A\rangle|1_B\rangle + \beta\gamma|1_A\rangle|0_B\rangle + \beta\delta|1_A\rangle|1_B\rangle$
  - Dans le détail cela signifie que le système peut être projeté
    - dans l'état $|0_A\rangle|0_B\rangle$ avec une probabilité de $\alpha\gamma$

    ou bien
    - dans l'état $|0_A\rangle|1_B\rangle$ avec une probabilité de $\alpha\delta$

    ou bien
    - dans l'état $|1_A\rangle|0_B\rangle$ avec une probabilité de $\beta\gamma$

    ou bien
    - dans l'état $|1_A\rangle|1_B\rangle$ avec une probabilité de $\beta\delta$
  - Avec la contrainte $|\alpha\gamma|^2 + |\alpha\delta|^2 + |\beta\gamma|^2 + |\beta\delta|^2 = 1$
    - Ces états sont **intriqués**, l'état individuel d'un qubit n'est pas défini, c'est le système qui est dans un état défini
    - Ce n'est que lors d'une mesure sur un des qubits que son état se révèle avec une probabilité donné par les coefficients de l'état intriqué

Exemple

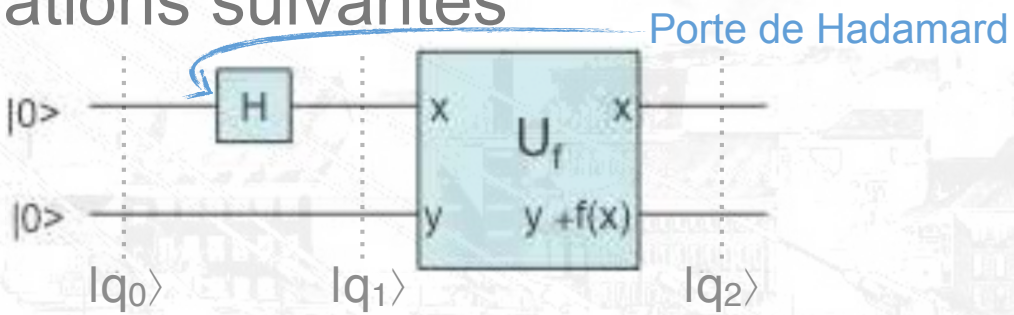
- Un exemple particulièrement utilisé d'état intriqué à deux qubits est le *premier état de Bell* défini par
  - $|\beta_{00}\rangle = 1/\sqrt{2}\ (1|00\rangle + 0|01\rangle + 0|10\rangle + 1|11\rangle) = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$
- Tant qu'aucune mesure n'est effectuée sur le système l'état de chaque qubit n'est pas défini.
- Mesurons le premier qubit, supposons qu'on trouve l'état $|0\rangle$
  - Cela signifie que l'état $|\beta_{00}\rangle$ est projeté sur l'état $|00\rangle$ car l'état $|01\rangle$ n'est pas possible (sa probabilité est de 0) ce qui entraîne que le deuxième qubit est forcément lui aussi dans l'état $|0\rangle$
    - Les deux états sont intriqués

Registre quantique

- On peut schématiser un ordinateur classique (machine de Turing) à l'aide de trois composants
  - des registres qui contiennent les données à traiter
  - une unité de calcul qui transforme les données suivant un algorithme défini en actionnant des portes logiques
  - une unité d'entrées/sorties qui initialise les registres au début du traitement et lit les résultats à la fin.
  - Un registre classique est un ensemble de n bits permettant de stocker les $N = 2^n$ entiers compris entre 0 et $2^n - 1$
- Un **registre quantique** est une registre contenant des qubits.
  - Un registre quantique de *n qubits* est donc un système quantique dont les états seront éléments de l'espace des états de dimension $N = 2^n$.
  - Là ou la "magie quantique" apparait c'est qu'en évaluant une fonction f sur un registre quantique on peut l'évaluer sur l'ensemble des 2^n valeurs
    - Si les qubits du registre sont dans des *états superposés*

Exemple simple

- Le parallélisme est un trait caractéristique de beaucoup d'algorithmes quantiques dans lesquels une fonction f(x) peut être évaluée simultanément pour plusieurs valeurs de x
- Prenons l'exemple d'une fonction sur un seul qubit
  - On a un registre d'entré et un registre de sortie, ces deux registres contiennent initialement la valeur $|0\rangle$ (ou $|00\rangle$)
- Effectuons la succession d'opérations suivantes
  - $|q_0\rangle = |00\rangle$
  - $|q_1\rangle = 1/\sqrt{2}\ (|00\rangle + |10\rangle)$
  - $|q_2\rangle = 1/\sqrt{2}\ (|0,f(0)\rangle + |1,f(1)\rangle)$



- L'état de sortie, $|q_2\rangle$, est remarquable car il contient à la fois 0,f(0) et 1,f(1) obtenus par une seule application de la porte U_f
  - Cela peut être généralisé à un nombre quelconque de bits d'entrée

Parallélisme quantique

- On peut dire que le phénomème que nous venons de voir permet de calculer “en même temps” ou “en parallèle” toutes les valeurs d’une fonction f
  - Cette propriété n’est toutefois pas, à priori, exploitable puisqu’au moment de ”lire” le qubit on ne récupère aléatoirement qu’un des états $|x,f(x)\rangle$

Pause……

L'algorithme de Deutsch

- En étant astucieux on peut quand même obtenir plus d'information qu'une seule valeur de la fonction f
- Deutsch s'est intéressé aux fonctions sur 1 bit
  - Soit $Z_2 = \{0,1\}$ et une fonction $f : Z_2 \rightarrow Z_2$
- En fait, il n'y a que quatre fonctions f possibles
  - $f_1(x)$ tel que: $f_1(0)=0$ et $f_1(1)=0$
  - $f_2(x)$ tel que: $f_2(0)=1$ et $f_2(1)=1$

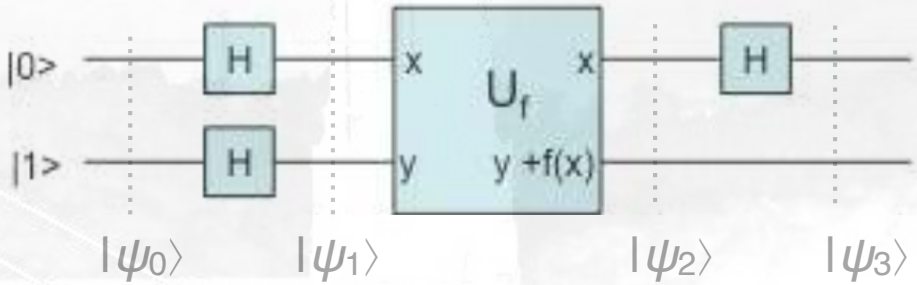
  } fonctions constantes

  - $f_3(x)$ tel que: $f_3(0)=0$ et $f_3(1)=1$
  - $f_4(x)$ tel que: $f_4(0)=1$ et $f_4(1)=0$

  } fonctions équilibrées

Algorithme de Deutsch

- On veut déterminer si une fonction f : $Z_2 \rightarrow Z_2$ inconnue est constante ou équilibrée
  - En informatique classique l'algorithme consiste à évaluer f(0) et f(1) et à comparer les deux valeurs obtenues
- Soit le circuit quantique suivant



  - Si l'on effectue les calculs on obtient pour le premier qubit de $|\psi_3\rangle$

$$\frac{1}{2\sqrt{2}}\left[(-1)^{f(0)}+(-1)^{f(1)}\right]|0\rangle+\frac{1}{2\sqrt{2}}\left[(-1)^{f(0)}-(-1)^{f(1)}\right]|1\rangle$$

    - Si la fonction f est constante
      - alors f(0) = f(1) et le premier qubit vaut $\pm|0\rangle$
    - Si la fonction est équilibrée
      - alors f(0)≠ f(1) alors le premier qubit vaut $\pm|1\rangle$
    - On a donc pu déterminer **en une seule action** de la porte U_f une propriété globale de f
    - Ce gain peut être beaucoup plus important avec un registre de donné à n qubits
      - Une seule action de U_f au lieu de en pire cas $2^{n-1} + 1$ pour une algo. classique

Détail du développement de l'algo de Deutsch

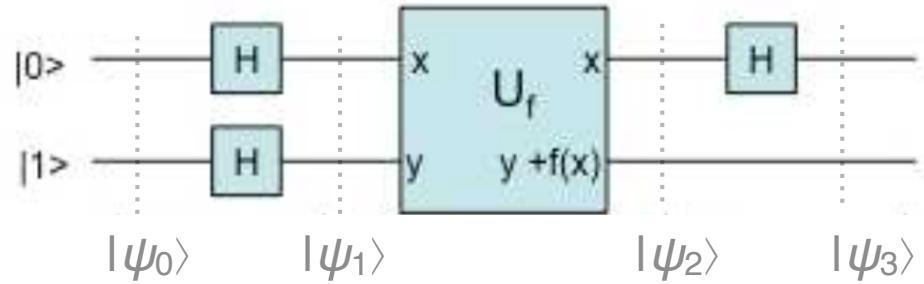


FIGURE 3.3 – algorithme de Deutsch

Introduction à l'information quantique
Y. Leroyer et G. Sénizergues
ENSEIRB-MATMECA , 2016-2017

- $|\psi_0\rangle = |01\rangle$
- $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}\left[\sum_{x=0,1}|x\rangle\right](|0\rangle - |1\rangle) = \frac{1}{2}\sum_{x=0,1}[|x,0\rangle - |x,1\rangle]$
- $|\psi_2\rangle = \frac{1}{2}\sum_{x=0,1}[|x,0\oplus f(x)\rangle - |x,1\oplus f(x)\rangle]$; pour déterminer cette expression remarquons que $y \oplus f(x) = y$ si $f(x) = 0$, et $\overline{y}$ (complément) sinon ; donc

$$\begin{aligned} |x,0\oplus f(x)\rangle - |x,1\oplus f(x)\rangle &= |x,0\rangle - |x,1\rangle \text{ si } f(x)=0 \\ &= |x,1\rangle - |x,0\rangle \text{ si } f(x)=1 \end{aligned}$$

En résumé $(|x,0\oplus f(x)\rangle - |x,1\oplus f(x)\rangle = (-1)^{f(x)}[|x,0\rangle - |x,1\rangle]$.
Donc $|\psi_2\rangle = \frac{1}{2}\sum_{x=0,1}(-1)^{f(x)}[|x,0\rangle - |x,1\rangle] = \left\{\frac{1}{2}\sum_{x=0,1}(-1)^{f(x)}|x\rangle\right\}\{|0\rangle - |1\rangle\}$

- On envoie le premier qubit sur une porte de Hadamard ; l'état résultant de *ce qubit* sera

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{2\sqrt{2}}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2\sqrt{2}}(-1)^{f(1)}(|0\rangle - |1\rangle) \\ &= \frac{1}{2\sqrt{2}}\left[(-1)^{f(0)} + (-1)^{f(1)}\right]|0\rangle + \frac{1}{2\sqrt{2}}\left[(-1)^{f(0)} - (-1)^{f(1)}\right]|1\rangle \end{aligned}$$

Si la fonction f est constante, alors $f(0) = f(1)$ et le qubit vaut $\pm|0\rangle$; si la fonction est *équilibrée* (balanced) c'est-à-dire $f(0) \neq f(1)$ alors le qubit vaut $\pm|1\rangle$.

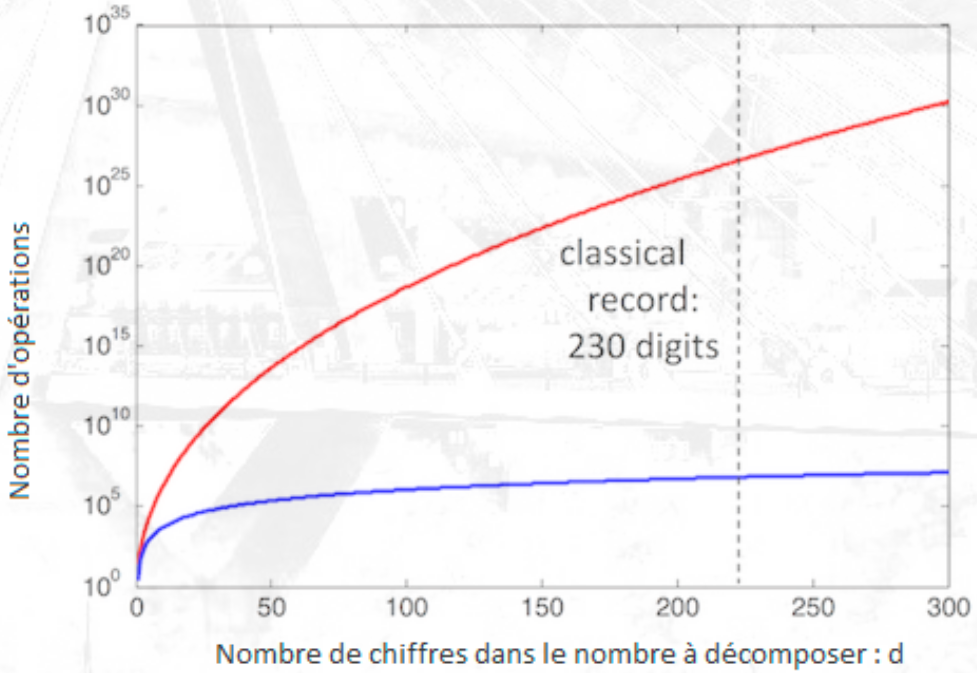
Difficultés

- Il faut que les qubits soient stables
  - L'environnement les entourant ne doit pas modifier leur valeur par accident
    - Par un transfert d'énergie thermique par exemple
    - Pour cela, certains ordinateurs quantiques sont refroidis à des températures très proches du zéro absolu (-273,15° !)
  - Faire en sorte que les qubits gardent leurs propriétés quantiques malgré leur manipulation via les portes quantiques est très délicat
    - La décohérence quantique est le problème majeur
- Toutefois..
  - IBM annonce le développement d'un ordinateur quantique capable de traiter 50 qubits quantiques.
    - IBM explique avoir réussi à maintenir l'état quantique des deux systèmes pendant 90 microsecondes.
  - Une annonce faite lors du Sommet de l'industrie de l'IEEE sur l'avenir de l'informatique qui se tenait à Washington ce vendredi (10 Novembre 2017)

http://sciencepost.fr/2017/11/ibm-annonce-ordinateur-quantique-a-50-qubits/

Faut-il avoir peur ?

- Pourquoi les ordinateurs quantiques inquiètent
  - Un algorithme quantique, **l'algorithme de Shor**, permet de casser le protocole RSA qui est utilisé pour le chiffrage des messages dans les connexions sécurisées entre ordinateurs
    - Chiffrage asymétrique sur lequel sont basés tout les protocoles sécurisés actuels
      - SSH, TLS,….



$\exp(\text{const} \times d^{1/3})$

Meilleur algorithme classique

$\text{const} \times d^3$

Algorithme quantique de Shor

16 nov. 2017

https://www.futura-sciences.com/tech/actualites/informatique-ibm-progresse-vers-ordinateur-quantique-futur-37117/

- IBM aurait réalisé un nouveau record en créant un circuit quantique supraconducteur utilisable pour faire du calcul quantique.
  - Le circuit en question contient 50 qubits et serait capable de lutter victorieusement contre la décohérence pendant 90 microsecondes.
- Une version avec 20 qubits sera disponible pour les clients d'IBM d'ici la fin de l'année.
  - Ces nouveaux hardwares le confirment : IBM s'est bien lancée dans la course aux ordinateurs quantiques. Big Blue pourrait bientôt apporter la preuve que ses machines ont atteint la suprématie quantique avec 50 qubits.
- 15 jan 2018 https://www.channelnews.fr/ibm-devoile-nouvel-ordinateur-quantique-ne-faire-fonctionner-78982
  - IBM dévoile son nouvel ordinateur quantique au CES mais ne peut pas le faire fonctionner

Conclusion

- Cette petite introduction a montré que l'on peut potentiellement exploiter les propriétés de la physique quantique pour réaliser des ordinateurs pouvant exécuter certains calculs de manière beaucoup plus rapide que les ordinateurs classiques
  - Un ordinateur quantique est toujours associé avec un ordinateur classique
    - Il agit comme un co-processeur de l'ordinateur classique qui prépare les registres quantiques d'entrée et lit le résultat

- mercredi 10 janvier 2018

http://www.clubic.com/technologies-d-avenir/actualite-841266-2018-puce-49-qubits-intel-prend-tete-course-quantique.html

  - Mike Mayberry, vice-président et directeur d'Intel Labs, estime qu'il faudra attendre au moins 5 ans avant que les ordinateurs quantiques ne soient en mesure de résoudre des problèmes complexes
  - Pour un système commercialement viable, en outre, il faudrait atteindre un minimum de 1 million de qubits : autant dire que ce n'est pas demain que ça arrivera