GRENOBLE INP Ensimag UGA

École nationale supérieure d'informatique et de mathématiques appliquées

Introduction à l'Informatique Quantique

Introduction, premiers éléments

2024

Alastair Abbott
Franck Balestro
Mnacho Echenim
Mehdi Mhalla

Présentation

Franck Balestro
- Enseignant-chercheur UGA
- franck.balestro@neel.cnrs.fr

Mehdi Mhalla
- Chargé de recherche CNRS
- mehdi.mhalla@univ-grenoble-alpes.fr

Alastair Abbott
- Chargé de recherche Inria
- alastair.abbott@inria.fr

Mnacho Echenim
- Enseignant-chercheur Ensimag
- mnacho.echenim@univ-grenoble-alpes.fr

Sommaire

- Les origines
  - De la mécanique quantique
  - De l'informatique quantique
- Les bases de l'informatique quantique
  - Qubits
  - Transformations
  - Mesures
  - Systèmes à deux qubits
  - Intrication
  - Le paradoxe EPR

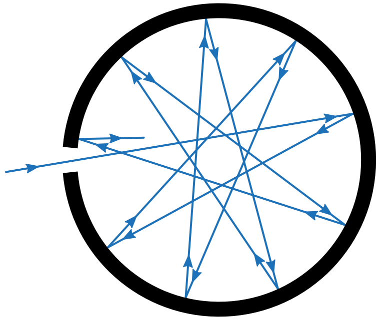
Les origines

Des failles dans la physique classique

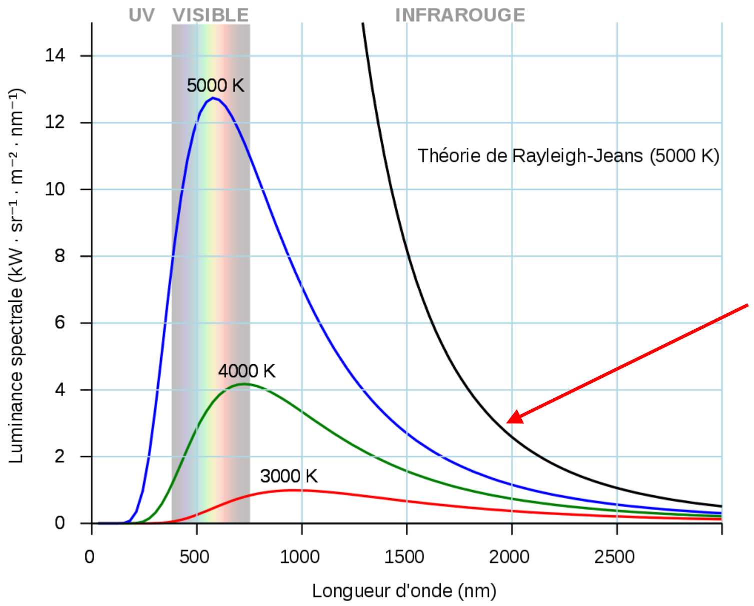
- A la fin du XIXe siècle, la physique classique est bien établie et explique les observations expérimentales
- Mais il reste quelques « *nuages dans le ciel serein de la physique théorique* » (Lord Kelvin):
    - Comment expliquer qu'un corps noir à une température donnée n'émette pas une quantité infinie d'énergie?
    - Comment expliquer qu'un métal éclairé par de la lumière émette des électrons dans certains conditions?
    - Comment expliquer que l'atome d'hydrogène soit stable et n'émette pas un spectre continu de lumière?
- Avis consensuel: la physique classique finira par expliquer ces observations

Les *quantas* d'énergie

- Le rayonnement de corps noir



Source: AG Caesar, CC BY-SA 4.0

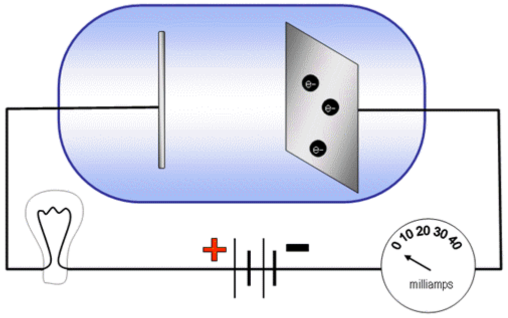


Source: Darth Kule, CC BY-SA 4.0

- La solution de Max Planck
  - L'énergie est transmise par paquets discrets
  - Les *quantas* d'énergie
  - Introduction de la constante de Planck
  - Prix Nobel en 1918

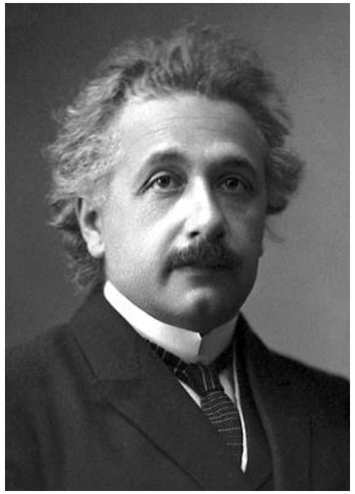
Les photons

- L'effet photoélectrique

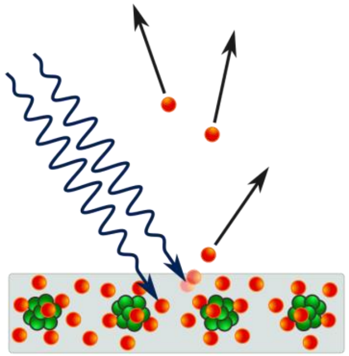


Source: Steemit

- La solution d'Albert Einstein
  - La lumière est constituée de *photons*
  - Chaque photon transporte un *quantum* d'énergie
  - Prix Nobel en 1921



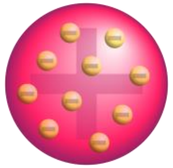
Auteur inconnu



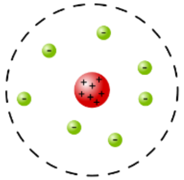
Source: Ponor, CC BY-SA 4.0

L'atome d'hydrogène

1897: découverte de l'électron

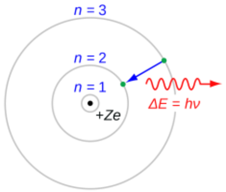


1904: modèle de Thomson



Source: [Bensteel1995]

1911: modèle de Rutherford



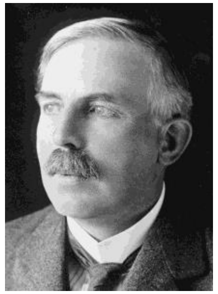
Source: [JabberWok]

1913: modèle de Bohr

Découverte du noyau atomique

Stabilité de l'atome?
Raies spectrales?

J. J. Thomson
(Nobel 1906)



E. Rutherford
(Nobel 1908)

N. Bohr
(Nobel 1922)

Le congrès de Solvay, 1927

E. Schroedinger
W. Pauli
W. Heisenberg
P. Dirac
L. De Broglie
M. Born
N. Bohr
M. Planck
A. Einstein

Les postulats de la physique quantique

- Un formalisme mathématique pour décrire les états quantiques
- Efficacité: il a permis de prédire de nombreux phénomènes quantiques
- Mais son interprétation suscite encore des débats
  - Le chat de Schrödinger est à la fois vivant et mort
  - La lumière est à la fois une onde et un corpuscule
  - Un électron se retrouve à plusieurs endroits en même temps
- Quelques conclusions:
  - *If you are not completely confused by quantum mechanics, you do not understand it* (John Wheeler)
  - *Quantum mechanics makes absolutely no sense* (Roger Penrose)

La naissance de l'informatique quantique

P. Benioff
(crédit: Justinhsb)

R. Feynman
(crédit: Fondation Nobel)

Bennet & Brassard
(crédits: IBM Research et Lëa-Kim Châteauneuf)

D. Deutsch
(crédit: David Deutsch)

1980 — Il est théoriquement possible de créer un ordinateur quantique

1981 — Pour simuler un système quantique, il faut construire un ordinateur quantique

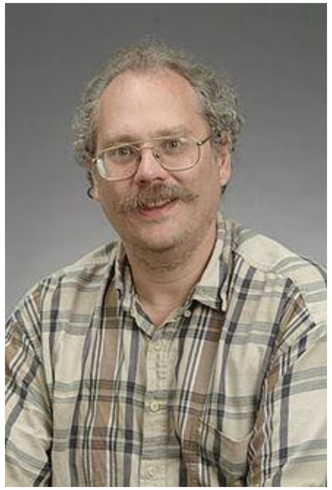
1984 — Premier protocole de cryptographie quantique

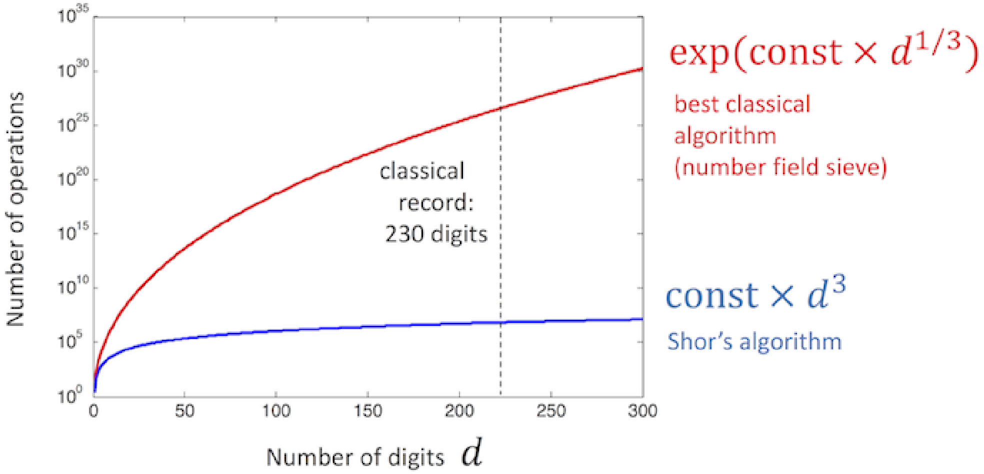
1985 — Machine de Turing Quantique

Conception des premiers algorithmes quantiques

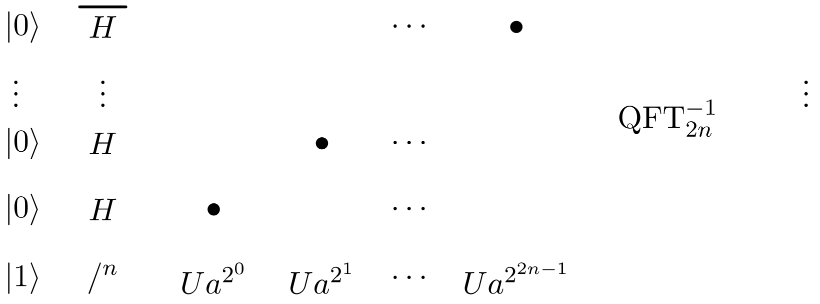
L'algorithme de Shor

- En 1994, Peter Shor développe un algorithme quantique pour factoriser les nombres entiers
  - Algorithme nécessitant $O(d)$ qubits et $O(d^3)$ portes quantiques pour un nombre à d chiffres
  - Les meilleurs algorithmes classiques nécessitent $O\left(e^{\sqrt[3]{d}}\right)$ opérations



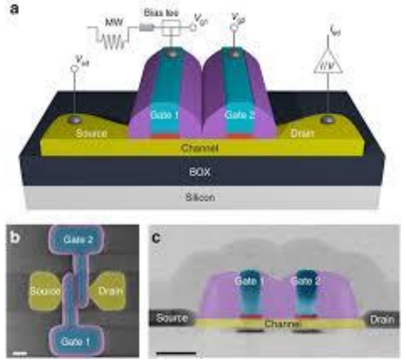


Source: [Medium]



Conséquences de l'algorithme de Shor

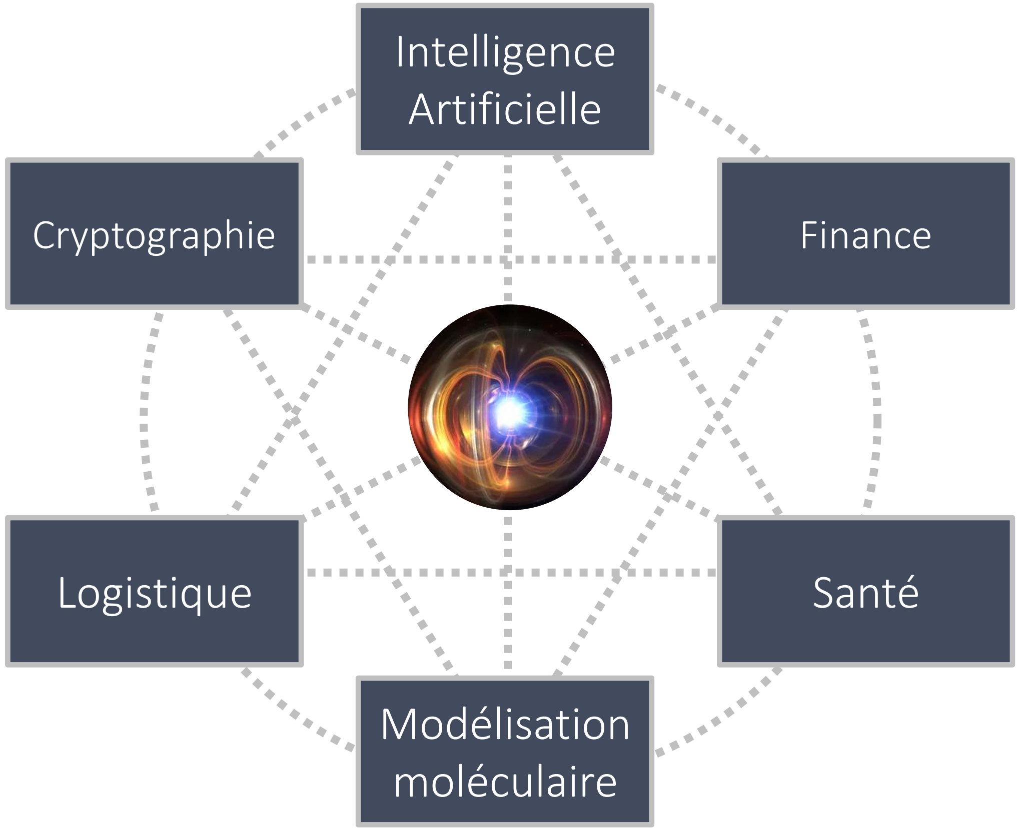
- Avec un ordinateur quantique, il serait possible de casser un chiffrement RSA de 2048 bits en 8 heures avec 2 millions de qubits
- Quelques conséquences
  - Quelle cryptographie pour demain?
    - Protocoles quantiques?
    - Cryptographie post-quantique?
    - NIST 2019: *post-quantum cryptography standardization* (4 finalistes en 2022)
  - Quelle technologie pour créer un ordinateur quantique?
    - Supraconducteurs?
    - Semi-conducteurs?
    - Atomes froids?
    - Autre?



L'informatique quantique aujourd'hui

- Domaine de recherche actif
  - *Quantum algorithm zoo:* https://quantumalgorithmzoo.org
    - Recherche dans une base non-ordonnée: $O(n) \rightarrow O(\sqrt{n})$
    - Résolution d'équations linéaires: $O(N \cdot \kappa) \rightarrow O(\log(N) \cdot \kappa^2)$
  - *Quantum protocol zoo:* https://github.com/quantumprotocolzoo/protocols
- Investissements publics et privés importants
  - USA (>2Md$), Chine (10Md$), UK (>1Md£), Allemagne (2Md€), France (1,8Md€)
  - IBM, Google
    - « Suprématie quantique » annoncée par Google en 2019
    - *IBM Quantum* Heron : processeur à 133 qubits en 2023
  - Sociétés dédiées au quantique
    - Pasqal (100 qubits), Alice & Bob, IonQ, Rigetti, Quobly

Impact de l'informatique quantique



Sources:

- *Inria* (Déc. 2020). « Sept domaines impactés par l'informatique quantique »
- *Les Notes scientifiques de l'Office* (Mars 2019): « Les technologies quantiques: introduction et enjeux »

Les bases de l’informatique quantique

Le qubit

- Le système quantique le plus simple est le **qubit**
- L'état d'un qubit est décrit par un vecteur d'état de dimension 2, à coefficients dans $\mathbb{C}$ et de norme 1
- Notations:

$$\vec{\psi} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

où $|\alpha_0|^2 + |\alpha_1|^2 = 1$

Le qubit

- Le système quantique le plus simple est le **qubit**
- L'état d'un qubit est décrit par un vecteur d'état de dimension 2, à coefficients dans $\mathbb{C}$ et de norme 1
- Notations:

$$\vec{\psi} = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

où $|\alpha_0|^2 + |\alpha_1|^2 = 1$

Le qubit

- Le système quantique le plus simple est le **qubit**
- L'état d'un qubit est décrit par un vecteur d'état de dimension 2, à coefficients dans $\mathbb{C}$ et de norme 1
- Notations:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

Notation de **Dirac**

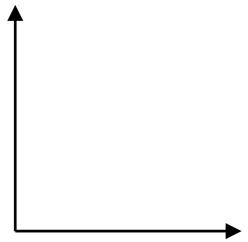
où $|\alpha_0|^2 + |\alpha_1|^2 = 1$

- Exemples:

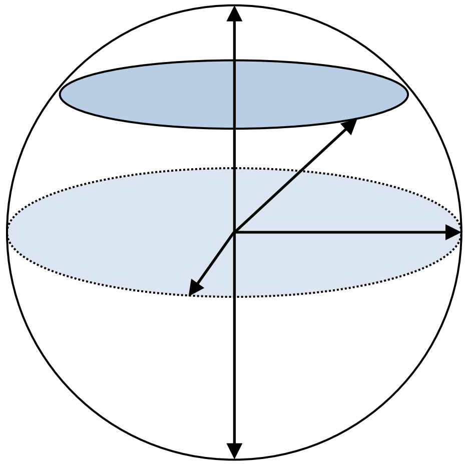
$$|0\rangle \qquad |1\rangle \qquad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \qquad \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

Bit classique et qubit

- Le bit classique
  - Deux vecteurs possibles

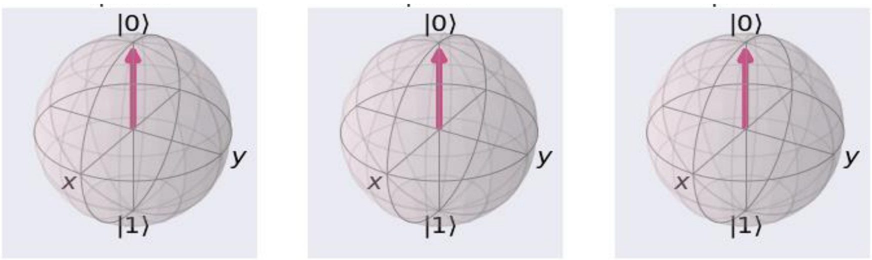


- Le qubit
  - N'importe quel vecteur sur la **sphère de Bloch**



Transformations de qubits

- On peut appliquer au qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ toute transformation U qui:
  - Est linéaire: $U(|\psi\rangle) = \alpha_0 U(|0\rangle) + \alpha_1 U(|1\rangle)$
  - Préserve les normes: $U(|\psi\rangle)$ est aussi un qubit



Source: [Quanta.Guru]

- Les transformations vérifiant ces propriétés sont les matrices unitaires
  - $U^\dagger U = UU^\dagger = I$, où $\left(U^\dagger\right)_{i,j} = \overline{U_{j,i}}$
  - L'image de $|\psi\rangle$ par U est le produit $U \cdot |\psi\rangle$
- **Nb:** les transformations quantiques sont inversibles
  - Toute manipulation sur un système quantique est nécessairement réversible

Exemples de transformations

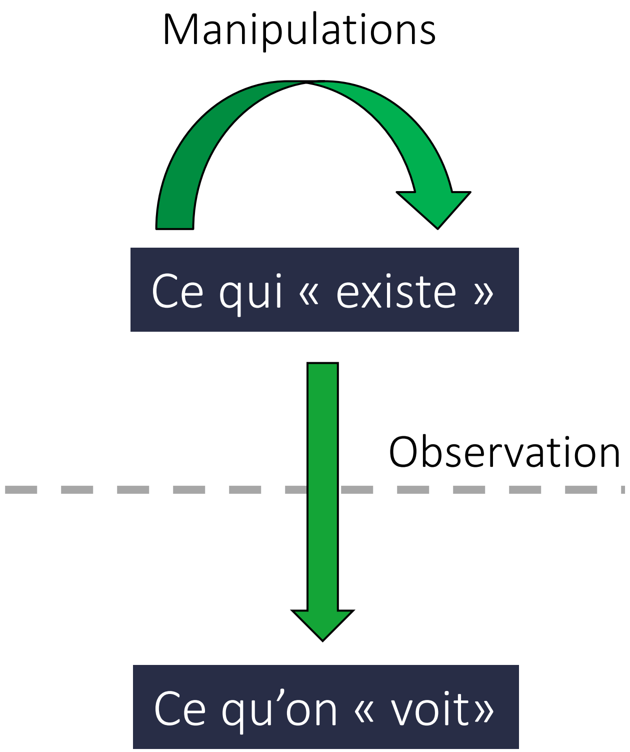
- La porte X (ou **NOT**): $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
  - $X|0\rangle = |1\rangle$ et $X|1\rangle = |0\rangle$

- La porte Z (ou « **phase-flip** »): $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
  - $Z|0\rangle = |0\rangle$ et $Z|1\rangle = -|1\rangle$

- La porte H (ou **de Hadamard**): $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
  - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ et $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$
  - $H|+\rangle = H\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |0\rangle$ et $H|-\rangle = H\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = |1\rangle$

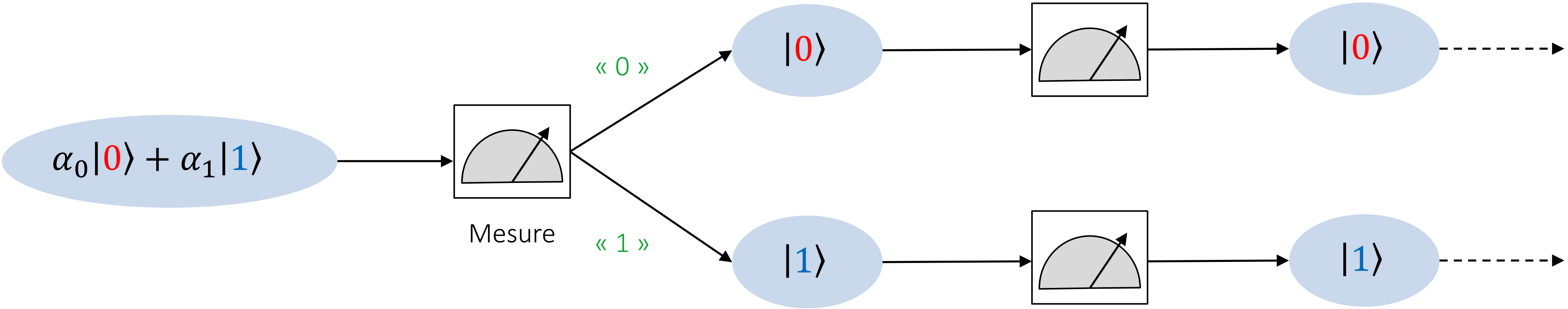
Description d’un qubit

- Que faut-il pour décrire totalement l’état du qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$?
  - Les valeurs des nombres complexes α_0 et α_1
- Peut-on mesurer ces valeurs?
  - Non!
- La mesure d’un qubit
  - Modifie l’état du qubit
  - Renvoie un résultat classique (« 0 » ou « 1 »)
  - Ce résultat classique est probabiliste



Mesure d'un qubit

- Un appareil mesurant le qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ renverra:
  - La valeur « 0 » avec une probabilité $|\alpha_0|^2$
  - La valeur « 1 » avec une probabilité $|\alpha_1|^2$
- Si la valeur renvoyée est « 0 » alors le qubit se retrouve dans l'état $|0\rangle$
  - Toute mesure sur ce nouvel état renverra également « 0 »
- Si la valeur renvoyée est « 1 » alors le qubit se retrouve dans l'état $|1\rangle$
  - Toute mesure sur ce nouvel état renverra également « 1 »



Exemples

- $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$
  - $P(0) = P(1) = \frac{1}{2}$
- $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right)$
  - $P(0) = P(1) = \frac{1}{2}$
- $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$
  - $P(0) = \frac{1}{4}$ et $P(1) = \frac{3}{4}$

Les systèmes à plusieurs qubits

- Le qubit est le système quantique le plus simple
- Pour pouvoir exploiter tout le potentiel de la mécanique quantique, il faut être capable de manipuler plusieurs qubits en même temps
- Ce qui suit:
  - Les systèmes à 2 qubits
    - Description
    - Transformation
    - Mesure
- Une conséquence des postulats

Systèmes à 2 qubits

- Soient deux qubits $|\psi\rangle$ et $|\phi\rangle$. Le système physique constitué de ces deux qubits est décrit par le vecteur $|\psi\rangle \otimes |\phi\rangle$
- Le symbole « $\otimes$ » représente le **produit tensoriel**
  - Comme $|\psi\rangle \in \mathbb{C}^2$ et $|\phi\rangle \in \mathbb{C}^2$, on a $|\psi\rangle \otimes |\phi\rangle \in \mathbb{C}^4$
  - Si $|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ et $|\phi\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$ alors $|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$
- **Nb:** on pourra noter $|\psi\phi\rangle$ ou encore $|\psi\rangle|\phi\rangle$ à la place de $|\psi\rangle \otimes |\phi\rangle$

Exemples

- $|1\rangle \otimes |0\rangle = |10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$

- $|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$

- $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = \frac{1}{2}\big(|00\rangle - |11\rangle + i(|01\rangle + |10\rangle)\big)$

Systèmes à 2 qubits: intrication

- L'état d'un système à 2 qubits est décrit par un vecteur d'état de dimension 4 à coefficients dans $\mathbb{C}$ et de norme 1
  - Quand ce vecteur s'écrit sous la forme $|\psi\rangle \otimes |\phi\rangle$, on dit que le système est dans un état séparable
- Y a-t-il des systèmes à 2 qubits dont l'état n'est pas séparable?
  - Oui, par exemple: $\Phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - On dit que de tels systèmes sont dans un état intriqué, ou bien enchevêtré

L'intrication quantique est une propriété clé en cryptographie quantique et pour les algorithmes quantiques

Transformations de systèmes à 2 qubits

- Ce sont les matrices unitaires sur $\mathbb{C}^{4\times 4}$
- Exemples:
  - Opérations locales sur chaque qubit

$$(X \otimes H)|01\rangle = X|0\rangle \otimes H|1\rangle = |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$$

  - Opérations sur les 2 qubits

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

$$\begin{cases} \text{CNOT}|00\rangle = |00\rangle \\ \text{CNOT}|01\rangle = |01\rangle \\ \text{CNOT}|10\rangle = |11\rangle \\ \text{CNOT}|11\rangle = |10\rangle \end{cases}$$

$$\text{CNOT}|xy\rangle = |x\rangle \otimes |x \oplus y\rangle$$

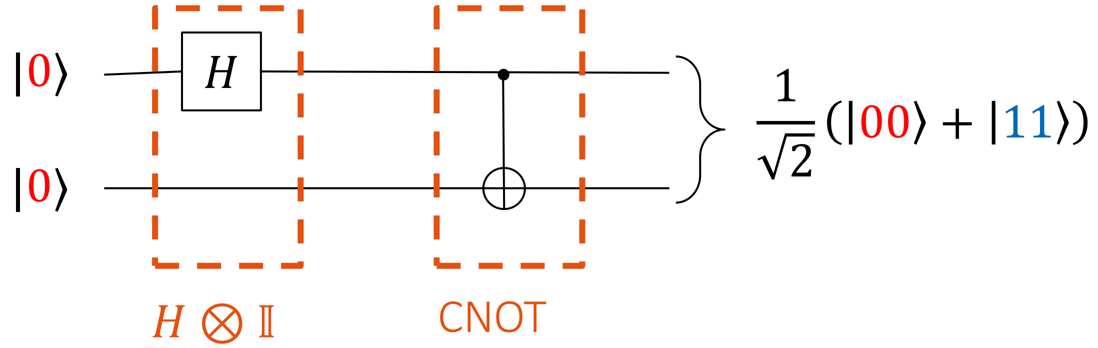
Exemple: construction d'un état intriqué

- Quelle transformation permet de passer de $|00\rangle$ à $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?
  - Réponse: $\text{CNOT} \cdot (H \otimes \mathbb{I})$

$$(H \otimes \mathbb{I})|00\rangle = H|0\rangle \otimes \mathbb{I}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

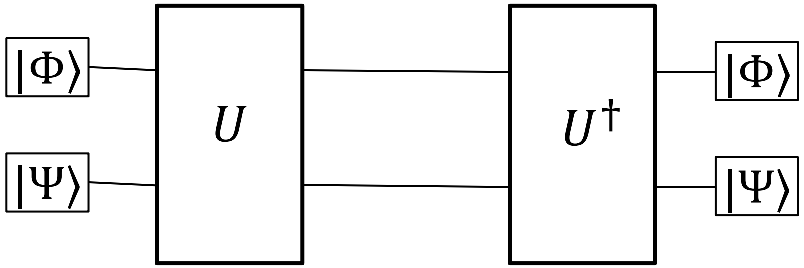
$$\text{CNOT} \cdot (H \otimes \mathbb{I})|00\rangle = \frac{1}{\sqrt{2}}\text{CNOT}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Représentation graphique:

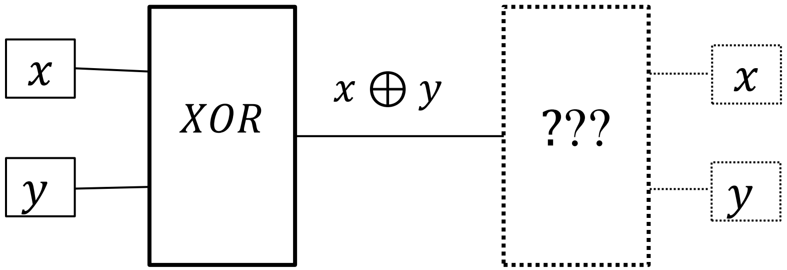


Quelles opérations logiques??

- Toutes les transformations sur les qubits sont *réversibles*



- Les opérations logiques sur les bits classiques ne sont *pas* réversibles



Comment va-t-on pouvoir programmer des algorithmes sans opération de base?

Aparté: *no cloning* en 3 minutes

« Il est impossible de construire une copie identique et indépendante d'un état quantique arbitraire et inconnu »

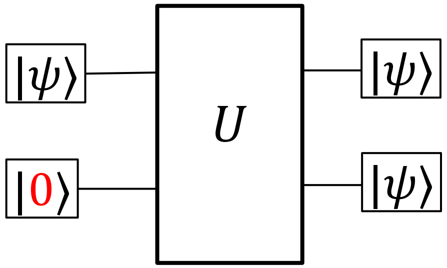
Un (tout petit) peu de mathématiques

- « Bra » et « Ket »
  - $|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ « ket de psi »
  - $\langle\psi| = \begin{pmatrix} \overline{\alpha_0} & \overline{\alpha_1} \end{pmatrix}$ « bra de psi »
  - Si $|\phi\rangle = U \cdot |\psi\rangle$ alors $\langle\phi| = \langle\psi| \cdot U^\dagger$
- Propriétés
  - Pour tout qubit $|\psi\rangle$, on a
    $$\langle\psi|\psi\rangle = \|\psi\|^2 = 1$$
  - Si U est unitaire et $|\phi\rangle = U \cdot |\psi\rangle$ alors
    $$\langle\phi|\phi\rangle = \left(\langle\psi| \cdot U^\dagger\right) \cdot (U \cdot |\psi\rangle) = \langle\psi|\psi\rangle$$
  - Produit scalaire d'un produit tensoriel:
    $$(\langle\phi| \otimes \langle\psi|) \cdot (|\phi'\rangle \otimes |\psi'\rangle) = \langle\phi|\phi'\rangle \cdot \langle\psi|\psi'\rangle$$
- Produit
  - $\langle\psi| = \begin{pmatrix} \overline{\alpha_0} & \overline{\alpha_1} \end{pmatrix}$
  - $|\phi\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$
  - $\langle\psi| \cdot |\phi\rangle = \overline{\alpha_0} \cdot \beta_0 + \overline{\alpha_1} \cdot \beta_1$
  - C'est le produit scalaire $\langle\psi|\phi\rangle$
  - Exemple:

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

Cloner un état quantique

- Existe-t-il une transformation unitaire U telle que $U \cdot (|\psi\rangle \otimes |0\rangle) = (|\psi\rangle \otimes |\psi\rangle)$?



Rappel: $\langle 1|+\rangle = \frac{1}{\sqrt{2}}(\langle 1|0\rangle + \langle 1|1\rangle) = \frac{1}{\sqrt{2}}$

Si U existe alors:

$$
\begin{aligned}
\langle 1|+\rangle &= \langle 1|+\rangle \cdot \langle 0|0\rangle \\
&= (\langle 1| \otimes \langle 0|) \cdot (|+\rangle \otimes |0\rangle) \\
&= (\langle 1| \otimes \langle 0|) \cdot U^\dagger \cdot U \cdot (|+\rangle \otimes |0\rangle) \\
&= (U \cdot (|1\rangle \otimes |0\rangle))^\dagger \cdot (U \cdot (|+\rangle \otimes |0\rangle)) \\
&= (|1\rangle \otimes |1\rangle)^\dagger \cdot (|+\rangle \otimes |+\rangle) \\
&= (\langle 1| \otimes \langle 1|) \cdot (|+\rangle \otimes |+\rangle) \\
&= (\langle 1|+\rangle)^2 \\
&= \frac{1}{2}
\end{aligned}
$$

On aurait $\frac{1}{\sqrt{2}} = \frac{1}{2}$: une contradiction

Fin de l'aparté

Mesure d'un système à 2 qubits

- Considérons un système à 2 qubits représenté par

$$\psi = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- Pour $i, j \in \{0,1\}$, un appareil mesurant simultanément les deux qubits renverra la valeur «ij» avec une probabilité $|\alpha_{ij}|^2$
  - Suite à cette mesure, le système se retrouvera dans l'état $|ij\rangle$
- Exemple: si $\psi = \frac{1}{3}|00\rangle + \frac{\sqrt{2}}{3}|01\rangle - \frac{1}{\sqrt{3}}|10\rangle - \frac{1}{\sqrt{3}}|11\rangle$, alors on renvoie:
  - «00» avec une probabilité $\frac{1}{9}$
  - «01» avec une probabilité $\frac{2}{9}$
  - «10» avec une probabilité $\frac{1}{3}$
  - «11» avec une probabilité $\frac{1}{3}$

Mesure d'un système à 2 qubits (suite)

- Que se passe-t-il si on mesure uniquement le premier qubit?

Règle de Born

Soit un système à deux qubits représenté par $\psi = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

- Un appareil mesurant le premier qubit renverra:
  - La valeur «0» avec une probabilité $P_0 = |\alpha_{00}|^2 + |\alpha_{01}|^2$
  - La valeur «1» avec une probabilité $P_1 = |\alpha_{10}|^2 + |\alpha_{11}|^2$

- Si le résultat renvoyé est «0» alors le système est dans l'état

$$\frac{1}{\sqrt{P_0}}(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle)$$

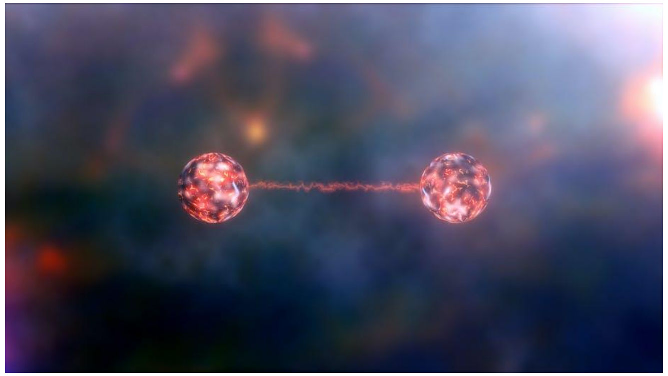
- Si le résultat renvoyé est «1» alors le système est dans l'état

$$\frac{1}{\sqrt{P_1}}(\alpha_{10}|10\rangle + \alpha_{11}|11\rangle)$$

Exemples

- $\psi = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$
  - On mesure «0» avec une probabilité $\frac{1}{2}$, l'état devient $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$
  - On mesure «1» avec une probabilité $\frac{1}{2}$, l'état devient $\frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$
- $\Phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - On mesure «0» avec une probabilité $\frac{1}{2}$, l'état devient $|00\rangle$
  - On mesure «1» avec une probabilité $\frac{1}{2}$, l'état devient $|11\rangle$

Le paradoxe EPR



- Considérons un système décrit par $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  - Par exemple une paire de photons intriqués, envoyés dans des directions opposées
- Prenons des appareils pour en mesurer la polarisation
  - «0» pour une polarisation horizontale, «1» pour une polarisation verticale
- Des mesures *simultanées* des deux qubits pourtant séparés produiront des résultats aléatoires mais identiques
  - Les deux photons auront la même polarisation
  - Transmission instantanée d'information???
  - Einstein: « *Spooky action at a distance* », la théorie de la relativité interdit ce phénomène!

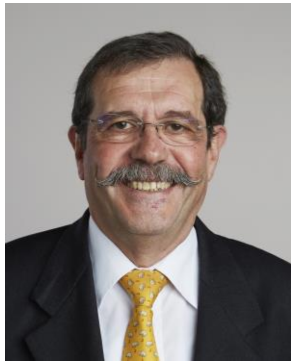
Réfutation de l'hypothèse d'Einstein

- Hypothèse d'Einstein
  - Les résultats des mesures dépendent de variables cachées
  - Mais comment confirmer/infirmer cette hypothèse?
- Inégalités de Bell
  - Si l'hypothèse d'Einstein est correcte, les mesures de certains états devraient être bornées
- Expérience d'Alain Aspect (1980-1982)
  - Les inégalités de Bell sont violées par les mesures d'états intriqués
  - L'hypothèse d'Einstein ne peut pas être correcte

$$p(a,b) = \int p_A(\omega,a,b)\cdot p_B(\omega,a,b)\cdot q(\omega)\cdot d\omega$$

Source: CERN

Nobel 2022



Source: Royal Society

Conclusion

- Ce qui a été présenté se généralise
  - Systèmes à plusieurs qubits
  - Mesure de n’importe quel sous-ensemble de qubits de ce système
- De quoi traiteront les prochaines conférences:
  - Construction d’algorithmes quantiques
  - Cryptographie quantique et codes correcteurs
  - Quelle technologie pour un ordinateur quantique?

Quelques ressources

- Livres
  - M. Burniat, T. Damour: *Le mystère du monde quantique* (https://www.dargaud.com/bd/le-mystere-du-monde-quantique-bda5133660)
  - O. Ezratty: *Comprendre l'Informatique Quantique* (https://www.oezratty.net/wordpress/2020/comprendre-informatique-quantique-edition-2020/)
  - M. Nielsen, I. Chuang: *Quantum Computation and Quantum Information* (http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf)
  - R. de Wolf: *Quantum Computing: Lecture Notes* (https://homepages.cwi.nl/~rdewolf/qcnotes.pdf)
- Programmation
  - Qiskit, Quantum Computing Hanbook (https://qiskit.org/textbook/preface.html)
- Vidéos
  - F. Magniez, cours au Collège de France (https://www.college-de-france.fr/site/frederic-magniez/course-2020-2021.htm)