Journée académique d'actualisation des connaissances scientifiques
des enseignants du 2nd degré en sciences physiques et en sciences,
sur le thème "Des signaux pour observer et communiquer".

27 juin 2017, Angers.

La physique quantique pour le traitement de l'information et du signal

François CHAPEAU-BLONDEAU
Département de Physique, Faculté des Sciences, Université d'Angers.

L'information quantique

Un domaine émergeant, qui exploite les propriétés et phénomènes quantiques, pour contribuer au traitement de l'information, du signal, au calcul automatique.

Les motivations

1) Par la miniaturisation et autres avancées technologiques, les dispositifs de traitement de l'information sont conduits au niveau des systèmes physiques élémentaires (photons, électrons, atomes, ions, nanodispositifs, . . .).

2) Pour profiter d'effets purement quantiques inexistant en classique (parallélisme, intrication, . . .)
offrant de nouveaux moyens pour le traitement de l'information.

1ère partie : Des bases théoriques

1) L'état d'un système quantique (le signal)

2) La mesure d'un système quantique (sa mesure)

3) L'évolution d'un système quantique (son traitement)

2ème partie : Des applications

pour le traitement de l'information,

la transmission de signaux,

le calcul automatique.

1ère partie : Des bases théoriques

1) L'état d'un système quantique (le signal)

2) La mesure d'un système quantique (sa mesure)

3) L'évolution d'un système quantique (son traitement)

2ème partie : Des applications

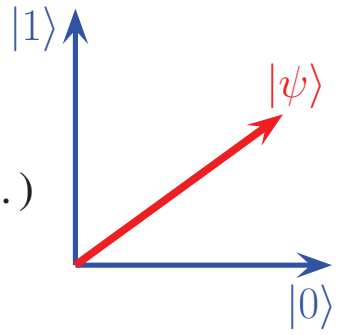
pour le traitement de l'information,

la transmission de signaux,

le calcul automatique.

1) L'état d'un système quantique

Un système quantique est représenté par un vecteur d'état $|\psi\rangle$
dans un espace de Hilbert $\mathcal{H}$ complexe,
de norme unité $\langle\psi|\psi\rangle = \||\psi\|^2 = 1$.

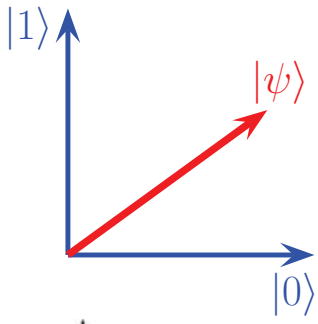


En dimension 2 : le qubit (photon, électron, atome, . . .)

État $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
dans une base orthonormée $\{|0\rangle, |1\rangle\}$ de $\mathcal{H}_2$,
avec les coordonnées $\alpha, \beta \in \mathbb{C}$ telles que $|\alpha|^2 + |\beta|^2 = \langle\psi|\psi\rangle = \||\psi\|^2 = 1$.

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \quad |\psi\rangle^\dagger = \langle\psi| = [\alpha^*, \beta^*] \quad \Longrightarrow \langle\psi|\psi\rangle = \||\psi\|^2 = |\alpha|^2 + |\beta|^2 \text{ scalaire.}$$

Représentation de Bloch du qubit

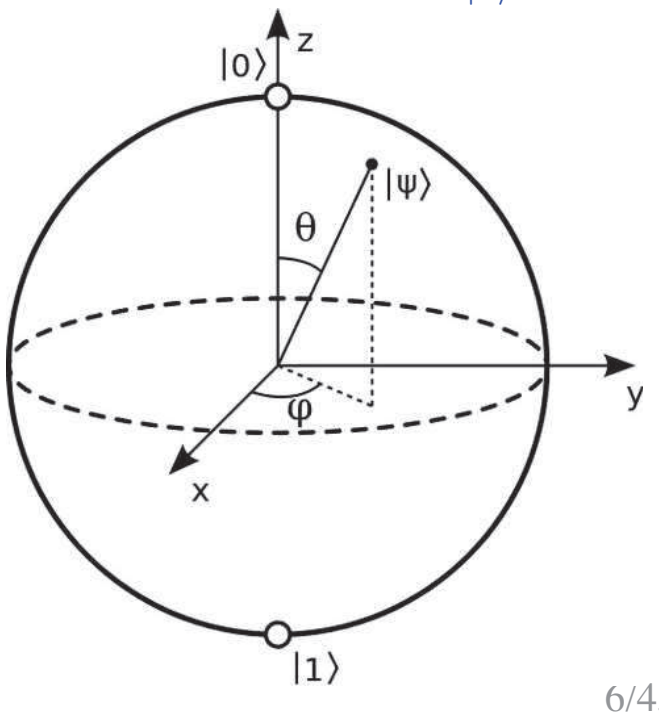


Un qubit dans l'état
$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$.

$$\Longleftrightarrow |\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\varphi}\sin(\theta/2)\,|1\rangle$$

avec $\theta \in [0, \pi]$,
$\varphi \in [0, 2\pi[$.

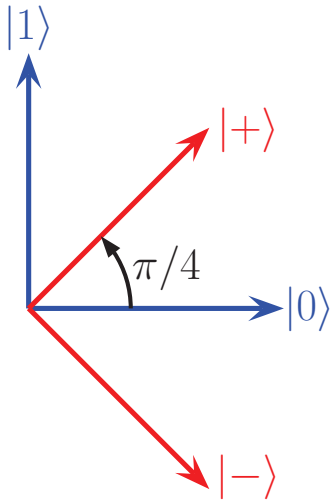
Deux états orthogonaux dans $\mathcal{H}_2$
sont antipodaux sur la sphère de Bloch.



Base de Hadamard

Une autre base orthonormale of $\mathcal{H}_2$

$$\left\{ |+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \; ; \quad |-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \right\} .$$



$\Longleftrightarrow$ Base orthonormale canonique

$$\left\{ |0\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle + |-\rangle\Big) \; ; \quad |1\rangle = \frac{1}{\sqrt{2}}\Big(|+\rangle - |-\rangle\Big) \right\} .$$

2) La mesure d'un système quantique

Quand un qubit dans l'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
est mesuré dans la base orthonormée $\big\{|0\rangle\,, |1\rangle\big\}$,

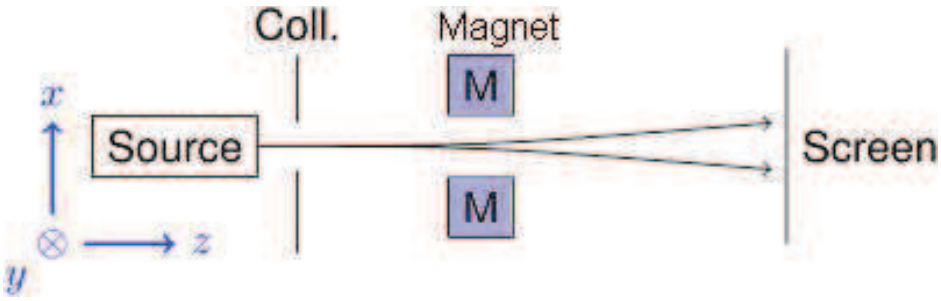
$\Longrightarrow$ uniquement 2 résultats possibles (règle de Born) :

état $|0\rangle$ avec probabilité $|\alpha|^2 = |\,\langle 0|\psi\rangle\,|^2$, ou
état $|1\rangle$ avec probabilité $|\beta|^2 = |\,\langle 1|\psi\rangle\,|^2$.

Mesure quantique : généralement :

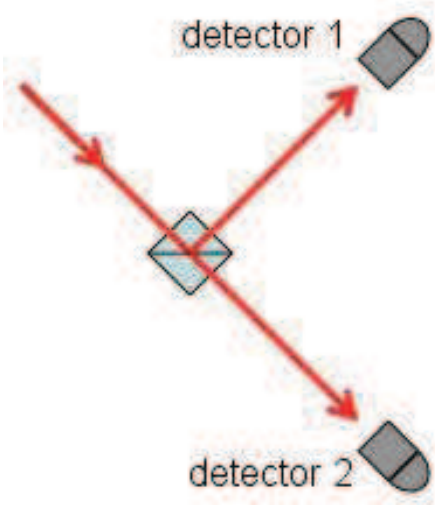
- un processus probabiliste,
- comme la projection destructive de l'état $|\psi\rangle$ dans une base orthonormée,
- avec des statistiques évaluables par des expériences répétées sur la même préparation $|\psi\rangle$.

Expériences



Appareil de Stern-Gerlach pour particules à deux états de spin (électron, atome).

Photon à deux états de polarisation :
(prisme de Nicol, Glan-Thompson,
polarizing beam splitter, . . .)

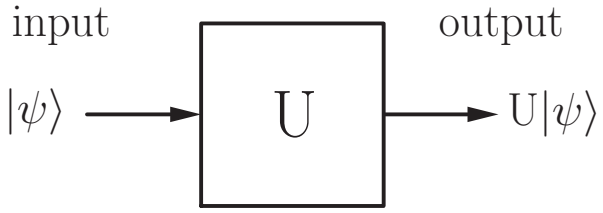


3) L'évolution d'un système quantique

Par un opérateur unitaire U sur $\mathcal{H}_2$ (une matrice 2×2) : (i.e. $\mathsf{U}^{-1} = \mathsf{U}^\dagger$)

vecteur normalisé $|\psi\rangle \in \mathcal{H}_2 \longrightarrow \mathsf{U}|\psi\rangle$ vecteur normalisé $\in \mathcal{H}_2$.

≡ porte quantique
(toujours réversible)



Porte identité $\mathrm{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Porte de Hadamard $\mathsf{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, telle que $\mathsf{H}|0\rangle = |+\rangle$ et $\mathsf{H}|1\rangle = |-\rangle$.

Portes ou opérateurs de Pauli

$$\mathsf{X} = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathsf{Y} = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \mathsf{Z} = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

$\{\mathsf{I}_2, \mathsf{X}, \mathsf{Y}, \mathsf{Z}\}$ une base pour les opérateurs sur $\mathcal{H}_2$.

Porte de Hadamard $\mathsf{H} = \frac{1}{\sqrt{2}}(\mathsf{X} + \mathsf{Z})$.

$\mathsf{X} = \sigma_x$ l'inversion ou porte quantique Non. $\mathsf{X}|0\rangle = |1\rangle$, $\mathsf{X}|1\rangle = |0\rangle$.

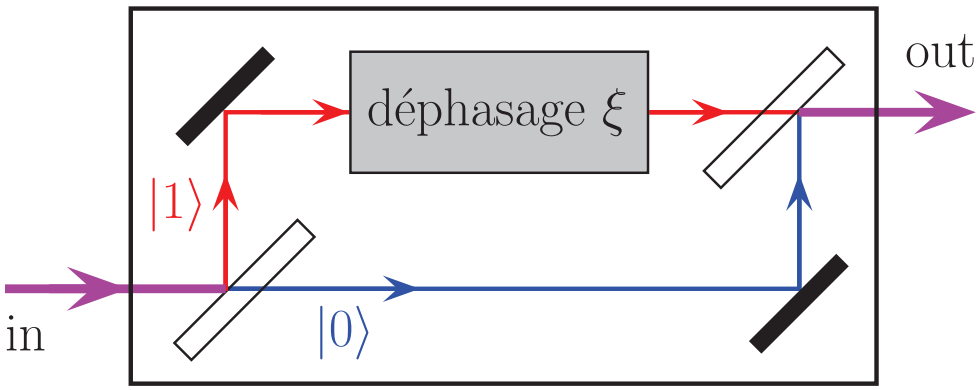
$$\mathsf{W} = \sqrt{\mathsf{X}} = \sqrt{\sigma_x} = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{bmatrix} \Longrightarrow \mathsf{W}^2 = \mathsf{X},$$

est la racine carrée de Non, porte spécifiquement quantique.

Une implémentation optique

Une porte à un qubit $\mathsf{U}_\xi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\xi} \end{bmatrix} = |0\rangle\langle 0| + e^{i\xi}|1\rangle\langle 1| = e^{i\xi/2}\exp(-i\xi\sigma_z/2)$

implémentée optiquement par un interféromètre de Mach-Zehnder



agissant sur des photons individuels à deux états de polarisation $|0\rangle$ and $|1\rangle$ déphasés sélectivement,

pour opérer aussi sur toute superposition $\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|0\rangle + \beta e^{i\xi}|1\rangle$.

Qubits multiples

Un système (un mot) de N qubits possède un état dans $\mathcal{H}_2^{\otimes N}$,

un espace vectoriel produit tensoriel de dimension 2^N,

de base orthonormale $\left\{|x_1 x_2 \cdots x_N\rangle\right\}_{\vec{x} \in \{0,1\}^N}$.

Exemple $N = 2$ qubits :

En général $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ (2^N coord.).

Ou, comme cas particulier, un état séparable ($2N$ coord.)

$$|\phi\rangle = \Big(\alpha_1|0\rangle + \beta_1|1\rangle\Big) \otimes \Big(\alpha_2|0\rangle + \beta_2|1\rangle\Big)$$
$$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle .$$

Un état multipartite qui n'est pas séparable (factorisable) est intriqué.

Un état intriqué se comporte comme un tout non local ; ce qui est fait sur une partie a une influence instantanée sur l'autre, quelle que soit leur distance.

États intriqués

• Exemple d'un état séparable à deux qubits AB (deux photons préparés séparément) :

$$|AB\rangle = |+\rangle \otimes |+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) = \frac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\Big).$$

Quand mesuré dans la base $\left\{|0\rangle, |1\rangle\right\}$, chaque qubit A et B peut être trouvé dans l'état $|0\rangle$ ou $|1\rangle$ indépendamment avec la probabilité $1/2$.

$$\Pr\Big\{A \text{ dans } |0\rangle\Big\} = \Pr\Big\{|AB\rangle = |00\rangle\Big\} + \Pr\Big\{|AB\rangle = |01\rangle\Big\} = 1/4 + 1/4 = 1/2.$$

• Exemple d'un état intriqué à deux qubits AB (deux photons préparés ensemble) :

$$|AB\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big). \qquad \Pr\Big\{A \text{ dans } |0\rangle\Big\} = \Pr\Big\{|AB\rangle = |00\rangle\Big\} = 1/2.$$

Quand mesuré dans la base $\left\{|0\rangle, |1\rangle\right\}$, chaque qubit A et B peut être trouvé dans l'état $|0\rangle$ ou $|1\rangle$ avec la probabilité $1/2$ (aléatoirement, sans prédétermination).
Mais si A est trouvé dans $|0\rangle$ nécessairement B est trouvé dans $|0\rangle$,
et si A est trouvé dans $|1\rangle$ nécessairement B est trouvé dans $|1\rangle$,
quelle que soit la distance des deux qubits avant la mesure.

Base de Bell

Une paire de qubits de $\mathcal{H}_2^{\otimes 2}$ est un système quantique de dimension $2^2 = 4$,

avec la base orthonormale (canonique) d'origine $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Une autre base orthonormale utile de $\mathcal{H}_2^{\otimes 2}$ est la base de Bell
$\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}$,

$$\text{avec} \qquad |\beta_{00}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$$

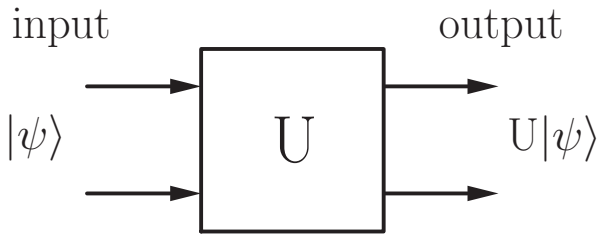
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\big(|01\rangle - |10\rangle\big).$$

Évolution, traitement d'une paire de qubits

Via un opérateur unitaire U sur $\mathcal{H}_2^{\otimes 2}$ (matrice 4×4) :

vecteur normalisé $|\psi\rangle \in \mathcal{H}_2^{\otimes 2} \longrightarrow \mathsf{U}|\psi\rangle$ vecteur normalisé $\in \mathcal{H}_2^{\otimes 2}$.

≡ porte quantique
(toujours réversible)



Complètement définie par exemple par la transformation des 4 vecteurs d'état de la base canonique $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Mais opère également sur toute superposition d'états quantiques
$\Longrightarrow$ parallélisme quantique.

• Exemple : Porte Controlled-Not

Via la fonction binaire XOR : $a \oplus b = a$ quand $b = 0$, ou $= \overline{a}$ quand $b = 1$;
inversible $a \oplus x = b \Longleftrightarrow x = a \oplus b = b \oplus a$.

Utilisé pour construire la porte quantique unitaire C-Not :
(T target, C control)

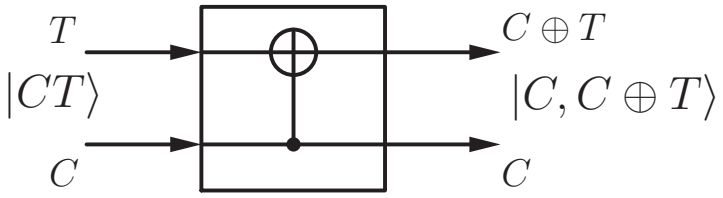
$|CT\rangle \longrightarrow |C, C \oplus T\rangle$

$|00\rangle \longrightarrow |00\rangle$

$|01\rangle \longrightarrow |01\rangle$

$|10\rangle \longrightarrow |11\rangle$

$|11\rangle \longrightarrow |10\rangle$



$$\mathsf{U} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Évolution, traitement d'un système à N qubits

Via un opérateur unitaire U sur $\mathcal{H}_2^{\otimes N}$ (matrice $2^N \times 2^N$) :

vecteur normalisé $|\psi\rangle \in \mathcal{H}_2^{\otimes N} \longrightarrow \mathsf{U}|\psi\rangle$ vecteur normalisé $\in \mathcal{H}_2^{\otimes N}$.

≡ porte quantique : N qubits d'entrée $\longrightarrow \boxed{\mathsf{U}} \longrightarrow N$ qubits de sortie.

Complètement définie par exemple par la transformation des 2^N vecteurs d'état de la base canonique $\left\{|\vec{x}\rangle\,, \vec{x} \in \{0,1\}^N\right\}$.
Ex. $N = 3$, base $\left\{|000\rangle\,, |001\rangle\,, |010\rangle\,, |011\rangle\,, |100\rangle\,, |101\rangle\,, |110\rangle\,, |111\rangle\right\}$.
Mais opère également sur toute superposition d'états quantiques (parallélisme).

Tout circuit ou porte quantique à N qubits peut toujours être composé de portes C-Not à deux qubits et de portes à un qubit (universalité).
Ce qui en principe garantit la réalisabilité expérimentale.

Ceci forme le fondement du calcul quantique.

États quantiques de dimension infinie

Une particule mobile selon une dimension

possède l'état $|\psi\rangle = \int_{-\infty}^{\infty} \psi(x)\,|x\rangle\,dx$

dans une base orthonormale $\{|x\rangle\}$

de l'espace de Hilbert $\mathcal{H}$ de dimension infinie continue.

(Par rapport au qubit en dimension deux : $|\psi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle$.)

La coordonnée $\psi(x) \in \mathbb{C}$ est la fonction d'onde,

vérifiant $\int_{-\infty}^{\infty} |\psi(x)|^2 dx = 1$,

avec $|\psi(x)|^2$ la densité de probabilité de trouver la particule en x
quand on mesure sa position.

Évolution à temps continu d'un état quantique

Par postulation empirique via l'équation de Schrödinger :

$$\frac{d}{dt}|\psi\rangle = -\frac{i}{\hbar}\mathsf{H}\,|\psi\rangle \Longrightarrow |\psi(t_2)\rangle = \underbrace{\exp\left(-\frac{i}{\hbar}\int_{t_1}^{t_2}\mathsf{H}dt\right)}_{\text{unitaire } \mathsf{U}(t_1,t_2)}|\psi(t_1)\rangle = \mathsf{U}(t_1,t_2)\,|\psi(t_1)\rangle$$

avec l'opérateur hermitique hamiltonien H, ou opérateur énergie,
construit à partir de l'énergie classique.

1ère partie : Des bases théoriques

1) L'état d'un système quantique (le signal)

2) La mesure d'un système quantique (sa mesure)

3) L'évolution d'un système quantique (son traitement)

2ème partie : Des applications

pour le traitement de l'information,

la transmission de signaux,

le calcul automatique.

Deutsch-Jozsa algorithm (1992) : Parallel test of a function (1/4)

A classical function $f(\cdot)$: $\{0,1\}^N \longrightarrow \{0,1\}$, 2^N values $\longrightarrow$ 2 values,

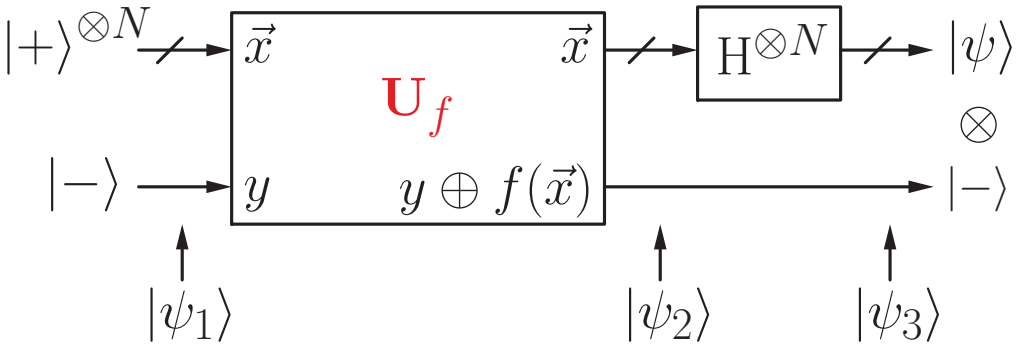
can be *constant* (all inputs into 0 or 1)

or balanced (equal numbers of 0, 1 in output).

Classically : Between 2 and $\frac{2^N}{2} + 1$ evaluations of $f(\cdot)$ to decide.

Quantumly : One evaluation of $f(\cdot)$ is enough (on a suitable superposition).

Deutsch-Jozsa algorithm (2/4)



Input state $|\psi_1\rangle = |+\rangle^{\otimes N}|-\rangle = \left(\frac{1}{\sqrt{2}}\right)^N \sum_{\vec{x}\in\{0,1\}^N} |\vec{x}\rangle|-\rangle$

Internal state $|\psi_2\rangle = \left(\frac{1}{\sqrt{2}}\right)^N \sum_{\vec{x}\in\{0,1\}^N} |\vec{x}\rangle|-\rangle(-1)^{f(\vec{x})}$

Deutsch-Jozsa algorithm (3/4)

Output state $|\psi_3\rangle = \left(\mathrm{H}^{\otimes N} \otimes \mathrm{I}_2\right)|\psi_2\rangle$

$$= \left(\frac{1}{\sqrt{2}}\right)^N \sum_{\vec{x}\in\{0,1\}^N} \mathrm{H}^{\otimes N}|\vec{x}\rangle|-\rangle(-1)^{f(\vec{x})}$$

$$= \left(\frac{1}{2}\right)^N \sum_{\vec{x}\in\{0,1\}^N} \sum_{\vec{z}\in\{0,1\}^N} (-1)^{\vec{x}\vec{z}}|\vec{z}\rangle|-\rangle(-1)^{f(\vec{x})},$$

or $|\psi_3\rangle = |\psi\rangle|-\rangle$, with $|\psi\rangle = \left(\frac{1}{2}\right)^N \sum_{\vec{z}\in\{0,1\}^N} u(\vec{z})|\vec{z}\rangle$

and the scalar weight $u(\vec{z}) = \sum_{\vec{x}\in\{0,1\}^N} (-1)^{f(\vec{x})+\vec{x}\vec{z}}$.

Deutsch-Jozsa algorithm (4/4)

So $|\psi\rangle = \dfrac{1}{2^N} \sum_{\vec{z}\in\{0,1\}^N} u(\vec{z})\,|\vec{z}\rangle$ with $u(\vec{z}) = \sum_{\vec{x}\in\{0,1\}^N} (-1)^{f(\vec{x})+\vec{x}\vec{z}}$.

For $|\vec{z}\rangle = |\vec{0}\rangle = |0\rangle^{\otimes N}$ then $u(\vec{z}=\vec{0}) = \sum_{\vec{x}\in\{0,1\}^N} (-1)^{f(\vec{x})}$.

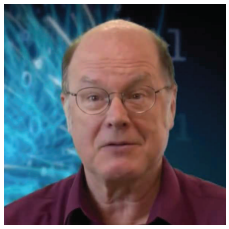
• When $f(\cdot)$ constant : $u(\vec{z}=\vec{0}) = 2^N(-1)^{f(\vec{0})} = \pm 2^N \Longrightarrow$ in $|\psi\rangle$ the amplitude of $|\vec{0}\rangle$ is ± 1, and since $|\psi\rangle$ is with unit norm $\Longrightarrow |\psi\rangle = \pm|\vec{0}\rangle$, and all other $u(\vec{z}\neq\vec{0})=0$.
$\Longrightarrow$ When $|\psi\rangle$ is measured, N states $|0\rangle$ are found.

• When $f(\cdot)$ balanced : $u(\vec{z}=\vec{0}) = 0 \Longrightarrow |\psi\rangle$ is not or does not contain state $|\vec{0}\rangle$.
$\Longrightarrow$ When $|\psi\rangle$ is measured, at least one state $|1\rangle$ is found.

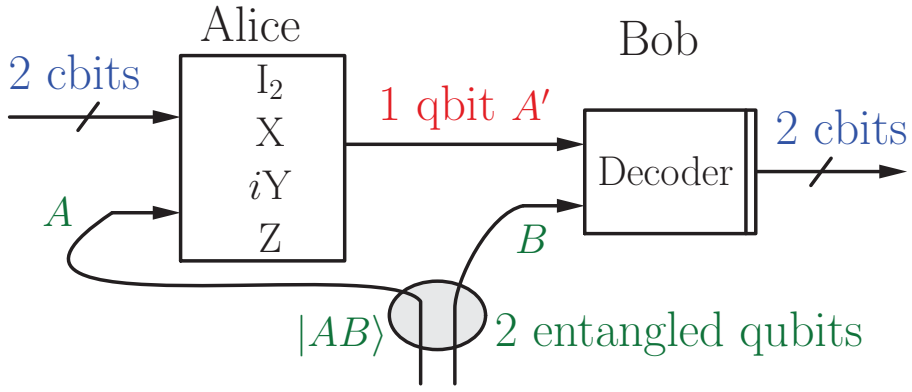
$\longrightarrow$ Illustrates quantum ressources of parallelism, coherent superposition, interference.
(When $f(\cdot)$ is neither constant nor balanced, $|\psi\rangle$ contains a little bit of $|\vec{0}\rangle$.)

Superdense coding (Bennett 1992) : signal transmission by entanglement

Alice and Bob share a qubit pair in entangled state $|AB\rangle = \dfrac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) = |\beta_{00}\rangle$.



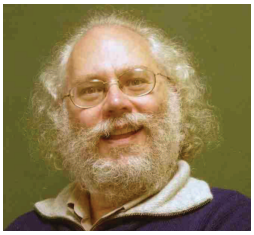
Alice chooses two classical bits, used to encode by applying to her qubit A one of $\{\mathrm{I}_2, \mathrm{X}, i\mathrm{Y}, \mathrm{Z}\}$, delivering the qubit A' sent to Bob.



$$|A'B\rangle =$$
$$\mathrm{I}_2 \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{00}\rangle$$
$$\mathrm{X} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{01}\rangle$$
$$\mathrm{Z} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{10}\rangle$$
$$i\mathrm{Y} \otimes \mathrm{I}_2\,|AB\rangle = |\beta_{11}\rangle$$

Bob receives this qubit A'. For decoding, Bob measures $|A'B\rangle$ in the Bell basis $\big\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\big\}$, from which he recovers the two classical bits.

Other quantum algorithms

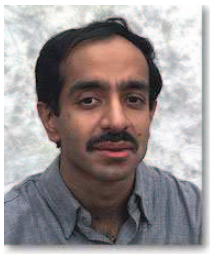


- Shor factoring algorithm (1997) :

  Factors any integer in polynomial complexity
  (instead of exponential classically).

  $15 = 3 \times 5$, with spin-1/2 nuclei (Vandersypen *et al.*, Nature 2001).

  $21 = 3 \times 7$, with photons (Martín-López *et al.*, Nature Photonics 2012).



- Grover quantum search algorithm (1997) :

  Finds an item out of N in an unsorted database,
  in $O(\sqrt{N})$ complexity instead of $O(N)$ classically.

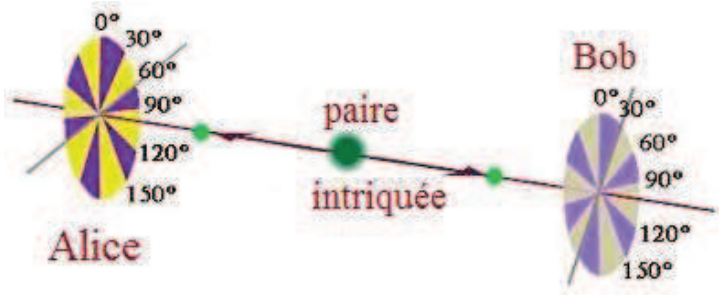
- HHL (Harrow, Hassidim, Lloyd) algo. for linear systems of equations (2009) :
  in $O(\log N)$ complexity instead of $O(N)$ classically.

- http://math.nist.gov/quantum/zoo/

  "A comprehensive catalog of quantum algorithms . . . "

Corrélations quantiques (1/3)

Alice et Bob se partagent une paire de qubits
dans l'état intriqué $|\psi_{\rm AB}\rangle = \dfrac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big)$.



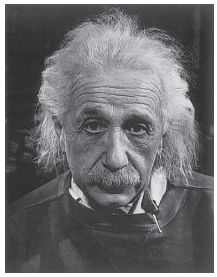
Alice ou Bob peut mesurer son qubit dans la base
$\Big\{|V_+(\theta)\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,|1\rangle\,, \quad |V_-(\theta)\rangle = \sin(\theta/2)\,|0\rangle - \cos(\theta/2)\,|1\rangle\Big\}$
en chiffrant le résultat de la mesure par ± 1.

Alice mesure selon $\theta = \alpha$ pour obtenir $A = \pm 1$,
et Bob mesure selon $\theta = \beta$ pour obtenir $B = \pm 1$.

On calcule les probabilités des 4 configurations de mesure possibles, par exemple
$\Pr\Big\{A = +1, B = -1\Big\} = \Big|\langle\psi_{\rm AB}|V_+(\alpha)\otimes V_-(\beta)\rangle\Big|^2 = \dfrac{1}{4}\Big[1 + \cos(\alpha - \beta)\Big]$.

On en déduit la moyenne $\langle AB\rangle = -\cos(\alpha - \beta)$.

Corrélations quantiques (2/3)



Dans une longue série d'expériences répétées sur la même préparation $|\psi_{AB}\rangle$
expérience EPR (Einstein, Podolsky, Rosen, 1935),

Alice bascule au hasard entre le choix de mesurer A_1 selon α_1 ou A_2 selon α_2,
et Bob bascule au hasard entre le choix de mesurer B_1 selon β_1 ou B_2 selon β_2.

Supposons qu'il existe des variables cachées qui déterminent à l'avance les résultats
$(A_1 = \pm 1, A_2 = \pm 1, B_1 = \pm 1, A_2 = \pm 1)$ des 4 mesures faisables.

Alors $\Gamma = (A_1 + A_2)B_1 - (A_1 - A_2)B_2 = A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2 = \pm 2$,
car comme $A_1, A_2 = \pm 1$, soit $(A_1 + A_2)B_1 = 0$ ou soit $(A_1 - A_2)B_2 = 0$,
et dans chaque cas le terme restant est ± 2.

Et quand les réalisations successives de (A_1, A_2, B_1, B_2) se produisent
selon n'importe quelle loi de probabilité, nécessairement
$\langle\Gamma\rangle = \langle A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2\rangle = \langle A_1B_1\rangle + \langle A_2B_1\rangle + \langle A_2B_2\rangle - \langle A_1B_2\rangle$
vérifie $-2 \leq \langle\Gamma\rangle \leq 2$. Inégalités de Bell (1964).

Corrélations quantiques (3/3)

Inégalités de Bell $-2 \leq \langle\Gamma\rangle \leq 2$.

Or la théorie quantique prévoit que pour
$\langle\Gamma\rangle = \langle A_1B_1\rangle + \langle A_2B_1\rangle + \langle A_2B_2\rangle - \langle A_1B_2\rangle$ on dispose de
$\langle\Gamma\rangle = -\cos(\alpha_1 - \beta_1) - \cos(\alpha_2 - \beta_1) - \cos(\alpha_2 - \beta_2) + \cos(\alpha_1 - \beta_2)$.

Le choix $\alpha_1 = 0$, $\alpha_2 = \pi/2$ et $\beta_1 = \pi/4$, $\beta_2 = 3\pi/4$ conduit à
$\langle\Gamma\rangle = -\cos(\pi/4) - \cos(\pi/4) - \cos(\pi/4) + \cos(3\pi/4) = -2\sqrt{2} < -2.$

La théorie quantique prédit une violation des inégalités de Bell !!

Le dilemme a été tranché par les expériences d'Aspect
(Aspect *et al.*, Phys. Rev. Let. 1981, 1982)

qui donnent raison à la théorie quantique
et conduisent à remplacer le réalisme local (classique)
par une réalité non locale non séparable (quantique).

EPR paradox (Einstein-Podolski-Rosen) :

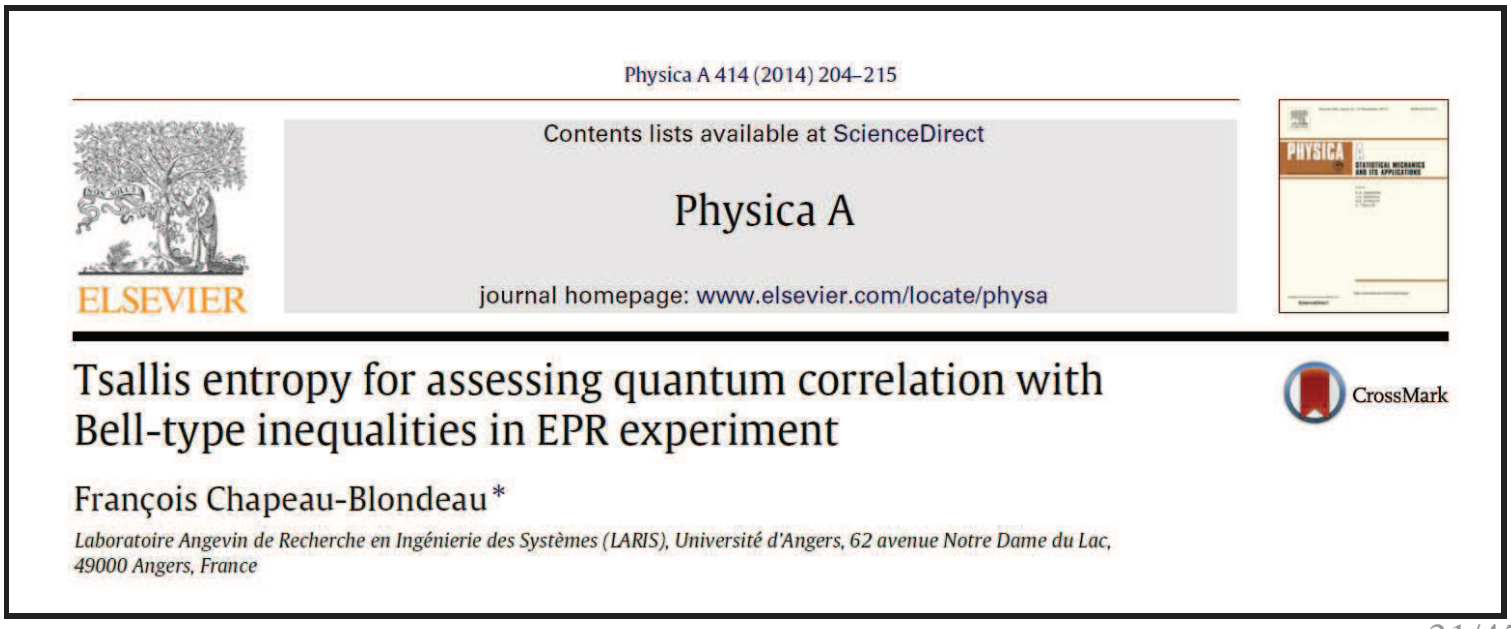
A. Einstein, B. Podolsky, N. Rosen ; “Can quantum-mechanical description of physical reality be considered complete ?”; *Physical Review*, 47 (1935) 777–780.

Bell inequalities :

J. S. Bell ; “On the Einstein–Podolsky–Rosen paradox”; *Physics*, 1 (1964) 195–200.

Aspect experiments :

A. Aspect, P. Grangier, G. Roger ; “Experimental test of realistic theories via Bell’s theorem”; *Physical Review Letters*, 47 (1981) 460–463.



Physica A 414 (2014) 204–215

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Tsallis entropy for assessing quantum correlation with Bell-type inequalities in EPR experiment

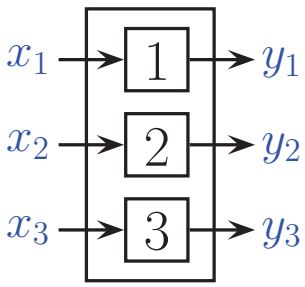
François Chapeau-Blondeau *

Laboratoire Angevin de Recherche en Ingénierie des Systèmes (LARIS), Université d'Angers, 62 avenue Notre Dame du Lac, 49000 Angers, France

GHZ states (1/5) (1989, Greenberger, Horne, Zeilinger)

3-qubit entangled states.

Three players, each receiving a binary input $x_j = 0/1$, for $j = 1, 2, 3$, with four possible input configurations $x_1x_2x_3 \in \{000, 011, 101, 110\}$.



Each player j responds by a binary output $y_j(x_j) = 0/1$, function only of its own input x_j, for $j = 1, 2, 3$.

Game is won if the players collectively respond according to the input–output matches :

$$x_1x_2x_3 = 000 \longrightarrow y_1y_2y_3 \text{ such that } y_1 \oplus y_2 \oplus y_3 = 0 \quad \text{(conserve parity)},$$

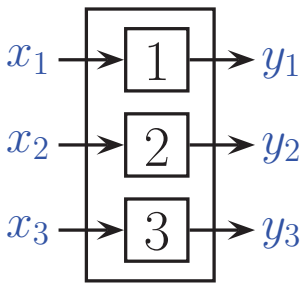
$$x_1x_2x_3 \in \{011, 101, 110\} \longrightarrow y_1y_2y_3 \text{ such that } y_1 \oplus y_2 \oplus y_3 = 1 \quad \text{(reverse parity)}.$$

To select their responses $y_j(x_j)$, the players can agree on a collective strategy before, but not after, they have received their inputs x_j.

GHZ states (2/5)

A strategy winning on all four input configurations
would consist in three binary functions $y_j(x_j)$ meeting the four constraints :

$$y_1(0) \oplus y_2(0) \oplus y_3(0) = 0$$
$$y_1(0) \oplus y_2(1) \oplus y_3(1) = 1$$
$$y_1(1) \oplus y_2(0) \oplus y_3(1) = 1$$
$$y_1(1) \oplus y_2(1) \oplus y_3(0) = 1$$



$0 \oplus 0 \oplus 0 = 1$, by summation of the four constraints,

$\Longrightarrow \quad 0 = 1$, so the four constraints are incompatible.

So no (classical) strategy exists that would win on all four input configurations.
Any (classical) strategy is bound to fail on some input configuration(s).

We show a strategy using quantum resources winning on all four input configurations,
(by escaping local realism, $y_j(0) = 0/1$ and $y_j(1) = 0/1$ not existing simultaneously).

GHZ states (3/5)

Before the game starts, each player receives one qubit from a qubit triplet prepared in the entangled state (GHZ state)

$$|\psi\rangle = |\psi_{123}\rangle = \frac{1}{2}\Big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\Big).$$

And the players agree on the common (prior) strategy :
if $x_j = 0$, player j obtains y_j as the outcome of measuring its qubit in basis $\{|0\rangle, |1\rangle\}$,
if $x_j = 1$, player j obtains y_j as the outcome of measuring its qubit in basis $\{|+\rangle, |-\rangle\}$.

We prove this is a winning strategy on all four input configurations :

1) When $x_1x_2x_3 = 000$, the three players measure in $\{|0\rangle, |1\rangle\}$
$\Longrightarrow y_1 \oplus y_2 \oplus y_3 = 0$ is matched.

GHZ states (4/5)

2) When $x_1x_2x_3 = 011$, only player 1 measures in $\{|0\rangle, |1\rangle\}$.

$$|\psi\rangle = \frac{1}{2}\big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\big) = \frac{1}{2}\Big[|0\rangle\big(|00\rangle - |11\rangle\big) - |1\rangle\big(|01\rangle + |10\rangle\big)\Big].$$

Since $|0\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle + |-\rangle\big)$, $\quad |1\rangle = \frac{1}{\sqrt{2}}\big(|+\rangle - |-\rangle\big) \Longrightarrow$

$$|00\rangle - |11\rangle = \frac{1}{2}\Big[\big(|+\rangle + |-\rangle\big)\big(|+\rangle + |-\rangle\big) - \big(|+\rangle - |-\rangle\big)\big(|+\rangle - |-\rangle\big)\Big]$$

$$= \frac{1}{2}\Big[\big(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle\big) - \big(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle\big)\Big]$$

$$= |+-\rangle + |-+\rangle\ ;$$

$$|01\rangle + |10\rangle = \frac{1}{2}\Big[\big(|+\rangle + |-\rangle\big)\big(|+\rangle - |-\rangle\big) + \big(|+\rangle - |-\rangle\big)\big(|+\rangle + |-\rangle\big)\Big] = |++\rangle - |--\rangle\ ;$$

$$\Longrightarrow |\psi\rangle = \frac{1}{2}\big(|0+-\rangle + |0-+\rangle - |1++\rangle + |1--\rangle\big) \Longrightarrow y_1 \oplus y_2 \oplus y_3 = 1 \quad \text{matched.}$$

GHZ states (5/5)

3) When $x_1x_2x_3 = 101$, only player 2 measures in $\{|0\rangle, |1\rangle\}$.

$$|\psi\rangle = \frac{1}{2}\big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\big) = \frac{1}{2}\Big[|\cdot 0\cdot\rangle\big(|0\cdot 0\rangle - |1\cdot 1\rangle\big) - |\cdot 1\cdot\rangle\big(|0\cdot 1\rangle + |1\cdot 0\rangle\big)\Big]$$

$$= \frac{1}{2}\Big[|\cdot 0\cdot\rangle\big(|+\cdot -\rangle + |-\cdot +\rangle\big) - |\cdot 1\cdot\rangle\big(|+\cdot +\rangle - |-\cdot -\rangle\big)\Big]$$

$$= \frac{1}{2}\big(|+0-\rangle + |-0+\rangle - |+1+\rangle + |-1-\rangle\big) \Longrightarrow y_1 \oplus y_2 \oplus y_3 = 1 \quad \text{matched.}$$

4) When $x_1x_2x_3 = 110$, only player 3 measures in $\{|0\rangle, |1\rangle\}$.

$$|\psi\rangle = \frac{1}{2}\big(|000\rangle - |011\rangle - |101\rangle - |110\rangle\big) = \frac{1}{2}\Big[|\cdot\cdot 0\rangle\big(|00\cdot\rangle - |11\cdot\rangle\big) - |\cdot\cdot 1\rangle\big(|01\cdot\rangle + |10\cdot\rangle\big)\Big]$$

$$= \frac{1}{2}\Big[|\cdot\cdot 0\rangle\big(|+-\cdot\rangle + |-+\cdot\rangle\big) - |\cdot\cdot 1\rangle\big(|++\cdot\rangle - |--\cdot\rangle\big)\Big]$$

$$= \frac{1}{2}\big(|+-0\rangle + |-+0\rangle - |++1\rangle + |--1\rangle\big) \Longrightarrow y_1 \oplus y_2 \oplus y_3 = 1 \quad \text{matched.}$$

Quantum cryptography

• The problem of cryptography

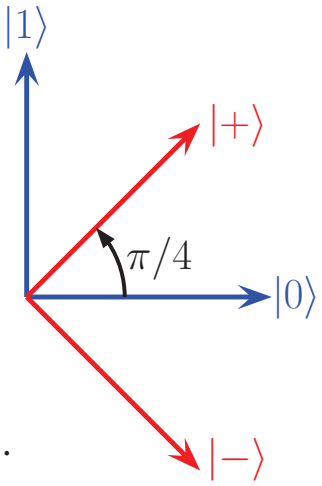
Message X, a string of bits.
Cryptographic key K, a completely random string of bits with proba. $1/2$ and $1/2$.

The cryptogram or encrypted message $C(X, K) = X \oplus K$ (encrypted string of bits),
deciphered as $X = C \oplus K$. This is Vernam cipher or one-time pad,
with provably perfect security, since mutual information $I(C; X) = H(X) - H(X|C) = 0$.

Problem : establishing a secret (private) key
between emitter (Alice) and receiver (Bob).

With quantum signals,
any measurement by an eavesdropper (Eve) perturbs the system,
and hence reveals the eavesdropping, and also identifies perfect security conditions.

• BB84 protocol (Bennett & Brassard 1984)



♦ Alice has a string of $4N$ random bits. She encodes with a qubit in a basis state either from $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ randomly chosen for each bit.

♦ Then Bob chooses to measure each received qubit either in basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ so as to decode each transmitted bit.

♦ Once the whole string of $4N$ bits from Alice has been received by Bob, Alice publicly discloses the sequence of her basis choices.

♦ Bob keeps only the positions where his choices of basis coincide with those of Alice to obtain a secret key, of length approximately $2N$.

♦ If Eve intercepts and measures Alice's qubit and forward her measured state to Bob, roughly half of the time Eve forwards an incorrect state, and from this Bob half of the time decodes an incorrect bit value.

♦ From their $2N$ coinciding bits, Alice and Bob classically exchange N bits at random. In case of eavesdropping, around $N/4$ of these N test bits will differ.
If all N test bits coincide, then the remaining N bits form the shared secret key.

T +41 22 301 83 71 | E info(

ID Quantique

Redefining the fields of Random Numbers,
Quantum-Safe Crypto & Photon Counting

ID Quantique

QUANTUM-SAFE CRYPTO – PHOTON COUNTING – RANDOMNESS

ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and

Cerberis QKD Server

Cerberis from IDQ is a standalone rack-mountable QKD server; providing secure quantum keys based on the BB84 and SARG protocols. Integrated with IDQ's Centauris Ethernet and Fiber Channel encryptors, Cerberis has been deployed by governments, enterprises and financial institutions since 2007.

Clavis^2 QKD Platform

Open QKD platform for R&D, based on BB84 and SARG protocols with auto-compensating interferometric set-up. Widely deployed in the academic community for quantum cryptography research , quantum hacking and certification, and technology evaluations.

FROM VISION TO TECHNOLOGY

USER CASE

REPUBLIC AND STATE OF GENEVA

POST TENEBRAS LUX

REDEFINING SECURITY

Geneva Government

Secure Data Transfer for Elections

Gigabit Ethernet Encryption with Quantum Key Distribution

"We have to provide optimal security conditions for the counting of ballots.... Quantum cryptography has the ability to verify that the data has not been corrupted in transit between entry & storage"

Robert Hensler, ex-

The Challenge

Switzerland epitomises the concept of direct democracy. Citizens of Geneva are called on to vote multiple times every year, on anything from elections for the national and cantonal parliaments to local referendums. The challenge for the Geneva government is to ensure maximum security to protect the data authenticity and integrity, while at the same time managing the process efficiently. They also have to guarantee the axiom of One Citizen One Vote.

The Solution

On 21st October 2007 the Geneva government implemented for the first time IDQ's hybrid encryption solution, using state of the art Layer 2 encryption combined with Quantum Key Distribution (QKD). The Cerberis solution secures a point-to-point Gigabit Ethernet link used to send ballot information for the federal

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information

Article Talk | Read Edit View history | Search Wikipedia

Quantum Experiments at Space Scale

From Wikipedia, the free encyclopedia

Quantum Experiments at Space Scale (**QUESS**; Chinese: 量子科学实验卫星; pinyin: *Liàngzǐ kēxué shíyàn wèixīng*; literally: "Quantum Science Experiment Satellite"), is an international research project in the field of quantum physics. A satellite, nicknamed **Micius** or **Mozi** (Chinese: 墨子) after the ancient Chinese philosopher and scientist, is operated by the Chinese Academy of Sciences, as well as ground stations in China. The University of Vienna and the Austrian Academy of Sciences are running the satellite's European receiving stations.[4][5] QUESS is a proof-of-concept mission designed to facilitate quantum optics experiments over long distances to allow the development of quantum encryption and quantum teleportation technology.[5] Quantum encryption uses the principle of entanglement to facilitate communication that is totally safe against eavesdropping, let alone decryption, by a third party. By producing pairs of entangled photons, QUESS will allow ground stations separated by many thousands of kilometres to establish secure quantum channels.[3] QUESS itself has limited communication capabilities: it needs line-of-sight, and can only operate when not in sunlight.[6] If QUESS is successful, further Micius satellites will follow, allowing a European–Asian quantum-encrypted network by 2020, and a global network by 2030.[6][7]

The mission will cost around US$100 million in total.[2]

Quantum Experiments at Space Scale

Names	Quantum Space Satellite Micius / Mozi
Mission type	Technology demonstrator
Operator	Chinese Academy of Science
COSPAR ID	2016-051A[1]
Mission duration	2 years (planned)
Spacecraft properties	
Manufacturer	Chinese Academy of Science
BOL mass	631 kg (1,391 lb)
Start of mission	
Launch date	17:40 UTC, 16 August 2016[2]
Rocket	Long March 2D
Launch site	Jiuquan LA-4
Contractor	Shanghai Academy of Spaceflight Technology

RESEARCH ARTICLE

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin[1,2], Yuan Cao[1,2], Yu-Huai Li[1,2], Sheng-Kai Liao[1,2], Liang Zhang[2,3], Ji-Gang Ren[1,2], Wen-Qi ...
+ See all authors and affiliations

Science
Vol 356, Issue 6343
16 June 2017

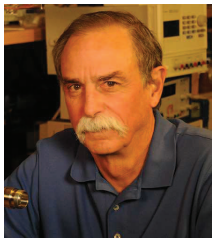
Table of Contents
Print Table of Contents
Advertising (PDF)
Classified (PDF)
Masthead (PDF)

Long-distance entanglement distribution is essential for both foundational tests of quantum physics and scalable quantum networks. Owing to channel loss, however, the previously achieved distance was limited to ~100 kilometers. Here we demonstrate satellite-based distribution of entangled photon pairs to two locations separated by 1203 kilometers on Earth, through two satellite-to-ground downlinks with a summed length varying from 1600 to 2400 kilometers. We observed a survival of two-photon entanglement and a violation of Bell inequality by 2.37 ± 0.09 under strict Einstein locality conditions. The obtained effective link efficiency is orders of magnitude higher than that of the direct bidirectional transmission of the two photons through telecommunication fibers.

Technologies for quantum computer

- Photons : with mirrors, beam splitters, phase shifters, polarizers.

- Light & atoms in cavity : Cavity quantum electrodynamics.
  2012 Nobel Prize in Physics of S. Haroche (France).



- Trapped ions : confined by electric fields,
qubits stored in stable electronic states,
manipulated with lasers. Interact via phonons.
  2012 Nobel Prize in Physics of D. Wineland (USA).

- Nuclear spin : manipulated with radiofrequency electromagnetic waves.

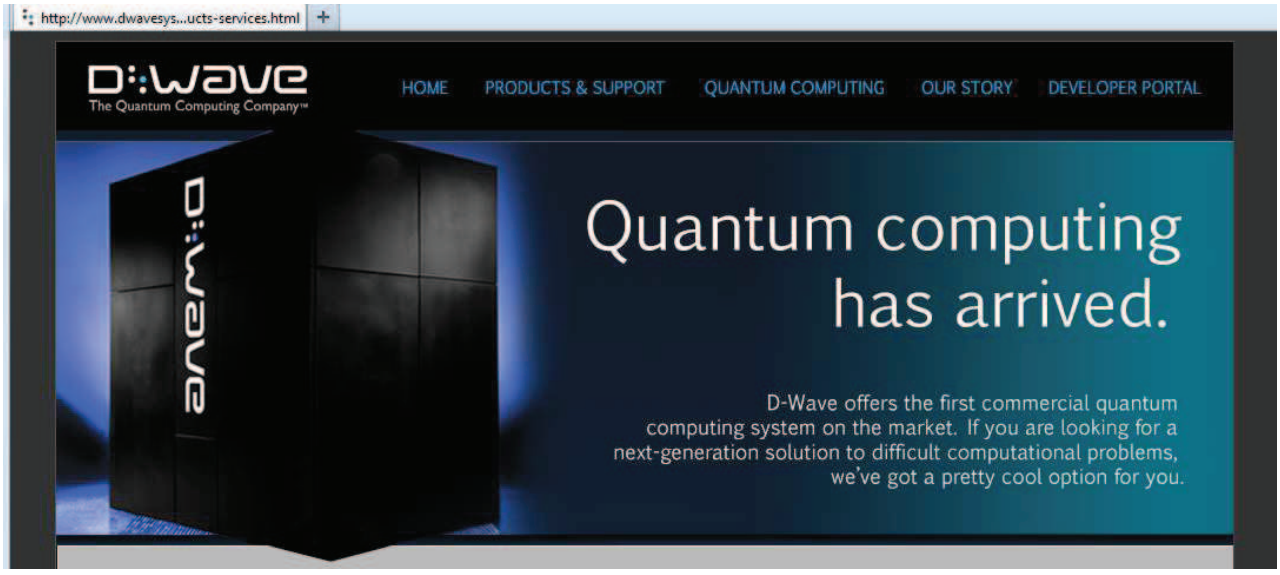
- Superconducting Josephson junctions : in electric circuits and control by electric signals. (Quantronics Group, CEA Saclay, France.)

- Electron spins : in quantum dots or single-electron transistor, and control by electric signals.

  M. Veldhorst *et al.*; "A two-qubit logic gate in silicon"; *Nature* 526 (2015) 410–414.

- ...

A commercial quantum computer : Canadian D-Wave :



Since 2011 : a 128-qubit processor, with superconducting circuit implementation.
Based on quantum annealing, to solve optimization problems.

May 2013 : D-Wave 2, with 512 qubits. $15-million joint purchase by NASA & Google.

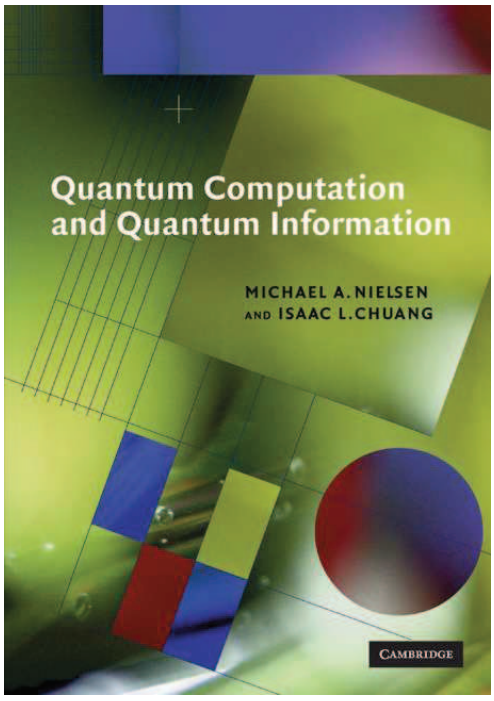
Aug. 2015 : D-Wave 2X with 1000 qubits. Jan. 2017 : D-Wave 2000Q with 2000 qubits.

M. W. Johnson, *et al.*; "Quantum annealing with manufactured spins"; *Nature* 473 (2011) 194–198.

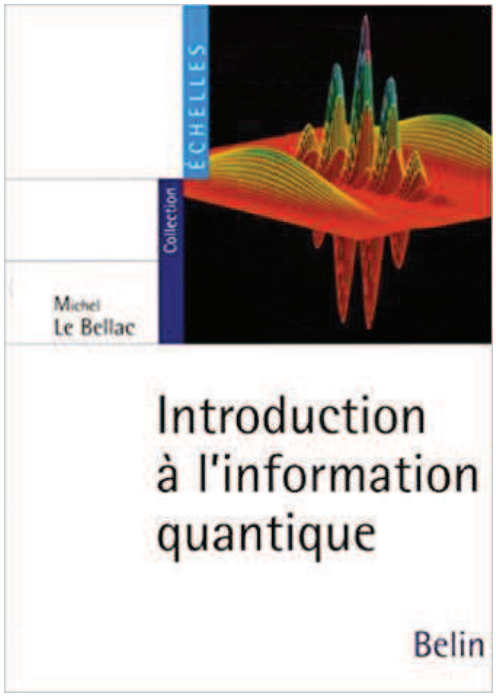
T. Lanting, *et al.*; "Entanglement in a quantum annealing processor"; *Phys. Rev. X* 4 (2014) 021041.

Merci de votre attention.

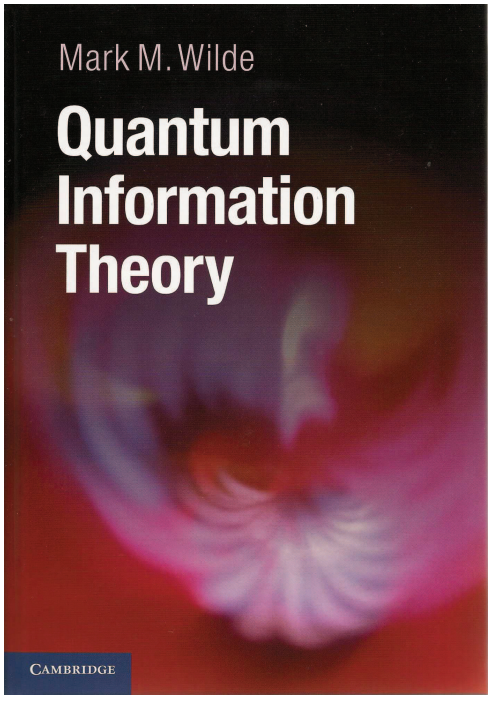
Quelques ouvrages récents



M. Nielsen & I. Chuang
2000, 676 pages



M. Le Bellac
2005, 126 pages



M. Wilde
2013, 655 pages

arXiv:1106.1445v5 [quant-ph] M. Wilde, "From classical to quantum Shannon theory", 670 pages.