Les  de l'IMT

*CNRS**

Qubit or not
Histoires de Bra et de Ket

Jean-Claude Yakoubsohn

Institut de Mathématiques de Toulouse

Jeudi 17 décembre 2015

*Centre National de la Retraite Scientifique

Merci

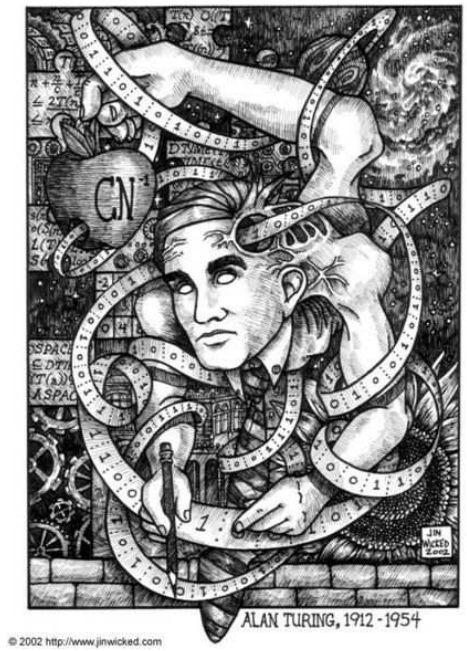
Mon Stormtrooper

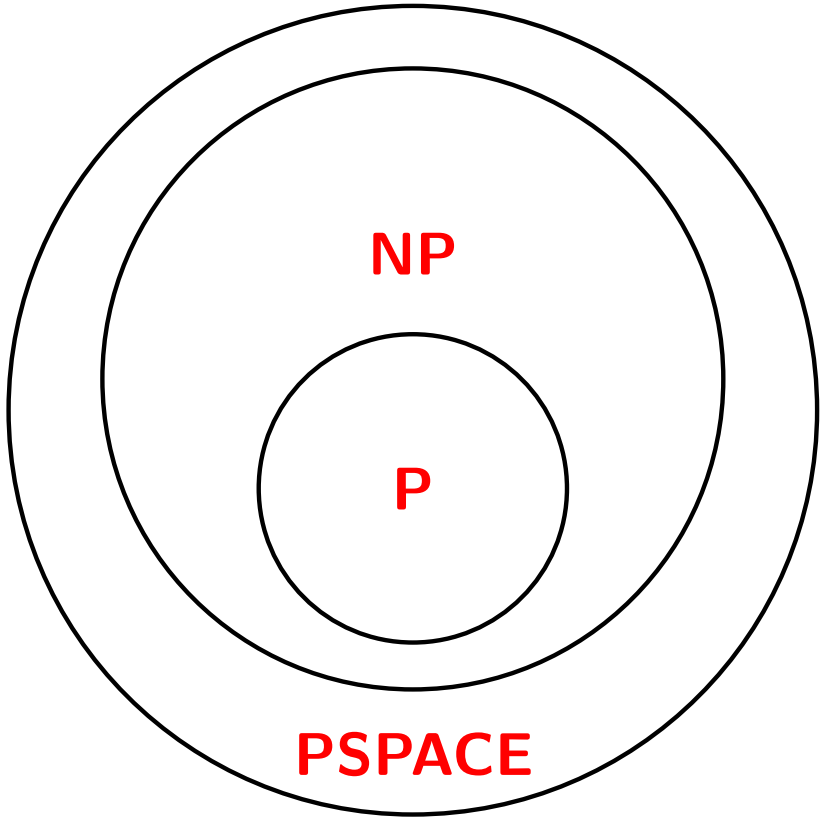
Habilité à Diriger des Retraités

Conférence FELIM, Mars 2015, Limoges.

Alexander Prokopenya.
Quantum Algorithm for Phase Estimation: Simulation with Wolfram Mathematica

Classes de Complexité des algorithmes



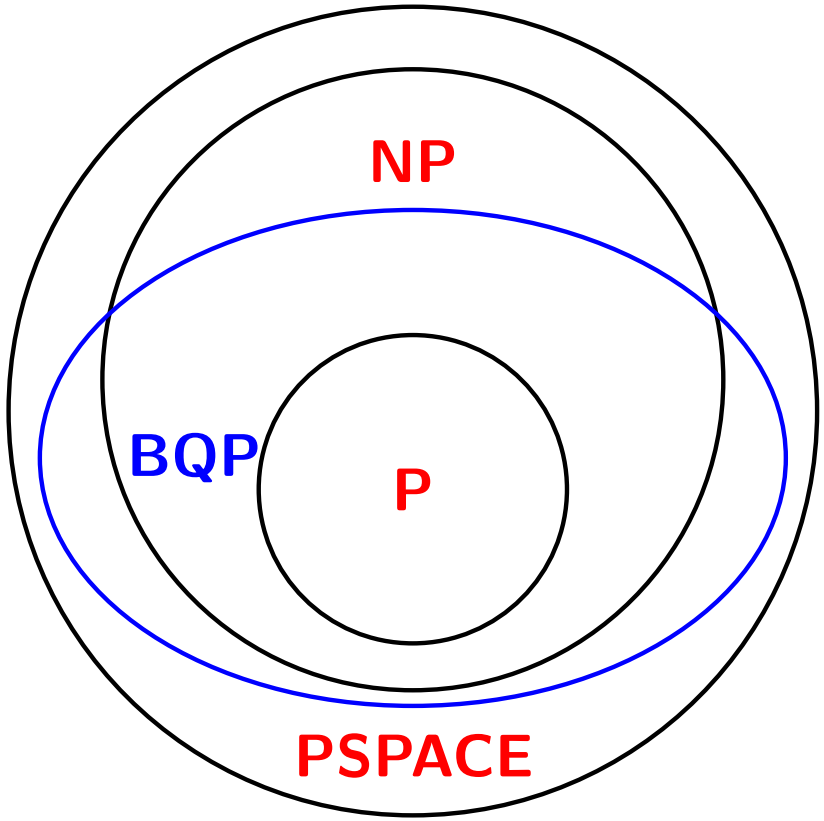


$\mathbf{P} \neq \mathbf{NP}^{\dagger}$

[†] This slide is too short to contain the proof!

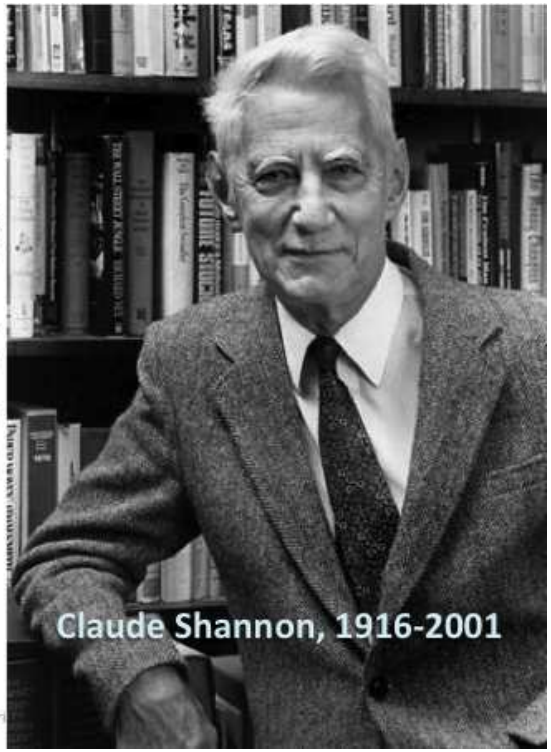
Classe BQP de Complexité des algorithmes quantiques

BQP : classe des problèmes qui peuvent être résolus à ϵ près avec une probabilité bornée en utilisant une taille polynomiale d'un "circuit quantique".



Bit = binary digit

"The enemy knows the system being used."
Claude Shannon,
Communication Theory of Secrecy Systems
(1949)

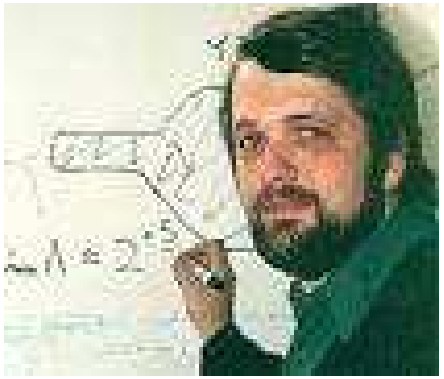


evans@virginia.edu

Engineer

Le bit possède deux états 0 et 1.
Byte= ensemble ordonné de bits.
Les Technologies utilisées pour encoder l'information reposent sur : tension électrique, intensité lumineuse, polarisation magnétique etc...

Qubit = quantun bit



Benjamin Schumacher, Qantum coding, 1995 :
The term "qubit" was coined in jest during one of the author's many intriguing and valuable conversations with W. K. Wootters, and became the initial impetus for this work.

Qubit = quantun bit

Un qubit se définit par son état à partir duquel on lui attribue une mesure (valeur).
Un qubit est une combinaison linéaire (superpositions) des bits 0 et 1.
Notation de Dirac : $|0\rangle$= ket 0 et $|1\rangle$= ket 1.
On écrit

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

où a et b sont deux nombres complexes tels que

$$|a|^2 + |b|^2 = 1.$$

La mesure du qubit $|\psi\rangle$ est 0 avec une probabilité de $|a|^2$ et 1 avec une probabilité de $|b|^2$.

bra = conjugué du ket, $\langle\psi|$

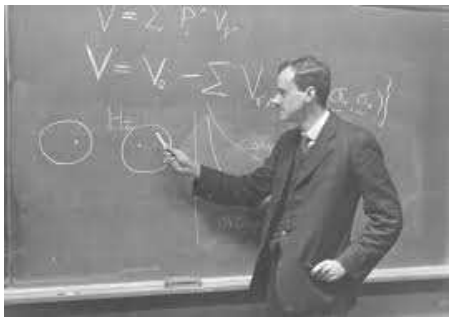
$$\langle\psi|\psi\rangle = 1$$

Exemple : si $|\psi\rangle = a|0\rangle + b|1\rangle$

$$\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1.$$

Le ket est un vecteur colonne.
Le bra est un vecteur ligne.

$$\begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \bar{a}a + \bar{b}b.$$



Paul Adrien Dirac, 1902-1984

N-qubit

1– 2-qubit :

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

avec $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

2– N-qubit :

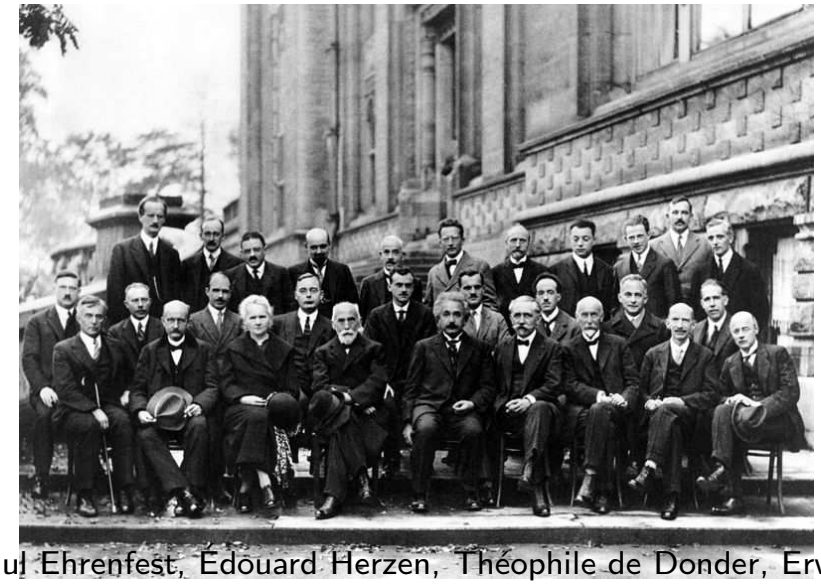
$$\sum_{k=0}^{2^N-1} a_k |k_{N-1} \dots k_0\rangle$$

avec $\sum |a_k|^2 = 1$ et

$$k = \sum_{j=0}^{N-1} k_j 2^j, \qquad \text{où les } k_j \text{ sont dans } \{0, 1\}$$

Postulat 0 de la quantique

Le formalisme mathématique de la quantique est celui de l'algèbre linéaire.



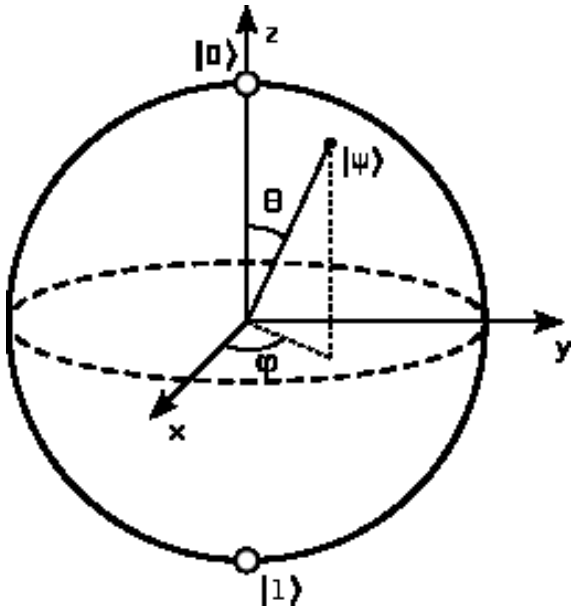
Auguste Piccard, Émile Henriot, Paul Ehrenfest, Édouard Herzen, Théophile de Donder, Erwin Schrödinger, Jules-Émile Verschaffelt, Wolfgang Pauli, Werner Heisenberg, Ralph H. Fowler, Léon Brillouin, Peter Debye, Martin Knudsen, William Lawrence Bragg, Hendrik Anthony Kramers, Paul Dirac, Arthur Compton, Louis de Broglie, Max Born, Niels Bohr, Irving Langmuir, Max Planck, Marie Curie, Hendrik Antoon Lorentz, Albert Einstein, Paul Langevin, Charles Eugène Guye, Charles Thomson Rees Wilson, Owen Willans Richardson

Postulat 1 de la quantique

À tout système physique isolé est associé un espace de Hilbert (espace des états). Le système est complètement décrit par un vecteur de norme 1 (vecteur d'état).

Interprétation géométrique du qubit

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right)$$



Henri Poincaré, 1854-1912.

Félix Bloch, 1905-1983.

$$U|\psi\rangle, \quad U \text{ unitaire}$$

Exemple 1.

$|\psi\rangle = a|0\rangle + b|1\rangle$, $U|\psi\rangle := b|0\rangle + a|1\rangle$. C'est l'opération NOT représentée par la matrice :

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

Exemple 2.

$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$,
$U|\psi\rangle := a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$.
C'est l'opération C-NOT représentée par la matrice :

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

Opérations logiques sur les bits et les qubits

1– AND,OR,NAND,XOR, NOR

2– non réversibilité

2– Toute opération logique sur des bits est égale à des compositions d'opérations comportant seulement l'opération NAND

George Boole, 1815-1864.

1– Matrice unitaire

2– Réversibilité

3– Toute opération logique sur des qubits est égale à des compositions d'opérations logiques comportant seulement les opérations C-NOT et 2-qubits.

Postulat 2 de la quantique

L'évolution d'un système fermé quantique est décrit par une transformation unitaire.

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

Erwin Schrödinger, 1887-1961.

Plus je pense la portion physique de la théorie de Schrodinger, plus je la trouve répugnante. Ce qu'écrit Schrodinger sur la possibilité de visualisation de sa théorie n'est probablement pas tout fait exact en d'autres termes, c'est des foutaises.

Werner Heisenberg.

Postulat 3 de la quantique

Les mesures quantiques sont modélisées par des opérateurs. La probabilité qu'un état $|\psi\rangle$ ait la valeur m est

$$p(m) = \langle\psi|U^* U|\psi\rangle$$

L'état après la mesure est

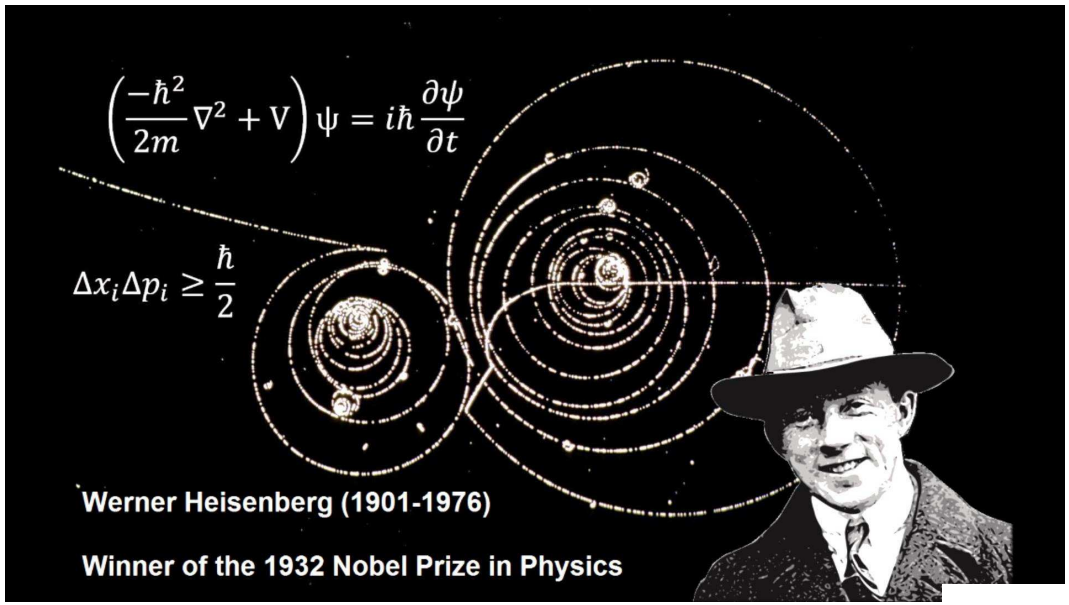
$$\frac{U|\psi\rangle}{p(m)}.$$

Il y a des conséquences subtiles:

Deux états non orthogonaux ne peuvent être distingué par des mesures quantiques.

Postulat 3 de la quantique

"Last but not least" : principe d'incertitude de Heisenberg.



Louis-Augustin Cauchy 1789-1857.

Inégalité de Cauchy-Schwarz.

$$\langle\psi|\phi\rangle \leq \langle\psi|\psi\rangle\,\langle\varphi|\varphi\rangle.$$

Hermann Amandus Schwarz 1843-1921.

Clonage de qubits

Il s'agit de cloner un ket $|\psi\rangle$ inconnu sur un ket $|\varphi\rangle$ connu.
Si le clonage d'ťat d'un qubit est possible, il est modélisée par une application unitaire telle que

$$U(|\psi\rangle.$$

On note par $\otimes$ le produit tensoriel. Par exemple

$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle.$$

Le clonage est en général impossible!

Suppossons que pour deux états $|\psi_1\rangle$ et $|\psi_2\rangle$ on a :

$$U(|\psi_1\rangle \otimes |\varphi\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle$$

et

$$U(|\psi_2\rangle \otimes |\varphi\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle$$

Alors en prenant le produit scalaire des deux identités ci-dessus et en tenant compte que U est unitaire on obtient :

$$\langle\psi_1|\psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2 \qquad \langle \text{ est le bra}$$

On a une équation du type $x^2 = x$. Donc

1– soit $x = 1$ et $|\psi_1\rangle = |\psi_2\rangle$.

2– soit $x = 0$ et $|\psi_1\rangle$ orthogonal à $|\psi_2\rangle$.

On peut cloner un état particulier ou un état orthogonal mais pas une combinaison linéaire des deux.

Postulat 4 de la quantique

L'espace des états d'un système composé d'états appartenant respectivement à deux espaces d'états est le produit tensoriel de ces deux espaces d'états.

Exemple :

Si un espace d'état est l'ensemble des $|\psi\rangle = a|0\rangle + b|1\rangle$ alors le produit tensoriel de cet espace avec lui même est l'ensemble des

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Superdense coding

Le problème

Alice et Bob partage un qubit disons $|\psi_1\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Le but est qu'Alice transmette un des quatre 00, 01, 10, 11 couple de bit sous la contrainte d'envoyer un qubit seulement.

La solution:

Alice

1– $00 \rightarrow |\psi_1\rangle$

2– $01 \rightarrow |\psi_2\rangle$

3– $10 \rightarrow |\psi_3\rangle$

4– $00 \rightarrow |\psi_4\rangle$

de telle sorte que la base $\{|\psi_1\rangle, \ldots, |\psi_4\rangle\}$ soit orthogonale.
Base de Bell

John Stewart Bell, 1928-1990

Bob dispose du qubit $|\psi_1\rangle$ et reçoit un des qubits $|\psi_k\rangle$.
En effectuant une mesure appropriée (postulat 3), Bob pourra distinguer le bon qubit.
Il en déduira le couple de bit envoyé par Alice.

Kwiat experimental quantum group

K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. Dense coding in exper- imental quantum communication. Phys. Rev. Lett., 76(25):4656?4659, 1996.

Calculs quantiques

1– un circuit quantique comporte deux parties : une partie classique (bit) et une partie quantique (qubit).

2– Un circuit quantyique opère sur des N-qubits. L'espace des états a une dimension de 2^N. Les éléments de la base sont des kets du type $|x_1, \ldots, x_n\rangle$ où les $x_i \in \{0, 1\}$. La complexité d'un tel ket est au plus N.

3– On dispose de "familles universelles" de transformations unitaires.

4– On dispose d'opérateurs de mesures.

Cryptographie RSA

Créations des clefs

1– soient p et q deux entiers premiers.
2– $n = pq$.
3– $\phi(n) = (p-1)(q-1)$.
4– soit e premier avec $\phi(n)$ et $e < \phi(n)$
5– détermination de d l'inverse de e modulo $\phi(n)$.
6– Clef publique : (n, e)
7– Clef privée : d

Chiffrement du message m entier plus petit que n.

1– $c = m^e \mod n$.

Déhiffrement du message c.

1– $c^d \mod n = m$.

Exemple.

1– $p = 5$ et $q = 13$ deux entiers premiers.
2– $n = 65$.
3– $\phi(n) = 48$.
4– $e = 5$.
5– $d = 29$ (puisque $5 \times 29 = 3 \times 48 + 1$.)
6– Clef publique : $(65, 5)$
7– Clef privée : 29

Soit le message $m = 19$.

1– $c = 19^5 \mod 48 = 54$.

Déhiffrement du message $c = 54$.

1– $54^{29} \mod 48 = 19 = m$.

Mais ...

Un des champions de la factorisation ... en pleine action.

Une façon de factoriser un entier n

1– Si $n > 2$ on choisit un nombre (pseudo aléatoire) $a < n$.

2– si a divise n alors  et $n := n/a$.

3– sinon on détermine l'entier r tel que $a^r - 1 = 0 \bmod n$.

4– Si r est impair alors  et on retourne en 1.

5– Si $r = 2q$ est pair alors alors  et $a^{2q} - 1 = (a^q - 1)(a^q + 1)$ et N ne divise pas $a^q - 1$.

6– on retourne en 1 avec $pgcd(n, a^q - 1)$ et $pgcd(n, a^q + 1)$.

Exemple.

1– $n = 65$ et $a = 54$.

2– $r = 12$, $a^6 - 1 = 24794911295$.

3– $pgcd(a^6 - 1, n) = 5$, $gcd(a^6 + 1, n) = 13$.

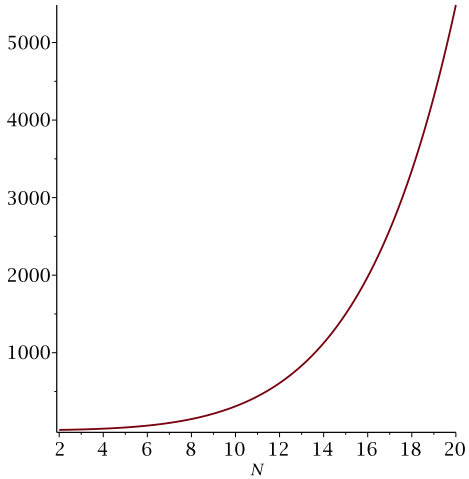
1– $n = 65$ et $a = 12$.

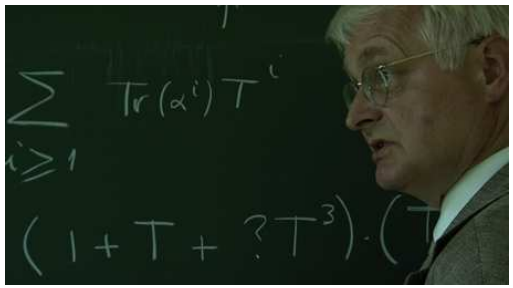
2– $r = 4$, $a^2 - 1 = 143$.

3– $pgcd(a^2 - 1, n) = 13$, $gcd(a^2 + 1, n) = 5$.

Complexité exponentielle en nombre de bits $N = \ln n$:

$exp((32N/9)^{1/3}(\ln N)^{2/3})$





Hendrik Lenstra

La difficulté est de déterminer $\boxed{\text{l'entier } r \text{ tel que } a^r - 1 = 0 \bmod n.}$

L'ingrédient est la transformée de Fourier quantique.
Sa complexité est en $O(N^2)$
Remarque :
la complexité du calcul de la transformée de Fourier est en $O(N2^N)$.

La complexité de l'algorithme quantique de Shor est $O(N^3)$.

$15 = 3 \times 5$!

1– Soit $x = 7$.

2– On considère le qubit

$$\frac{1}{2^{t/2}} \left(|0\rangle + \ldots + |2^{t/2} - 1\rangle \right) |0\rangle$$

La théorie dit qu'il faut choisir $t = 11$ pour que la probabilité d'avoir une erreur "petite" soit d'au moins égale à $3/4$.

3– Par transformée Fourier quantique appliquée à $f(k) = 7^k \bmod 15$, $k = 0..2^t - 1$ on obtient le qubit

$$\frac{1}{2^{t/2}} \left(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle \ldots \right)$$

4– C'est le point crucial où interviennent la transformée de Fourier inverse et une application d'un principe dit de mesure implicite.

5– La mesure finale donne 0, 512, 1024, 1536 : chacune de ces valeurs a une probabilité $1/4$.

6– La théorie dit que l'exposant r cherché est un des dénominateurs des fractions suivantes :

$$\frac{0}{2048} = \frac{0}{?}, \quad \frac{512}{2048} = \frac{1}{4}, \quad \frac{1024}{2048} = \frac{1}{2}, \quad \frac{1536}{2048} = \frac{3}{4}.$$

Soit $r = 2$ ou 4.

$15 = 3 \times 5$!

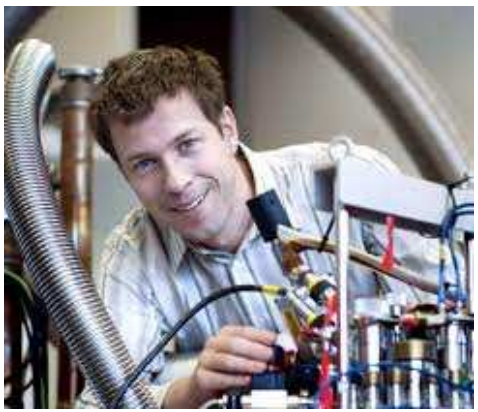
7– À l'aide du circuit classique (bit) on essaye $r = 2$ et $r = 4$.

7.1– $7^{2/2} - 1 = 6 \neq 0 \mod 15$ donc $r = 2$ ne convient pas.

7.2– $7^{4/2} - 1 = 48 = 3 \mod 15$. Donc 3 divise 15.

8– On en déduit alors que $15 = 3 \times 5$. Yes we win!

Isaac Chuang



L.M. K. Vandersypen

Matthias Steffen

Lieven M. K. Vandersypen , Matthias Steffen , Gregory Breyta ,Costantino S. Yannoni , Mark H. Sherwood, Isaac L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature,2001

Le bonheur est-il dans le pré?

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they?ll read our email,
Till we get crypto that's quantum, and daunt 'em.
Jennifer et Peter Schor

Peter Shor

Après la FLOP21 ... le D-wave 2 X

Si vous aimez l'ordinateur classique vous allez adorer l'ordinateur quantique.

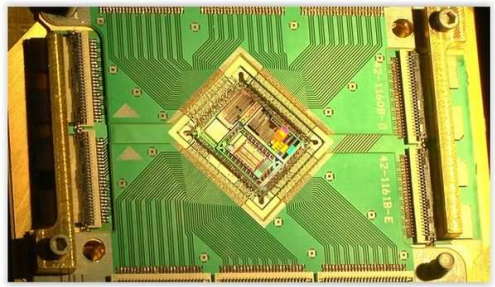
1– investissement de Google et de la NASA :10 à 15 milliards de dollars.

2– Il ne parle pas en bits mais en qubits

3– Ce qu'une machine D-Wave fait en une seconde, prendrait 10 000 ans à un ordinateur conventionnel.

4– Attention pour le stocker chez soi il faut un bon frigo : sa puce fonctionne à une température proche du zéro absolu !

Demandez-le au Père Noël!



Pour conclure

Plutôt que

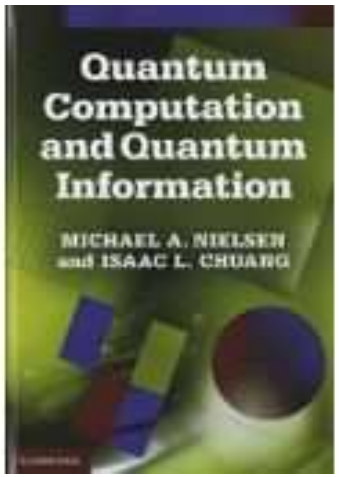
Qbit or bit

je prendrai

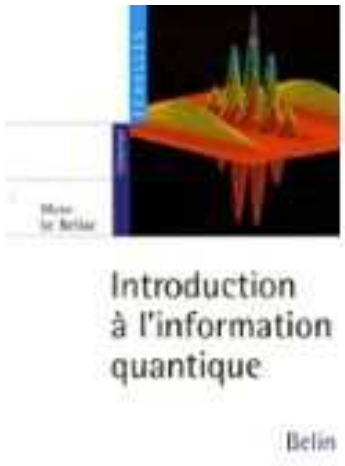
Qbit et bit

Et pour la prochaine fois, ça sera sans bra ni ket!

De la lecture pour Noël

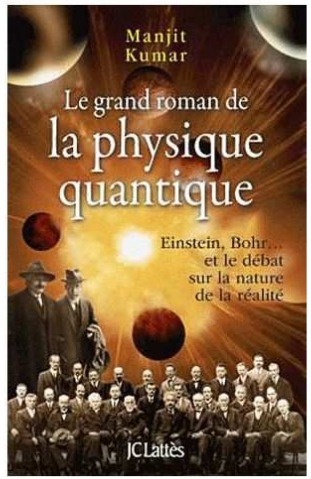


Nielsen-Chuang

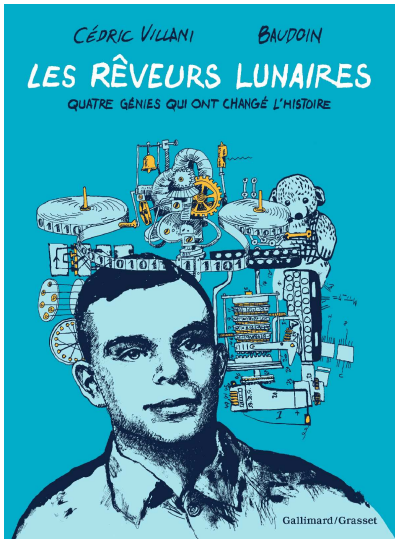


Michel Bellac

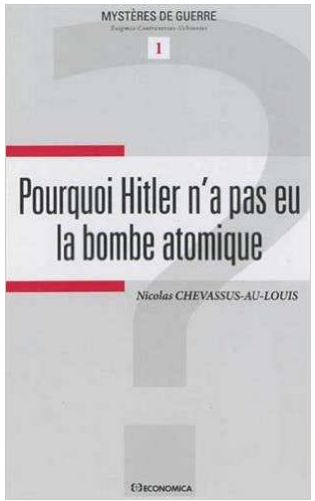
Perez et all



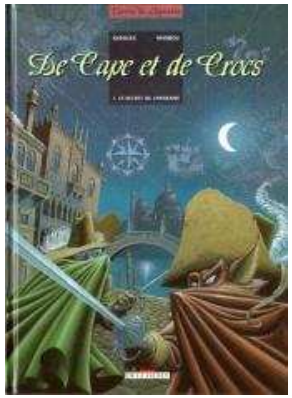
Kumar



Villani-Baudoin



Chevassus-au-Louis



Jean-Luc Masbou

N'ai-je donc tant vécu
Que pour te voir au traitre,
Rallier ce vil roi
Dont un peuple est le maître?

Je t'aimais comme un frère,
Et ce frère, aujourd'hui
Tu l'aimes plus que moi ...
Je le hais plus que lui!