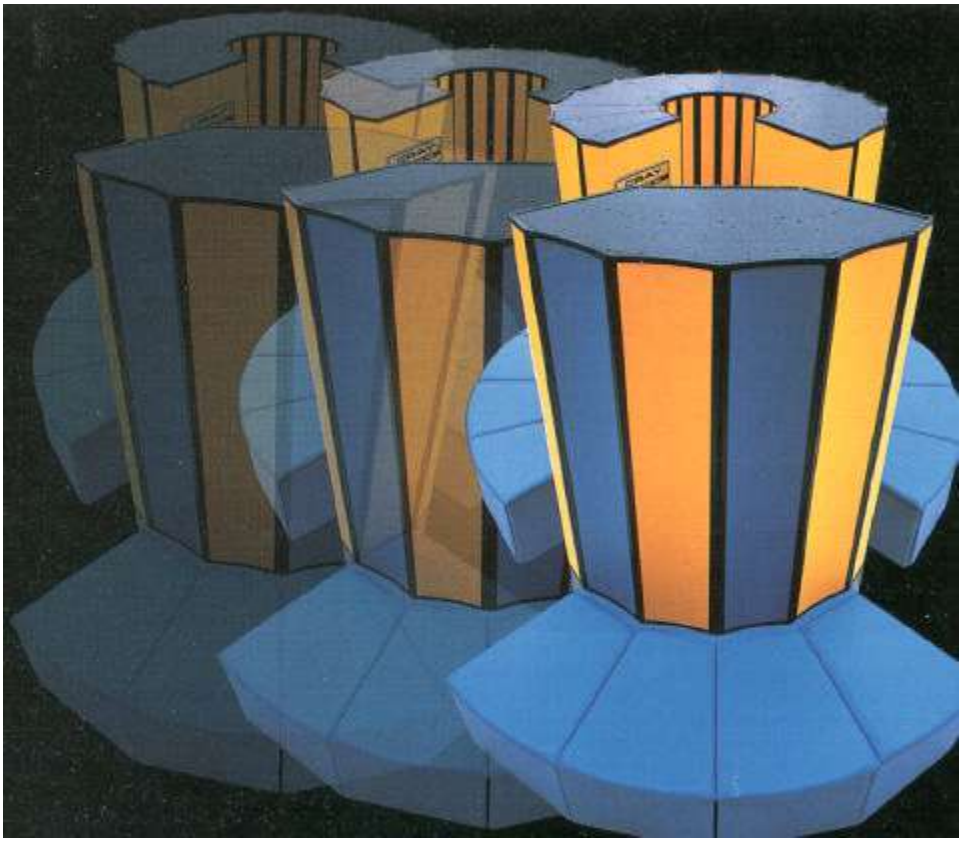
Ordinateur quantique: rêves et réalité



$$\frac{1}{\sqrt{2}}\left(\left|\ \right\rangle + \left|\ \right\rangle\right)$$

J.M. Raimond

Laboratoire Kastler Brossel

Qu'est ce qu'un ordinateur quantique?

logique classique: *bits* *0,1*

logique quantique: *qubits* $|0\rangle, |1\rangle$ *(système à deux nx)*

Il existe des superpositions d'états logiques

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

n bits classiques codent une valeur parmi $N=2^n$

n qubits peuvent coder une superposition des 2^n *valeurs*

Un ordinateur quantique manipulant des qubits peut effectuer 2^n *opérations en un seul cycle !*

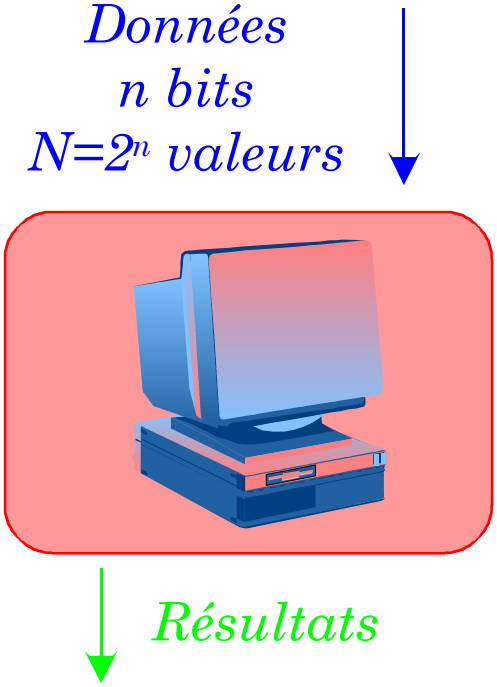
Parallélisme quantique massif

Enorme puissance de calcul

Rend aisée la solution de problèmes difficiles

$$\frac{1}{\sqrt{2}}\left(\left|\ \right\rangle + \left|\ \right\rangle\right)$$

Ordinateurs classiques et complexité



Codage des données sur des états physiques

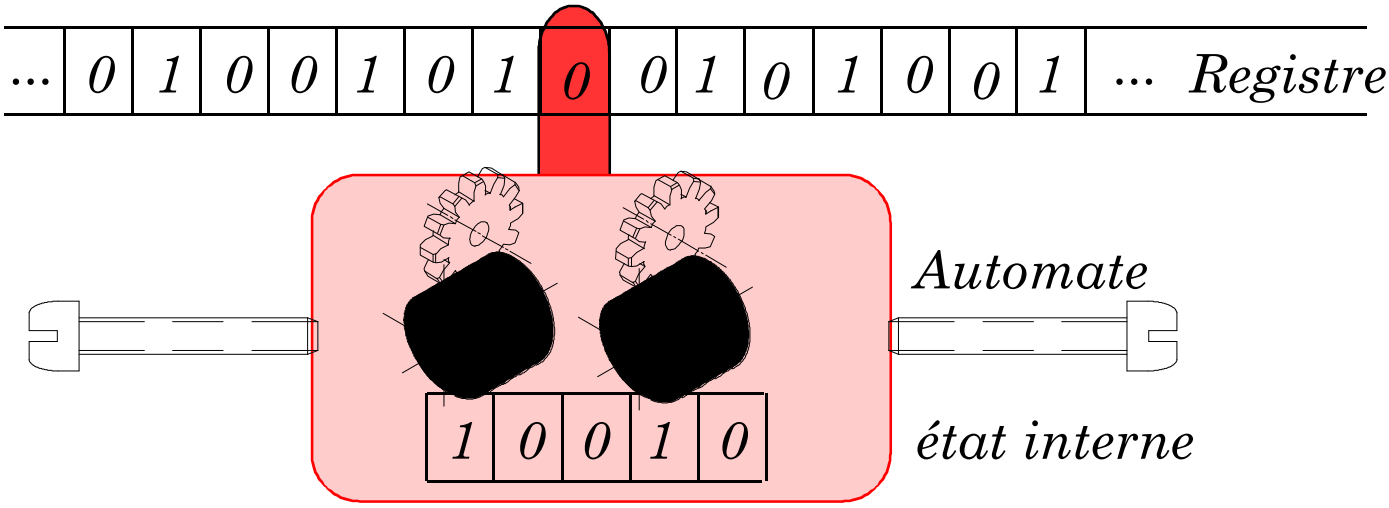
Mécanisme physique produisant les résultats à partir des données

Problème crucial: coût
- *en temps*
- *en ressources*

Problème facile: Polynomial en n (log en N) P

Problème difficile: Exponentiel en n (polynomial en N) NP

Principe de Church-Turing:
Du point de vue de la complexité, tous les ordinateurs classiques sont équivalents entre eux et au plus simple:
La machine de Turing



Un seul registre infini
Quelques opérations simples

Quelques problèmes faciles

Opérations arithmétiques élémentaires

Addition: $a \quad n$

Multiplication: $a \quad n^2$

Recherche dans une base de données triées

Tri dichotomique $a \quad Log(nombre\ éléments)$

Quelques problèmes difficiles

Factorisation

Algorithme naïf $\sqrt{N} = 2^{n/2}$

Recherche dans une base de données non triée

Meilleure tactique: essai aléatoire $N/2 = 2^{n-1}$

Problème du "voyageur de commerce"

Visiter n villes par l'itinéraire le plus court

Problèmes d'échecs à n coups

Un problème difficile: factorisation

Algorithme naïf: essai de tous les diviseurs $\sqrt{N}$

Meilleur algorithme connu (grands nombres) $e^{1.9n^{1/3}}$

Problème "parallélisable"

(dualité ressources/temps)

temps de calcul exponentiel remplacé par un nombre de processeurs exponentiel

Factorisation de 129 chiffres (94)

Quelques mois
Quelques centaines de machines
Quelques 100 Mips/machine .....

} 10^{16} instructions

Une application: la cryptographie

Clé x Message = Cryptogramme

Cryptogramme / Clé = Message

} Très facile

Facteur (Cryptogramme)= Message Très difficile

La plupart de codes cryptographiques utilisent la factorisation ou le logarithme discret ($b^x = q \quad [N]$)

Tout problème facile dont le problème inverse est difficile pourrait convenir

Enorme importance économique (et stratégique)

Ordinateur quantique

Equivalent à une machine de Turing dont les bits (0 ou1) sont remplacés par des qubits *systèmes à deux niveaux*
Il existe des superpositions d'états $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Calcul: évolution unitaire de l'état de la machine

$$|e_1, e_2, \cdots, e_n\rangle \rightarrow U|e_1, e_2, \cdots, e_n\rangle \qquad e = 0,1$$

U: matrice unitaire commandée par l'utilisateur
"programme" de l'ordinateur quantique

Représentation de l'état

Registre de n qubits

Espace des états de dimension 2^n. Base:

$$|0,0,\cdots,0\rangle = |0\rangle$$
$$|0,0,\cdots,1\rangle = |1\rangle$$
$$|1,1,\cdots,1\rangle = |2^n - 1\rangle = |N\rangle$$

Comment calculer?

Préparation de $|a,0\rangle$

Evolution unitaire pour "calculer" f $|a,0\rangle \xrightarrow{U} |a, f(a)\rangle$

Mesure des n derniers qubits: obtention du résultat

Tout calcul effectué par une machine de Turing classique peut aussi être effectué par un ordinateur quantique

Evolution unitaire:

Pas de bruit ou de relaxation

Utilisation parcimonieuse de la mesure

Calcul réversible

$$|x\rangle \rightarrow |f(x)\rangle \quad \forall x$$

interdit si f n'est pas inversible, mais

$$|x,0\rangle \rightarrow |x, f(x)\rangle \quad \forall x$$

autorisé

Ne pas effacer un qubit à moins que l'état ne soit certain

Mais un ordinateur quantique peut aussi

calculer simultanément 2^n valeurs de f !!!!

Parallélisme quantique massif

Exponentiellement plus efficace qu'un calculateur classique

Lecture du résultat?

mesure des n derniers qubits:

$$|b, f(b)\rangle$$

Une valeur pour un argument arbitraire (connu)

Perte de l'efficacité

Algorithmes subtils pour profiter du parallélisme et extraire le résulat

Algorithmes quantiques

Très peu d'algorithmes connus

(en dépit d'une recherche intensive)

Problèmes ad hoc

Deutsch Josza (réalisation expérimentale à 1 bit !)

Simon (précurseur de Shor)

Problème utile, accélération faible

Grover et variantes

Recherche dans une base non triée

Ne change pas la classe de complexité

(de $N/2$ à $\sqrt{N}$)

Problème utile et accélération exponentielle

Shor

Algorithme polynomial de factorisation !

Responsable de l'engouement pour le sujet

(et des craintes des services du chiffre)

"Simulateurs quantiques"

Llyod

Utiliser le parallélisme pour simuler l'évolution d'un système quantique

Que des idées de principe

Brève histoire de l'informatique quantique

73	Bennett	Calcul réversible classique
80	Benioff	Proposition de principe
82	Feynman	"Quantum simulator"
		espace de Hilbert de taille exponentielle
85	Deutsch	Machine de Turing quantique
		bases conceptuelles
92	Deutsch	Premiers algorithmes ad hoc (inutiles)
		Notion de "portes logiques quantiques"
94	Shor	Algorithme de factorisation
		Utile et accélération exponentielle
95		Propositions théoriques de portes
95	Wineland	Première réalisation d'une porte
97	Grover	Algorithme de recherche
		Utile mais accélération faible

Algorithme de Deutsch Josza

Intérêt anecdotique, mais réalisé expérimentalement (1 bit!)

Fonction f de (0...2N-1) vers 0 ou 1

Définitions:

Fonction constante: *2N valeurs identiques*
Fonctions "équilibrées": *exactement N zéros et N un*

Si f est constante, elle n'est pas équilibrée
Si f est équilibrée, elle n'est pas constante

Donc des 2 propositions
(A) f n'est pas constante
(B) f n'est pas équilibrée
au moins une est vraie

Problème: déterminer quelle proposition est vraie
(ou une quelconque si les deux sont vraies)

Algorithme classique (optimal)

Calcul de N+1 valeurs de f
Toutes égales:
f est non équilibrée donc (B) est vraie
Au moins une différente:
f n'est pas constante donc(A) est vraie

N+1 évaluations de f dans le pire des cas:
problème exponentiel

Algorithme quantique

1 registre de n+1 bits (0 à 2N-1)

1 registre de 1 bit (évaluation de f)

Etat initial

$$|0,0\rangle$$

Préparation d'une superposition de tous les nombres

$$|0,0\rangle \xrightarrow{U_H} |\Phi\rangle = \frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} |i,0\rangle$$

U_H: *Transformation de Hadamard sur chaque qubit*

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Calcul de f

$$|\Phi\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} |i, f(i)\rangle$$

U_f: *transformation unitaire du dernier bit*

Application d'une phase conditionnelle

$$\frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} |i, f(i)\rangle \longrightarrow \frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} (-1)^{f(i)} |i, f(i)\rangle$$

Nouveau calcul de f (équivalent au calcul de l'inverse)

$$\frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} (-1)^{f(i)} |i, f(i)\rangle \longrightarrow |\Psi\rangle = \frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} (-1)^{f(i)} |i,0\rangle$$

Transformation de Hadamard inverse

$$|\Psi\rangle \longrightarrow U_H^+ |\Psi\rangle$$

Mesure individuelle de tous les qubits du premier registre

Probabilité que tous les qubits soient à 0:

$$P_0 = \left(\langle \Psi | U_H\right) |0,0\rangle\langle 0,0| \left(U_H^+ |\Psi\rangle\right)$$

mais

$$U_H |0,0\rangle = |\Phi\rangle$$

donc

$$P_0 = \langle \Psi | \Phi\rangle\langle \Phi | \Psi\rangle = |\langle \Psi | \Phi\rangle|^2$$

$$= \frac{1}{(2N)^2} \left| \sum_{i=0}^{2N-1} (-1)^{f(i)} \right|^2$$

f constante: P_0=1

f balancée: P_0=0

Si tous les qubits mesurés sont à 0:
f n'est pas balancée
(B) vraie

Si un au moins des qubits est à 1
f n'est pas constante
(A) vraie

Solution du problème avec une seule évaluation de f:
accélération exponentielle par rapport au calcul classique
gain: parallélisme quantique dans l'évaluation de f
Le problème est que ce problème n'a ni intérêt, ni application

Algorithme de Shor

Problème: factoriser un nombre N arbitraire et grand
(qui ne doit pas être une puissance de 2 ni un carré)

Un tout petit peu d'arithmétique

Soit x quelconque, x<N

Si x n'est pas premier avec N: on a un diviseur de N

Si x est premier avec N, on définit l'ordre de x comme le plus petit entier r tel que:

$$x^r = 1 \quad [N]$$

f(a)=x^a [N] est donc une fonction périodique de période r

Si on connaît r, alors on a une chance sur 2 environ que
r soit pair
et $x^{r/2} \neq -1 \quad [N]$

Alors, le $\gcd(N, x^{r/2} \pm 1)$ *est un facteur non trivial de N*

(il existe des algorithmes classiques efficaces pour trouver le gcd de deux nombres)

Factoriser ou trouver l'ordre d'un entier arbitraire (i.e. le logarithme discret de 1 en base x) sont des problèmes équivalents.
Tous deux sont difficiles avec un ordinateur classique
(pas de preuve mathématique)
L'algorithme de Shor fournit l'ordre en un temps polynomial

Exemple trivial

N=15

(le premier non premier, non pair, non carré)

Au hasard x=7

On calcule 7^a *[15]*

a	7^a [15]
1	7
2	4
3	13
4	1

$7^4=1$ *[15]: l'ordre r de 7 est donc 4*

le gcd de 4+1 et 15 est donc un facteur de 15: 5
le gcd de 4-1 et 15 est donc un facteur de 15: 3

Donc

15=5x3

qui l'eut cru??

Algorithme quantique

idée: *calculer beaucoup de valeurs de x^a [N]*
(en utilisant le parallélisme quantique)
Extraire la période r

On travaille sur 2 registres de m qubits

$$q = 2^m \qquad 2N^2 \le q < 4N^2$$

Etat initial

$$|0,0\rangle$$

Choix de x

Générateur aléatoire classique ou mesure quantique

Préparation d'une superposition de tous les nombres
dans le premier registre

$$|0,0\rangle \xrightarrow{U_H} |j\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a,0\rangle$$

U_H: transformation de Hadamard

sur chaque qubit $|0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Exponentiation modulaire

$$|j\rangle \longrightarrow \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \ [N]\rangle$$

Faisable en temps polynomial

Calcul simultané de toutes les valeurs de x^a
Intervention du parallélisme quantique

Mesure des m derniers qubits

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}\left|a, x^a\ [N]\right\rangle$$

On obtient une valeur aléatoire y.

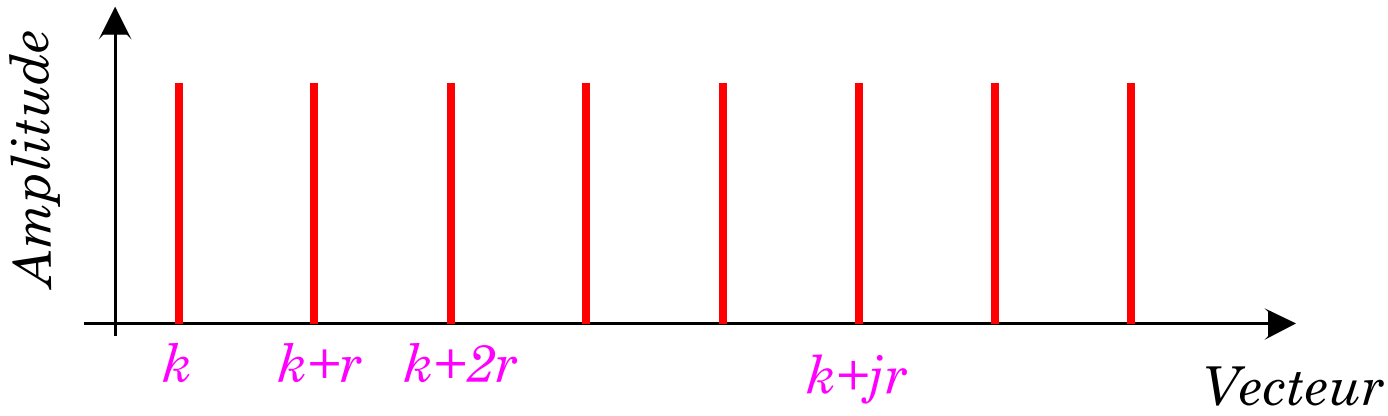
Mais cette valeur a pour antécédent toutes les valeurs de la forme $k+jr$ *où* k *est le plus petit entier tel que* $x^k=y$ *et* j *un entier quelconque*

Les m premiers qubits sont corrélés quantiquement (intriqués) avec ceux que l'on mesure. La mesure les projette sur les états correspondant au résultat obtenu.

L'état, après la mesure du premier registre, est donc:

$$\frac{1}{A}\sum_{j}\left|k+jr\right\rangle$$

Les amplitudes de probabilité sur les différents vecteurs de base forment un peigne de période r



Comme q est de l'ordre de N^2 *et que* $r<N$, *on a au moins N périodes*

On doit extraire cette période et éliminer le décalage aléatoire k.

Pour cela, on effectue sur les premiers qubits une...

Transformée de Fourier discrète

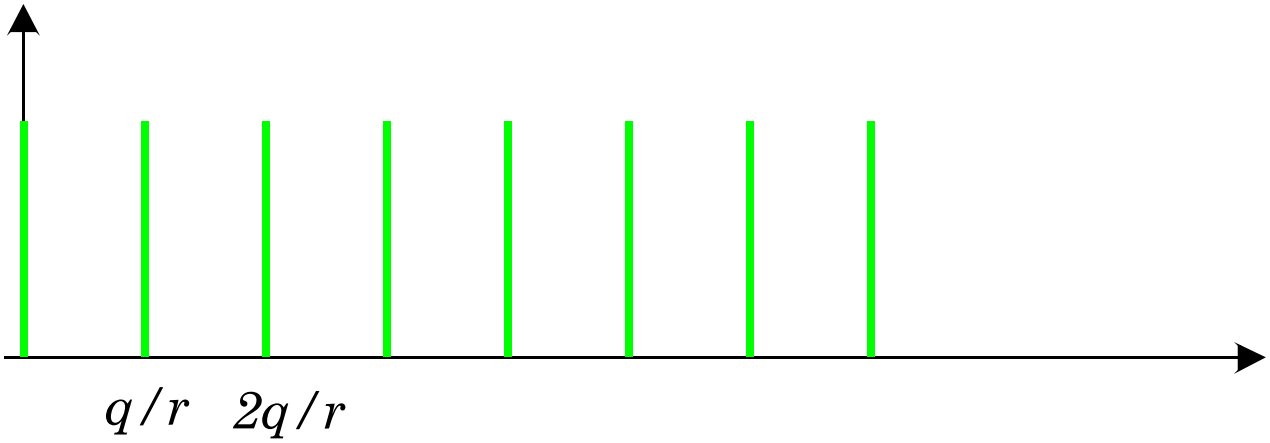
$$\sum_0 a_a |a\rangle \longrightarrow \sum_b b_b |b\rangle$$

avec

$$b_b \propto \sum_a e^{2ip\frac{ab}{q}}$$

Faisable en m^2 opérations au plus (i.e. en un temps polynomial)

Les a_a étant périodique de période r,
les b_b sont périodiques de période q/r (grand entier)



Si on mesure les m premiers bits, on obtient une valeur de la forme

$$l\frac{q}{r}$$

où l est un entier aléatoire

A partir de là, on peut extraire (avec un calculateur classique) avec une probabilité finie la période r
(les détails de cette extraction sont fastidieux)

Quelques caractéristiques importantes de l'algorithme de Shor

Probabiliste

On a une probabilité finie d'obtenir le bon résultat

Mais il est trivial de tester la solution obtenue

et cette probabilité ne décroit pas exponentiellement avec le nombre de bits

Utilise le parallélisme quantique

Pour effectuer en une seule opération toutes les exponentiations modulaires possibles

Revient à "essayer tous les diviseurs à la fois"

Utilise les corrélations quantiques et le postulat de la mesure:

Les deux registres dans l'état

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}\left|a, x^a \left[N\right]\right\rangle$$

sont corrélés quantiquement au même titre que la "paire EPR" dans l'état

$$\frac{1}{\sqrt{2}}\left(\left|\uparrow\downarrow\right\rangle - \left|\downarrow\uparrow\right\rangle\right)$$

La non-localité de la mécanique quantique est essentielle

L'algorithme utilise donc des propriétés authentiquement quantiques

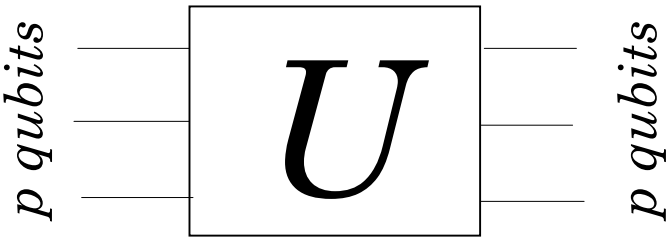
Très différent de ce qu'on pourrait faire avec un calculateur analogique

(même s'il manipulait des superpositions d'états)

Architecture d'un ordinateur quantique

Machine de Turing irréaliste (délocalisation de la tête)

Tout algorithme peut être décomposé en portes logiques élémentaires (cf ordinateur classique)



p qubits en entrée et sortie (réversible) Définie entièrement par la matrice U

en y ajoutant fils (transport de qubits), mémoires..

Exemples de portes

1 qubit

Rotation arbitraire $U(j,y) = \begin{pmatrix} \cos j & e^{iy} \sin j \\ -e^{-iy} \sin j & \cos j \end{pmatrix}$

Transformation de Hadamard $U_H = U(j = p/2, y = 0)$

2 qubits

Controlled NOT

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

Dynamique du deuxième bit (cible) conditionnée par l'état du premier (contrôle) (version réversible de XOR)

3 qubits

Toffoli

double dynamique conditionnelle

CCNOT

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

Universalité

Tout réseau est réalisable avec une seule porte

Toffoli

Toute dynamique conditionnelle non triviale (sauf CNOT)

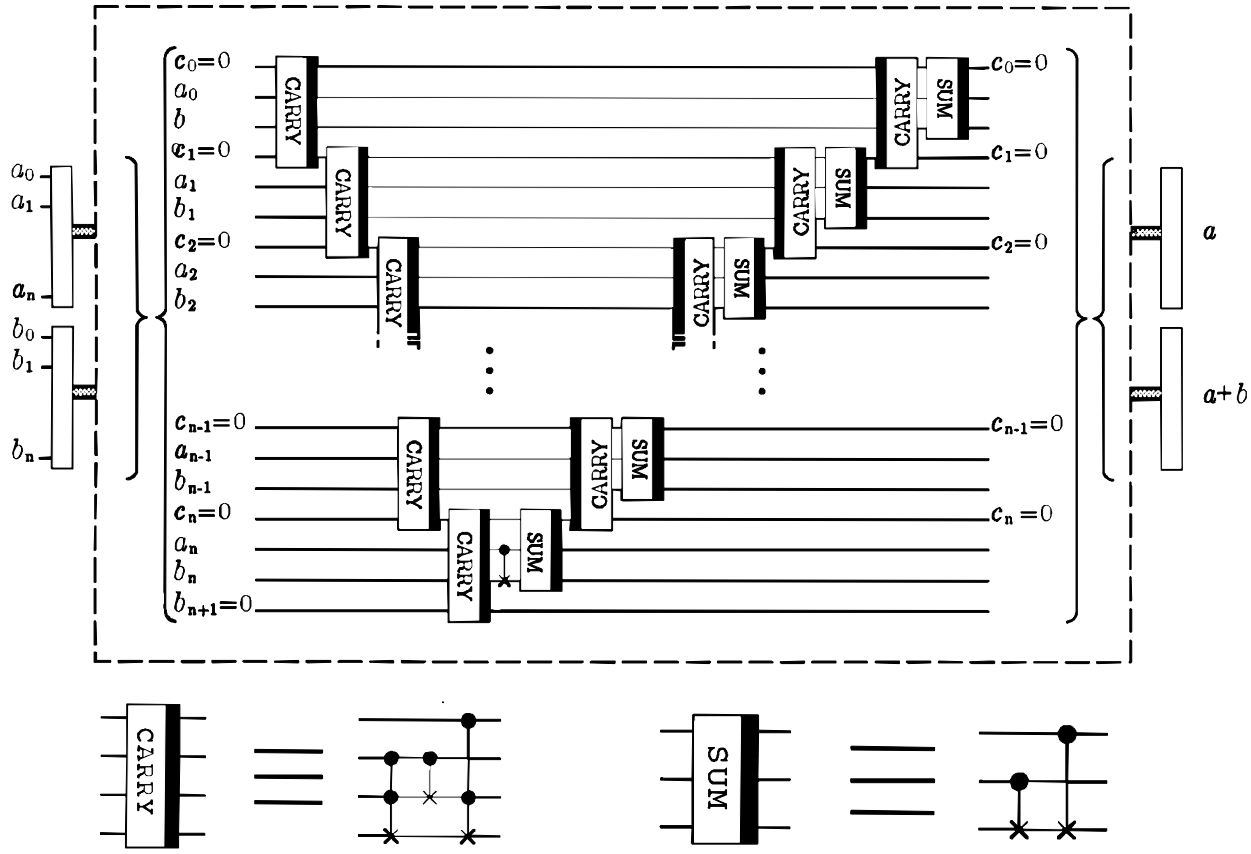
Ensemble suffisant de portes

CNOT + rotations à un bit

Permet en principe de dessiner tous les réseaux.

Exemple: additionneur

(Barenco)



Complexe:

Ne pas laisser de données dans les mémoires de travail.

Effacer toutes ces mémoires par des transformations unitaires (portes). Déjà nécessaire pour les calculateurs réversibles classiques

Une affaire de vocabulaire

qubit	Atome	Spin
$\|1\rangle$	$\|e\rangle$	$\|\uparrow\rangle$
$\|0\rangle$	$\|g\rangle$	$\|\downarrow\rangle$

N'importe quel système à deux niveaux est un qubit !

Beaucoup d'expériences récentes (optique quantique surtout) s'intéressent à un système à deux niveaux unique dans un environnement bien contôlé:

manipulent en fait des qubits !

Beaucoup d'opérations standard sont des portes logiques:

Transformation de Hadamard =
rotation de p/2 d'un spin autour de l'axe x
Réalisable avec un champ résonant sur la transition entre les deux états d'amplitude et de phase convenable (impulsion p/2 de Rabi).

De nombreuses possibilités aussi pour réaliser la dynamique conditionnelle du CNOT

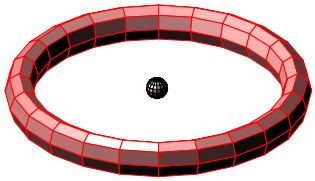
L'opticien quantique était, en 1994, comme M. Jourdain, il faisait du calcul quantique sans le savoir...

94-96: une phase intense de réécriture des vieilles idées en termes différents.

Les systèmes les plus prometteurs:
Atomes et cavités
Ions piégés
RMN...

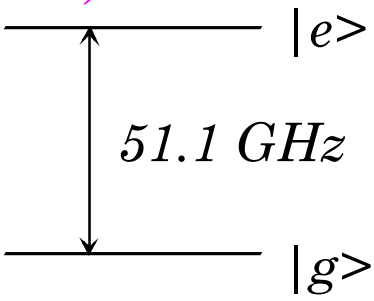
Atomes et cavités:

un exemple de porte simple



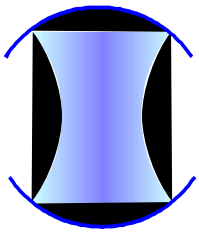
Atome de Rydberg circulaire

- Grand nombre quantique principal (50 ou 51)
- Très grande durée de vie
- Très fortement couplé au rayonnement
- Système à deux niveaux
- Facilement détectable



Cavité microoonde supraconductrice

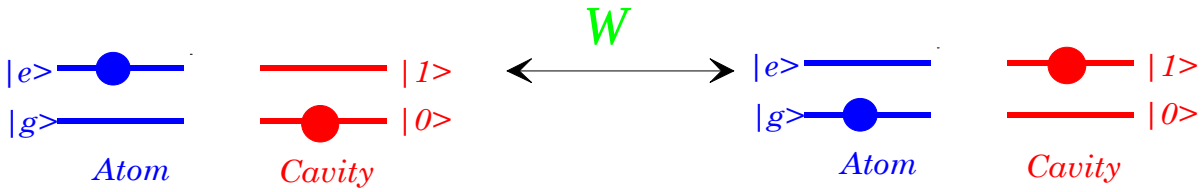
- Très grande durée de vie du champ
- Fort couplage à l'atome
- Oscillateur harmonique



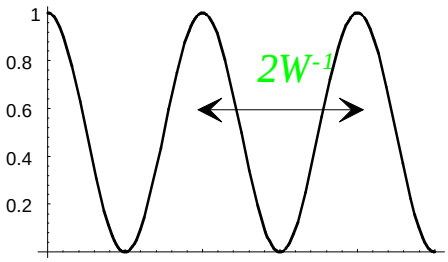
Qubits: atome $|e\rangle,|g\rangle$ *champ dans la cavité* $|0\rangle,|1\rangle$

Manipulations possible:

Interaction résonnante



$$|e,0\rangle \longleftrightarrow |g,1\rangle$$



Impulsion p:

$$\left(c_e|e\rangle + c_g|g\rangle\right)|0\rangle \longrightarrow |g\rangle\left(c_e|1\rangle + c_g|0\rangle\right)$$

transfert de qubit de l'atome à la cavité (et réciproquement)

Possibilité d'une mémoire de l'état atomique.

Interaction non résonnante:

Pas d'échange d'énergie *mais:*

La fréquence de la cavité dépend de l'état de l'atome

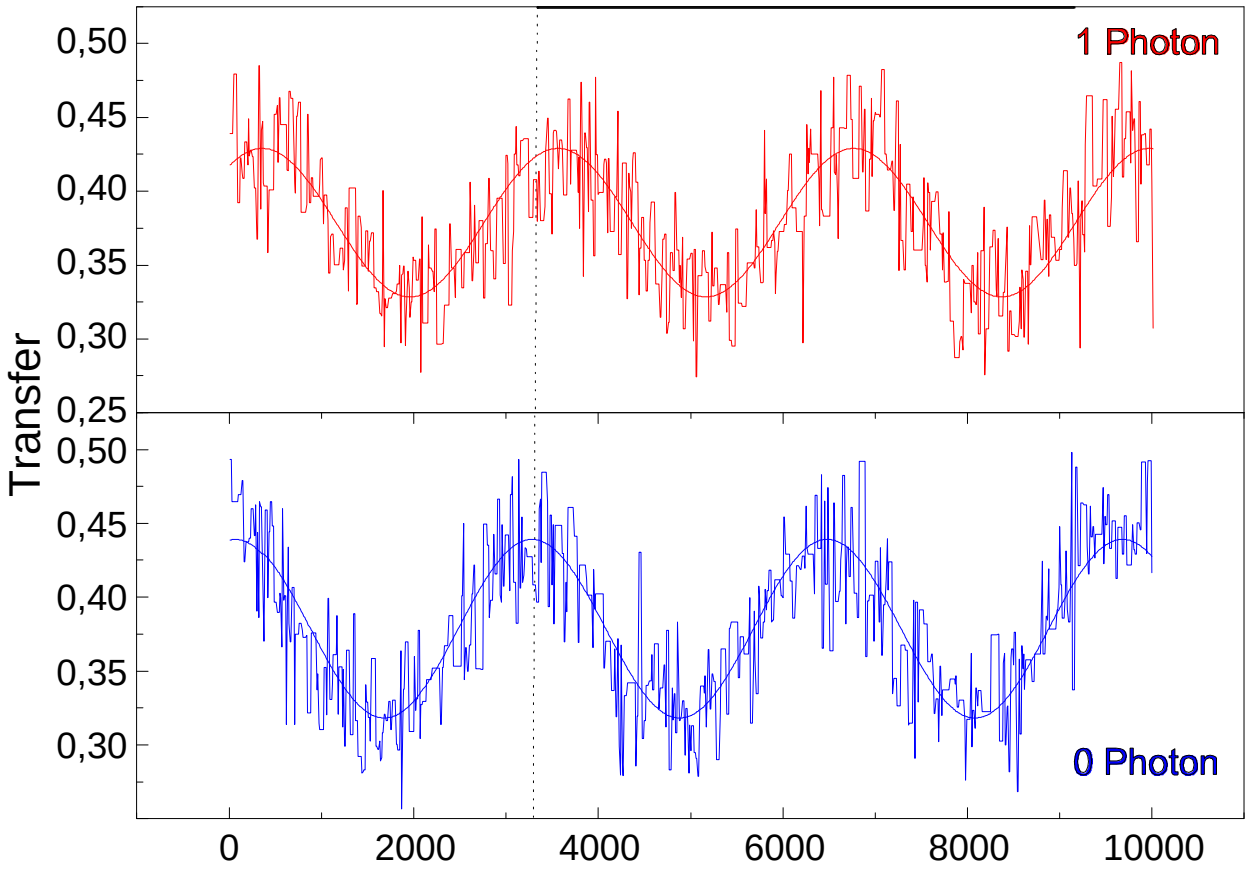
(effet d'indice de réfraction)

La fréquence de la transition atomique dépend de la présence ou non d'un photon dans la cavité

(effet de déplacement lumineux)

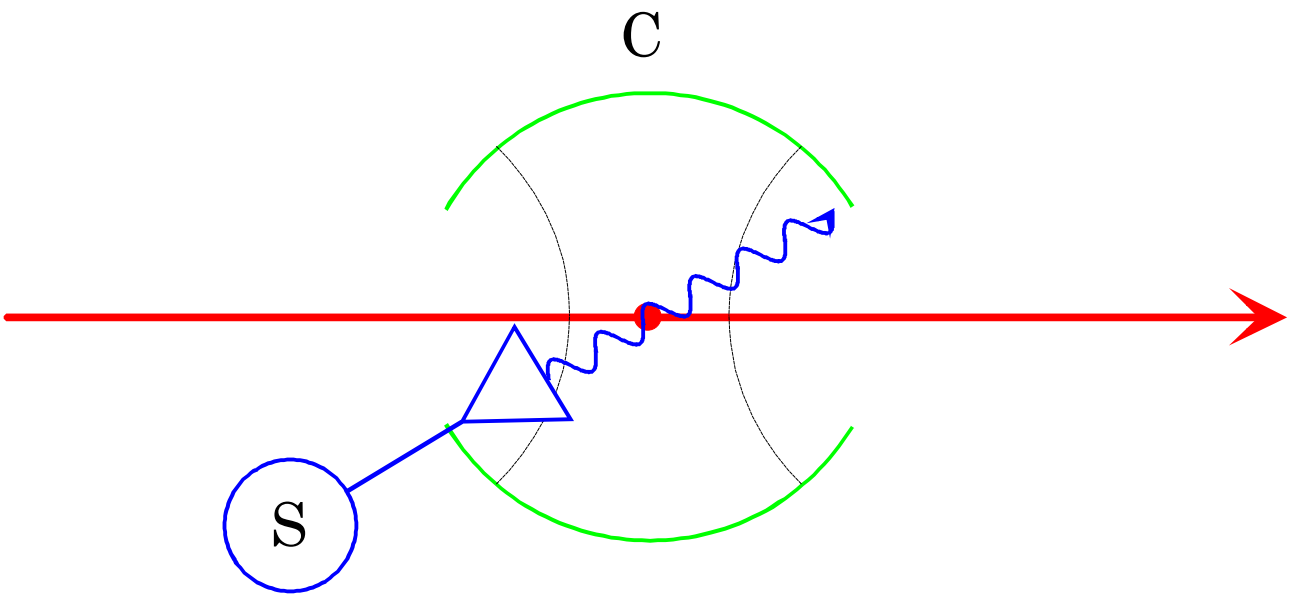
Tous les ingrédients d'une dynamique conditionnelle.

Exemple: dynamique de l'atome dépendant du champ dans la cavité



L'état final de l'atome dépend du champ: presque tous les ingrédients d'un CNOT....

Principe d'une porte logique universelle



Cavité contient un photon

Source S accordée avec la transition atomique

Réalise une rotation arbitraire du qubit

(en ajustant amplitude et phase)

Cavité vide

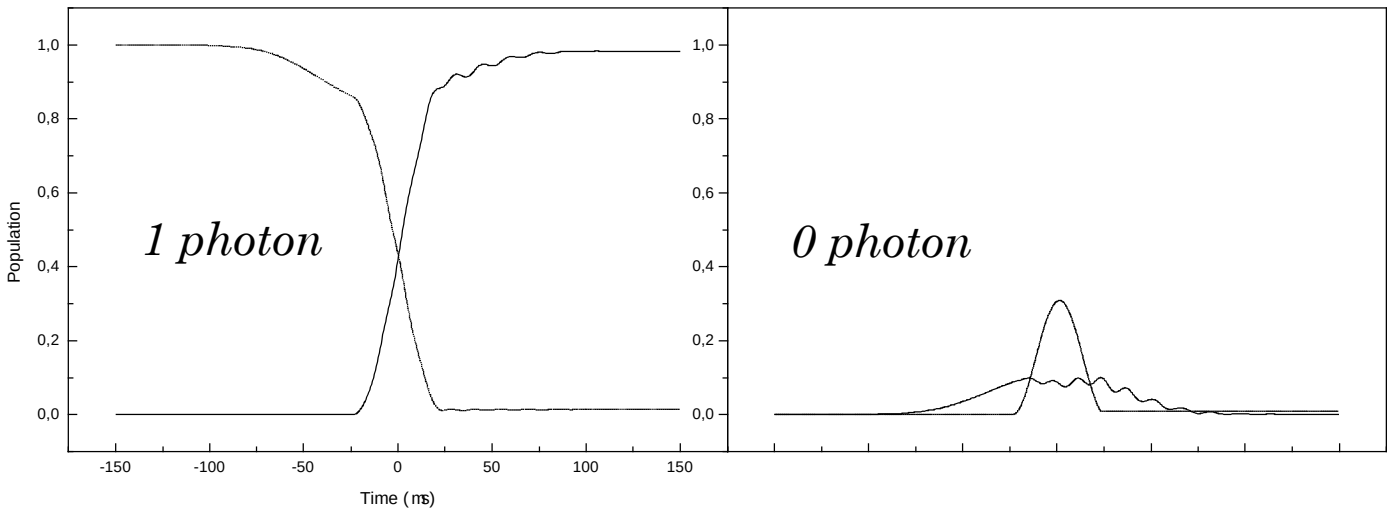
Source S hors de résonance

Le qubit atomique n'évolue pas

Dynamique conditionnelle arbitraire:

Porte logique universelle

Simulation numérique



Déjà réalisé avec des atomes et des cavités:

Mémoire quantique

*Maître et al PRL, **79**, 769*

Intrication quantique contrôlée de deux atomes

Préparation d'une paire EPR

*Hagley et al. PRL **79**, 1* $\frac{1}{\sqrt{2}}\left(|e,g\rangle - |g,e\rangle\right)$

Equivalent à une porte.

Perspectives à moyen terme (dans ce domaine)

Intrication de trois atomes (triplet GHZ) ou 4

Tests de la non-localité quantique

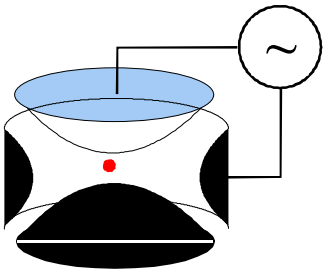
Porte

Difficultés

Temps d'acquisition exponentiel / nombre d'atomes

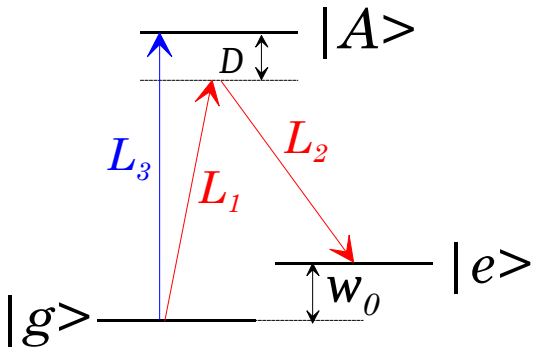
Facteur de qualité des cavités

Ions piégés



Ion unique piégé dans un champ quadrupolaire alternatif

Piège harmonique. Fréquence d'oscillation W qq MHz



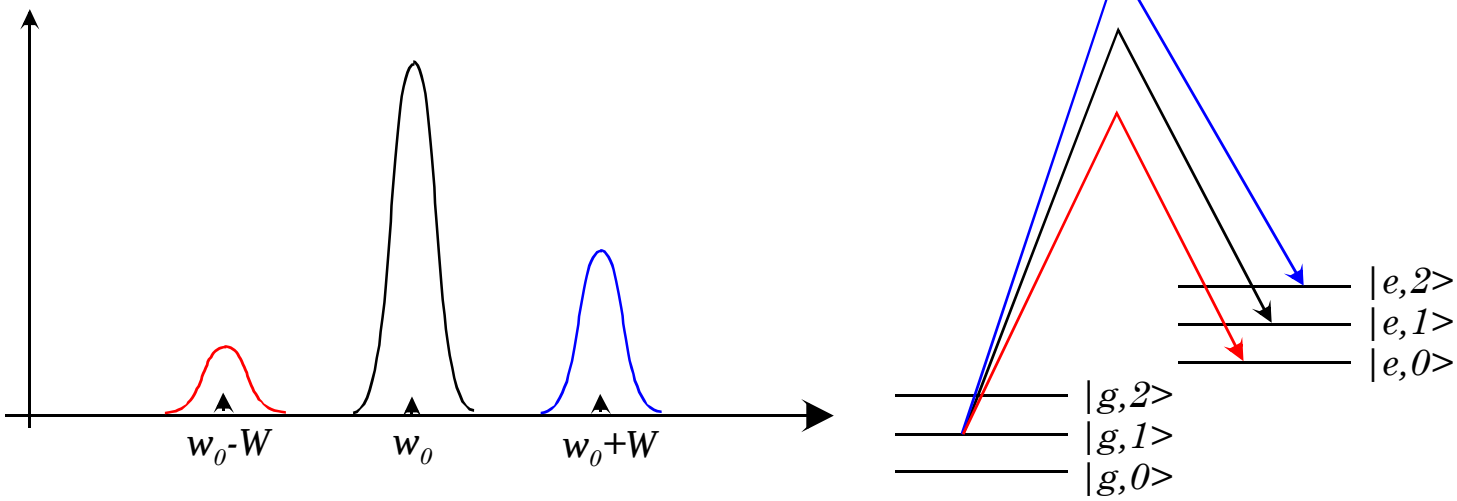
Structure hyperfine de l'ion: qubit de grande duré de vie

Refroidissement Doppler: quelques quanta de vibration

Transition Raman entre niveaux (L1 et L2):
haute résolution

Détection par fluorescence (L3) efficacité 100%

Spectre de la transition Raman



Transitions de g,n vers e,n porteuse
de g,n vers e,n-1 bande latérale rouge
de g,n vers e,n+1 bande latérale bleue

Refroidissement jusqu'au fondamental de vibration

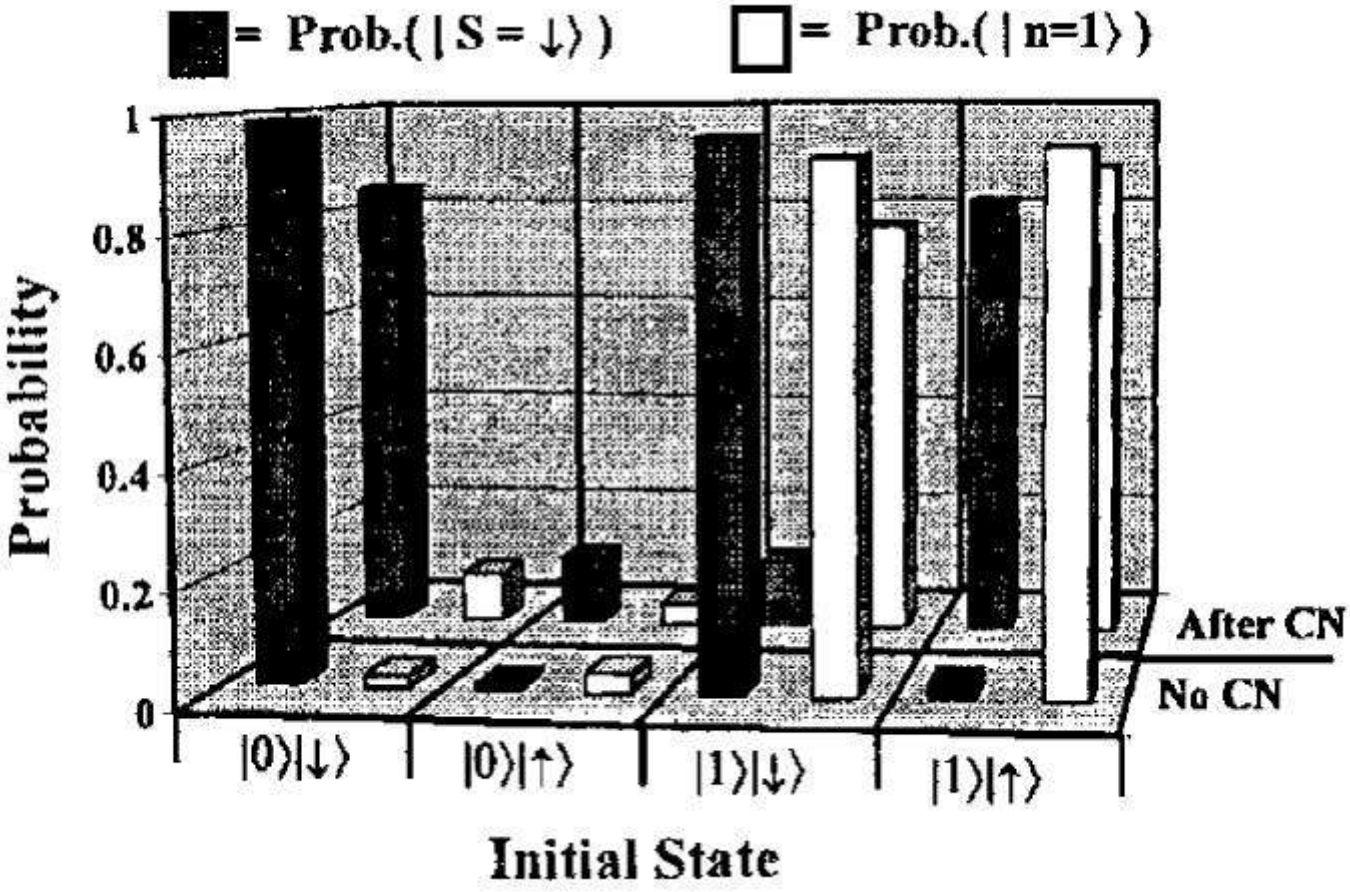
Analogie avec les atomes en cavité

Dynamique conditionnelle

Bande "rouge" g,1 couplé à e,0
mais g,0 n'est couplé à rien:

dynamique de l'état interne de l'ion conditionnée au nombre de phonons.

Elément d'une porte CNOT.
*Réalisée en 1995 par Monroe et al (PRL **75**, 4714)*



Résonance magnétique nucléaire

Spin nucléaire 1/2 dans un champ magnétique:

système à deux niveaux de grande durée de vie (mn)
manipulable par des champs radiofréquence
qubit idéal

Déplacements chimiques dans une molécule

fréquence de la transition dépend de la position dans la molécule
adressage individuel des spins

Couplage entre spins

interaction d'échange
la fréquence de transition pour un spin dépend de l'orientation des voisins
clé de la dynamique conditionnelle

Détection

capte les champs magnétiques produits par les spins en précession
le spectre du signal pour un spin donné révèle l'orientation des voisins

Deux difficultés

Echantillon macroscopique à haute température

populations pratiquement égales entre les deux niveaux
(écart à l'équilibre de l'ordre de 10^{-6})

Seul l'écart à l'équilibre contribue à la détection.

Au prix de quelques manipulations:
tout se passe comme si on avait un cas pur

Accès seulement à des valeurs moyennes

Pas de systèmes quantiques uniques

Pas d'utilisation directe du postulat de la mesure:
pas d'algorithme de Shor

Un avantage énorme:

Utilise des appareils commerciaux développés pour la RMN analytique (et les chimistes qui vont avec)

Déjà réalisé

Intrication de trois spins (Laflamme et al.)

Algorithme de Deutsch Josza à un bit (Jones et al.)
le résultat est donné par une valeur moyenne

Code correcteur d'erreur à trois bits (Cory et al.)

Sans doute la technique la plus avancée sur le plan ***pratique***

Perspectives

Quelques jeux supplémentaires avec 4 ou 5 spins

Limitations

Impossibilité de dépasser quelques spins

complexité croissante du spectre

décroissance exponentielle du signal "utile" avec le nombre de spins dans la molécule

Pas de mesure quantique au sens propre

D'autres propositions

Electrodynamique en cavité dans le domaine optique

Atomes froids piégés

Spins nucléaires dans des cristaux à basse température

Points quantiques

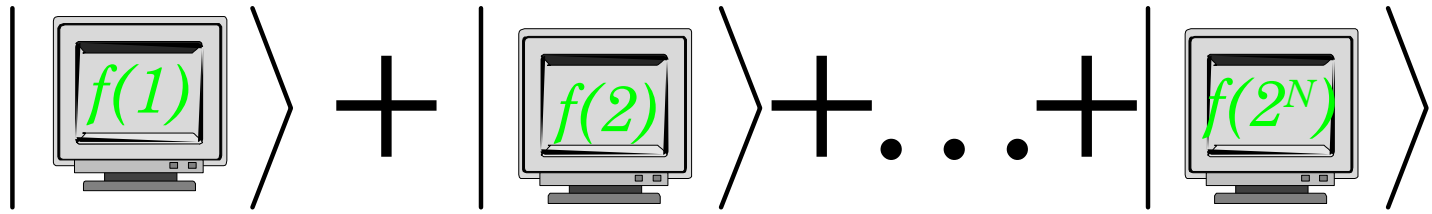
Iles quantiques supraconductrices

Aucune ne semble proposer d'avantages définitifs

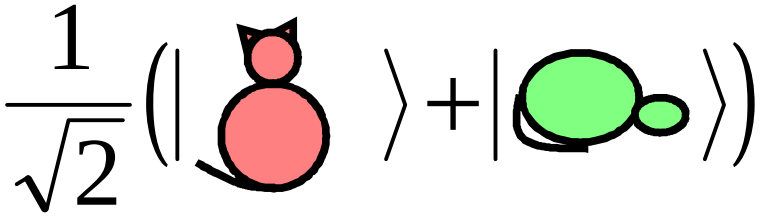
La technique la plus prometteuse et la plus flexible est sans doute celle des ions piégés.

Sommes nous en route vers un quantium?
oui, s'il n'y avait la...

La décohérence



est très similaire au chat de Schrödinger



Superpositions quantiques macroscopiques.

Pourquoi ne les observe-t-on pas ?

extrêmement sensibles au bruit, au couplage avec l'environnement

La durée de vie d'une superposition quantique est inversement proportionnelle à sa taille.

Très court pour un chat, assez court pour un calculateur.

Une approche simple

$e^{-\Gamma t}$ *probabilité de garder un qubit intact*

$e^{-n\Gamma t}$ *probabilité de garder la cohérence d'un registre de n qubits*

Le taux d'erreur d'un calculateur quantique est une fonction exponentielle de sa taille.

Le temps nécessaire pour obtenir un résultat exact est une fonction exponentielle de la taille du calcul.....

Facteur de qualité

Algorithme quantique

n qubits

N_{op} opérations logiques élémentaires

T_{op} durée d'une opération

$G=1/T_{rel}$ taux de relaxation d'un qubit

Probabilité de succès $e^{-nN_{op}T_{op}/T_{rel}} = e^{-nN_{op}/Q}$

Facteur de qualité $Q=T_{rel}/T_{op}$

nombre d'opérations avant relaxation

Quelques chiffres

	T_{op}	T_{rel}	Q
Atomes de Rydberg	*10 µs*	*1ms fait* *10 ms faisable*	*100* *1000*
Ions piégés	*100 µs*	*1ms fait* *1s faisable*	*10* *10 000*
RMN	*10 ms*	*qq s*	*1000*

Limite pratique actuelle aux environs de 10 000

Algorithme de Shor pour p bits

$n=5p$

$N_{op}= 300\ p^3$

Permet de factoriser un nombre de 2 bits: 4=2x2.....

Limites pratiques et fondamentales

Q=10 000 limite pratique envisageable

Il existe hélas aussi des limites fondamentales

necessité d'agir sur les qubits:

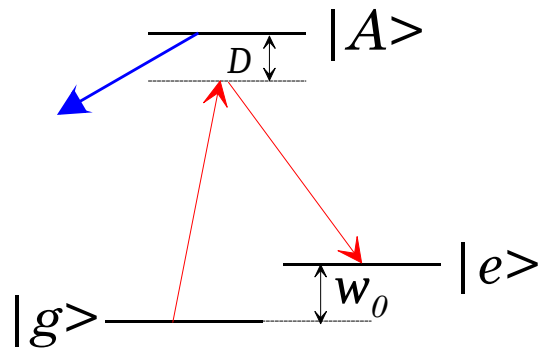
bruit quantique sur le canal de contrôle

Exemple piège à ions

Si toutes les causes de relaxation sont éliminées, il reste

l'émission spontanée des niveaux excités

W_r fréquence de Rabi des transitions à un photon de g ou e vers A



$1/T_{op}$ est de l'ordre de W_r^2/D

Population de A de l'ordre de W_r^2/D^2

Si g est le taux d'émission spontanée depuis A, le taux de relaxation du qubit est gW_r^2/D^2.

Facteur de qualité:

$$Q=D/g.$$

Au mieux, D est de l'ordre de la fréquence optique.

Le facteur de qualité est au plus celui d'une transition atomique permise:

$$Q<a^3$$

a: constante de structure fine.

La limite fondamentale est aux environs de 10^6

Codes correcteurs d'erreur

Combattre la décohérence comme on combat les erreurs d'un ordinateur classique.

n bits codés dans n+p. Les p bits supplémentaires indiquent s'il se produit une erreur (syndrome) et les moyens de la corriger.

Redoutablement efficace avec des signaux classiques

Schéma général des codes quantiques

encodage	*n bits dans n+p*
évolution	*et erreurs*
décodage	*extraction des p bits supplémentaires*
extraction	*du syndrome lecture de p bits:*
correction	*des n bits: opération unitaire*

Exemple simple (réalisé expérimentalement en RMN)

Erreurs de phase à 1 bit (variation des nx d'énergie)

$$|b\rangle \longrightarrow e^{-i\Theta s_z}|b\rangle = e^{-i\Theta(-1)^b}|b\rangle$$

En s'accumulant, ces erreurs transforment un état quelconque en mélange statistique (populations constantes)

Pour trois bits (si les erreurs sont indépendantes

$$|b_1,b_2,b_3\rangle \longrightarrow e^{-i\left(\Theta_1 s_z^1+\Theta_2 s_z^2+\Theta_3 s_z^3\right)}|b_1,b_2,b_3\rangle$$

En posant,

$$|\pm\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right), \quad s_z|\pm\rangle = \pm|\mp\rangle$$

1 bit à protéger, état initial $a|0\rangle + b|1\rangle$
2 bits de contrôle, à zéro

Etat initial $a|0,0,0\rangle + b|1,0,0\rangle$

Codage

CNOT de 1 sur 2 $a|0,0,0\rangle + b|1,1,0\rangle$

CNOT de 1 sur 3 $a|0,0,0\rangle + b|1,1,1\rangle$ *(Triplet GHZ)*

Rotation de 90° $|\Psi\rangle = a|+,+,+\rangle + b|-,-,-\rangle$

Evolution et erreurs
au premier ordre en Q

$$|\Psi\rangle \longrightarrow |\Psi\rangle - i\Theta_1\left(a|-,+,+\rangle + b|+,-,-\rangle\right) - i\Theta_2\left(a|+,-,+\rangle + b|-,+,-\rangle\right) - i\Theta_3\left(a|+,+,-\rangle + b|-,-,+\rangle\right)$$

Décodage

Rotation de 90° $\left(a|0\rangle + b|1\rangle\right)|0,0\rangle$
CNOT de 1 sur 3 $-i\Theta_1\left(a|1\rangle + b|0\rangle\right)|1,1\rangle$
CNOT de 1 sur 2 $-i\Theta_2\left(a|0\rangle + b|1\rangle\right)|1,0\rangle$
$-i\Theta_3\left(a|0\rangle + b|1\rangle\right)|0,1\rangle$

Syndrome

Mesure des deux derniers bits
Donnent le numéro du bit ayant subi l'erreur
Erreur sur le premier bit s'ils sont tous deux à 1
Erreur sur les bits de contrôle si un seul est à un
Pas d'erreur si tous deux à zéro

Correction

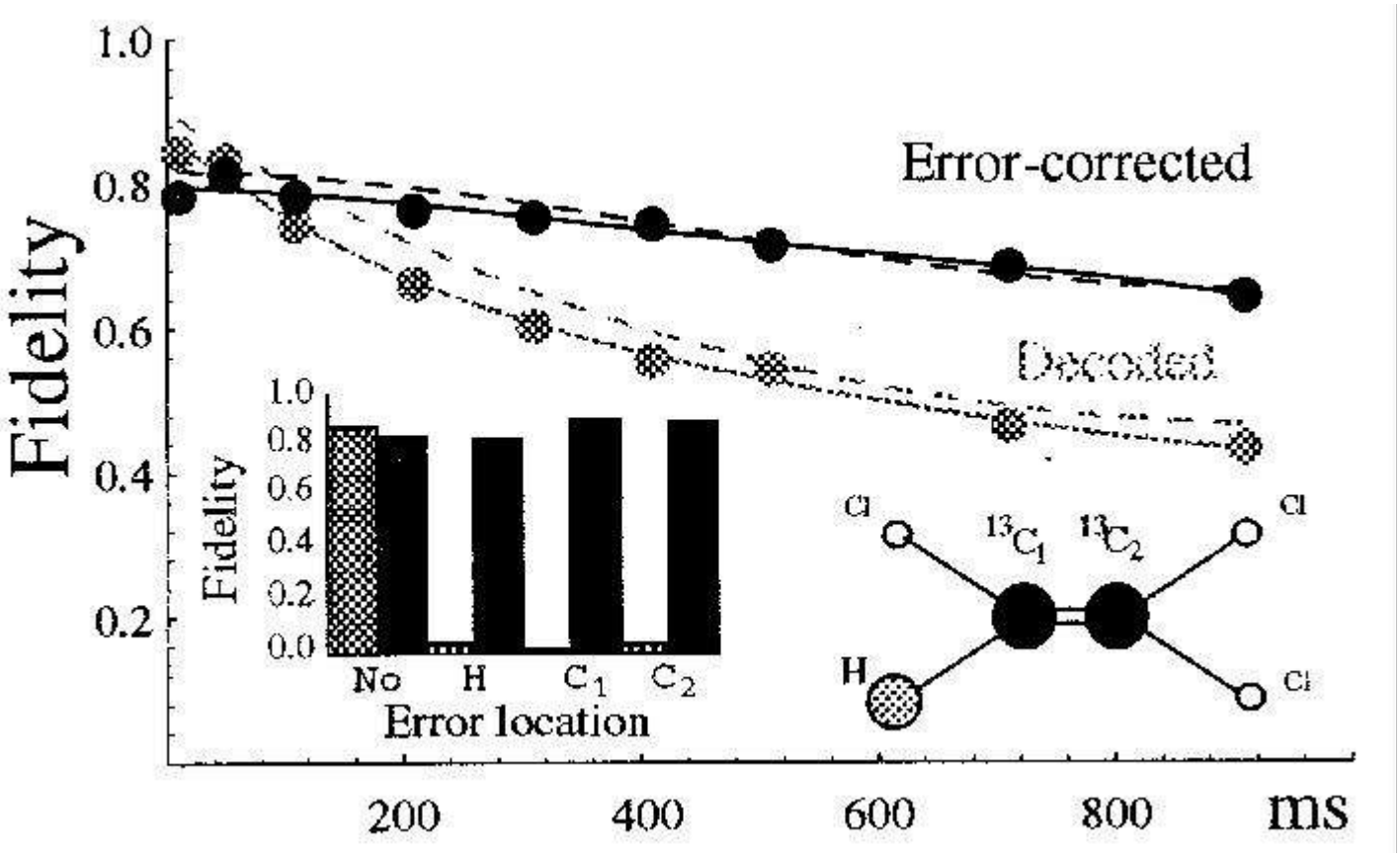
Deux bits à un: échange de 1 et 0 sur le qubit
(double CNOT ou Toffoli)

Restauration de l'état initial....

Réalisation expérimentale en RMN

bruit artificiel: manipulations du champ magnétique

Cory et al PRL, 81, 2152



Correction des erreurs au premier ordre:
le taux d'erreurs est une fonction quadratique du temps

remarquable, mais ne compense qu'un type d'erreurs au premier ordre

Est-ce l'issue?

Pour corriger toutes les erreurs à tous les ordres:

codage sur un nombre suffisant de qubits

taux d'erreur maximal sur

l'opération d'une porte

la mémorisation d'un qubit

code optimal (A. Steane, preprint)

Pour la factorisation d'un nombre de 130 chiffres (i.e. 430 qubits)

22 qubits par bit

Taux d'erreur par porte $2\ 10^{-5}$

Taux d'erreur par mémoire $2\ 10^{-6}$

Rend le circuit logique beaucoup plus complexe

(les expériences sont encore loin de manipuler 22 qubits, i.e. un seul qubit corrigé)

Taux d'erreur limite redoutablement proche de la limite fondamentale

taux d'erreur actuels quelques %

La valeur limite du taux d'erreur décroit avec la taille du problème

Enormes difficultés. Risque fort de ne pas être réalisable avec les techniques actuelles

Les concurrents de l'ordinateur quantique

Ordinateur à ADN

utiliser les techniques de génie génétique
10^{23} calculateurs dans une éprouvette
réalisé pour le problème du voyageur (7 sites)
programmation et algorithmique difficiles

Des perles

PRL 81, 2156: un système dynamique classique, chaotique, bistable peut calculer.....
50 ans après le transistor

Et le silicium

Los Alamos 200 TéraFlops en 2005
1 minute pour factoriser 130 chiffres
1 mois pour factoriser 600 chiffres

Calcul dilué (internet)
10^{8} processeurs à 10^{8} Flops
10^{16} instructions par seconde

On aura probablement à revoir les systèmes cryptographiques dans un proche avenir, mais pas à cause des ordinateurs quantiques

Réalités:

Très belle illustration des principes de la mécanique quantique

Utile pour la théorie de la complexité
(nouvelle classe de machines)

Application à échelle utile très peu probable
dans l'état actuel de la technologie
Manque d'algorithmes
Impossible sans correction d'erreurs
Terrible complexité des codes correcteurs

Comme Babbage, nous avons l'idée mais il nous manque le transistor

Mais:

Langage commode
pour décrire les opérations quantiques et les systèmes intriqués

Nouveaux tests
des processus fondamentaux de la mécanique quantique

Applications possibles
pour des petits nombres de qubits

Communication quantique
Cryptographie quantique (paires EPR)
Purification d'intrication