Bertrand Georgeot

Ordinateur quantique et algorithmique

groupe chaos et cohérence quantiques
Laboratoire de Physique Théorique, IRSAMC, UMR 5152 du CNRS
Université Paul Sabatier, Toulouse

Information quantique

- Nouvelle manière de traiter l'information, utilisant les propriétés de la mécanique quantique.
- Ceci n'est pas lié à un système particulier: tout système quantique possédant quelques propriétés spécifiques peut être choisi $\Longrightarrow$ de nombreuses implémentations expérimentales différentes sont possibles
- Applications: cryptographie quantique, téléportation...
- Machine quantique générale polyvalente: ordinateur quantique

Une brève idée du calcul quantique...

- Un ordinateur quantique n'est pas seulement plus rapide qu'un ordinateur classique, il représente quelque chose d'autre: nouvelle informatique, avec de nouvelles propriétés $\Rightarrow$ peut changer la classe de complexité des problèmes
- L'efficacité du calcul quantique comparé au calcul classique dépend du problème: pour bénéficier de la puissance du calcul quantique, on doit poser certains types de questions.
- Peut être réalisé au moyen de nombreux systèmes physiques différents
- Mais: beaucoup plus sensible au bruit qu'un ordinateur classique $\Rightarrow$ énorme défi expérimental, mais aucune raison physique n'interdit sa réalisation.
- Applications importantes: décryptage, simulation de systèmes physiques

Pourquoi un ordinateur quantique?

- Processeurs de plus en plus petits sur les ordinateurs classiques $\Rightarrow$ les échelles quantiques seront atteintes à un moment
- plus facile de simuler la mécanique quantique sur un ordinateur quantique (Feynman)
- gain massif de temps de calcul sur certains problèmes non quantiques (Shor, Grover)
- donne un nouveau point de vue sur la mécanique quantique

Eléments de base

$\Longrightarrow$ ordinateur classique: éléments de base: bits 0 ou 1

Mécanique quantique: le système est décrit par une fonction d'onde, vecteur dans un espace de hilbert, noté $|\psi\rangle$; les projections sur une base notées $|\langle i|\psi\rangle|^2$ donnent la probabilité de i

$\Longrightarrow$ ordinateur quantique: éléments de base: qubits: systèmes à deux niveaux $|0\rangle$ et $|1\rangle$ (espace vectoriel de dimension deux, de base $|0\rangle$ et $|1\rangle$)

Tout état de la forme $(\alpha|0\rangle + \beta|1\rangle)$ est possible, mais une mesure quantique fournit seulement une valeur (avec probabilités $|\alpha|^2$ et $|\beta|^2$).

Deux qubits pris ensemble: espace de dimension 4, base: $|00\rangle$ $|10\rangle$, $|01\rangle$ et $|11\rangle$

Trois qubits pris ensemble: espace de dimension 8, base: $|000\rangle$ $|001\rangle$, $|010\rangle$, $|011\rangle$ $|100\rangle$, $|101\rangle$, $|110\rangle$ et $|111\rangle$

Ordinateur quantique

- Un ordinateur quantique peut être vu comme un ensemble de n qubits (espace de Hilbert de dimension $N = 2^n$). Etat quantique de l'ordinateur: $\sum_{i=0}^{N-1} a_i |i\rangle$ avec $\sum_{i=0}^{N-1} |a_i|^2 = 1$.
- Un état quantique est donc une somme sur 2^n registres chacun correspondant à un nombre entre 0 et $2^n - 1$ notés en base deux, de 000...0 à 111....1
- La puissance du calcul quantique ne vient pas du caractère continu des valeurs de a_i. L'ordinateur quantique est effectivement digital.
- Opérations logiques: transformations unitaires dans l'espace de Hilbert $\Rightarrow$ calcul réversible, pas de dissipation ($\neq$ calcul classique). La seule source d'irréversibilité correspond aux mesures quantiques.
- Théorie de l'information quantique: $\Rightarrow$ L'information contenue dans un état quantique peut se mesurer en unités de qubits

Instructions élémentaires: Portes quantiques

On agit sur la fonction d'onde de l'ordinateur quantique par des transformations unitaires. En pratique, on utilise des portes quantiques élémentaires qui sont locales et on les compose pour construire l'évolution unitaire voulue.

- **porte d'Hadamard**: s'applique à un qubit $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$; $|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$
- **porte de phase** s'appliquant à un qubit $|0\rangle \rightarrow |0\rangle$; $|1\rangle \rightarrow i|1\rangle$
- **controlled not** ou **CNOT** s'appliquant à deux qubits: $|00\rangle \rightarrow |00\rangle$; $|01\rangle \rightarrow |01\rangle$;$|10\rangle \rightarrow |11\rangle$; $|11\rangle \rightarrow |10\rangle$; le deuxième qubit est inversé si le premier est dans l'état $|1\rangle$
- **controlled controlled not** ou **porte de Toffoli** s'appliquant à trois qubits: le troisième qubit est inversé si les deux premiers sont dans l'état $|1\rangle$.

Certains ensembles dits universels de portes quantiques suffisent pour construire toutes les transformations unitaires (par exemple CNOT combiné aux transformations à un qubit).
Différents ensembles universels de portes sont possibles, leur choix dépend de l'implémentation expérimentale.

Superposition quantique

PRINCIPE DE SUPERPOSITION : $\Rightarrow$ Possibilité de manipuler plusieurs registres en même temps

n qubits $\Rightarrow N = 2^n$ états tels que $|00100...\rangle$

Etats quantiques: de la forme $\Sigma_{i=0}^{N-1} a_i |i\rangle$; l'information est contenue dans les amplitudes a_i associées aux registres.

Pour agir sur N amplitudes:

- Classique: N opérations nécessaires
- Quantique: possible en 1 opération

$\rightarrow$ Gain exponentiel (en temps de calcul) possible

Intrication quantique

Les qubits peuvent présenter des corrélations impossibles à obtenir classiquement (cf théorème de Bell)

- L'intrication d'un état quantique décrit son degré de non-factorisabilité en produits d'états à un qubit.
- Exemple: paradoxe d'Einstein-Podolsky-Rosen; mesurer un qubit de l'état $(|01\rangle - |10\rangle)/\sqrt{2}$ influence l'autre qubit, quelle que soit leur distance.
- L'intrication peut être quantifiée (bien qu'il y ait plusieurs manière de le faire). Elle est cruciale pour, par exemple, la téléportation quantique.
- L'intrication est considérée comme une ressource essentielle pour le calcul quantique, mais on ne sait pas exactement comment.

Interférence quantique

- Les états quantiques peuvent interférer entre eux.
- En particulier, on peut produire des interférences destructrices ou constructrices entre différents chemins computationnels
- Les algorithmes quantiques présentent souvent une succession de phases créant de l'interférence et créant de l'intrication.

Algorithmes classiques

- Modifient des chaînes de bits 0 et 1 par des transformations parfois irréversibles ($\Rightarrow$ dissipation, production de chaleur)
- Input: chaîne de N bits
- Modifie l'input en M opérations $\Rightarrow$ complexité
  M polynômial en N $\Rightarrow$ algorithme polynômial (classe de complexité P)
  (exemple: opérations arithmétiques,...)
  M exponentiel en N $\Rightarrow$ algorithme exponentiel (exemple: factoriser, voyageur de commerce,...)
- Problème du millénaire: $P = NP$
- Résultat d'informatique classique: la classe de complexité ne dépend pas de l'appareil qui effectue le calcul

Algorithmes quantiques

n qubits $\Rightarrow N = 2^n$ états d'une base quantiques tels que $|011001...\rangle$
Procédure pour réaliser un algorithme:

- Construire un état initial $|\Psi_i\rangle = \sum_{i=0}^{N-1} a_i |i\rangle$. Exemple: $1/\sqrt{N} \sum_{i=0}^{N-1} |i\rangle$ (superposition uniforme) peut être produit à partir de $|00..00\rangle$ par l'application de n portes d'Hadamard.
- Transformer cet état $|\Psi_i\rangle \rightarrow |\Psi_f\rangle = \sum_{i=0}^{N-1} b_i |i\rangle$ par une suite de portes quantiques élémentaires (locales)
- Extraire de l'information par des mesures quantiques de $|\Psi_f\rangle$

Le résultat est d'habitude probabiliste: la mesure quantique donne le bon résultat avec une certaine probabilité. L'algorithme est correct si 1) on peut reconnaître le bon résultat et 2) la probabilité de succès est significative (particulièrement quand n augmente).
La complexité de l'algorithme est mesurée par le nombre de portes quantiques nécessaires, en prenant en compte que le processus peut devoir être itéré puisque le résultat est probabiliste.

Exemple de routine quantique: addition d'entiers

But: ajouter tous les entiers entre 0 et N-1=2^n-1; nécessite 3 registres de n, n+1 et n-1 qubits

- Partir de $|000...000\rangle$
- Appliquer $2n$ portes d'Hadamard $\Rightarrow 1/N \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} |i\rangle|j\rangle|0...000\rangle$
- Appliquer une suite de CNOT (addition mod 2 de bits) et de portes de Toffoli (qui mettent les retenues sur le troisième registre), mettre le bit le plus significatif de la somme sur le deuxième registre, puis inverser la suite de portes pour effacer le troisième registre tout en mettant la somme sur le deuxième registre.
- Le résultat est $1/N \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} |i\rangle|i+j\rangle|0...000\rangle$

$\rightarrow$ Nécessite seulement $\approx 8n$ portes quantiques pour effectuer N^2 additions $\rightarrow$ Le troisième registre (workspace) est remis à zéro à la fin $\rightarrow$ Tout est réversible $\rightarrow$ Multiplications et exponentiations peuvent être effectuées de la même manière, en utilisant la décomposition en base deux $\Rightarrow$ nombre de portes quantiques $\sim n^2$ (multiplication) et $\sim n^3$ (exponentiation).

Addition quantique

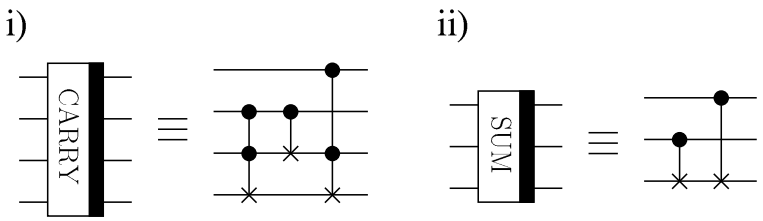
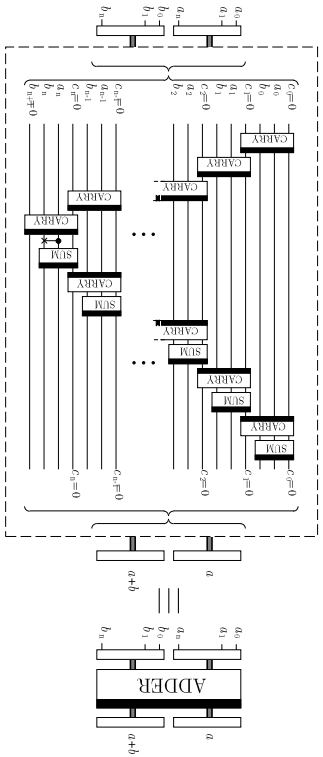


Figure 3)

V. Vedral, A. Barenco and A. Ekert

Figure 2)

V. Vedral, A. Barenco and A. Ekert



Multiplication et exponentiation quantiques

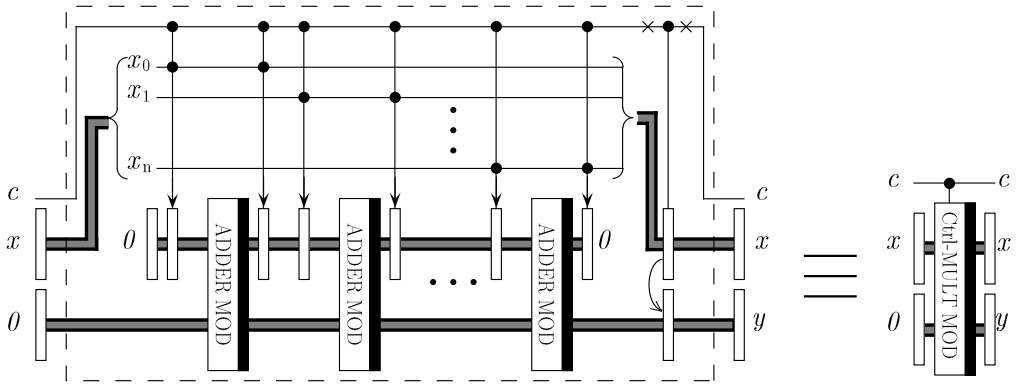


Figure 5)

V. Vedral, A. Barenco and A. Ekert

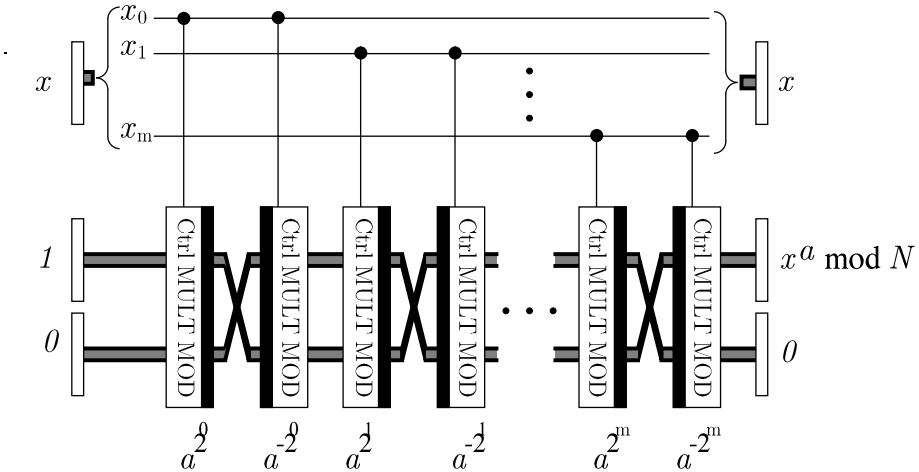


Figure 6)

V. Vedral, A. Barenco and A. Ekert

Transformée de Fourier quantique

Utilise n qubits pour transformer un vecteur de taille 2^n par:

$\sum_{k=0}^{2^n-1} a_k |k\rangle \longrightarrow \sum_{l=0}^{2^n-1} (\sum_{k=0}^{2^n-1} e^{2\pi i k l/2^n} a_k)|l\rangle = \sum_{l=0}^{2^n-1} \tilde{a}_l |l\rangle$.

Peut être décomposée au moyen des transformations élémentaires:

- H_j : porte d'Hadamard appliquée au qubit j
- B_{jk}: porte à deux qubits appliquée aux qubits j et k, caractérisée par $|00\rangle \rightarrow |00\rangle$; $|01\rangle \rightarrow |01\rangle$;$|10\rangle \rightarrow |10\rangle$; $|11\rangle \rightarrow \exp(i\pi/2^{k-j})|11\rangle$).

On peut vérifier que la suite: $\Pi_{j=1}^{n}[(\Pi_{k=j+1}^{n} B_{jk})H_j]$
effectue la transformée de Fourier d'un vecteur de taille 2^n en $n(n+1)/2$ opérations.
A comparer avec $\sim N \log N$ pour la transformée de Fourier rapide classique!

Période d'une fonction

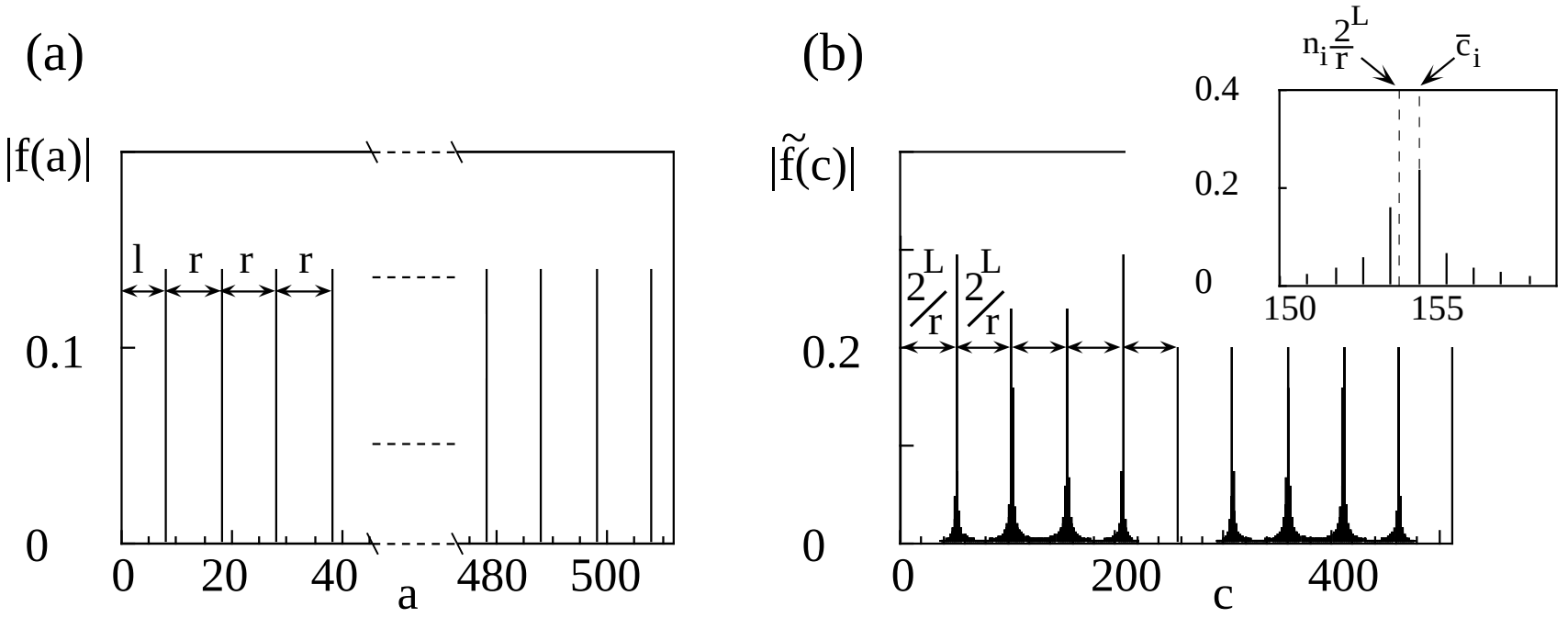
Simon (1994), Shor (1994)

f fonction sur Z périodique de période r: $f(x) = f(x+r)$, où $r < N$

Deux registres a et b avec $\sim 2 \log N$ qubits chacun

- Construire l'état $2^{-n/2} \Sigma_{x=0}^{2^n-1} |x\rangle|0\rangle$
- Transformer cet état en $2^{-n/2} \Sigma_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$
- Mesurer le registre b. Résultat: $|u\rangle$. Etat après la mesure: $M^{-1/2} \Sigma_{j=0}^{M-1} |x_j\rangle|u\rangle$ où les x_j sont tous les x tels que $f(x_j) = u$, et $M \approx 2^n/r$.
- Appliquer une transformée de Fourier, et mesurer le registre a $\Rightarrow$ multiple de $M \approx 2^n/r$.

Période d'une fonction



Tiré de Barenco et al., Phys Rev A **54**, 139 (1996)

Factorisation des grands nombres

Algorithme de Shor (1994): factorise N en facteurs premiers

- Choisir $a < N$ aléatoirement
- Trouver la période r de $f(x) = a^x \bmod(N)$
- Pour la plupart des a, r est pair et $a^{r/2} \pm 1$ possède un facteur commun avec N, qui peut être trouvé rapidement.

avantages:
$\Rightarrow$ Requière $\sim 300(\log N)^3$ opérations logiques (classiquement $\sim \exp(2(\log N)^{1/3}(\log \ln N)^{2/3})$)
$\Rightarrow$ limite actuelle avec des ordinateurs classiques: $N \sim 10^{130}$ $\Rightarrow \sim 2 \times 10^{10}$ opérations avec ~ 1000 qubits. Pour $N \sim 10^{260}$ $\Rightarrow$ $\times 10^7$ classiquement mais $\times 8$ quantiquement!
$\Rightarrow$ L'ordinateur quantique peut changer la classe de complexité!

Algorithme de recherche de Grover

But: étant donnée une liste de N données i sans structure, en trouver une particulière $i = j$
Classiquement: meilleure solution: parcourir la liste $\Rightarrow \sim N/2$ en moyenne pour N données
Quantiquement: nécessite un opérateur S qui reconnaît $i = j$ ($S(|j\rangle = -|j\rangle)$ ("oracle")

- Construire $|\Psi_i\rangle = 1/\sqrt{N}\sum_{i=0}^{N-1}|i\rangle$ (superposition uniforme)
  $= \sin\theta_0|j\rangle + \cos\theta_0/\sqrt{N-1}\sum_{i\neq j}|i\rangle$ with $\sin\theta_0 = 1/\sqrt{N}$
- Appliquer $S \Rightarrow -\sin\theta_0|j\rangle + \cos\theta_0/\sqrt{N-1}\sum_{i\neq j}|i\rangle$
- Appliquer une transformée de Fourier + inverser tous les signes saufs celui de $|0\rangle$ + transformée de Fourier
- Résultat: $= \sin(\theta_0+\phi)|j\rangle + \cos(\theta_0+\phi)/\sqrt{N-1}\sum_{i\neq j}|i\rangle$
- Itérer $\approx \sqrt{N}$ fois $\Rightarrow \sin\theta \approx 1 \Rightarrow$ algorithme quantique $\sim \sqrt{N}$ (gain prouvé $\neq$ Shor).

peut être utilisé pour résoudre des problèmes où trouver des solutions est difficile, mais tester un candidat est facile

Applications cryptographiques

RSA: cryptographie à clef publique (équivalent à une boîte aux lettre)

$\longrightarrow$ fondée sur le fait que certaines opérations mathématiques sont asymétriques: multiplier deux nombres est facile, factoriser est difficile.

$\longrightarrow$ RSA utilise la direction facile pour coder; l'opération inverse difficile rend impossible le décodage par quelqu'un qui n'a pas la clef.

l'algorithme de Shor détruit RSA

l'algorithme de Grover peut aussi être utilisé en cryptographie (recherche de clefs).

Remarque: la cryptographie quantique est une alternative à la cryptographie classique.

Simulation de systèmes physiques quantiques

- De nombreux problèmes de mécanique quantique requièrent de larges espaces de Hilbert
- Exemples: systèmes à plusieurs corps (n particules, m orbitales $\Rightarrow m^n$ états), limite semiclassique...
- Feynman (1982): Utiliser des systèmes quantiques pour simuler la mécanique quantique
- Lloyd (1996): Algorithme quantique pour simuler des systèmes à plusieurs corps avec interactions locales.

Applications quantiques: exemple de simulation quantique

(B. G. and D. Shepelyansky, Phys. Rev. Lett. **86**, 2890 (2001))
$\hat{U} = e^{-2i\pi\hat{p}^2/N} e^{2i\pi\alpha\hat{q}}$ sur une fonction d'onde de dimension N, $N = 2^n$. Requiert n qubits.

- En représentation q : $e^{2i\pi\alpha\hat{q}}$ est diagonal. $q = \sum_{j=0}^{n-1} q_j 2^j$ (décomposition binaire) $\Rightarrow$ $\exp(2i\pi\alpha\hat{q})$ correspond à l'application des n portes à un qubit $|0\rangle \rightarrow |0\rangle$, $|1\rangle \rightarrow \exp(2i\pi\alpha 2^j)|1\rangle$.
- Transformée de Fourier quantique $\Rightarrow$ fait passer de la représentation q à la représentation p, au moyen de $n(n+1)/2$ portes.
- En représentation p, le second opérateur $e^{-2i\pi\hat{p}^2/N}$ est diagonal. $p = \sum_{j=0}^{n-1} p_j 2^j$ $\Rightarrow$ $\exp(-2i\pi p^2/N) = \prod_{j_1,j_2} \exp(-2i\pi p_{j_1} p_{j_2} 2^{j_1+j_2}/N)$ $\Rightarrow n^2$ portes à deux qubits appliquées à toutes les paires de qubits (j_1, j_2), qui gardent les états $|00\rangle, |01\rangle, |10\rangle$ inchangés avec $|11\rangle \rightarrow \exp(-2i\pi 2^{j_1+j_2}/N)|11\rangle$.
- Transformée de Fourier quantique $\Rightarrow$ fait passer de la représentation p à la représentation q.

Au total, une itération requiert $2n^2 + 2n$ portes quantiques ($N \log N$ classiquement).

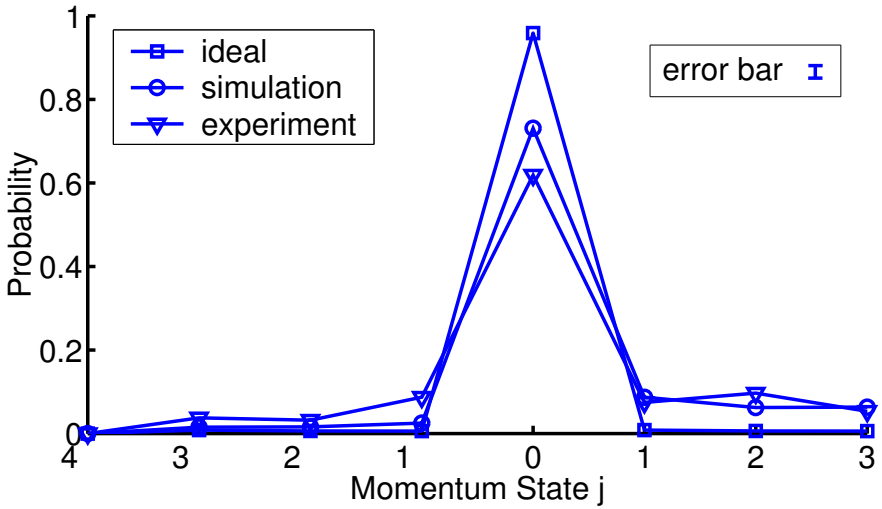
Extraction d'information

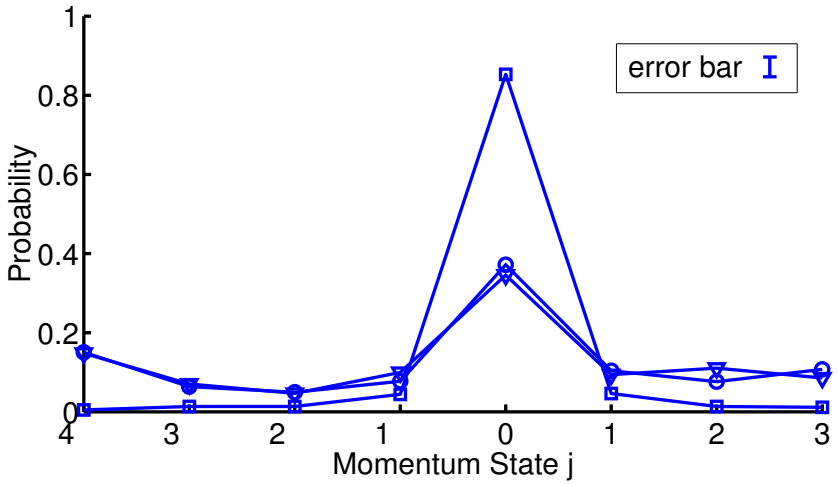
Une itération d'application quantique est exponentiellement rapide. Extraire de l'information peut demander de nombreuses mesures $\Rightarrow$ Efficacité totale de l'algorithme?

- Longueur de localisation (Benenti et al, 2003): Mesure directe de la fonction d'onde finale d'un système localisé $\rightarrow$ gain polynômial.
- Facteur de forme (D. Poulin et al, 2003): Utilise un circuit additionnel pour obtenir $\mathrm{Tr}U^n$, fournit les corrélations spectrales $\rightarrow$ gain polynômial.
- Décroissance de la fidélité (Emerson et al, 2002): Mesure la sensibilité aux perturbations du système quantique $\rightarrow$ possibilité de gain exponentiel.
- Spectre (Abrams and Lloyd, 1999): Mesure les valeurs propres par des versions de l'algorithme d'estimation de phase $\rightarrow$ possibilité de gain exponentiel.

  Fonction de Wigner (Miquel et al, 2002, Terraneo et al, 2004): Utilise un circuit additionnel et/ou une transformée de Fourier quantique pour obtenir les distributions de Wigner et Husimi $\rightarrow$ gain polynômial.

Réalisation expérimentale





Simulation d'une application quantique sur un ordinateur quantique à trois qubits (groupe de D. Cory, MIT, USA). La localisation de la fonction d'onde est visible, mais diffère du résultat idéal. Une simulation numérique incluant bruit et décohérence peut reproduire les données expérimentales. (M. K. Henry, J. Emerson, R. Martinez, D. Cory, Physical Review A **74**, 062317 (2006)).

Simulateurs quantiques

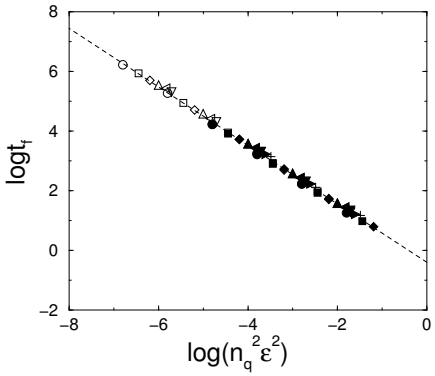
- Condensats de Bose-Einstein d'atomes froids dans des réseaux optiques
- Quand les paramètres du réseau sont changés, transition de phase quantique d'un superfluide vers un isolant de Mott (modèle de Bose-Hubbard) (observée par Greiner et al, Nature 2002).
- Ajouter des champs électriques et magnétiques et changer les paramètres du réseau optique $\Rightarrow$ Possibilité de simuler de nombreux Hamiltoniens différents à plusieurs corps, d'une manière contrôlable.

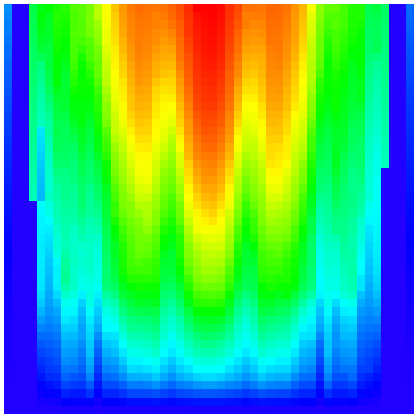
$\rightarrow$ "ordinateur quantique analogue": pas universel, mais plus facile à construire et utiliser qu'un ordinateur quantique polyvalent

$\rightarrow$ D'autres implémentations physiques sont possibles

Problème: décohérence

- Interaction avec l'environnement détruit la cohérence des états quantiques.
- La nécessité de manipuler ces états pour réaliser les portes quantiques complique encore plus le problème
- Les effets de décohérence dépendent de l'implémentation expérimentale
- Imperfections statiques: couplage résiduel entre qubits, fluctuations dans la différence en énergie des qubits. $\Rightarrow$ Chaos, "fusion" de l'ordinateur quantique (B.G. et D. Shepelyansky, 2000)
- Peuvent être unitaires ou non unitaires
- Les échelles de temps ne sont pas exponentiellement petites: peuvent être contrôlées en principe





Correction d'erreurs classique

Exemple : code de Hamming

$0000 \rightarrow 0000000$; $0001 \rightarrow 1010101$; $0010 \rightarrow 0110011$; $0011 \rightarrow 1100110$, etc...

4 bits $\rightarrow$ 7 bits; chaque encodage diffère de tous les autres en au moins trois endroits $\Rightarrow$ toute erreur sur un bit peut être corrigée

Shannon: en général, il est possible de corriger les erreurs dûes au bruit au prix de codes de plus en plus longs; le processus est plus efficace si on a des informations sur le type de bruit

Correction d'erreurs quantique

(Calderbank, Shor (1996), Steane(1996))

- Doit corriger à la fois les erreurs de bit et les erreurs de phase
- ajouter des registres supplémentaires qui évoluent en cohérence avec l'ordinateur quantique
- mesurer ces registres supplémentaires $\Rightarrow$ donne des informations sur l'opérateur de bruit M
- utiliser cette information pour appliquer M^{-1} à l'ordinateur
- les opérations supplémentaires produisent du bruit, mais le processus corrige plus de bruit qu'il n'en produit si l'intensité du bruit est au dessus d'un seuil de tolérance
- prix: augmente énormément le nombre de qubits pour lutter contre les niveaux usuels de bruit
- Introduit de l'irréversibilité, dissipation
- Les codes peuvent être adaptés à des types d'erreurs spécifiques (exemple: PAREC (Kern, Alber et Shepelyansky, 2004) pour les imperfections statiques)
- Développement récent: decoherence-free subspaces

Qu'est-ce donc qu'un ordinateur quantique?

Un ensemble de n qubits (espace de Hilbert de dimension 2^n) tel que (Steane 1997):

- Chaque qubit peut être préparé dans un état choisi $|0\rangle$
- Chaque qubit peut être mesuré dans la base $|0\rangle$, $|1\rangle$
- Des portes quantiques universelles peuvent être appliquées à des sous-ensembles de qubits
- Les qubits n'évoluent pas autrement que par ces transformations

Défi expérimental: Trouver des systèmes physiques à deux niveaux qui satisfont à ces critères

Ces systèmes doivent être protégés de l'environnement (longs temps de décohérence) mais faciles à manipuler $\Rightarrow$ exigences contradictoires

Point crucial: scalabilité

Réalisation 1: RMN (Gershenfeld et Chuang, 1997)

- qubits: spins nucléaires dans des molécules
- portes quantiques: champs magnétiques oscillants appliqués en impulsions de durée contrôlée; des centaines de portes peuvent être appliquées.
- avantage: utilise des techniques bien développées pour par exemple les applications médicales.
- problèmes: on mesure l'état moyen de spin d'un très grand nombre de molécules; le signal diminue exponentiellement avec le nombre de qubits; pas d'intrication globale.
- meilleur résultat: factoriser 15 avec 7 qubits (Vandersypen et al, 2001).

$\rightarrow$ Bon pour les démonstrations, mais probablement pas la bonne manière de construire un ordinateur quantique de grande taille.
$\rightarrow$ De loin la plus avancée actuellement.

Réalisation 2: piège à ions (Cirac, Zoller (1995))

- qubits: 2 états internes d'ions froids dans un piège à ions
- rotation d'un qubit: par impulsion laser
- portes à deux qubits: impulsion laser excitant le mouvement collectif quantifié des ions $\Rightarrow$ interaction Coulombienne nécessaire
- préparation: pompage optique et refroidissement laser
- mesure: lasers + détection de fluorescence
- problèmes: température: doit atteindre le microKelvin pour mettre les ions dans l'état fondamental
- Porte à deux qubits réalisée, téléportation, intrication de six ions (Boulder, Innsbruck)

Réalisation 3: jonctions Josephson

Deux ilôts supraconducteurs (condensats de Bose-Einstein de paires de Cooper) séparés par une couche mince isolante.

- qubits: différence de charge entre les deux ilôts (“charge qubit”) ou flux magnétique à travers un circuit supraconducteur (“flux qubit”).
- portes quantiques: couplage inductif entre circuits supraconducteurs
- avantages: taille mésoscopique; scalabilité possible en principe.
- Premier qubit en 1999 (Nakamura et al), puis premier qubit à longue durée de vie 2002 (Vion et al.). Couplage entre deux qubits et CNOT réalisés (Yamamoto et al, 2003).

Autres propositions

- Réseaux de spins (Privman, Vagner, Kventsel (1998), Kane (1998)) qubits: spins nucléaires; rotation d'un qubit, CNOT : contrôlées électroniquement par des potentiels de portes (champs électriques locaux) (l'interaction hyperfine couple électrons et spins nucléaires) $+$ un champ magnétique; mesure: courants d'électrons polarisés en spin; problèmes: extrême précision pour placer les atomes et pour les champs électriques; impuretés, etc...
- Réseaux optiques (Jaksch et al (1999), Brennen et al (1999), Sorensen and Molmer (1999)) qubits: états internes d'atomes; rotation d'un qubit: par impulsion laser; porte à deux qubits: deux réseaux optiques, l'un de $|0\rangle$, l'autre de $|1\rangle$, sont déplacés l'un par rapport à l'autre pour créer une interaction.
- Cavités optiques: couplage entre un atome ou un ion (qubit) et un mode du champ électromagnétique de la cavité (LKB Paris).
- Points quantiques: qubit: état de spin d'un point quantique à un électron; opérations effectuées par l'ajustement d'une barrière tunnel entre points voisins..

Quelle est la situation?

- Construction théorique des opérations logiques quantiques: machines de Turing quantiques.
- Théorie de l'information quantique.
- Des algorithmes spécifiques existent.
- Des codes correcteurs d'erreurs quantiques existent.
- Des implémentations expérimentales sur de petits systèmes ont été réalisées (algorithme de Shor sur 7 qubits, permettant de factoriser 15, Vandersypen, Steffen, Breyta, Yannoni, Sherwood, Chuang, *Nature* **414**, 883, (2001); technique: RMN).
- Autres types d'ordinateurs quantiques: calcul quantique adiabatique, ordinateur quantique unidirectionnel.
- Nouveau développement dans les algorithmes quantiques: marches aléatoires quantiques.

Quel est le futur?

- “Feuille de route” américaine (http://qist.lanl.gov/)
- “Feuille de route” européenne (http://www.cordis.lu/ist/fet/qipc-sr.htm)
- Enorme effort expérimental; mais les problèmes sont si difficiles que résultats limités à quelques qubits.
- Cependant, aucune raison physique n’interdit la réalisation d’un ordinateur quantique de grande taille.
- Sauf percée technologique inattendue, un ordinateur quantique réellement utile (avec des centaines de milliers de qubits) ne sera pas construit dans un futur proche. En attendant, des ordinateurs quantiques de quelques dizaines de qubits pourraient être construits.
- Il y a un besoin de nouveaux algorithmes quantiques.

Pendant ce temps

- le calcul quantique a des applications en calcul classique. Exemple: simulation de systèmes quantiques à plusieurs corps.
- Les simulateurs quantiques (“ordinateurs quantiques spécialisés”) semblent plus facile à construire.
- La cryptographie quantique a été utilisée pour les élections suisses en 2007.
- “plan” pour mener au contrôle de systèmes quantiques $\Longrightarrow$ développement d’une nouvelle physique dans plusieurs implémentations

Organisation de la recherche

- Programmes américains: agences militaires et de renseignement (National Security Agency et Army Research Office), DARPA (Defense Advanced Research Projects Agency) et NSF
- Europe: programme “Quantum Information Processing”, inclus dans “Future and Emerging Technologies” partie d’IST (Information society technologies). Budget FP7 $\approx$ 30 MEuros
- Programmes nationaux dans plusieurs pays européens, quelquefois comme parties de programmes de nanotechnologie.

Tendance vers de larges projets intégrant théoriciens et expérimentateurs

Plus d'information ...

- B.Georgeot and D.L.Shepelyansky, *Les ordinateurs quantiques affrontent le chaos*, Images de la physique 2003-2004 (2004), 17 (quant-ph/0307103) **(courte introduction, en français)**.
- A. Eckert and R. Josza, *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys. **68**, 733 (1996) **(surtout algorithme de factorisation)**.
- A. Steane, *Quantum Computing*, Rep. Progr. Phys. **61**, 117 (1998) (quant-ph/9708022) **(très bon article de revue)**.
- G. Benenti, G. Casati and G. Strini, *Principles of quantum computation and information*, World Scientific (2004) **(bonne introduction au domaine)**.
- M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press (2000) **(référence très complète)**.