THÈSE

présentée par

Andrei A. Pomeransky

pour obtenir le grade de

Docteur de l'Université Paul Sabatier

Intrication et Imperfections dans le Calcul Quantique

Directeur de thèse :

Dima L. Shepelyansky

Co-directeur de thèse :

Bertrand Georgeot

Avec le soutien financier de

NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Plan de la thèse

- Introduction
- Calcul quantique de la transition d'Anderson en présence d'imperfections statiques
- Algorithme quantique de recherche de Grover en présence d'imperfections
- L'équivalence des conjectures de l'additivité et de la superadditivité forte de l'intrication de formation
- Entropie moyenne informationnelle des états quantiques
- Conclusion

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Information quantique

Le qubit est un bit quantique.

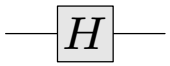
Bit classique : états 0,1

Le qubit est un système à deux niveaux (spin 1/2, deux états d'un atome ...) : $|0\rangle$, $|1\rangle$.

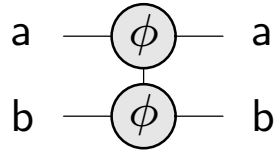
Le principe de superposition mène au parallélisme quantique. La superposition générique des plusieurs qubits n'est pas un produit des états de qubits, l'état générique est intriqué. L'intrication quantique est une des raisons de l'efficacité des ordinateurs quantiques.

Les perturbations détruisent les superpositions et l'intrication. Il faut donc étudier le calcul quantique en présence d'imperfections.

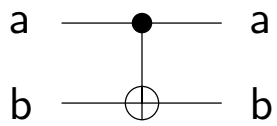
Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

La porte d'Hadamard : 

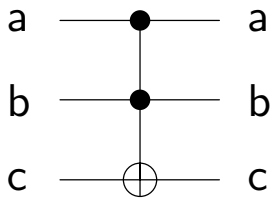
$$|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2},$$
$$|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}.$$

La porte de phase contrôlée : 

$$|11\rangle \rightarrow e^{i\phi}|11\rangle,\ |00\rangle \rightarrow |00\rangle,$$
$$|01\rangle \rightarrow |01\rangle,\ |10\rangle \rightarrow |10\rangle.$$

L'opération NOT contrôlée (ou CNOT) : 

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle,$$
$$|10\rangle \rightarrow |11\rangle, \quad |11\rangle \rightarrow |10\rangle.$$

La porte de Toffolli (opération NOT doublement contrôlée) : 

$$|110\rangle \rightarrow |111\rangle,\ |111\rangle \rightarrow |110\rangle,$$

et $|abc\rangle \rightarrow |abc\rangle$ si $ab \neq 11$.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Applications et réalisations pratiques

Factorisation des grands nombres entiers : algorithme quantique de Shor (1994). Celui-ci est très intéressant pour la cryptographie à cause de la méthode de cryptage RSA.

Recherche dans une base de donne non-structurée : algorithme de Grover (1997). Ansi que la recherche des solutions d'un problème NP-complet.

Simulation des systèmes quantique par les ordinateurs quantiques (R. Feynman, 1982).

Implémentations expérimentales : RMN, pièges à ions, jonctions Josephson, électrons dans les boites quantiques etc.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Calcul quantique en présence d'imperfections

Imperfections statiques

Hamiltonien des imperfections statiques (B. Georgeot et D.L. Shepelyansky, 2000) :

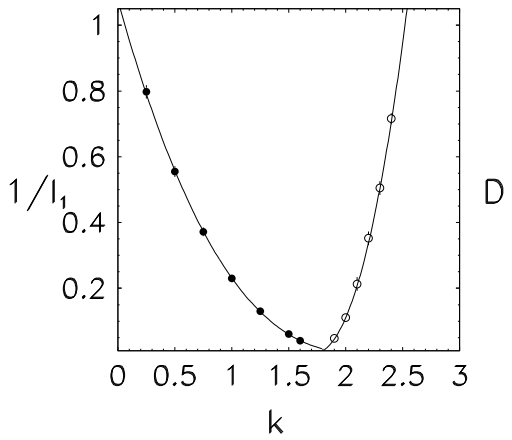
$$H = \sum_i a_i \sigma_i^z + \sum_{i<j} b_{ij} \sigma_i^x \sigma_j^x .$$

Les différences des niveaux d'énergie a_i et les couplages entre qubits b_{ij} sont distribués de façon aléatoire et uniformément dans les intervalles $[-\alpha, \alpha]$ et $[-\beta, \beta]$, respectivement.

La "mémoire quantique" présente une transition entre les régimes intégrable ($a << b$ ou $b << a$) et chaotique ($a \sim b$). Cette transition est moins évidente dans un ordinateur quantique qui exécute un algorithme complexe.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Localisation et transition d'Anderson



Le modèle d'Anderson décrit une particule sur un réseau d-dimensionnel. L'équation de Schrödinger stationnaire du modèle est :

$$\sum_{\mathbf{m}} w_{\mathbf{m}} \psi_{\mathbf{m+n}} + v_{\mathbf{n}} \psi_{\mathbf{n}} = E \psi_{\mathbf{n}},$$

où $v_{\mathbf{n}}$ sont les nombres aléatoires et $w_{\mathbf{m}}$ diminuent rapidement avec $\mathbf{m}$ ($\mathbf{m}$ est un vecteur de d nombres entiers).

Notre modèle est le rotateur pulsé avec modulation de fréquence :

$$H = H_0(n) + k(1 + \epsilon \cos(\Omega_1 t) \cos(\Omega_2 t)) \cos\theta \sum_m \delta(t - mT),$$

qui présente une transition d'Anderson.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Algorithme quantique

Évolution unitaire de la fonction d'onde ψ entre deux pulses consécutifs :

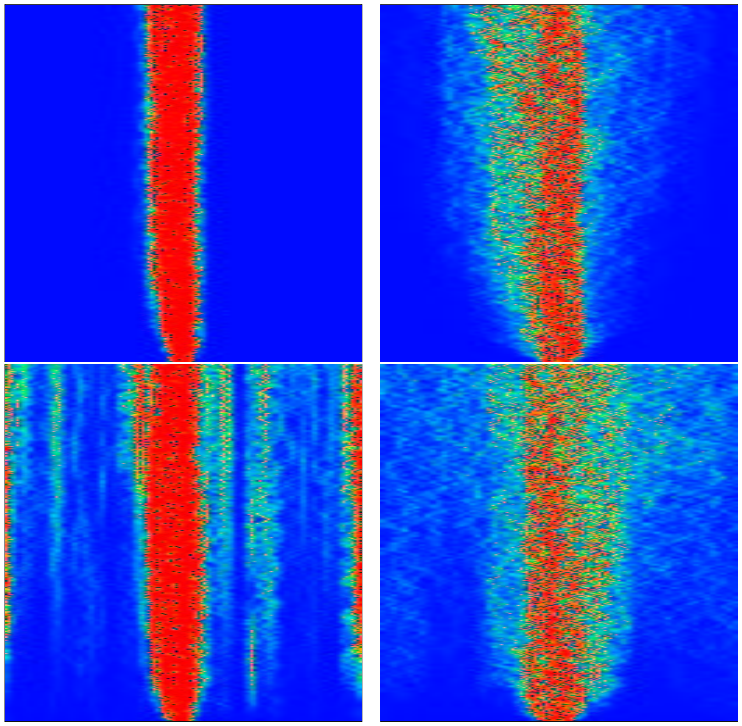
$$\bar{\psi} = \hat{U}\psi = \exp(-ik(t)\cos\theta)\exp(-iH_0(\hat{n}))\psi\ .$$

Dans la représentation du moment angulaire l'opérateur $\exp(-iH_0(\hat{n}))$ est une multiplication par des phases aléatoires. Il a été réalisé par une séquence de portes CNOT et des rotations de phase à un qubit.

Ensuite la transformation de Fourier quantique (TFQ) est effectuée pour passer à la représentation de θ. Elle est réalisée par des portes d'Hadamard et d'opérations de phase contrôlées. Ensuite l'opérateur $\exp(-ik(t)\cos\theta)$ est réalisé approximativement par les portes d'Hadamard, les rotations de phase à un qubit et les portes de phase contrôlées ; et enfin on fait la TFQ inverse. Au total une itération de l'application quantique exige $n_g = 2[k/\gamma](n_q+2) + n_q^2 + 12n_q + 9$ portes élémentaires, où γ est un paramètre (les γ plus petits donnent plus de précision à l'algorithme).

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

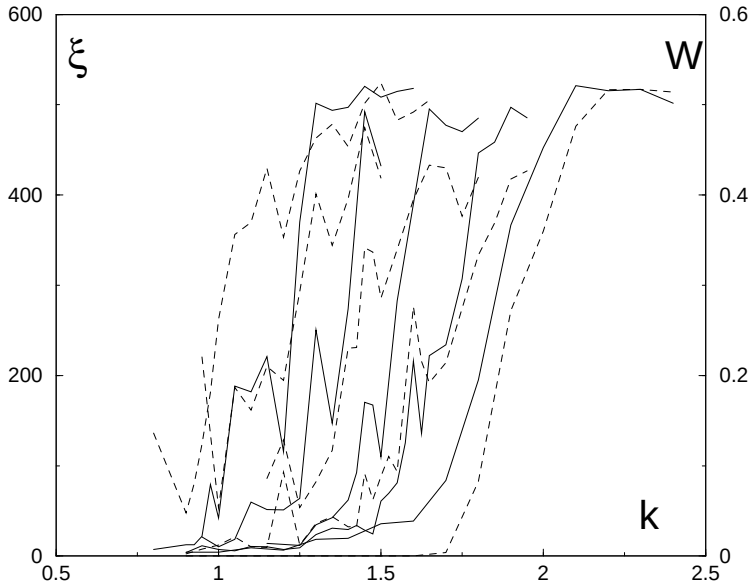
Evolution temporelle et imperfections



Évolution temporelle de la distribution de probabilité $|\psi_n|^2$ dans la phase localisée (colonne de gauche, $k = 1.2$) et dans la phase délocalisée (colonne de droite, $k = 2.4$) pour $n_q = 7$ qubits ($N = 2^{n_q}$), avec $0 \leq t \leq 400$ (axe vertical) et $-N/2 < n \leq N/2$ (axe horizontal) ; $k_c = 1.8$. L'intensité des imperfections statiques est zéro pour la ligne supérieure et 10^{-4} pour la ligne inférieure.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

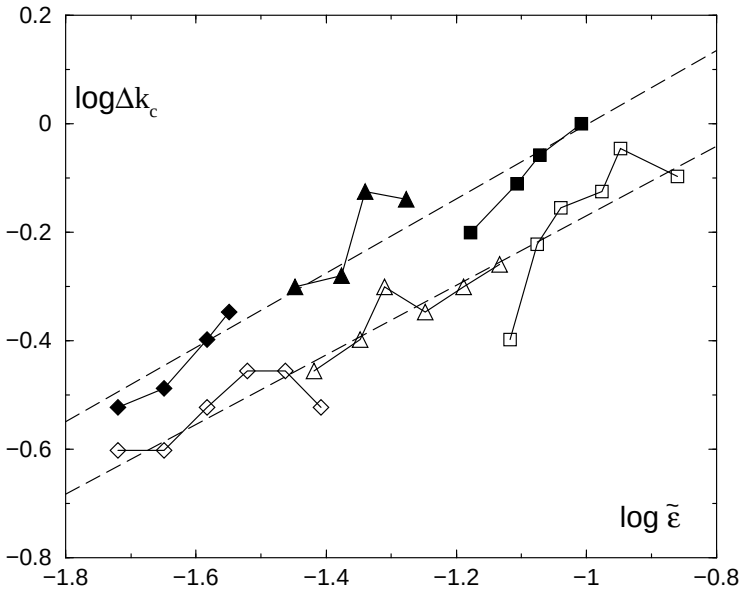
Transition d'Anderson et imperfections



IPR ξ (courbes pleines, ordonnées lues sur l'axe de gauche) et probabilité d'excitation W (courbes tiretées, ordonnées lues sur l'axe de droite) en fonction de l'intensité k du pulse pour $n_q = 10$ et pour (de droite à gauche) $t \geq 10^5$, $\epsilon = 0; 10^{-5}; 2 \times 10^{-5}; 4 \times 10^{-5}; 8 \times 10^{-5}$; $b_{ij} = 0$.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Décalage du point critique par les imperfections



Déviation par rapport au point critique $\Delta k_c(\epsilon) = k_c - k_c(\epsilon)$ en fonction de l'intensité des imperfections $\tilde{\epsilon} = \epsilon n_g \sqrt{n_q}$ pour $\epsilon = 2 \times 10^{-5}$ (losanges), 4×10^{-5} (triangles) et 8×10^{-5} (carrés) ; les symboles ouverts/pleins correspondent respectivement à $\beta = 0$, $8 \leq n_q \leq 13$ et $\alpha = \beta$, $8 \leq n_q \leq 11$; $k_c = 1.8$. Les lignes tiretées illustrent la relation d'échelle

Loi d'échelle : $\Delta k_c(\epsilon) = A \tilde{\epsilon}^{\,\nu}$, $\tilde{\epsilon} = \epsilon n_g \sqrt{n_q}$,
avec $A = 3.0$, $\nu = 0.64$ pour $\beta = 0$ et $A = 4.8$, $\nu = 0.68$ pour $\alpha = \beta$.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

L'efficacité du calcul quantique

À proximité du point critique du système réel en dimensions d, le nombre d'états croît avec le temps suivant la relation $N^d \sim t$ et le nombre de niveaux excités est aussi $N^d \sim t$.

Ainsi, le nombre d'opérations classiques pour t pulses peut être estimé à $n_{gcl} \sim tN^d \log^d N \sim t^2 \log^d t$. L'algorithme quantique nécessitera $n_g \sim dn_q^2 t \sim t \log^2 t$ portes avec d registres quantiques de $N^d = 2^{dn_q} \sim t$ états.

Ainsi, le gain en rapidité est seulement quadratique à proximité du point critique.

Au dessus de celui-ci, nous avons une croissance diffusive avec $N^d \sim t^{d/2}$ et le gain en rapidité est plus important : $n_{gcl} \sim n_g^{(1+d/2)}$ pour $d > 2$.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Algorithme quantique de recherche de Grover

La base de données est décrite par $N = 2^{n_q}$ des états d'un registre de n_q qubits.

La fonction d'*oracle* $g(x)$ est $g(x) = 1$ si x est l'état recherché τ et sinon $g(x) = 0$.

Opérateur d'évolution $\hat{G}$ pendant une itération : $\hat{G} = \hat{D}\hat{O}$.

Opérateur d'oracle a la forme $\hat{O} = (-1)^{g(\hat{x})}$.

Opérateur de diffusion $\hat{D}$ est donné par : $D_{ii} = -1 + \frac{2}{N}$ et $D_{ij} = \frac{2}{N}$ $(i \neq j)$.

État initial : $|\,\psi_0\,\rangle = \sum_{x=0}^{N-1} |\,x\,\rangle/\sqrt{N}$.

t applications de l'opérateur $\hat{G}$ à l'état initial donnent :

$$|\,\psi(t)\,\rangle = \hat{G}^t|\,\psi_0\,\rangle = \sin\left((t+1/2)\omega_G\right)|\,\tau\,\rangle + \cos\left((t+1/2)\omega_G\right)|\,\eta\,\rangle,$$

où la fréquence de Grover $\omega_g \approx 2/\sqrt{N}$ et $|\,\eta\,\rangle = \sum_{x\neq\tau}^{(0\leq x<N)} |\,x\,\rangle/\sqrt{N-1}$.

L'état du registre quantique après $\frac{\pi}{2\omega_G} \approx \frac{\pi}{4}\sqrt{N}$ itérations est l'état recherché $|\,\tau\,\rangle$.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

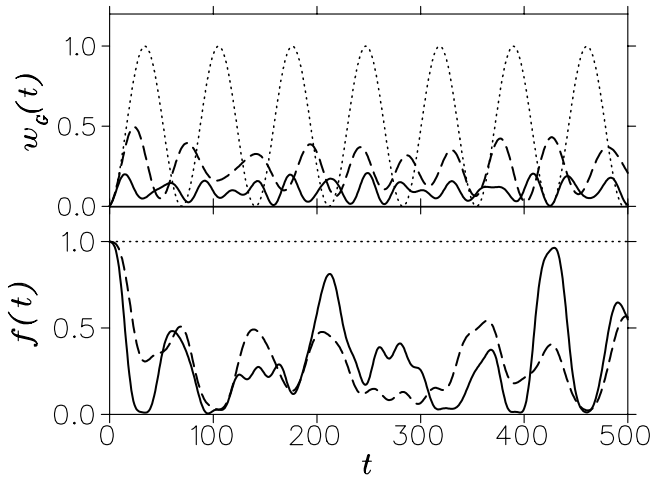
Portes quantiques dans l'algorithme de Grover

La représentation de l'opérateur D comme une séquence de portes élémentaires exige un qubit supplémentaire.

Cela permet de réaliser l'opérateur de Grover G avec $n_q + 1$ qubits par $n_g = 12n_q - 30$ portes élémentaires, à savoir les rotations d'un qubit, les portes NOT contrôlée et les portes de Toffoli (l'opérateur $\hat{O}$ est supposé implémenté par ailleurs).

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

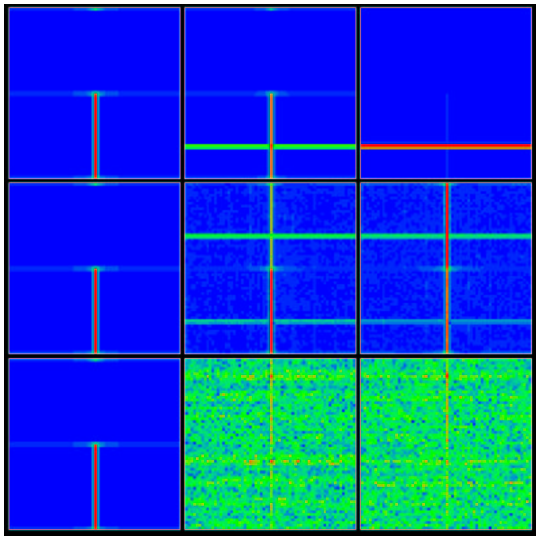
Oscillations de probabilité en présence d'imperfections



Probabilité d'état cherché $w_G(t)$ (panneau supérieur) et fidélité $f(t)$ (panneau inférieur) en fonction des pas d'itération t dans l'algorithme de Grover pour $n_{tot} = 12$ qubits. Les courbes pointillées montrent les résultats pour l'algorithme idéal $(\varepsilon = 0)$, les courbes tiretées et pleines correspondent respectivement à des intensités d'imperfection $\varepsilon = 4 \cdot 10^{-4}$ et 10^{-3}.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Evolution de la fonction de Husimi



Evolution de la fonction de Husimi pour l'algorithme de Grover aux temps $t = 0$, 17, et 34 (de gauche à droite), et pour $\varepsilon = 0$, 0.001, et 0.008 (de haut en bas). Le réseau de qubits et la réalisation du désordre sont les même que ceux utilisés pour la figure précédente. L'axe vertical désigne la base de calcul $x = 0, \ldots, 2N - 1$, tandis que l'axe horizontal désigne la base du moment conjugué. La valeur de la fonction de Husimi est proportionnelle à la couleur variant du maximum (rouge) à zéro (bleu).

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Efficacité de l'algorithme

La probabilité de trouver le bon résultat est :

$$\bar{w}_G = \sqrt{\pi/2}(1 - \mathrm{erf}(\sqrt{2}\omega_G/\sigma)) \exp\left(2\omega_G^2/\sigma^2\right) \omega_G/\sigma,$$

où $\sigma \approx 0.56\varepsilon n_g\sqrt{n_q}$, $\omega_G = 2/\sqrt{N}$. Le nombre total d'opérations quantiques N_{op} requises pour la détection de l'état recherché peut être estimé à $N_{op} \sim N_M/\omega \sim \sigma/\omega_G^2 \sim \varepsilon N/\varepsilon_c$, où $N_M \sim 1/w_G \sim \sigma^2/\omega_G^2$ est un nombre de mesures requises pour la détection de l'état cherché ; $\varepsilon_c \approx 1.7/(n_g\sqrt{n_{tot}})$.

Le gain efficace paramétrique de l'algorithme de Grover est de l'ordre de $\varepsilon_c/\varepsilon$ en comparaison avec un algorithme classique. Pour $\varepsilon \sim \omega_G$, l'efficacité est comparable à celle de l'algorithme de Grover idéal, tandis que pour $\varepsilon \sim \varepsilon_c >> \omega_G$, il n'y a pas de gain en comparaison avec le cas classique.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Intrication quantique

Les états séparables peuvent être factorisés : $|\,\psi\,\rangle = |\,\psi_1\,\rangle|\,\psi_2\,\rangle$.

Exemple d'un état pur intriqué : $\Psi = \frac{1}{\sqrt{2}}(|\,\uparrow\downarrow\,\rangle - |\,\downarrow\uparrow\,\rangle)$.

Un état mélangé ρ n'est pas intriqué s'il peut être représenté comme un ensemble d'états purs séparables.

Un système composé de deux parties, A et B : $A - - - - - - - - - - B$

Intrication d'un état pur : $E(\psi) = S(\mathrm{Tr}_B(|\,\psi\,\rangle\langle\,\psi\,|)) = S(\mathrm{Tr}_A(|\,\psi\,\rangle\langle\,\psi\,|))$.

Intrication de formation (IDF) d'un état mélangé :

$E_F(\rho) = \min\{\sum_i p_i E(\psi_i) :\ \rho = \sum_i p_i |\,\psi_i\,\rangle\langle\,\psi_i\,|\}$

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Les propriétés d'additivité de l'intrication de formation

Étant donné deux états ρ_1 et ρ_2 de deux systèmes séparés 1 et 2 (chacun étant un système bipartite avec les parties respectives $1A$, $1B$ et $2A$, $2B$, en considérant l'intrication entre A et B), on peut se demander quelle est l'IDF de l'état $\rho_1 \otimes \rho_2$ du système composé.

A1 B1
– – – – –
A2 B2

Il a été conjecturé que l'IDF est additive : $E_F(\rho_1 \otimes \rho_2) \stackrel{?}{=} E_F(\rho_1) + E_F(\rho_2)$.

Il est naturel de comparer l'IDF d'un système dans un état ρ à la somme des IDF de ses sous-systèmes. Il a été conjecturé : $E_F(\rho) \stackrel{?}{\geq} E_F(\mathrm{Tr}_2\rho) + E_F(\mathrm{Tr}_1\rho)$.

Cette propriété de la superadditivité forte est intéressante parce qu'elle implique l'additivité de l'IDF (Vollbrecht et Werner, 2001 ; Matsumoto et al., 2002). Nous prouvons que l'inverse est aussi vrai.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Équivalence des conjectures

L'IDF est une fonction convexe : $E_F(\sum_i p_i\rho_i) \leq \sum_i p_i E_F(\rho_i)$.

En utilisant les méthodes de l'analyse convexe (K.M.R. Audenaert, S.L. Braunstein, 2003) nous prouvons l'équivalence des conjectures de l'additivité et de la superadditivité forte de l'IDF. La superadditivité forte de l'IDF implique aussi l'additivité de la capacité classique de Holevo-Schumacher-Westmorland d'un canal quantique (Matsumoto et al., 2002).

Ce travail a été fait indépendamment de celui de P.W. Shor, qui a prouvée l'équivalence de ces conjectures, ainsi que l' équivalence de certaines autres conjectures.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Entropie informationnelle et mesure quantique

Une mesure quantique est spécifiée par une base des états (purs) $|a\rangle$ ou par un opérateur hermitien $\mathcal{A}$. La probabilité d'avoir a comme le résultat d'une mesure est $\langle a|\rho|a\rangle$. L'entropie informationnelle pour cette mesure est :

$$S[\rho|\mathcal{A}] = -\sum_a \langle a|\rho|a\rangle \ln(\langle a|\rho|a\rangle)$$

Il existe une base $\mathcal{H}$ dans laquelle ρ est diagonale : $\rho = \mathrm{diag}\{p_r\}$. L'entropie de Von-Neumann est définie comme

$$S_{\mathsf{H}}[\rho] = S[\rho|\mathcal{H}] = -\sum_r p_r \ln(p_r).$$

Pour un état quantique pur l'entropie de Von Neumann égale zéro.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Définition de l'entropie moyenne informationnelle

La définition d'entropie informationnelle quantique ne devrait supposer aucune base spéciale. Par conséquent, nous suggérons la définition la plus naturelle suivante :

$$S[\rho] \;=\; \overline{S[\rho|\mathcal{A}]} \;=\; S_0(N) + F(p_1, p_2, ...)$$

où la quantité surlignée est la moyenne sur toutes les bases possibles avec la mesure uniforme (aucune base préférée) de GUE (Ensemble unitaire gaussien).

$S_0(N)$: l'entropie moyenne informationnelle d'un état pur.

$F(p_1, p_2, ...)$: une mesure de manque de pureté, numériquement elle est corrélée avec l'entropie de Von Neumann.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Calcul de l'entropie moyenne informationnelle

$$S = \overline{\sum_a f\left(\sum_r p_r |\langle r|a\rangle|^2\right)}^{A} = \overline{\sum_s f\left(\sum_r p_r |\langle r|U|s\rangle|^2\right)}^{U}$$
$$= \overline{Nf\left(\sum_r p_r |\langle r|\Psi\rangle|^2\right)}^{\Psi} = N\int_0^\infty f(s)\ P(s)ds$$

où $f(s) = -s\ln(s)$, $s = \sum_r p_r |\Psi_r|^2$ et $P(s)$ est une distribution de probabilité qui dépend de ρ.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Expression explicite pour l'entropie moyenne

$$P(s) = (N-1) \sum_{(p_r > s)} \left[\prod_{r'(\neq r)} \frac{1}{p_r - p_{r'}} \right] (p_r - s)^{N-2}$$

Comme $S = -N \int_0^\infty s \ln(s)\ P(s) ds,$

On a : $S = S_0(N) - \sum_r \left[\prod_{r'(\neq r)} \frac{p_r}{p_r - p_{r'}} \right] p_r \ln(p_r),$

où $S_0(N) = \sum_{k=2}^{N} \frac{1}{k} \approx \ln(N) - (1-\gamma) + \frac{1}{2N}.$

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553

Conclusion

- Nous avons montré que la transition d'Anderson peut être simulée par un ordinateur quantique avec 7-10 qubits.
- Nous avons montré que l'algorithme de Grover reste robuste en présence des erreurs statiques, dans un domaine de paramètres bien défini.
- Nous avons montré l'équivalence des deux propriétés conjecturées de l'intrication de formation : son additivité et sa superadditivité forte.
- Nous avons proposé une nouvelle mesure pour l'incertitude du résultat d'une mesure quantique pour les états mélangés.

Avec le soutien financier de NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553