Intrication et Imperfections dans le Calcul Quantique

Andrei Pomeransky

THÈSE

présentée par

Andrei A. POMERANSKY

(Octobre 2004)

pour obtenir le grade de

Docteur de l'Université Paul Sabatier

Spécialité :

Physique Théorique

École Doctorale : Physique de la Matière

Intrication et Imperfections dans le Calcul Quantique

Soutenue le 22 Octobre 2004, devant le Jury composé de

M. Vladimir Akulin (LAC, Orsay)	Examinateur
M. Klaus Frahm(UPS et LPT, Toulouse)	Président du Jury
M. Bertrand Georgeot (LPT, Toulouse)	Co-directeur de thèse
M. Jean-Louis Pichard (CEA, Saclay)	Rapporteur
M. Rüdiger Schack (Royal Holloway, London)	Rapporteur
M. Dima Shepelyansky (LPT, Toulouse)	Directeur de thèse

LABORATOIRE DE PHYSIQUE THÉORIQUE
CNRS-UMR 5152

Remerciements

Je tiens à remercier toutes les personnes qui m'ont entouré durant ces trois années de thèse et plus généralement tous les membres de Laboratoire du Physique Théorique et de l'IRSAMC.

Tout d'abord, j'aimerais remercier Dima Shepelyansky, mon directeur de thèse, pour ses conseils, ses encouragements et son constant intérêt pour mon travail. La plus grande partie de ma thèse correspond à notre collaboration.

Je remercie très vivement Bertrand Georgeot, mon co-directeur de thèse, pour les discussions enrichissantes, pour ses conseils, pour son aide constante, en particulier, pour son aide et ses conseils dans la rédaction de ma thèse.

J'ai eu le plaisir de collaborer avec Oleg Zhirov, qui m'a beaucoup appris et aidé au cours de ma thèse.

Je remercie Doron Cohen, avec qui j'ai eu le plaisir de collaborer pendant ma thèse. Cette collaboration a été extrêmement instructive et profitable pour moi. Son résultat est le chapitre 3 de cette thèse.

Je remercie aussi les membres du groupe de Chaos quantique, Robert Fleckinger et Klaus Frahm, pour leur aide constante.

Je tiens à remercier tout particulièrement José Lages, qui m'a aidé avec le français dans les Chapitres 4 et 5, et Muriel Mirandon qui a lu et corrigé toutes les autres parties de ma thèse. Un grand merci aussi à Fabien Mégi qui a corrigé l'Introduction.

Et je tiens à remercier mon collègue de bureau Stefano Bettelli pour les nombreuses discussions cruciales, ses conseils et la bonne ambiance. J'ai employé son ensemble de commandes Latex pour dessiner les schémas d'algorithmes quantiques dans ma thèse.

Je remercie Vladimir Akulin d'avoir accepté de participer à mon jury de thèse, Klaus Frahm d'avoir accepté de le presider, et Jean-Louis Pichard et Rüdiger Schack de m'avoir fait l'honneur d'être les rapporteurs.

J'aimerais également remercier mes amis et collègues Pierre-Henri Chavanis, Raphaël Cherrier, Giampaolo Cristadoro, Vianney Desoutter, Eric Giglio, Olivier Giraud, José Lages, Benjamin Lévi, Jae-Weon Lee, Ming Ma, Fabien Mégi, Marcello Terraneo et tous les autres. Grâce à mes amis, je n'ai pas vraiment eu l'impression d'être à l'étranger pendant toutes ces années que j'ai passées à Toulouse.

Merci beaucoup à mes amis de Novossibirsk : Roman Senkov, Peter Tarasov, Benjamin Abalmassov et tous les autres, qui m'ont apporté un immense soutien continuel.

Je remercie mes professeurs de Novossibirsk, qui m'ont appris la Physique Théorique, et particulièrement, Iosif Khriplovich.

Et enfin, merci beaucoup à toute ma famille, mes parents et ma soeur.

Merci à tous les autres, que je n'ai pas mentionné. Si je continuais cette liste des remerciements, elle pourrait devenir trop longue.

Table des matières

Introduction

L'information a une place de plus en plus importante dans le monde moderne. Les moyens de traitement et de transmission de l'information (les ordinateurs et leurs réseaux, les moyens divers de communication, etc.) ne cessent de se développer à une cadence rapide. Sans l'aide de la physique, ce développement serait impossible. La mécanique quantique est nécessaire à la description de la structure interne de plusieurs composants électroniques qui constituent les moyens modernes du traitement de l'information, même si jusqu'à présent un traitement au niveau classique suffisait à décrire ce dernier.

Cependant, au cours de ces dernières années, de sérieuses raisons ont poussé à réfléchir au traitement de l'information au niveau quantique et à examiner la théorie de l'information du point de vue de la mécanique quantique :

- Premièrement, selon la loi de Moore, on peut doubler le nombre de transistors sur une surface donnée tous les dix-huit mois. La réduction constante des tailles des composants électroniques des ordinateurs amènera dans un futur proche ces éléments à travailler en régime quantique. Le progrès technologique permet déjà de manipuler des petits systèmes quantiques (avec l'espace de faible dimension) sans perdre la cohérence.
- Deuxièmement, l'utilisation des systèmes quantiques permet d'obtenir dans certains cas des résultats qui restent inaccessibles par des moyens classiques. De nombreux exemples l'ont illustré au cours des deux dernières décennies. Dans le champ du calcul, la notion d'ordinateur quantique a été introduite pour décrire un système quantique qui fait des calculs. Les applications les plus importantes des ordinateurs quantiques sont aujourd'hui l'algorithme quantique de factorisation de Shor et la simulation des systèmes quantiques par les ordinateurs quantiques, proposée pour la première fois par R. Feynman. Une autre découverte importante a eu une forte influence sur le développement de la théorie quantique de la communication : la cryptographie quantique, proposée pour la première fois par Bennett et Brassard en 1984. Cette découverte permet de transmettre à distance des données confidentielles en toute sécurité. De plus, deux grands piliers de la communication quantique ont aussi joué un rôle majeur : les effets de téléportation quantique et de codage supradense.
- Troisièmement, le rôle croissant de l'information nous amène à réfléchir aux restrictions fondamentales imposées par la mécanique quantique sur nos possibilités de traiter et de transmettre l'information. Un travail considérable a été réalisé dans

cette direction avec l'étude des capacités de transmission des diverses catégories de l'information par les canaux quantiques.
– Quatrièmement, une reconsidération des bases de la mécanique quantique du point de vue de la théorie de l'information pouvait aider à mieux comprendre la mécanique quantique même, dont l'interprétation soulève encore certains questions (en particulier, en ce qui concerne la théorie de la mesure).

En vertu de toutes ces raisons, la théorie quantique de l'information a vu le jour (pour une introduction au domaine de l'information quantique, voir [1]).

Il s'est avéré que le phénomène quantique le plus important pour l'information quantique qui rend possible toutes ses applications est l'intrication quantique. Cependant, malgré la grande attention portée ces dernières années au phénomène de l'intrication, plusieurs de ses propriétés restent encore insuffisamment étudiées. Le seul cas complètement clarifié est le cas de l'état pur à deux parties. Mais en ce qui concerne l'état mélangé à deux parties, il existe déjà plusieurs problèmes non résolus. Jusqu'à présent, il existe plusieurs mesures de l'intrication pour les états mélangés qui pour chacune d'entre elles possède ses propres applications et propriétés utiles. Cependant, on ignore encore les formules mathématiques qui permettent le calcul explicite de ces mesures de l'intrication. Par ailleurs, les plus importantes de ses propriétés n'ont pas encore été prouvées, notamment les réponses aux questions d'additivité de l'intrication ne sont pas encore connues. Par exemple, si on dispose de deux copies d'un état intriqué, a-t-on deux fois plus d'intrication ? On suppose que l'intrication est additive, mais la preuve de cette hypothèse nous échappe encore. Dans cette thèse, nous montrons l'équivalence de deux hypothèses importantes de ce type.

Les ordinateurs quantiques envisageables dans la pratique seraient influencés par des perturbations diverses telles que les interactions avec l'environnement, les interactions résiduelles à l'intérieur de l'ordinateur et les effets de la précision finie des implémentations des portes quantiques. Les influences de ces imperfections sont différentes entre elles et dépendent aussi fortement du caractère de l'algorithme exécuté sur l'ordinateur qui peut induire une dynamique complexe et chaotique ou une dynamique simple et intégrable. Nous examinerons l'influence des perturbations statiques (qui ne dépendent pas du temps) sur l'ordinateur quantique qui exécute deux algorithmes différents : simulation de la transition d'Anderson dans le modèle de rotateur pulsé et recherche quantique dans une base de données non structurée (l'algorithme de Grover). Ces deux algorithmes nous donnent des exemples des deux types d'algorithmes quantiques mentionnés ci-dessus. La simulation du rotateur pulsé donne l'exemple d'un algorithme à la dynamique complexe chaotique, tandis que l'algorithme de Grover donne l'exemple d'une dynamique simple intégrable. Ces algorithmes sont aussi d'un intérêt non négligeable du fait que le rotateur pulsé représente un des modèles les plus populaires de la théorie de chaos quantique et que l'algorithme de Grover représente le deuxième algorithme quantique le plus important après celui de Shor.

Dans le premier chapitre, nous présentons une introduction pédagogique à l'ensemble des problèmes abordés dans cette thèse : l'intrication, le calcul quantique, la transition d'Anderson et le rotateur pulsé. Le deuxième chapitre est consacré à la preuve de

l'équivalence des deux propriétés conjecturées de l'intrication de formation : son additivité et sa superadditivité forte. Dans le troisième chapitre, nous proposons une nouvelle mesure de l'incertitude du résultat d'une mesure quantique pour les états mélangés et trouvons la formule explicite de cette mesure. Nous étudions aussi les plus importantes de ses propriétés. Dans le quatrième chapitre, nous considérons l'exécution par l'ordinateur quantique avec les imperfections statiques de la simulation du modèle de rotateur pulsé qui permet d'étudier la transition d'Anderson. Dans le cinquième chapitre, nous étudions l'algorithme quantique de Grover de recherche dans une base de données non structurée en présence des imperfections statiques. Les résultats de notre recherche présentés dans cette thèse ont été publiés dans [2, 3, 4, 5]. Mon travail pendant la thèse a été entièrement soutenu par NSA et ARDA sous le contrat ARO No. DAAD19-01-1-0553 et aussi partiellement par le projet EDIQIP de EC IST-FET. Je remercie également CalMiP à Toulouse et IDRIS à Orsay pour l'accès à leurs super-ordinateurs.

Chapitre 1

Intrication, ordinateurs quantiques et chaos

1.1 Ordinateurs quantiques

1.1.1 La notion d'ordinateur quantique et de qubit

Feynman [6] fût l'un des premiers à proposer l'emploi de la mécanique quantique pour accomplir les tâches encore inaccessibles par les systèmes classiques. Il a noté que la croissance exponentielle de la dimension de l'espace de Hilbert avec le nombre de degrés de liberté, rend impossible la simulation des grands systèmes quantiques par les ordinateurs classiques. Il proposa donc en 1982 d'employer des systèmes *quantiques* pour simuler d'autres systèmes quantiques. On peut considérer ceci comme la naissance de l'idée de l'ordinateur quantique. Mais c'est seulement douze années après, en 1994, que de sérieuses recherches sur le sujet ont commencé après la découverte de P.W. Shor sur l'algorithme quantique de la factorisation [7] qui déclencha une véritable avalanche de recherches dans le domaine du calcul quantique et de l'information quantique en général. Cette grande impulsion donnée par la découverte de P.W. Shor au développement de la théorie quantique de l'information va surtout se révéler dans l'importance réelle que pouvait avoir une réalisation de cet algorithme exponentiellement plus rapide que tous les algorithmes classiques connus. Une des méthodes de cryptographie les plus souvent utilisées est appelée RSA d'après les initiales de ses inventeurs, R. Rivest, A. Shamir et L. Adleman. Cette technique de cryptage est basée sur la complexité exponentielle des algorithmes connus de factorisation des nombres entiers. C'est pourquoi la découverte de l'algorithme quantique avec sa complexité polynomiale a soudainement suscité chez les chercheurs un vif intérêt pour le domaine de l'information quantique.

Dans la théorie quantique de l'information, on considère généralement les systèmes physiques comme les ensembles des systèmes à deux niveaux quantiques, les qubits. Cette approche convient bien aux physiciens, pour qui le système à deux niveaux est un modèle habituel et souvent utilisé, tout comme aux informaticiens, avec la notion de bit d'information. Le plus important est que cette approche permet la comparaison directe des capacités des systèmes quantiques et classiques grâce à cette analogie entre le bit et le

qubit. On utilise la notation $|0\rangle$ et $|1\rangle$ pour les états de ce système à deux niveaux, correspondants aux états 0 et 1 d'un bit classique. Un exemple important de système à deux niveaux est le spin 1/2. Tous les systèmes à deux niveaux étant isomorphes, on peut tous les considérer comme les spins 1/2. Les matrices de Pauli σ_x, σ_y et σ_z sont utilisées pour la description des opérations sur les qubits.

Nous examinerons ensuite les systèmes composés de n_q qubits, avec l'espace de Hilbert à N dimensions, $N = 2^{n_q}$. Ces systèmes sont appelés les registres quantiques.

Le calcul quantique comprend la préparation de l'état initial du registre quantique, le calcul proprement dit qui consiste en l'application vers ce registre d'une certaine transformation unitaire et la mesure de l'état final. La succession de ces opérations est décrite par l'algorithme quantique. L'ensemble de ces trois étapes de calcul quantique ont de nouvelles propriétés essentielles, grâce à l'existence d' un certain nombre de phénomènes caractéristiques de la mécanique quantique.

Le premier d'entre eux est le principe de superposition qui permet à un système quantique d'être dans une superposition de différents états. Le principe de superposition est la cause du parallélisme quantique : on peut préparer un registre quantique dans un état initial qui est une superposition de plusieurs différents états et on peut effectuer des opérations unitaires sur ce registre. Ces opérations agissent simultanément sur tous les états dans la superposition, ainsi plusieurs opérations de calcul sont faites en parallèle. La possibilité d'avoir des superpositions de différents états d'un registre quantique constitue un contraste frappant avec les propriétés d'un registre classique qui ne peut être que dans un seul état à la fois. Le nombre des états de base différents dans une superposition peut être de l'ordre de la dimension de l'espace d'Hilbert, $N = 2^n_q$. Le nombre N étant exponentiellement grand, il est évident que le parallélisme quantique peut augmenter dans certains cas l'efficacité de calcul de manière significative.

Les opérations quantiques utilisées dans le calcul ont aussi des propriétés très différentes de celles de ses contreparties classiques. Tout d'abord, les opérations quantiques sont des opérations unitaires, elles sont donc nécessairement réversibles. Cela peut sembler être une restriction très étroite, car les opérations irréversibles sont largement utilisées dans le calcul classique. En réalité, on sait bien depuis les années soixante-dix, que les opérations irréversibles ne sont pas nécessaires pour le calcul, elles peuvent toujours être remplacées par des opérations réversibles.

Un autre phénomène caractéristique de la mécanique quantique très important pour le calcul quantique est le théorème de non clonage. On peut toujours copier un état de registre classique, mais cette opération est impossible avec un registre quantique car elle est interdite par ce théorème. Le théorème de non clonage [8, 9] est une simple implication du principe de superposition. A titre d'illustration, supposons qu'un opérateur unitaire U peut cloner deux états d'un qubit : $U|\psi_{1,2}\rangle = |\psi_{1,2}\rangle|\psi_{1,2}\rangle$. Mais l'opérateur U ne peut cloner aucune superposition de $|\psi_1\rangle$ et $|\psi_1\rangle$. Par exemple, en utilisant la linéarité de U nous avons :

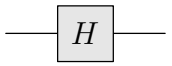
$$U(|\psi_1\rangle + |\psi_2\rangle)/\sqrt{2} = (|\psi_1\rangle|\psi_1\rangle + |\psi_2\rangle|\psi_2\rangle)/\sqrt{2}) \neq (|\psi_1\rangle + |\psi_2\rangle)(|\psi_1\rangle + |\psi_2\rangle)/2. \quad (1.1)$$

La partie la plus subtile d'un algorithme quantique est son étape finale : la mesure de

l'état du registre quantique. Il est important d'effectuer cette mesure de manière à ce que l'efficacité gagnée grâce au parallélisme quantique ne soit pas perdue pendant cette étape. Imaginons que le registre soit préparé dans une superposition de plusieurs états puis, tout en appliquant une séquence d'opérations unitaires, on fait le calcul en parallèle pour tous les états dans la superposition. Alors, si on fait simplement la mesure de l'état final, on obtient le résultat de calcul pour un état initial choisi de façon aléatoire. Cela peut aussi se faire avec un ordinateur classique tout en obtenant la même efficacité et par conséquent le parallélisme quantique n'est pas utilisé dans cette procédure. Dans les algorithmes quantiques particuliers, cette difficulté est surmontée par des procédés spécifiques. Par exemple, l'algorithme de Shor utilise la transformation de Fourier quantique pour amplifier l'information utile avant la mesure. Néanmoins, il n'existe encore aucune méthode générale connue.

1.1.2 Ensemble universel de portes quantiques.

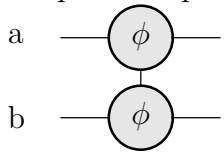
La transformation unitaire qui réalise le calcul quantique est construite comme une succession de transformations unitaires élémentaires que l'on appelle les portes quantiques. Il suffit d'un ensemble de portes fixe pour exécuter n'importe laquelle de ces transformations unitaires ; chacun de ces portes agissant sur un petit nombre de qubits seulement. On appelle cet ensemble de portes, l'ensemble universel. Il existe des ensembles universels qui ne comprennent que des portes à un et deux qubits. Nous décrirons un de ces ensembles universels qui nous servira par la suite. L'ensemble des portes universelles le plus simple (voir [10] et les références auxquelles il se rapporte) comprend les rotations d'un qubit et les opérations NOT contrôlées (CNOT). En plus de ces opérations, nous utiliserons la porte de phase contrôlée $C(\phi)$ et les portes de Toffolli à trois qubits pour réduire le nombre d'opérations dans l'algorithme, bien qu'il soit possible de les exprimer comme des combinaisons des portes de l'ensemble universel. Dans notre études des différents algorithmes quantiques ci-dessous, nous emploierons la porte d'Hadamard :



$$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2},$$
$$H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}. \qquad (1.2)$$

C'est un exemple de porte à un qubit.

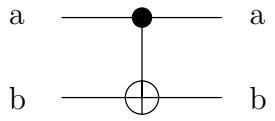
la porte de phase contrôlée :



$$C(\phi)|11\rangle = e^{i\phi}|11\rangle, \quad C(\phi)|00\rangle = |00\rangle,$$
$$C(\phi)|01\rangle = |01\rangle, \quad C(\phi)|10\rangle = |10\rangle. \qquad (1.3)$$

Cette porte à deux qubits fait la multiplication par la phase $e^{i\phi}$ l'état $|11\rangle$ et ne change pas les autres états.

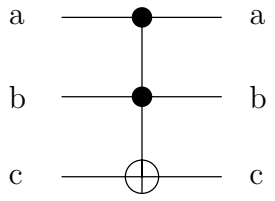
l'opération NOT contrôlée (ou CNOT) :



$$C_N|00\rangle = |00\rangle, \quad C_N|01\rangle = |01\rangle,$$
$$C_N|10\rangle = |11\rangle, \quad C_N|11\rangle = |10\rangle,$$

C'est l'analogue quantique de la porte NOT contrôlée classique bien connue. Elle fait inversion du qubit cible, si le qubit de contrôle est en état $|1\rangle$.

et la porte de Toffolli (opération NOT doublement contrôlée) :



$$CC_N|000\rangle = |000\rangle, \quad CC_N|001\rangle = |001\rangle,$$
$$CC_N|010\rangle = |010\rangle, \quad CC_N|011\rangle = |011\rangle,$$
$$CC_N|100\rangle = |100\rangle, \quad CC_N|101\rangle = |101\rangle,$$
$$CC_N|110\rangle = |111\rangle, \quad CC_N|111\rangle = |110\rangle.$$

Cette porte est l'analogue quantique de la porte de Toffoli (la porte NOT doublement contrôlée) classique. Elle fait inversion du qubit cible, si les deux qubits de contrôle sont en état $|11\rangle$.

Le nombre d'opérations quantiques élémentaires nécessaire pour faire une transformation unitaire générale, est exponentiel en nombre de qubits n_q. Elle est d'ordre de $O(N^2)$, où $N = 2^{n_q}$ est la dimension de l'espace d'Hilbert du système. Les réalisations des ces transformations unitaires sont peu utiles pour le calcul car cela nécessiterait trop d'opérations élémentaires. Mais, heureusement, le nombre polynomial d'opérations élémentaires est suffisant dans des situations très importantes, et c'est uniquement ces algorithmes quantiques qui peuvent être utiles en pratique. Dans la sous-section suivante, nous décrivons un exemple d'algorithmes pareil, la transformation de Fourier quantique.

1.1.3 Transformation de Fourier quantique

La transformation de Fourier quantique (TFQ) est probablement l'algorithme quantique le plus utile, parce que cette transformation fait partie de presque tous les algorithmes quantiques, notamment l'algorithme de factorisation de Shor et des algorithmes de simulation des systèmes quantiques. La TFQ est une traduction directe dans le langage des opérateurs quantiques de la transformation de Fourier rapide bien connue. Dans la forme utilisée ici, la TFQ a été présentée dans [12] et [13] (voir aussi [7]).

Commençons par décrire la transformation de Fourier rapide classique. Soit une fonction complexe $f(x)$, définie dans les points discrets sur un cercle : $x = 2\pi l/N, l = 0, 1, ..., N-1$. La transformée de Fourier de cette fonction $f(x)$ est une autre fonction $f_k, k = 0, 1, ..., N-1$, qui est définie comme

$$f_k = \frac{1}{\sqrt{N}} \sum_{x=0}^{N} e^{-ikx} f(x), \quad k = 0, 1, ..., N-1. \tag{1.4}$$

L'ensemble de toutes les fonctions $f(x)$ est un espace d'Hilbert de dimension N et la transformation de Fourier est une transformation linéaire de cet espace. L'exécution

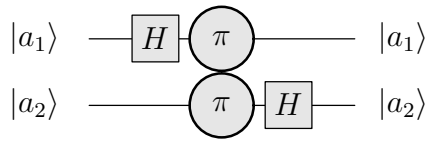


FIG. 1.1 – Le circuit pour la transformée de Fourier pour $n_q = 2$

d'une transformation linéaire par un ordinateur classique sur un vecteur de dimension N nécessite généralement un ordre de N^2 opérations élémentaires. Mais la transformation de Fourier peut être réalisée seulement avec un ordre de $N \log N$ opérations grâce à l'existence de l'algorithme de transformation de Fourier rapide. Nous considérerons le plus simple et le plus intéressant des cas, quand N est une puissance de 2 : $N = 2^{n_q}$. Écrivons l'angle x divisé par 2π dans la forme binaire : $x/2\pi = 0.a_1a_2...a_{n_q}$. On peut considérer l'espace d'Hilbert des fonctions $f(x)$ comme un produit tensoriel de n_q espaces à deux dimensions, correspondants aux deux valeurs des bits $a_i = 0, 1$.

Pour $n_q = 1, N = 2$ la transformation de Fourier discrète (1.4) est :

$$f_0 = (f(0) + f(1/2))/\sqrt{2},$$
$$f_1 = (f(0) - f(1/2))/\sqrt{2}.$$

On peut vite constater que cette transformation est en effet la transformation d'Hadamard (1.2) qui est appliquée au vecteur $(f(0), f(1/2))$.

Dans le cas un peu plus complexe de $n_q = 2, N = 4$, la transformation de Fourier discrète (1.4) va comprendre les étapes suivantes, illustrées sur la Fig.1.1. On commence par la transformation d'Hadamard dans l'espace bidimensionnel qui correspond au bit a_1. Ensuite, la transformation de phase qui consiste à multiplier par -1 la composante $f(3/4)$ est appliquée. Il n'est pas difficile de reconnaître dans cette transformation l'opération de phase contrôlée (1.3) avec les bits de contrôle a_1 et a_2 et la phase égale à π. Finalement, la transformation d'Hadamard dans l'espace bidimensionnel correspondant au bit a_2 est appliquée. Le résultat est un vecteur f_k, $k = 0, 1, 2, 3$. L'index k a la forme binaire $k = a_2a_1$. Notons que l'ordre de bits dans la forme binaire de k est inverse de celui de $x/2\pi = 0.a_1a_2$!

Dans le cas général, la transformation de Fourier rapide est aussi composée de transformations d'Hadamard et d'opérations de phase contrôlées comme dans le cas $n_q = 2$, et elle peut être présentée sous la forme itérative suivante. On commence par l'application de la transformation d'Hadamard dans l'espace bidimensionnel, correspondant au bit a_1. Puis, on fait $n_q - 1$ opérations de phase contrôlées avec un des bits de contrôle a_1, l'autre bit de contrôle a_i, $i = 2, 3, ..n_q$ et la phase égale à $2^{2-i}\pi$. Ces opérations de phase contrôlées peuvent être aussi exécutées comme une seule opération, parce qu'elles ne changent pas la base. Finalement, la transformation de Fourier rapide pour $n_q - 1$ bits est appliquée dans l'espace d'Hilbert correspondant aux bits $2, 3...n_q$. Le résultat de cette transformation est un vecteur f_k, $k = 0, 1, ...2^{n_q}$. L'index k a la forme binaire $k = a_{n_q}a_{n_q-1}...a_2a_1$ (l'ordre de bits dans la forme binaire de k est, comme ci-dessus, inverse

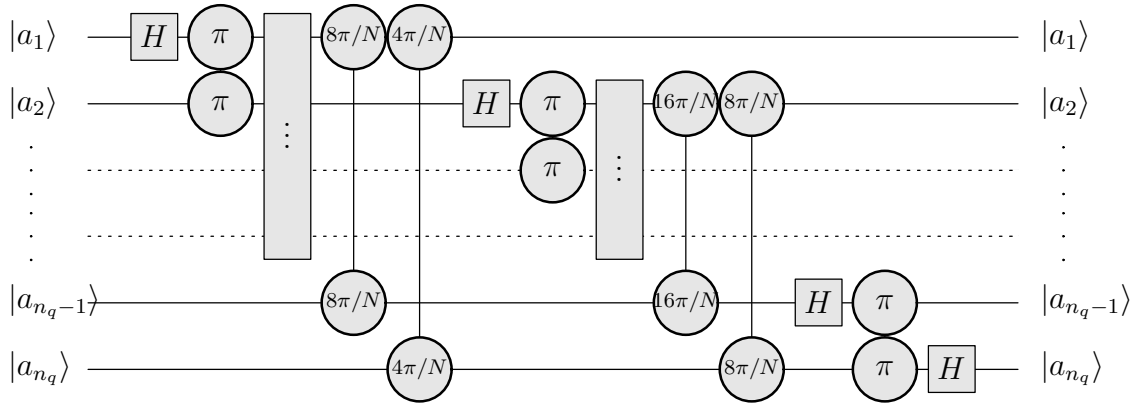


FIG. 1.2 – Le circuit pour la transformée de Fourier rapide et la TFQ

de celui de $x/2\pi = 0.a_1a_2...a_{n_q}$). L'exécution de la transformation nécessite n_q transformations d'Hadamard et opérations de phase, soit $O(n_qN)$ opérations élémentaires au total.

La construction de l'algorithme quantique est maintenant simple et directe. Pour appliquer la TFQ à un registre de n_q qubits, il faut exécuter l'algorithme de transformation de Fourier rapide comme ci-dessus (voir Fig.1.2), à la différence près que les transformations d'Hadamard et les opérations de phase contrôlées sont maintenant les opérations quantiques élémentaires, à savoir les portes quantiques. Par conséquence, dans le cas quantique, le nombre d'opérations nécessaires est d'ordre $n_q^2 = (\log N)^2$, ce qui est exponentiellement plus petit que dans le cas d'ordinateur classique.

1.1.4 L'algorithme de Grover

L'algorithme quantique de recherche dans une base de données non structurée a été proposé par Grover [14] en 1997. Imaginons, par exemple, un annuaire téléphonique qui contiendrait N noms arrangés dans un ordre aléatoire. Il faudrait examiner l'annuaire en moyenne $N/2$ fois pour trouver le numéro de téléphone d'une personne avec une probabilité de 50%. Grover proposa un algorithme quantique qui permet de trouver le résultat avec le nombre d'opérations d'ordre de $\sqrt{N}$ seulement. On réalisa plus tard que la meilleure application de cet algorithme n'était pas la recherche dans la base de données, mais la recherche des solutions aux problèmes NP-complètes [1]. Les traits caractéristiques des problèmes NP-complètes réside dans la grande difficulté à trouver une solution et la facilité à vérifier sa validité, une fois cette solution trouvée.

La base de données (ou l'espace des solutions d'un problème NP-complète) est présentée par $N = 2^{n_q}$ des états d'un registre quantique avec n_q qubits : $\{|x\rangle\}$, $x = 0, \ldots, N-1$. L'état recherché $|\tau\rangle$ peut être identifié par la fonction d'*oracle* $g(x)$, définie par $g(x) = 1$ si $x = \tau$ ou $g(x) = 0$. L'algorithme de Grover est un algorithme itératif, qui consiste en l'application alternée au registre quantique de deux de certains opérateurs. L'opérateur d'évolution $\hat{G}$ pendant une itération d'algorithme de Grover est un produit de l'opérateur d'oracle $\hat{O}$ et de l'opérateur $\hat{D}$ dit de diffusion : $\hat{G} = \hat{D}\hat{O}$. L'opérateur d'oracle a la forme

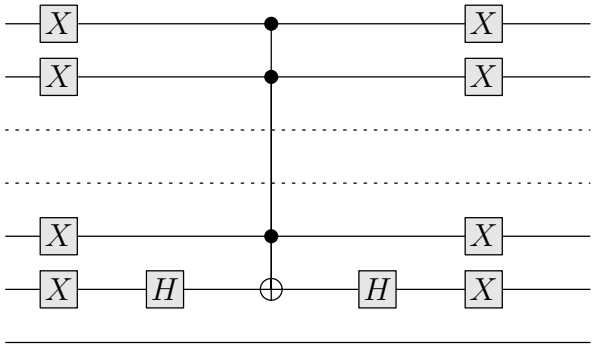


FIG. 1.3 – Le circuit pour l'opérateur de phase n_q fois contrôlée R de l'algorithme de Grover

$\hat{O} = (-1)^{g(\hat{x})}$ et sa réalisation concrète dépend du problème considéré. L'opérateur d'oracle peut être réalisé avec un nombre polynomial de portes élémentaires, grâce à la facilité de vérification de la validité des solutions aux problèmes NP-complètes (le calcul de la fonction $g(\hat{x})$) et grâce au parallélisme quantique qui permet de faire cette vérification pour tous les nombres $0, 1, ..., N$ simultanément. L'opérateur de diffusion $\hat{D}$ est universel pour tous les problèmes, il est donné par la matrice : $D_{ii} = -1 + \frac{2}{N}$ et $D_{ij} = \frac{2}{N}$ $(i \neq j)$. On commence avec la préparation de l'état initial $|\psi_0\rangle = \sum_{x=0}^{N-1} |x\rangle/\sqrt{N}$. Ensuite, l'opérateur $\hat{G}$ est appliqué plusieurs fois. t applications de cet opérateur à l'état initial donnent [1] :

$$|\psi(t)\rangle = \hat{G}^t|\psi_0\rangle = \sin\left((t+1/2)\omega_G\right)|\tau\rangle + \cos\left((t+1/2)\omega_G\right)|\eta\rangle \ , \tag{1.5}$$

où la fréquence de Grover $\omega_g = 2\arcsin(\sqrt{1/N})$ et $|\eta\rangle = \sum_{x\neq\tau}^{(0\leq x<N)} |x\rangle/\sqrt{N-1}$. Par conséquent, l'algorithme idéal donne une rotation dans un plan à deux dimensions $(|\tau\rangle, |\eta\rangle)$. L'état du registre quantique de $\pi/2\omega_G$ itérations est l'état recherché $|\tau\rangle$.

La représentation de l'opérateur D comme une séquence des portes élémentaires exige un qubit supplémentaire. Par conséquent, l'espace de Hilbert devient une somme de deux sous-espaces $\{|x\rangle\}$ et $\{|x+N\rangle\}$, qui sont différenciés seulement par la valeur du (n_q+1)-ème qubit. Ces sous-espaces sont invariants par rapport aux opérateurs O et D : $O = 1-2|\tau\rangle\langle\tau| - 2|\tau+N\rangle\langle\tau+N|$, $D = 1-2|\psi_0\rangle\langle\psi_0| - 2|\psi_1\rangle\langle\psi_1|$, où $|\psi_1\rangle = \sum_{x=0}^{N-1} |x+N\rangle/\sqrt{N}$ et $|\psi_{0,1}\rangle$ correspond aux états $|0\rangle$, $|1\rangle$ du qubit supplémentaire.

La transformation D peut être réalisée comme $D = WRW$ [14]. Ici, la transformation $W = W_{n_q} \dots W_k \dots W_1$ est composée de n_q portes d'Hadamard à un qubit W_k et R est l'opération de phase n_q fois contrôlée, définie comme $R_{ij} = 0$ si $i \neq j$, $R_{00} = 1$ et $R_{ii} = -1$ si $i \neq 0$ $(i, j = 0, \dots, N-1)$. A son tour, cet opérateur peut être exprimé comme $R = W_{n_q}\sigma^x_{n_q-1} \dots \sigma^x_1 \wedge_{n_q} \sigma^x_{n_q-1} \dots \sigma^x_1 W_{n_q}$ comme l'illustre la Fig.1.3, où $\wedge_{n_q}$ est la porte de Toffoli généralisée à n_q qubits, qui fait l'inversion du n_q-ème qubit si les $n_q - 1$ qubits précédents sont dans l'état $|1\rangle$. La construction de $\wedge_{n_q}$ à partir des portes de Toffolli à trois qubits avec l'aide d'un seul qubit supplémentaire est illustrée par la Fig.1.4 et la Fig.1.5 comme cela était proposé dans [10]. Cette procédure permet de réaliser l'opérateur de Grover G avec $n_g = 12n_{tot} - 42$ portes élémentaires, à savoir les rotations d'un qubit,

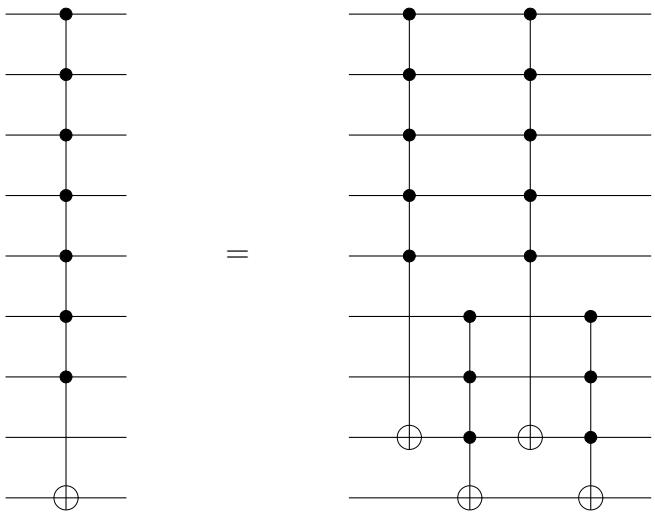


FIG. 1.4 – Le circuit pour l'opération NOT avec le contrôle multiple et un qubit supplémentaire

les portes NOT contrôlée et les portes de Toffoli. Ici, $n_{tot} = n_q + 1$ est le nombre de qubits total.

1.2 Modèles chaotiques et localisation

1.2.1 L'application "dent de scie"

l'application "dent de scie" quantique est la version quantique d'application "dent de scie" classique donnée par

$$\overline{n} = n + k(\theta - \pi), \quad \overline{\theta} = \theta + T\overline{n}, \tag{1.6}$$

où (n, θ) sont les variables action-angle conjuguées $(0 \leq \theta < 2\pi)$ et les quantités surlignées dénotent les variables après une itération de l'application.

En introduisant une variable nouvelle pour le moment $p = Tn$, on peut voir que la dynamique classique dépend seulement d'un paramètre unique $K = kT$. On peut considérer l'application (1.6) sur le cylindre $(p \in (-\infty, +\infty))$. De plus, ce cylindre peut être fermé pour former un tore de la longueur $2\pi L$, où L est un nombre entier. Pour $K > 0$, le mouvement est complètement chaotique et manifeste la diffusion normale : $< (\Delta p)^2 > \approx D(K)t$, où t est le temps discret mesuré en unités d'itérations d'application et la moyenne $< \cdots >$ est réalisée sur un ensemble de particules avec le moment initial p_0 et les phases aléatoires $0 \leq \theta < 2\pi$. Pour $K > 1$, le coefficient de diffusion est assez proche de la valeur trouvée dans l'approximation de phase aléatoire, $D(K) \approx (\pi^2/3)K^2$.

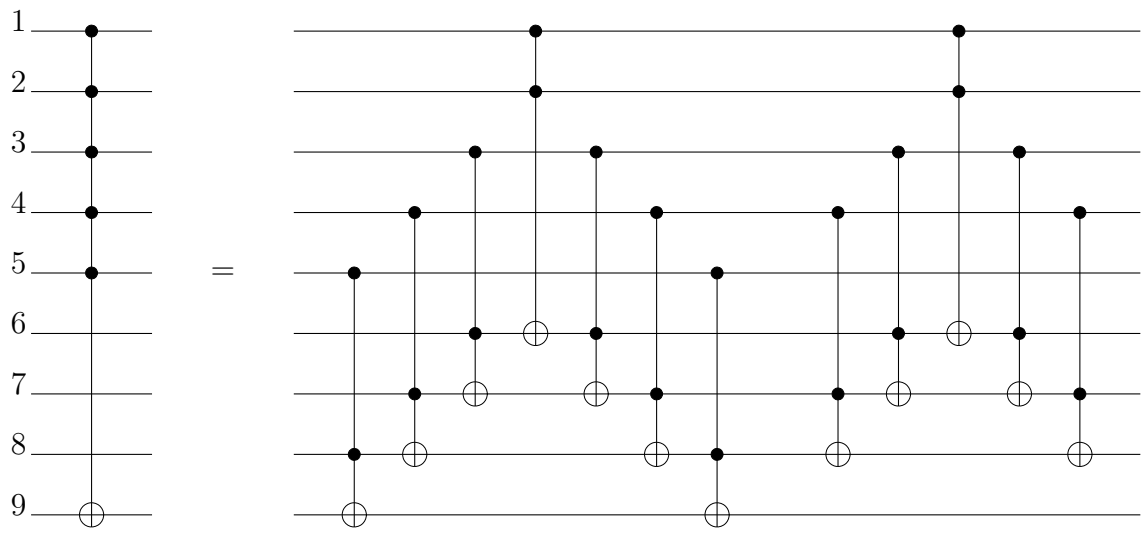


FIG. 1.5 – Le circuit pour l'opération NOT avec le contrôle multiple et un registre supplémentaire

L'évolution quantique pendant une itération de l'application est décrite par l'opérateur unitaire $\hat{U}$, appelé opérateur de Floquet qui agit sur la fonction d'onde ψ :

$$\overline{\psi} = \hat{U}\psi = e^{-iT\hat{n}^2/2} e^{ik(\hat{\theta}-\pi)^2/2}\psi, \tag{1.7}$$

où $\hat{n} = -i\partial/\partial\theta$ et $\psi(\theta+2\pi) = \psi(\theta)$ (nous imposons la condition $\hbar = 1$). La limite classique correspond à $k \to \infty$, $T \to 0$ et $K = kT = \text{const}$. L'application (1.7) a été étudiée dans Refs. [15, 16, 17] dans le régime semiclassique. Elle est réalisable en augmentant le nombre de qubits $n_q = \log_2 N$ (N est le nombre total de niveaux), avec $T = 2\pi L/N$, $K = \text{const}$. De cette façon, le nombre de niveaux à l'intérieur de la "maille primitive" $-\pi \leq p < \pi$ ($L = 1$) croît exponentiellement avec le nombre de qubits ($-N/2 \leq n < N/2$) et la constante de Planck effective $\hbar_{\text{eff}} \sim \hbar/k \sim 1/N \to 0$ quand $N \to \infty$.

Dans ce modèle, on peut observer des phénomènes physiques importants tels que la localisation dynamique (voir [18] et les références auxquelles il se rapporte). En effet, grâce aux effets de l'interférence quantique, la diffusion chaotique dans le moment est supprimée de manière semblable à la localisation d'Anderson en solides désordonnées. Au voisinage d'un tore de KAM détruit, la localisation de cantores (cantori en anglais) a lieu car un cantore commence à agir en tant que barrière parfaite à l'évolution de paquet d'onde quantique, si le flux qui traverse le cantore devient moins que $\hbar$.

La manière la plus efficace de simuler la dynamique quantique (1.7) sur un ordinateur classique est basée sur la transformation de Fourier rapide entre les représentations θ et n. C'est avantageux parce que l'opérateur d'évolution $\hat{U}$ est le produit de deux opérateurs unitaires, $\hat{U}_k = \exp(ik(\hat{\theta} - \pi)^2/2)$ (le pulse) est $\hat{U}_T = \exp(-iT\hat{n}^2/2)$ (la rotation libre), qui sont diagonales en représentations de θ et n, respectivement. Par conséquent, pour

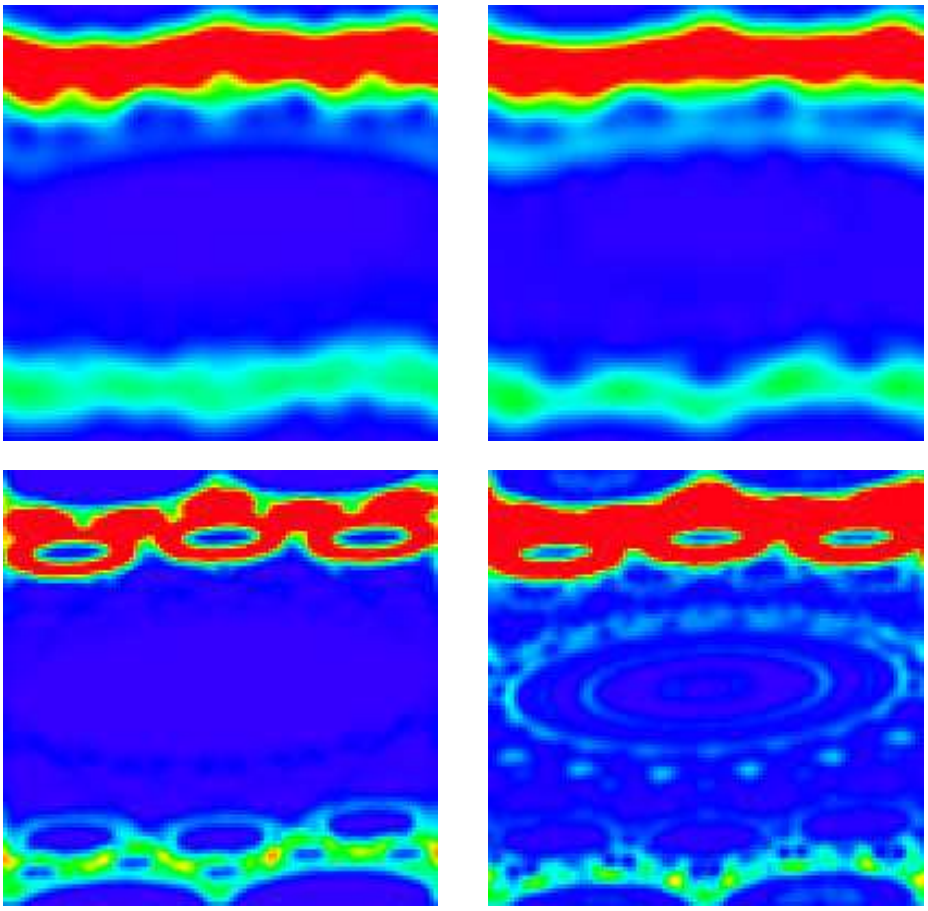


FIG. 1.6 – La fonction d'Husimi pour l'application "dent de scie" en variables action-angles (p, θ), avec $-\pi \leq p < \pi$ (l'axe vertical) et $0 \leq \theta < 2\pi$ (l'axe horizontal), pour $K = -0.1$, $T = 2\pi/2^{n_q}$, $n_0 = p_0/T = [0.38 \times 2^{n_q}]$, avec le moyen calculé dans l'intervalle $950 \leq t \leq 1000$. De haut en bas : $n_q = 6, 9, 16$ et la dernière figure montrent l'espace de phase classique avec la couleur correspondante à la probabilité, obtenu d'un ensemble de 10^8 trajectoires, avec le moment initial $p_0 = 0.38 \times 2\pi$ et les angles aléatoires. La couleur est proportionelle à la densité : bleu pour la densité zéro et rouge pour la densité maximale.

un système à N niveaux, une itération de l'application (1.7) exige deux transformations de Fourier et deux multiplications diagonales. Elle peut être exécutée avec $O(N \log_2(N))$ opérations.

La dynamique (1.7) peut être simulée exponentiellement plus vite sur un ordinateur quantique avec $n_q = \log_2 N$ qubits au moyen de l'algorithme quantique suivant :

(i) la fonction d'onde $|\psi\rangle = \sum_{n=0}^{N-1} a_n |n\rangle$ (donnée en représentation de n) est multipliée par $\hat{U}_T$, de sorte que $\hat{U}_T|\psi\rangle = \sum_n a_n \exp(-iTn^2/2)|n\rangle$. Cette étape peut être faite avec n_q^2 portes d'opération de phase contrôlée, comme on l'a expliqué dans [19] ;

(ii) on peut obtenir la fonction d'onde dans la représentation de θ via la TFQ (voir la

sous-section 1.1.3), ce qui exige n_q portes à un qubit (d'Hadamard) et $n_q(n_q-1)/2$ portes à deux qubits (opérations de phases contrôlées) ;

(iii) l'action de $\hat{U}_k$ est diagonale dans la représentation d'angle et peut être simulée de manière semblable à (i) avec n_q^2 portes à deux qubits (on note que c'est possible grâce à la forme particulière de $\hat{U}_k$ pour l'application "dent de scie") ;

(iv) on retourne à la base de moment en exécutant la QFT inverse avec $n_q(n_q+1)/2$ portes.

Par conséquent, l'algorithme exige au total $n_g = 3n_q^2 + n_q$ portes quantiques pour une itération de l'application.

Dans [15], l'application "dent de scie" a été étudiée dans le régime de diffusion anomale, avec $K = -0.1$, $-\pi \leq p < \pi$ (la géométrie de tore). La limite classique a été obtenue en augmentant le nombre de qubits n_q, avec ($k = k/t$, $-n/2 \leq n < N/2$). L'état initial au temps $t = 0$ a été pris pour être un état propre de moment angulaire, $|\psi(0)\rangle = |n_0\rangle$, avec $n_0 = [0.38N]$. Cet état peut être préparé dans $O(n_q)$ rotations d'un qubit à partir de l'état fondamental $|0, \ldots, 0\rangle$. La dynamique de l'application "dent de scie" indique la complexité de la structure de l'espace de phase, comme le montre les fonctions de Husimi dans la Fig.1.6, prises après 1000 itérations de l'application. $n_q = 6$ qubits suffisent pour observer la localisation quantique de la propagation diffusive anomale par les îles intégrables hiérarchiques. On peut voir la création des îles intégrables avec $n_q = 9$ et avec $n_q = 16$, la fonction de Husimi quantique explore la structure hiérarchique complexe de l'espace de phase classique.

1.2.2 Transition d'Anderson

Le problème de la transition métal-isolant dans les systèmes électroniques sans interaction a été considéré pour la première fois en 1958 par P.W. Anderson [20]. Depuis, ce problème continue d'éveiller un vif intérêt chez les chercheurs du monde entier (voir, par exemple, [21, 22, 23] et les références auxquelles il se rapporte). En plus des études analytiques et expérimentales du problème, une importante contribution à la compréhension de ses propriétés a été faite avec l'aide des simulations numériques basées sur diverses méthodes informatiques adaptées à la physique de ce phénomène. En effet, les études numériques ont permis d'obtenir des valeurs des exposants critiques à proximité de la transition et d'étudier certaines caractéristiques de système au point critique comprenant des statistiques d'espacement de niveaux et des fluctuations de conductibilité pour les cases de différentes symétries et de dimensions de système (voir, par exemple, [22, 23, 24, 25, 26]). Ces simulations numériques sont effectuées à l'aide d'énormes ordinateurs modernes et sont à la frontière de leur capacité informatique.

Le modèle d'Anderson décrit le mouvement d'une particule quantique sur un réseau d-dimensionnel. L'équation de Schrödinger stationnaire a la forme suivante :

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

où $v_{\mathbf{n}}$ sont le nombres aléatoires et $w_{\mathbf{m}}$ diminuent rapidement avec $\mathbf{m}$, l'index $\mathbf{m}$ court sur tous les ensembles de d nombres entiers. Le premier terme dans l'hamiltonien décrit l'énergie cinétique d'une particule, c'est la partie régulière de l'hamiltonien. Le deuxième terme est l'énergie potentielle de la particule qui dépend de façon aléatoire du noeud du réseau, c'est la partie désordonnée. En l'absence de désordre, les solutions de l'équation de Schrödinger sont les ondes de Bloch quasipériodiques. En présence de désordre, un nouveau phénomène de localisation complètement quantique peut apparaître. Les solutions de l'équation de Schrödinger dans le régime localisé ont une décroissance exponentielle avec la distance et par conséquent, la particule ne peut pas se déplacer loin sur le réseau. Ce régime insulant est impossible dans le cadre de la mécanique classique parce qu'il n'y a aucune barrière potentielle et que tout le réseau est classiquement accessible. En $d \geq 3$ dimensions, les fonctions d'ondes sont exponentiellement localisées pour $v_{\mathbf{n}}$ suffisamment grands et delocalisées pour $v_{\mathbf{n}}$ plus petits (P.W. Anderson (1958)). Cette transition entre le deux régimes est appelée la transition d'Anderson. En $d \leq 2$ dimensions, les fonctions d'ondes sont toujours localisées (E. Abrahams et al. (1979)) et la transition d'Anderson n'a pas lieu.

Dans le quatrième chapitre de cette thèse, nous étudierons un algorithme quantique qui permet la simulation numérique efficace de la transition d'Anderson. Cet algorithme est fondé sur une analogie entre la localisation d'Anderson et la localisation dynamique dans le modèle de rotateur pulsé. La sous-section suivante est consacrée à la description de ce modèle.

1.2.3 Le rotateur pulsé

Le rotateur pulsé est un des modèles les plus importants dans la théorie du chaos quantique. C'est la quantification de l'application standard de Chirikov. L'application standard (pour une revue, voir [27]) est une transformation d'espace de phase (I, θ) :

$$\begin{aligned} \bar{I} &= I + K \sin\theta \\ \bar{\theta} &= \theta + \bar{I}. \end{aligned} \tag{1.8}$$

Ici, I est le moment angulaire (variable d'action) et θ est l'angle, $0 \geq \theta < 2\pi$, $\bar{I}$ et $\bar{\theta}$ sont les nouvelles variables après une itération de l'application. La dynamique du modèle peut être décrite par l'hamiltonien

$$H = \frac{I^2}{2} + K \cos\theta \sum_m \delta(t - m), \tag{1.9}$$

qui est composé de la rotation libre et de courtes impulsions périodiques. L'application (1.8) lie les coordonnées du système dans l'espace de phase dans les deux moments avant deux impulsions consécutives.

Le système est intégrable pour $K = 0$ (c'est simplement une rotation libre), pour $K > 0$ le système montre une transition vers le chaos qui suit le théorème de Kolmogorov-Arnold-Moser. Les régions chaotiques sont séparées par les trajectoires régulières restantes

et le mouvement dans l'espace de phase est restreint par ces trajectoires. Quand K augmente au-dessus de la valeur critique $K \approx 0.9716$, la dernière trajectoire régulière qui séparait l'espace de phase disparaît et le mouvement devient illimité ; on a la diffusion vers les valeurs du moment angulaire toujours plus grandes. Les simulations numériques montrent que pour $K \gtrsim 5$, le mouvement est complètement chaotique : il y a l'instabilité locale, le mélange, la décroissance rapide des corrélations et l'entropie de Kolmogorov-Sinai positive. Dans ce régime chaotique pour les grandes valeurs de K, la dynamique se réduit à la diffusion dans l'espace de phase, avec une croissance linéaire avec le temps du carré moyen de moment angulaire : $\langle I^2 \rangle = Dt$. Il est facile de calculer le coefficient de diffusion D dans l'approximation de phases θ indépendantes, valide pour les valeurs de K assez grandes. On obtient dans ce cas

$$D = \frac{1}{2\pi} \int_0^{2\pi} (\sin\theta)^2 d\theta = \frac{1}{2}. \tag{1.10}$$

Ensuite, la quantification de l' hamiltonien (1.9) conduit à l'évolution unitaire suivante ($n = I/\hbar$) :

$$\bar{\psi} = e^{-i\hbar n^2/2} e^{-iK\cos\theta/\hbar} \psi. \tag{1.11}$$

Ce système quantique a déjà été étudié via des méthodes numériques dans [28, 29, 30] (pour une revue, voir [31]). Dans ces simulations numériques, il a été découvert, que dans ce système quantique la diffusion n'est pas perpétuelle ; elle s'arrête une fois la longueur de localisation atteinte. Il existe une seule exception pour les valeurs spéciales de K qui correspondent aux résonances quantiques pour lesquelles la diffusion ne s'arrête pas. Dans ce qui suit, nous regarderons seulement les valeurs génériques, quand la localisation a lieu,

L'effet de la localisation se manifeste dans la forme de vecteurs propres de l'opérateur d'évolution temporelle (1.11) (vecteurs propres de quasiénergie). Deux exemples typiques des fonctions propres localisées sont montrées dans la Fig. 1.7. Les vecteurs propres sont localisés exponentiellement dans la représentation de moment angulaire : ils tombent vers le zéro comme $\sim \exp(-|n - n_0|/l)$, où n_0 est la position du centre du paquet d'onde (le moment angulaire moyen). Il est facile de voir que la localisation exponentielle des fonctions propres de quasiénergie mène à son tour à la localisation dans l'évolution temporelle des paquets d'ondes. En effet, il y a seulement un nombre fini de vecteurs propres dans la décomposition de n'importe quel paquet d'onde au commencement localisé. Puisque chaque vecteur propre est localisé dans un intervalle de la longueur $\sim l$, le paquet d'onde ne peut donc pas acquérir une diffusion plus grande que $\sim l$.

On a montré dans [29, 32] que la longueur de localisation est proportionelle au coefficient de diffusion classique D : $l = \alpha D$, avec une constante numérique α de l'ordre de l'unité. L'argument est le suivant. Le paquet d'onde est effectivement composé d'un nombre fini de vecteurs propres de quasiénergie (soit perturbés ou non-perturbés). Cependant, le principe d'incertitude de temps-énergie mène à l'existence d'une énergie minimale qui peut être résolue dans un intervalle donné de temps ; cette résolution d'énergie est inversement proportionnelle au temps. Par conséquent, le spectre de quasiénergie peut être considéré comme continu, jusqu'à ce que la résolution d'énergie atteigne la séparation moyenne de niveaux dans le paquet d'onde. Finalement, la diffusion classique s'arrête.

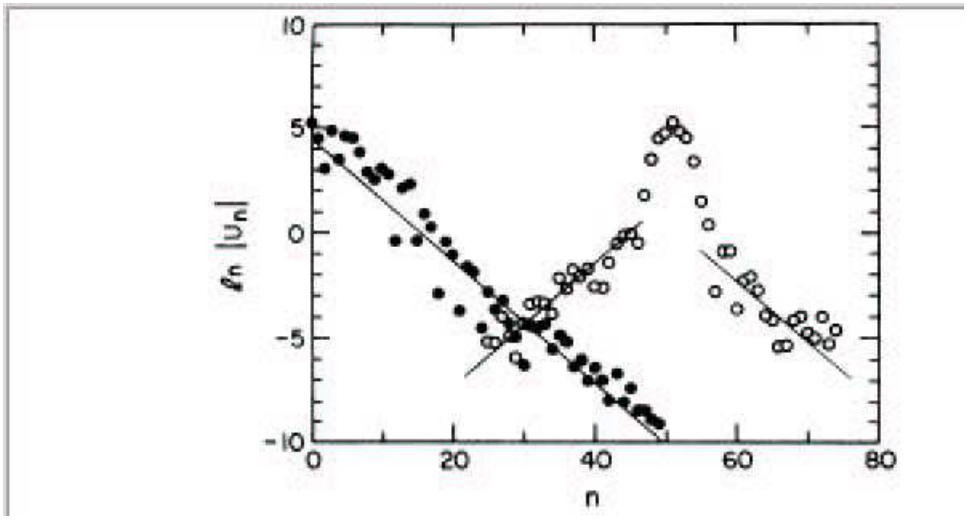


FIG. 1.7 – La localisation des fonctions propres de quasiénergie dans le modèle de rotateur pulsé (k=2.8, T=4.867) selon [32]. Les disques blancs et noirs représentent les données numériques de [33]. Les droites correspondent à la valeur de l obtenue par la méthode d'exposante de Lyapunov minimale.

La taille du paquet d'onde augmente grâce à la diffusion comme racine carrée de temps : $n \sim \sqrt{Dt}$. En conséquence, le nombre efficace de composants avec les valeurs de moment angulaire différentes dans le paquet d'onde augmente également comme $\sqrt{Dt}$. La moyenne séparation de niveaux de quasiénergie non-perturbés δE (ici, nous considérons le "pulse" comme une perturbation) est inversement proportionnelle au nombre de ces états de moment angulaire : $\delta E \sim 1/\sqrt{Dt}$. En comparant la résolution d'énergie $1/t$ à la séparation de niveaux $1/\sqrt{Dt}$, nous pouvons constater que la diffusion s'arrête dans le moment de temps $t_D = D$ et que la longueur de localisation correspondante est également égale à D. Cette relation est illustrée dans la Fig. 1.8.

1.2.4 Le rotateur pulsé et le modèle d'Anderson

Le phénomène de localisation dynamique a été expliqué dans [33] où une correspondance exacte avec le modèle d'Anderson a été établie. Pour montrer ce lien, nous commencerons par généraliser le modèle puis nous étudierons un système avec le nombre de dégrés de liberté d quelconque et les énergies cinétiques potentielles arbitraires décrites par l'hamiltonien :

$$H = H_0 + kV \sum_m \delta(t - mT). \tag{1.12}$$

L'opérateur d'évolution pour une itération est maintenant le produit $U = U_2 U_1$ de l'opérateur de "pulse" $U_1 = e^{-iKV/\hbar}$ et de l'opérateur de rotation généralisé $U_2 = e^{-iTH_0/\hbar}$.

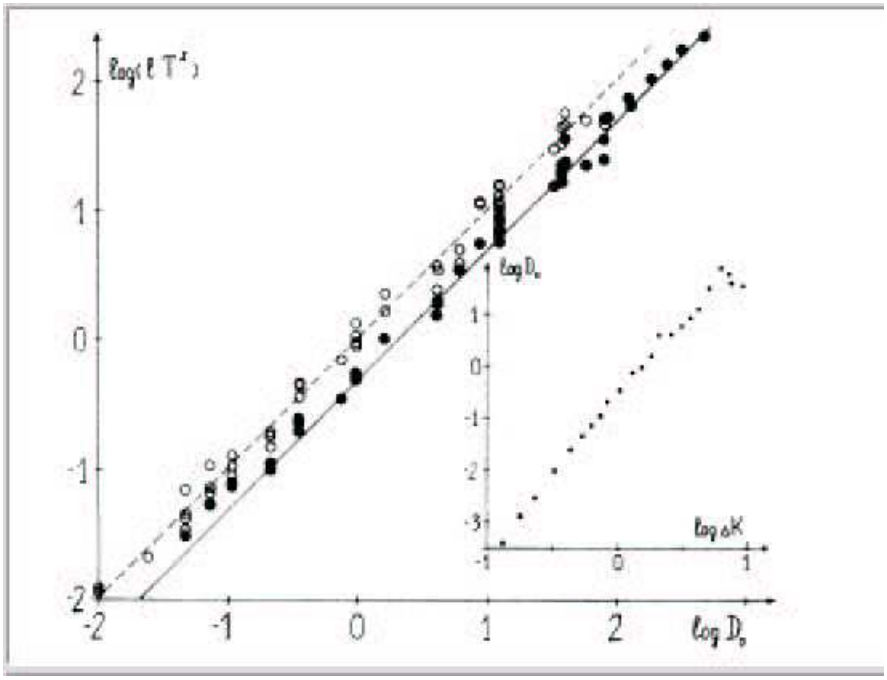


FIG. 1.8 – La dépendance de la longueur de localisation du coefficient de diffusion D_0 de l'application standard classique selon [32]. Les disques blancs représentent les données numériques pour la longueur de localisation des distributions stationnaires, c'est-à-dire des distributions moyennes par rapport au temps. La ligne tiretée correspond au moyen. Les disques noirs montrent les longueurs de localisation obtenues des fonctions propres de quasiénergie par la méthode d'exposante de Lyapunov minimale. La ligne continue montre la localisation théorique $l = D/2$. L'encart montre la dépendance de D_0 de $\Delta K = K - K_{cr}$, $K_{cr} = 0.971635$.

L'équation de Schrödinger pour les états propres de quasiénergie (l'équation de Floquet)

$$U\psi' = U_2 U_1 \psi' = e^{-i\nu}\psi' \tag{1.13}$$

peut être réécrite dans la forme $U_1\psi' = e^{-i\nu}U_2^{-1}\psi'$ ou d'une manière équivalente,

$$(1 \pm U_1)\psi' = (1 \pm e^{-i\nu}U_2^{-1})\psi'. \tag{1.14}$$

En introduisant la notation $\psi = (1 + U_1)\psi' = (1 + e^{-i\nu}U_2^{-1})\psi'$, on peut transformer l'équation précédente vers la forme

$$\frac{(1 - U_1)}{(1 + U_1)}\psi = -\frac{(1 - U_2 e^{i\nu})}{(1 + U_2 e^{i\nu})}\psi. \tag{1.15}$$

Après la substitution de U_1 et U_2 par les expressions explicites, on obtient

$$\tan(\frac{1}{2}(\nu - TH_0))\psi + \tan(\frac{k}{2}V)\psi = 0. \tag{1.16}$$

C'est l'équation de Schrödinger pour le modèle d'Anderson, où le premier terme joue le rôle de $(v_{\mathbf{n}} - E)\psi_{\mathbf{n}}$ et où le deuxième joue le rôle de $\sum_{\mathbf{m}} w_{\mathbf{m}}\psi_{\mathbf{m+n}}$ avec $w_{\mathbf{m}}$ qui sont les composantes de Fourier de $\tan(\frac{k}{2}V(\theta, \theta_1, \theta_2))$. Le choix particulier du potentiel

$$V = \frac{2}{k}\arctan(E - \sum_{j=1}^{d}\cos\theta_j) \tag{1.17}$$

mène à un modèle avec les transitions entre les sites voisins seulement. Ce modèle, avec la statistique de désordre résultante de Eq. (1.16), est connu sous le nom de modèle de Lloyd.

On peut considérer plus particulièrement le cas d'une application quantique à trois dimensions : $H_0 = H_0(n, n_1, n_2)$, $V = V(\theta, \theta_1, \theta_2)$, qui correspond au modèle d'Anderson tridimensionnel avec la transition de phase. L'étude numérique de ce modèle à trois dimensions est compliqué, mais il existe heureusement une méthode qui permet de réduire ce modèle à un système unidimensionnel avec la modulation temporelle [34, 35]. Il faut, pour cela, choisir H_0 qui est une fonction linéaire de n_1 et de n_2 :

$$H_0(n, n_1, n_2) = H_0(n) + \Omega_1 n_1 + \Omega_2 n_2,$$

. En passant par le système de coordonnées en rotation avec des fréquences angulaires Ω_1 et Ω_2 autour des directions respectives, on obtient dans cette représentation nouvelle, l'hamiltonien suivant :

$$H = H_0(n) + kV(\theta, \theta_1 - \Omega_1 t, \theta_2 - \Omega_2 t)\sum_m \delta(t - mT) \tag{1.18}$$

Maintenant, les angles θ_1 and θ_2 sont bien évidemment conservés et le système devient unidimensionnel. Ce modèle avec sa transition entre les régimes diffusifs et localisés a été étudié en détail dans [34, 35, 36]. Les résultats de ces simulations numériques sont présentés dans la Fig.1.9(a) pour le modèle de Lloyd avec le potentiel (1.17) et dans la Fig.1.9(b) avec le potentiel

$$V = k(1 + \epsilon\cos\theta_1\cos\theta_2)\cos\theta\,. \tag{1.19}$$

Dans le quatrième chapitre, nous présenterons un algorithme quantique efficace pour la simulation de ce modèle, ce qui donnera le moyen d'étudier la transition d'Anderson.

1.3 Ordinateurs quantiques et decohérence

1.3.1 La decohérence. Les portes avec bruit aléatoire

L'obstacle principal à la réalisation pratique de l'information quantique est la perte de cohérence provoquée par les interactions avec l'environnement et par les interactions à l'intérieur du système. On peut mettre en relief les trois sources majeures de la decohérence

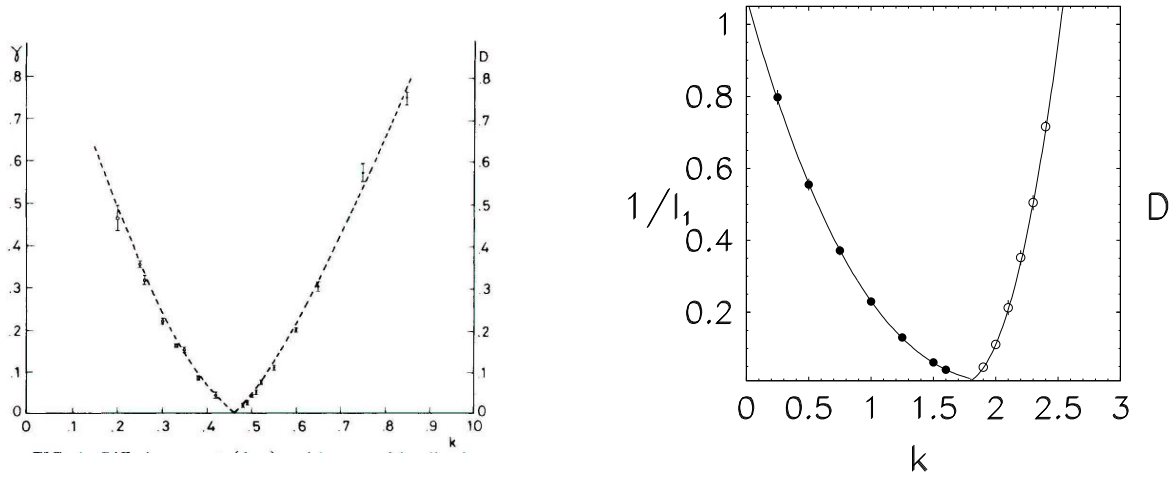


FIG. 1.9 – (a) Le coefficient de diffusion D (points) et la longueur de localisation inverse $\gamma = 1/l$ (cercles) en fonction du paramètre de perturbation k pour le modèle de Lloyd Eq.(1.17) selon [34]. (b) La même chose pour le modèle (1.18), avec le potentiel de (1.19) selon [36].

dans les ordinateurs quantiques. Premièrement, il y a l'interaction avec l'environnement (pour une revue, voir [37]). Dans ce cas-ci, la simulation numérique directe est difficile car le système de l'ordinateur quantique et l'environnement ont une dimension trop grande de l'espace d'Hilbert, ce qui exige une quantité importante de mémoire et un temps de calcul prolongé. C'est pourquoi l'effet de l'environnement est souvent modélisé par application au registre quantique des transformations unitaires aléatoires. Cette approche ne permet pas de reproduire exactement l'effet d'environnement mais, en règle générale, elle reproduit ces traites qualitativement. En pratique, il est convenable d'introduire ce bruit unitaire comme les erreurs aléatoires dans les portes [38, 39, 40, 41]. Par exemple, on peut ajouter des petits décollages dans les phases de valeurs propres des portes. Outre la decohérence dûe à l'environnement, ce modèle peut être interprété comme une description de la précision finie de la réalisation des portes, ce qui amènera des erreurs aléatoires.

La mesure naturelle de la précision de reproduction d'un état pur quantique est sa fidélité, définie comme la probabilité de trouver le système en état désirable :

$$f(t) = |\langle\psi_0(t)|\psi_\epsilon(t)\rangle|^2. \tag{1.20}$$

Alors que cette quantité reste proche de l'unité, l'état réel reste proche de l'état idéal. Dans la majorité des cas, la fidélité d'ordre de l'unité est encore acceptable car la probabilité

de trouver le système en état désirable est aussi de l'ordre de l'unité. Quand la fidélité chute considérablement vers le zéro, le travail de l'ordinateur quantique devient inutile. La condition qui demande que la fidélité doit rester de l'ordre de l'unité, impose une restriction sur le nombre de portes maximales que l'ordinateur quantique peut exécuter. Comment s'ajoutent les erreurs qui proviennent des différentes portes ? Dans la mesure où les erreurs sont aléatoires et indépendantes, c'est de celles-ci au carré qui s'ajoutent et l'erreur après le nombre n_g des portes a l'ordre de grandeur de $\sqrt{n_g}\epsilon$. Alors, la condition $\sqrt{n_g}\epsilon \sim 1$ amène au nombre des portes qui peuvent être exécutées avant la perte de la cohérence égale à $n_g \sim 1/\epsilon^2$. Dans le cas opposé où des erreurs statiques indépendantes du temps apparaitraient, les erreurs s'ajoutent simplement et l'erreur après l'exécution de n_g portes est $n_g\epsilon$. Par conséquent, le nombre maximal de portes sera dans ce cas précis de l'ordre de $n_g \sim 1/\epsilon$. Évidemment, les erreurs statiques sont plus dangereuses que le bruit aléatoire de même magnitude. Nous étudierons plus en détail les effets des erreurs statiques dans la prochaine sous-section.

1.3.2 Imperfections statiques

Les effets des imperfections statiques peuvent être étudiés dans le modèle présenté dans [42]. Dans ce modèle, le matériel d'ordinateur quantique est décrit par l'hamiltonien H :

$$H = \sum_i \frac{\Delta}{2}\sigma_i^z + H_S, \quad H_S = \sum_i a_i\sigma_i^z + \sum_{i<j} b_{ij}\sigma_i^x\sigma_j^x. \tag{1.21}$$

Ici, σ_i sont les matrices de Pauli pour les qubits i et Δ est la différence moyenne entre les niveaux d'énergie d'un qubit. Tous les n_{tot} qubits sont placés sur un réseau rectangulaire et la deuxième somme dans H_S est sur les qubits proches voisins avec les conditions au bord périodiques. 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. Après [15, 43, 44, 4], nous supposons que la différence moyenne de niveaux δ est compensée par des impulsions de laser particulièrement appliquées de sorte qu'entre les portes élémentaires consécutives, l'évolution de la fonction d'onde soit donnée par le propagateur $U_s = \exp(-iH_S t_g)$. Ainsi, toutes les erreurs statiques sont exprimées par l'intermédiaire de ce propagateur tandis que les portes élémentaires sont considérées comme parfaites. Le changement approprié des paramètres a_i et b_{ij} laisse mettre $t_g = 1$ sans aucune perte de généralité. Nous concentrons nos études sur le cas $\alpha = \beta \equiv \varepsilon$ où les couplages entre qubits mènent au chaos quantique développé [42, 15].

Pour commencer, on peut tout d'abord étudier les effets des imperfections statiques sur une mémoire quantique, c'est-à-dire sur un ordinateur quantique sans aucun algorithme, d'après [42]. Dans ce cas-ci, l'évolution temporelle de l'ordinateur est entièrement décrite par l'hamiltonien (1.21). Avec le couplage entre qubits égal à zéro $\beta = 0$, les vecteurs de la base de calcul sont les vecteurs propres de l'hamiltonien et par conséquent sont préservés par l'évolution temporelle. Pour la constante de couplage β suffisamment petite , on peut traiter l'interaction comme une petite perturbation et les vecteurs propres à l'hamiltonien restent voisins des valeurs non perturbées. La théorie de perturbation peut être appliquée

quand les éléments de matrice de perturbation sont bien plus petits que les différences d'énergie entre les niveaux correspondants. Le régime de la perturbation suffisamment forte, si la théorie de perturbation n'est pas applicable, est connu sous le nom de chaos quantique et la transition correspondante entre les régimes s'appelle la transition au chaos.

Estimons la distance moyenne entre les niveaux d'énergie. Dans le cas de Δ différent de zéro, la taille de l'intervalle qui inclut toutes les valeurs propres est de l'ordre de $n_q\Delta$. Si Δ est zéro, alors la taille d'intervalle est de l'ordre de $\sqrt{n_q}\alpha$. Le nombre de niveaux dans cet intervalle est la dimension de l'espace d'Hilbert $N = 2^{n_q}$. La séparation moyenne Δ_{n_q} des niveaux d'énergie est le rapport de l'intervalle de l'énergie avec le nombre de niveaux dans celle-ci. On a $\Delta_{n_q} = n_q\Delta/N$ avec Δ différent de zéro et $\Delta_{n_q} = \sqrt{n_q}\alpha/N$ si $\Delta = 0$. En raison de la dimension de l'espace d'Hilbert exponentiellement grande, la séparation des niveaux augmente exponentiellement avec le nombre de qubits. Si on le compare aux éléments de matrice de perturbation, on pourrait penser que la validité de la théorie de perturbation se termine déjà pour des perturbations exponentiellement petites. Cependant, comme on l'a précisé dans [42], le problème n'est pas aussi simple, puisque l'interaction est toujours de nature de deux-corps et que tous les états multi-qubits ne sont pas directement couplés. En fait, le nombre d'états directement couplés à un état de registre quantique n'augmente pas plus vite que quadratiquement avec n_q. Ce problème existe déjà dans d'autres systèmes physiques à plusieurs corps avec interaction, tels que les noyaux, les atomes complexes, les points quantiques et les verres de spin quantiques.

On a réalisé que l'interaction suffisamment forte mène au chaos quantique et à la thermalisation interne (dynamique), où les propriétés d'états propres suivent les prévisions de la théorie des matrices aléatoires (RMT). La frontière de chaos quantique pour cette thermalisation dynamique a été établie tout récemment et il a été démontré que la magnitude de couplage dans le régime chaotique devrait être plus grande que la distance moyenne entre les niveaux d'énergie d'états directement couplés Δ_c. Puisque Δ_c tombe algébriquement avec n_q, elle est exponentiellement plus grande que $\Delta_n \sim n2^{-n}\Delta_0$ et il est donc nécessaire d'avoir une force de couplage relativement grande pour l'apparition du chaos et de l'ergodicité quantique. La valeur critique de la constante de couplage β_c peut être trouvée selon la condition suivante :

$$\beta_c \approx \Delta_c \approx C\alpha/\sqrt{n_q}, \tag{1.22}$$

où C est une constante. Une telle frontière pour les systèmes de qubits avec l'interaction permettrait un régime raisonnable de la stabilité de la "mémoire quantique".

Dans le domaine du chaos quantique, il est bien connu que la transition aux états propres ergodiques est reflétée dans la transition dans la statistique de séparations des niveaux entre la distribution de Poisson pour les états non-ergodiques et la distribution de Wigner-Dyson (WD) $P_W(s) = (\pi s/2)\exp(-\pi s^2/4)$, correspondant à RMT, pour les états ergodiques. Ici, s est la distance mesurée entre les niveaux les plus proches dans les unités de la distance moyenne où $P(s)$ est la probabilité de trouver deux niveaux adjacents dont la séparation est dans l'intervalle $[s, s + ds]$. La statistique de séparations des niveaux pour l'hamiltonien (1.21) a été étudiée dans [42]. On peut voir un exemple de la transition dans la statistique spectrale dans Fig.1.10. Le modèle (1.21) a deux classes

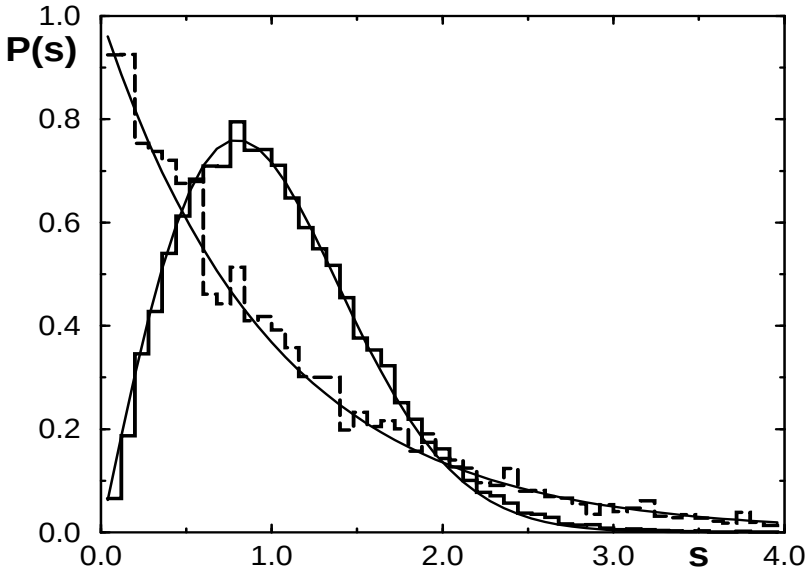


FIG. 1.10 – Transition de la statistique de Poisson vers la statistique WD dans le modèle (1.21) pour les états au milieu de la bande d'énergie selon [42] ($\pm 6.25\%$ autour du centre) pour n_q=12 : $J/\Delta_0 = 0.02, \eta = 1.003$ (l'histogramme à ligne tiretée) ; $J/\Delta_0 = 0.48, \eta = 0.049$ (l'histogramme à ligne complète). Les lignes complètes montrent $P_P(s)$ et $P_W(s)$; $N_S > 2.5 \times 10^4$, $N_D = 100$, $\delta = \Delta_0$.

de symétrie caractérisées par le nombre de qubits en état $|1\rangle$ pair ou impair et les données sont présentées pour une classe de symétrie. Les valeurs propres et les vecteurs propres ont été calculés par la diagonalisation exacte de la matrice hamiltonienne (1.21) pour chaque réalisation.

1.4 Intrication quantique

L'intrication quantique est un phénomène exclusivement quantique, qui n'existe pas en mécanique classique. On dit qu'il y a intrication entre différentes parties d'un système quantique si l'état du système ne peut être représenté comme un produit des états de ses sous-systèmes ou comme un mélange statistique des produits. Par exemple, on dit que l'état singulet de deux spins 1/2

$$\Psi^- = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \tag{1.23}$$

est intriqué. Les spins dans cet état peuvent être considérablement éloignés l'un de l'autre en espace, mais ils auront toujours des directions opposées, une fois qu'il auront été mesurés par rapport à un axe quelconque. C'est le célèbre effet d'Einstein-Podolsky-Rosen

[45]. Bell [46] et Clauser *et al.* [47] ont prouvé que les statistiques de cet état violent les inégalités qui doivent être satisfaites dans tous les modèles avec variables cachées. La confirmation expérimentale répétitive [48] des corrélations non-locales prévues par la mécanique quantique est considérée comme une évidence qui renforce sa nécessité.

L'intrication quantique permet de réaliser un grand nombre de nouvelles applications de la mécanique quantique dans les domaines du calcul, de la communication et de la cryptographie. Pour donner un exemple de ce type d'applications, décrivons brièvement l'effet de téléportation quantique. Cet effet consiste à envoyer d'un lieu vers un autre lieu un état inconnu quantique sans le mesurer préalablement. Pour être capable d'effectuer la téléportation on doit auparavant partager un état intriqué entre l'expéditeur et le récepteur et être aussi en mesure de pouvoir envoyer l'information classique. Dans la situation la plus simple, on veut transmettre l'état d'un spin 1/2 en utilisant une paire intriquée de particules de spin 1/2 dans l'état singulet ψ^- (1.23). D'abord, l'expéditeur effectue la mesure dans la base de Bell sur sa paire de particules de spin 1/2 (une de ces deux particules est la particule dont l'état doit être envoyé et l'autre est la moitié d'expéditeur de la paire intriquée partagée). La base de Bell se compose de l'état singulet ψ^- et des trois états du triplet

$$\Psi^+ = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle) \tag{1.24}$$

$$\Phi^\pm = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle). \tag{1.25}$$

Ensuite l'expéditeur communique le résultat de sa mesure au récepteur. Si le résultat de mesure était que la paire est dans l'état de singulet, alors la particule de récepteur sera déjà dans l'état qu'on a voulu transmettre par la téléportation. Dans l'autre cas, si la paire était trouvée dans un des états de triplet, le récepteur doit alors appliquer une certaine transformation unitaire à sa particule, selon laquelle des états de triplet ont été trouvés. Finalement, après cette transformation, la particule du récepteur sera dans l'état téléporté.

Une des tâches de base de la théorie de l'information quantique est de définir les caractéristiques quantitatives appropriées de *combien* un état est intriqué. Une mesure simple et universelle existe uniquement dans le cas de deux sous-systèmes dans un état pur. Pour un état pur ψ d'un système composé de sous-systèmes A et B, l'intrication $E(\psi)$ est donnée par l'entropie de sa matrice de densité réduite :

$$E(\psi) = S(\mathrm{Tr}_B(|\psi\rangle\langle\psi|)) = S(\mathrm{Tr}_A(|\psi\rangle\langle\psi|)), \tag{1.26}$$

où S est l'entropie de von Neumann : $S(\rho) = -\mathrm{Tr}\rho\log_2\rho$. Ici et plus loin, le symbole Tr avec des indices inférieurs signifie la trace partielle de sous-système correspondant (le sous-système B ou A dans ce cas-ci) en considérant uniquement des systèmes avec les espaces d'Hilbert de dimension finie.

Contrairement au cas d'état pur, les différents aspects de l'intrication des mélanges statistiques sont caractérisés par des mesures différentes. Par exemple, *le coût d'intrication*, soit la quantité d'intrication nécessaire pour préparer un état indiqué, diffère généralement

de l'*intrication distillable*, soit la quantité d'intrication qui peut être extraite à partir d'un état indiqué. Une des mesures les plus importantes et les plus répandues est *l'intrication de formation* (IDF). Il a été présenté dans la [49] comme l'intrication moyenne minimum de tous les ensembles d'états purs réalisant ρ :

$$E_F(\rho) = \min_{\{p_i,\psi_i\}} \sum_i p_i E(\psi_i), \tag{1.27}$$

où un ensemble $\{p_i, \psi_i\}$ réalise ρ si $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, c'est-à-dire si l'état pur ψ_i peut être trouvé dans ρ avec la probabilité p_i. Nous appellerons *ensemble optimal* de ρ un ensemble pour lequel le minimum est atteint.

Une autre mesure d'intrication, proposée pour la première fois dans [50] est basée sur l'idée que l'intrication devrait être zéro pour l'ensemble des matrices de densités séparables et devrait augmenter tandis que nous nous éloignons de cet ensemble. Une telle fonction pourrait être regardée comme une fonction qui mesure un certain genre de distance de l'état à l'ensemble d'états séparables. Si on prend cette idée littéralement et que l'on emploie l'entropie relative [51]

$$S(\rho, \sigma) = \mathrm{Tr}\rho(\log \rho - \log \sigma) \tag{1.28}$$

pour mesurer la "distance", on arrive à *l'entropie relative d'intrication*

$$E_{\mathrm{RE}}(\rho) = \inf\{S(\rho, \sigma), \quad \sigma \quad \text{est séparable}\}. \tag{1.29}$$

On employait aussi d'autres fonctions de distance auparavant pour définir des mesures d'intrication. Cependant, celle basée sur l'entropie relative est la seule proposition qui coïncide avec le choix "canonique" décrit dans Eq. (1.26)sur les états purs. Puisque E_{RE} s'avère facilement convexe, il doit être plus petit que la plus grande fonction convexe avec cette propriété, à savoir E_f.

L'interprétation physique de l'IDF dépend du fait qu'elle soit additive ou non. 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 continuant de considérer 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. On a conjecturé que l'IDF est additive :

$$E_F(\rho_1 \otimes \rho_2) \stackrel{?}{=} E_F(\rho_1) + E_F(\rho_2), \tag{1.30}$$

c'est à dire l'IDF du système composé égale la somme des IDF de ses pièces. Cela est évidemment vrai dans le cas des états purs ρ_1 et ρ_2. Cette conjecture d'additivité a été prouvée pour quelques classes particulières d'états (voir [52]). De plus, la conjecture est soutenue par un certain nombre de calculs numériques et aucun contre-exemple n'a été jusqu'à présent trouvé.

Il est connu [53], que le coût d'intrication E_C d'un état ρ est égal au rapport asymptotique de l'IDF des n copies de l'état ρ au nombre de copies n, c'est à dire $E_C = \lim_{n\to\infty} E_F(\rho^{\otimes n})/n$. Si la conjecture d'additivité est vraie, alors l'IDF nous donne le coût

d'intrication ($E_C = E_F$), ce qui simplifierait considérablement le problème du calcul pratique de E_C.

Il est naturel de considérer un problème plus général qui consiste à comparer l'IDF d'un système à la somme des IDF de ses sous-systèmes. De plus, il a été conjecturé [54, 55] que le précédent n'est pas moins que le dernier :

$$E_F(\rho) \stackrel{?}{\geq} E_F(\mathrm{Tr}_2\rho) + E_F(\mathrm{Tr}_1\rho). \tag{1.31}$$

On appelle cette propriété la superadditivité forte. Elle est intéressante non seulement pour ce qu'elle représente mais aussi parce qu'elle implique l'additivité de l'IDF [54, 55].

Il est bien connu [55], que la superadditivité forte de l'IDF implique aussi l'additivité de la capacité classique de Holevo-Schumacher-Westmorland d'un canal quantique. Le problème de l'additivité de cette quantité est d'importance considérable pour la théorie de communication quantique [56], mais reste encore sans solution dans le cas général, bien que l'additivité a été prouvée pour quelques classes particulières de canaux quantiques (pour un exemple important, voir le [57]). Ici, nous découvrons un lien encore plus étroit entre le superadditivité forte de l'IDF, l'additivité de l'IDF et l'additivité de la capacité de canal classique : nous prouvons que l'additivité de l'IDF *implique la superadditivité forte* et que, par conséquent, ces deux conjectures sont équivalentes et impliquent l'additivité de la capacité de canal classique.

Chapitre 2

L'équivalence des conjectures de l'additivité et de la superadditivité forte de l'intrication de formation

2.1 Convexité et fonction conjuguée

Nous avons vu don le chapitre précédent que l'intrication de formation est une des mesures les plus utilisées de l'intrication. Une des plus importantes propriétés de l'IDF est sa convexité. La convexité signifie que pour un ensemble de matrices de densité ρ_i et de probabilité p_i quelconque, l'IDF de la matrice de densité moyenne $\rho = \sum_i p_i \rho_i$ n'est pas plus grande que l'IDF moyenne :

$$E_F(\rho) \leq \sum_i p_i E_F(\rho_i). \tag{2.1}$$

Pour se convaincre de la convexité de l'IDF, on peut considérer l'état ρ comme si ce dernier était préparé selon le procédé suivant : prendre avec la probabilité p_i un index i puis préparer le système dans un état pur choisi d'un ensemble optimal de ρ_i, avec la probabilité correspondante à cet état pur dans l'ensemble. L'intrication moyenne pour l'ensemble d'états purs résultant est égale au membre droit de l'Eq. (2.1) et l'intrication moyenne minimale $E_f(\rho)$ ne peuvent être plus grandes que cela.

Introduisons la notion indispensable de la fonction conjuguée de l'IDF suivant [58]. La transition d'une fonction à sa conjuguée est une opération standard de l'analyse convexe [61] et en ce qui concerne l'IDF, nous obtenons la fonction d'une matrice hermitienne H suivante :

$$E^*(H) = \max_{\rho} \left[\mathrm{Tr}(\rho H) - E_F(\rho) \right], \tag{2.2}$$

où la maximisation est exécutée sur toutes les matrices de densité ρ. Au lieu de cela, on peut maximiser sur tous les états purs seulement [58] :

$$E^*(H) = \max_{\psi} \left[\langle \psi | H | \psi \rangle - E(\psi) \right], \tag{2.3}$$

parce que l'expression $E_f(\rho)$ est l'intrication moyenne pour un ensemble d'états purs ψ_i ; le membre droit entier (2.2) est donc également une moyenne :

$$\mathrm{Tr}(\rho H) - E_F(\rho) = \sum_i p_i \left[\langle\psi_i|H|\psi_i\rangle - E(\psi_i)\right] \tag{2.4}$$

et une moyenne ne peut pas être plus grande que ces nombres qui entrent dans la moyenne. L'opération de conjugaison qui s'applique deux fois à une fonction convexe laisse cette fonction inchangée [58, 61]. Pour l'IDF, cela signifie que

$$E_F(\rho) = \max_H \left[\mathrm{Tr}(\rho H) - E^*(H)\right], \tag{2.5}$$

où le maximum est cherché parmi toutes les matrices hermitiennes H.

Rappelons maintenant quelques faits bien connus liés aux conjectures d'additivité et de superadditivité forte. Considérons un système déjà étudié dans l'introduction, composé de deux sous-systèmes bipartites 1 et 2 : le sous-système 1 est composé des pièces $1A$ et $1B$ et le sous-système 2 est composé des pièces $2A$ et $2B$. Nous considérons toujours l'intrication entre les sous-systèmes A et B. Une des raisons pour lesquelles la conjecture de superadditivité forte (voir la section 1.4) est intéressante, est qu'elle implique l'additivité de l'IDF [52, 55]. Il est facile de le voir si on considère une décomposition optimale pour ρ_1 :

$$\rho_1 = \sum_i p_i^{(1)} |\psi_i^{(1)}\rangle\langle\psi_i^{(1)}|, \quad E_F(\rho_1) = \sum_i p_i^{(1)} E(\psi_i^{(1)})$$

et une décomposition optimale analogique pour ρ_2. Nous avons une décomposition du produit tensoriel suivante :

$$\rho_1 \otimes \rho_2 = \sum_{ij} p_i^{(1)} p_j^{(2)} |\psi_i^{(1)}\rangle|\psi_j^{(2)}\rangle\langle\psi_j^{(2)}|\langle\psi_i^{(1)}|. \tag{2.6}$$

La moyenne IDF de cette décomposition ne peut pas excéder $E_F(\rho_1 \otimes \rho_2)$:

$$E_F(\rho_1 \otimes \rho_2) \leq \sum_{ij} p_i^{(1)} p_j^{(2)} E(|\psi_i^{(1)}\rangle|\psi_j^{(2)}\rangle) = E_F(\rho_1) + E_F(\rho_2), \tag{2.7}$$

où nous avons employé l'additivité de l'IDF pour les états purs. La propriété ci-dessus s'appelle la sous-additivité. Combinée avec la superadditivité conjecturée, (Eq. (1.31) avec $\rho = \rho_1 \otimes \rho_2$) elle donne l'additivité Eq. (1.30).

Eq. (1.31) est vérifiée pour tous les états ρ si et seulement si elle est vérifiée pour les états purs, c'est-à-dire si pour tous les états purs ψ [52] :

$$E(\psi) \stackrel{?}{\geq} E_F(\mathrm{Tr}_1(|\psi\rangle\langle\psi|)) + E_F(\mathrm{Tr}_2(|\psi\rangle\langle\psi|)). \tag{2.8}$$

Considérons une décomposition optimale de ρ :

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad E_F(\rho) = \sum_i p_i E(\psi_i). \tag{2.9}$$

Si Eq. (2.8) est satisfaite pour tous les états purs ψ_i, alors

$$\begin{aligned} E_F(\rho) &= \sum_i p_i E(\psi_i) \\ &\geq \sum_i p_i \left[E_F(\mathrm{Tr}_2(|\psi_i\rangle\langle\psi_i|)) + E_F(\mathrm{Tr}_1(|\psi_i\rangle\langle\psi_i|))\right]. \end{aligned}$$

En utilisant la linéarité de trace : $\sum_i p_i \mathrm{Tr}_1(|\psi_i\rangle\langle\psi_i|) = \mathrm{Tr}_1\rho$ (idem pour le système 2) et en utilisant la convexité de l'IDF Eq. (2.1), nous obtenons Eq.(1.31) pour l'état ρ.

La conjecture de la superadditivité forte peut être redite en termes de fonction conjuguée $E^*(h)$. À cette fin, faisons la substitution de l'Eq. (2.5) dans le membre droit de l'Eq. (2.8) :

$$\begin{aligned} E(\psi) &\stackrel{?}{\geq} \max_{H_1} \left[\mathrm{Tr}_1(\mathrm{Tr}_2(|\psi\rangle\langle\psi|)H_1) - E^*(H_1)\right] + \max_{H_2} \left[\mathrm{Tr}_2(\mathrm{Tr}_1(|\psi\rangle\langle\psi|)H_2) - E^*(H_2)\right] \\ &= \max_{H_1} \left[\langle\psi|H_1 \otimes 1|\psi\rangle - E^*(H_1)\right] + \max_{H_2} \left[\langle\psi|1 \otimes H_2|\psi\rangle - E^*(H_2)\right]. \end{aligned} \tag{2.10}$$

Une proposition équivalente est que pour tous les ψ, H_1 et H_2

$$E(\psi) \stackrel{?}{\geq} \langle\psi|(H_1 \otimes 1 + 1 \otimes H_2)|\psi\rangle - E^*(H_1) - E^*(H_2). \tag{2.11}$$

On peut le réécrire plus en profondeur comme

$$\langle\psi|(H_1 \otimes 1 + 1 \otimes H_2)|\psi\rangle - E(\psi) \stackrel{?}{\leq} E^*(H_1) + E^*(H_2).$$

L'inégalité ci-dessus est vraie pour tous les ψ si et seulement si elle est vraie pour la valeur maximale du membre gauche de l'équation :

$$\max_{\psi} \left[\langle\psi|(H_1 \otimes 1 + 1 \otimes H_2)|\psi\rangle - E(\psi)\right] \stackrel{?}{\leq} E^*(H_1) + E^*(H_2),$$

c'est-à-dire [58] :

$$E^*(H_1 \otimes 1 + 1 \otimes H_2) \stackrel{?}{\leq} E^*(H_1) + E^*(H_2). \tag{2.14}$$

D'autre part, considérons les vecteurs ψ_1 et ψ_2, optimaux (dans le sens de la définition de la fonction conjuguée dans Eq. (2.2)) pour H_1 et H_2 respectivement. En employant leur produit $|\psi_1\rangle|\psi_2\rangle$ comme une fonction d'essai pour la recherche de $E^*(H_1 \otimes 1 + 1 \otimes H_2)$, nous avons

$$\begin{aligned} E^*(H_1 \otimes 1 + 1 \otimes H_2) &\geq \langle\psi_2|\langle\psi_1|(H_1 \otimes 1 + 1 \otimes H_2)|\psi_1\rangle|\psi_2\rangle - E(|\psi_1\rangle|\psi_2\rangle) \\ &= \langle\psi_1|H_1|\psi_1\rangle - E(\psi_1) + \langle\psi_2|H_2|\psi_2\rangle - E(\psi_2) \\ &= E^*(H_1) + E^*(H_2). \end{aligned} \tag{2.15}$$

Pris ensemble, Eqs. (2.14) et (2.15) permettent de reformuler la conjecture de superadditivité forte comme la conjecture d'additivité pour les fonctions conjuguées suivantes [58] :

$$E^*(H_1 \otimes 1 + 1 \otimes H_2) \stackrel{?}{=} E^*(H_1) + E^*(H_2). \tag{2.16}$$

2.2 Propriétés des vecteurs optimaux

Dans cette section, nous étudions les propriétés des vecteurs pour lesquels le maximum est atteint dans l'Eq. (2.3). Ces propriétés ont été trouvées dans [59] et également dans [60] dans un arrangement légèrement différent. Considérons dans un système bipartite $A - B$, un opérateur hermitien H et un vecteur optimal $\widetilde{\psi}$ (dans le sens de la définition de $E^*(h)$, Eq. (2.3)) :

$$E^*(H) = \langle\widetilde{\psi}|H|\widetilde{\psi}\rangle - E(\widetilde{\psi}). \tag{2.17}$$

Dénotons par $f(\psi)$, la fonction dont le maximum est $E^*(H)$:

$$f(\psi) = \langle\psi|H|\psi\rangle - E(\psi). \tag{2.18}$$

La condition nécessaire pour que la fonction $f(\psi)$ ait un maximum au point ψ est que ses dérivées soient égales a zéro : $\delta f(\psi) = 0$. Pour calculer ces dérivées, nous devons retourner à la définition de $E(\psi)$ et la réécrire plus explicitement dans les termes des composants ψ_{ij} du vecteur $|\psi\rangle$, où le premier index se rapporte au sous-système A et le deuxième index se rapporte au sous-système B. On peut considérer ψ_{ij} comme les composants d'une matrice ψ. Pour cette matrice, la définition de $E(\psi)$ devient

$$E(\psi) = -\mathrm{Tr}(\psi\psi^\dagger \log_2(\psi\psi^\dagger)) = -\mathrm{Tr}(\rho \log_2(\rho)),$$

où $\rho = \psi\psi^\dagger$. On a aussi

$$\langle\psi|H|\psi\rangle = \sum_{ijkl} \psi^*_{ij} H_{ij|kl} \psi_{kl}.$$

Notons que puisque la trace d'un produit des matrices est invariante sous les permutations cycliques, nous avons $\delta\mathrm{Tr}F(\rho) = \mathrm{Tr}(F'(\rho)\delta\rho)$ pour une fonction quelconque d'une variable $F(x)$ et pour sa dérivée $F'(x)$. Afin de le prouver, on peut employer l'expansion de $F(x)$ en série de Taylor. Dans notre cas, $F(x) = -x \log_2 x$ et $F'(x) = -\log_2 x - 1/\ln 2$; ce qui donne

$$\delta E(\psi) = -\mathrm{Tr}((\log_2 \rho + 1/\ln 2)\delta\rho) = -\mathrm{Tr}(\delta\rho \log_2 \rho).$$

En faisant la substitution $\rho = \psi\psi^\dagger$ nous obtenons :

$$\delta E(\psi) = -\mathrm{Tr}(\psi^\dagger \log_2(\psi\psi^\dagger)\delta\psi + \log_2(\psi\psi^\dagger)\psi\delta\psi^\dagger).$$

Pour la variation de $f(\psi)$, nous avons maintenant

$$\delta f(\psi) = \sum_{ijkl} (\delta\psi^*_{ij} H_{ij|kl}\psi_{kl} + \psi^*_{ij} H_{ij|kl}\delta\psi_{kl}) - \delta E(\psi).$$

La variation du vecteur $|\delta\psi\rangle$ est orthogonale à $|\psi\rangle$ dûe à la condition de normalisation $\langle\psi|\psi\rangle = 1$, mais hormis cette condition, la variation est arbitraire. A la place des parties réelles et imaginaires de ses composants $\mathrm{Re}(\delta\psi_{ij})$ et $\mathrm{Im}(\delta\psi_{ij})$, on peut considérer comme

indépendantes leurs combinaisons linéaires complexes $\delta\psi_{ij}$ et $\delta\psi^*_{ij}$. Alors, la condition nécessaire pour le maximum prend la forme :

$$\sum_{kl} H_{ij|kl}\widetilde{\psi}_{kl} + (\log_2(\widetilde{\psi}\widetilde{\psi}^\dagger)\widetilde{\psi})_{ij} = C\widetilde{\psi}_{ij}.$$

En calculant les produits scalaires des deux membres de cette équation avec $\langle\widetilde{\psi}|$, nous constatons que la constante C est égale à $E^*(h)$. En tenant compte de cela, nous avons finalement

$$\sum_{kl} H_{ij|kl}\widetilde{\psi}_{kl} = -(\log_2(\widetilde{\psi}\widetilde{\psi}^\dagger)\widetilde{\psi})_{ij} + E^*(H)\widetilde{\psi}_{ij}. \tag{2.25}$$

Cette équation détermine comment l'opérateur H agit sur les vecteurs optimaux et comment cet opérateur agit sur n'importe quelle combinaison linéaire des vecteurs optimaux. L'hermiticité de H exige que pour une paire de vecteurs optimaux quelconques $\widetilde{\psi}_\alpha$ et $\widetilde{\psi}_\beta$ la condition suivante soit vérifiée [59, 60] :

$$\mathrm{Tr}\left\{\widetilde{\psi}_\alpha\widetilde{\psi}^\dagger_\beta\left[\log_2(\widetilde{\psi}_\alpha\widetilde{\psi}^\dagger_\alpha) - \log_2(\widetilde{\psi}_\beta\widetilde{\psi}^\dagger_\beta)\right]\right\} = 0. \tag{2.26}$$

2.3 Lien entre additivité et superadditivité forte

Nous pouvons à présent établir le lien suivant entre l'additivité et la superadditivité forte de l'intrication de formation. Pour un état quelconque du système entier (composé de quatre parties : $1A$, $1B$, $2A$ et $2B$) avec la matrice de densité correspondante ρ, calculons ses matrices de densité partiellement réduite $\rho_1 = \mathrm{Tr}_2(\rho)$ et $\rho_2 = \mathrm{Tr}_1(\rho)$. Si, pour ces deux matrices de densité ρ_1 et ρ_2, l'IDF est additive, c'est-à-dire si

$$E_F(\rho_1 \otimes \rho_2) = E_F(\rho_1) + E_F(\rho_2), \tag{2.27}$$

alors, l'IDF est fortement superadditive pour l'état ρ :

$$E_F(\rho) \geq E_F(\rho_1) + E_F(\rho_2). \tag{2.28}$$

Nous prouverons cette proposition en quatre étapes.

Étape I. Considérons une matrice hermitienne H, optimale pour $\rho_1 \otimes \rho_2$ dans le sens d'Eq. (2.5), c'est-à-dire

$$E_F(\rho_1 \otimes \rho_2) = \mathrm{Tr}\left[H(\rho_1 \otimes \rho_2)\right] - E^*(H). \tag{2.29}$$

De la définition de fonction conjuguée (Eqs. (2.2) et (2.3)), nous avons aussi :

$$\begin{aligned} E^*(H) &\geq \langle\psi|H|\psi\rangle - E(\psi), \\ E^*(H) &\geq \mathrm{Tr}(H\rho') - E_F(\rho'), \end{aligned} \tag{2.30}$$

pour tous les états purs ψ et toutes les matrices de densité ρ'. Soit

$$\begin{aligned} \rho_1 &= \sum_m p_m^{(1)} |\psi_m^{(1)}\rangle\langle\psi_m^{(1)}|, \\ p_m^{(1)} &> 0, \quad E_F(\rho_1) = \sum_m p_m^{(1)} E(\psi_m^{(1)}) \end{aligned} \tag{2.31}$$

une décomposition optimale pour ρ_1, soit $\{p_n^{(2)}, \psi_n^{(2)}\}$ une décomposition optimale analogique pour ρ_2. Alors, pour tous les m et n, les produits $|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle$ sont les états purs optimaux pour H dans le sens de Eq. (2.3) :

$$E^*(H) = \langle\psi_m^{(1)}|\langle\psi_n^{(2)}|H|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle - E(|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle). \tag{2.32}$$

En effet, en substituant les décompositions optimales dans Eqs. (2.29) et (2.30), nous avons

$$\begin{aligned} E^*(H) &= \sum_{mn} p_m^{(1)} p_n^{(2)} (\langle\psi_m^{(1)}|\langle\psi_n^{(2)}|H|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle \\ &- E(|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle)), \\ E^*(H) &\geq \langle\psi_m^{(1)}|\langle\psi_n^{(2)}|H|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle - E(|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle), \end{aligned}$$

avec toutes les probabilités strictement positives :

$$p_m^{(1)} p_n^{(2)} > 0, \quad \sum_{mn} p_m^{(1)} p_n^{(2)} = 1. \tag{2.33}$$

Cela est évidemment possible seulement si Eq. (2.32) se tient pour tous les m et n.

Étape II. Dénotons par V_1 le sous-espace engendré par les vecteurs $\psi_m^{(1)}$ puis dénotons par $V_1^\perp$ son complément orthogonal et enfin dénotons par V_2 et $V_2^\perp$ les sous-espaces analogiques pour le sous-système 2. Notons que l'état ρ doit être un ensemble de combinaisons linéaires des vecteurs optimaux $|\psi_m^{(1)}\rangle|\psi_n^{(2)}\rangle$, c'est-à-dire un ensemble d'états purs de $V_1 \otimes V_2$:

$$\rho = \sum_k p_k |\phi^k\rangle\langle\phi^k|, \quad \phi^k \in V_1 \otimes V_2. \tag{2.34}$$

En effet, nous avons $\phi^k \in \left[(V_1^\perp \otimes V_2) \oplus (V_1^\perp \otimes V_2^\perp)\right]^\perp$, car pour chaque vecteur $|v\rangle \in V_1^\perp$, la relation d'orthogonalité $\sum_i \phi_{ij}^{k*} v_i = 0$ (le premier index i correspond ici au sous-système 1 et le second index j correspond au sous-système 2) résulte de

$$\sum_{jk} p_k \left| \sum_i \phi_{ij}^{k*} v_i \right|^2 = \langle v|\rho_1|v\rangle = 0. \tag{2.35}$$

De manière analogique, on a $\phi^k \in \left[(V_1 \otimes V_2^\perp) \oplus (V_1^\perp \otimes V_2^\perp)\right]^\perp$ et par conséquent

$$\phi^k \in \left[(V_1^\perp \otimes V_2) \oplus (V_1 \otimes V_2^\perp) \oplus (V_1^\perp \otimes V_2^\perp)\right]^\perp = V_1 \otimes V_2. \tag{2.36}$$

Étape III. Maintenant,démontrons que pour la matrice H de Eq. (2.29), on a

$$\mathrm{Tr}\left[(\rho_1 \otimes \rho_2)H\right] = \mathrm{Tr}(H\rho). \tag{2.37}$$

À cette fin, on ne doit connaître que les éléments de matrice H entre les états de $V_1 \otimes V_2$ (ces éléments matriciels ne sont présents que dans Eq. (2.37)). On peut trouver ces éléments à partir d'Eq. (2.25), en l'écrivant pour un vecteur optimal $|\psi_s^{(1)}\rangle|\psi_t^{(2)}\rangle$ et en calculant les produits scalaires des deux membres de cette équation avec un vecteur optimal $\langle\psi_m^{(1)}|\langle\psi_n^{(2)}|$:

$$\begin{aligned}\langle\psi_m^{(1)}|\langle\psi_n^{(2)}|H|\psi_s^{(1)}\rangle|\psi_t^{(2)}\rangle &= -\mathrm{Tr}\left[\psi_s^{(1)}\psi_m^{(1)\dagger}\log_2(\psi_s^{(1)}\psi_s^{(1)\dagger})\right]\mathrm{Tr}(\psi_t^{(2)}\psi_n^{(2)\dagger}) \\ &- \mathrm{Tr}\left[\psi_t^{(2)}\psi_n^{(2)\dagger}\log_2(\psi_t^{(2)}\psi_t^{(2)\dagger})\right]\mathrm{Tr}(\psi_s^{(1)}\psi_m^{(1)\dagger}) \\ &+ E^*(H)\mathrm{Tr}(\psi_s^{(1)}\psi_m^{(1)\dagger})\mathrm{Tr}(\psi_t^{(2)}\psi_n^{(2)\dagger}).\end{aligned} \tag{2.38}$$

Ici, nous avons écrit les produits scalaires comme les traces des produits de matrices, par exemple $\langle\psi_m^{(1)}|\psi_s^{(1)}\rangle = \mathrm{Tr}(\psi_s^{(1)}\psi_m^{(1)\dagger})$ et nous avons considéré le fait que le logarithme d'un produit tensoriel des matrices est la somme de logarithmes de ces matrices : $\log_2(X\otimes Y) = \log_2(X)\otimes 1 + 1\otimes\log_2(Y)$. Nous avons également employé la multiplicativité de l'opération de trace : $\mathrm{Tr}(X\otimes Y) = \mathrm{Tr}(X)\mathrm{Tr}(Y)$. Il est facile de voir à partir d'Eq. (2.38), que les éléments matriciels de H entre les états de $V_1 \otimes V_2$ ont la forme :

$$\langle\psi'|H|\psi\rangle = \langle\psi'|(H_1 \otimes 1 + 1 \otimes H_2)|\psi\rangle, \tag{2.39}$$

pour certaines matrices H_1 et H_2. Alors Eq. (2.37) résulte de cette formule appliquée à la moyenne $\mathrm{Tr}(H\rho)$.

Étape IV. Maintenant, nous avons tous les moyens nécessaires pour le prouver. En remplaçant ρ' par ρ dans la deuxième inégalité dans Eq. (2.30), nous obtenons l'inégalité suivante :

$$E^*(H) \geq \mathrm{Tr}(H\rho) - E_F(\rho), \tag{2.40}$$

Si on utilise Eqs. (2.29) et (2.27) pour trouver $E^*(H)$, cette inégalité prend la forme suivante :

$$\mathrm{Tr}\left[H(\rho_1 \otimes \rho_2)\right] - E_F(\rho_1) - E_F(\rho_2) \geq \mathrm{Tr}(H\rho) - E_F(\rho).$$

Finalement, en prenant en compte Eq. (2.37), on obtient l'inégalité (2.28) qui conclut notre preuve.

Le théorème ci-dessus montre que la superadditivité forte de l'IDF est vérifiée pour un état ρ si l'additivité se tient pour ses matrices de densité réduite ρ_1 et ρ_2. Alors, il devient clair que la superadditivité forte de l'IDF pour tous les états du système résulte de l'additivité de l'IDF pour tous les états ρ_1 et ρ_2 des sous-systèmes 1 et 2. Si la conjecture d'additivité n'est généralement pas vraie, le théorème ci-dessus sera encore utile car il relie la superadditivité forte d'un état à l'additivité pour ses matrices de densité réduite ρ_1 et ρ_2 seulement et n'exige pas d'additivité pour tous les états.

Ce travail a été publié et correspond à la référence [2] (voir article I en appendice). Après que ce travail a été terminé, le preprint [62] par P.W. Shor est apparu, qui contient

entre autres résultats une preuve de l'équivalence de l'additivité et de la superadditivité forte de l'IDF qui est le résultat principal de ce chapitre. Notre preuve est analogique à celle de [62] mais utilise un langage différent. Ce deux preprints sont apparus sur le base de données arXiv à quelques jours d'intervalle (quant-ph/0305035 et quant-ph/0305056).

Chapitre 3

Entropie moyenne informationnelle des états quantiques

3.1 Définition et propriétés de l'entropie informationnelle

En mécanique classique, l'état statistique d'un système est décrit par la fonction de probabilité, alors qu'en mécanique quantique, il est décrit par une matrice de probabilité. L'entropie informationnelle S est la quantité d'information supplémentaire nécessaire pour prévoir les résultats d'une mesure. Si aucune information supplémentaire n'est nécessaire, nous disons que le système est dans un état statistique défini avec l'entropie égale à zéro. Si un système classique est préparé dans un état défini, on peut prévoir le résultat de n'importe quelle mesure. Mais, cela n'est pas vrai pour un système quantique. Chaque état pur est un état défini pour certaines mesures, mais pas forcément pour les autres. Même si le système est préparé dans un état pur, il reste une *incertitude* inhérente concernant les résultats d'une mesure générique. Par conséquent, l'entropie informationnelle d'un état quantique est plus grande que zéro pour une mesure générique.

Il est clair que la définition usuelle de l'entropie de Von-Neumann en mécanique quantique ne reflète pas l'incertitude inhérente généralement associée aux états quantiques. Pour un état pur, elle donne $S = 0$. Supposons que nous avons préparé deux spins 1/2 dans l'état singulet. Dans ce cas précis, l'entropie de Von-Neumann d'un seul spin est $S = \ln(2)$, alors que l'entropie du système entier est $S = 0$. Si on pouvait fournir à ces résultats une interprétation dans le cadre de la théorie de l'information, cela supposerait que la quantité d'information nécessaire pour déterminer les résultats d'une mesure d'un sous-système serait plus grande que la quantité d'information qui est exigée pour déterminer les résultats d'une mesure du système entier. Cette conclusion ne semble pas avoir de sens.

Ainsi, nous sommes confrontés à la nécessité de donner une définition appropriée pour l'entropie informationnelle d'un état quantique. Comme dans le cas de l'entropie de Von-Neumann, elle peut être considérée comme une mesure pour le manque de pureté d'un état (mélangé) général. Mais, à la différence de l'entropie de Von-Neumann, elle ne donne

pas $S = 0$ pour les états purs et elle ne coïncide pas avec l'entropie thermodynamique en cas d'état thermique.

Dans ce chapitre, nous présentons une définition de l'entropie informationnelle quantique qui est basée sur la définition de Shannon dans le cas classique, dérivons les expressions explicites pour le calcul de cette entropie et discutons de certaines de ses propriétés. Pour une revue de la définition de l'entropie traditionnelle dans le contexte du calcul quantique et de l'information quantique, voir [63].

L'état statistique d'un système classique, qui peut être trouvé dans N états possibles r, est caractérisé par les probabilités correspondantes p_r, avec la normalisation $\sum p_r = 1$. La quantité d'information exigée pour prévoir les résultats d'une mesure quantique est fournie par la formule de Shannon : $\mathcal{S} = -\sum_r p_r \ln(p_r)$. Notez que $S = 0$ si le système est dans un état défini, tandis que $S = \ln(N)$ dans le plus mauvais cas d'une distribution uniforme. Cette définition coïncide avec la définition de l'entropie de Boltzmann, si r sont considérées comme les cellules dans l'espace de phase.

En mécanique quantique, l'état statistique d'un système est décrit par une matrice de densité ρ. Une mesure est spécifiée par une base des états (purs) $|a\rangle$. Sans aucune perte de généralité, on peut définir cette base en indiquant un opérateur hermitien $\mathcal{A}$. Notons que dans le contexte semi-classique, la base $\mathcal{A}$ peut être considérée comme une *partition* de l'espace de phase par les mailles. La probabilité d'avoir a comme le résultat d'une mesure est $\langle a|\rho|a\rangle$. Par conséquent, l'entropie informationnelle pour cette mesure est

$$S[\rho|\mathcal{A}] = -\sum_a \langle a|\rho|a\rangle \ln(\langle a|\rho|a\rangle) \tag{3.1}$$

Notre notation souligne le fait que cette définition est celle d'une d'entropie conditionnelle. Ceci signifie que nous connaissons déjà la base de mesure. Plus particulièrement, il y a une base $\mathcal{H}$ dans laquelle ρ est diagonale : $\rho = \mathrm{diag}\{p_r\}$. L'entropie de Von-Neumann est définie comme

$$S_{\text{H}}[\rho] = S[\rho|\mathcal{H}] = -\sum_r p_r \ln(p_r). \tag{3.2}$$

Ainsi, nous pouvons voir que la définition de Von-Neumann assume une pré-connaissance d'une base préférée pour laquelle l'entropie d'information (conditionnelle) est minimale. En mécanique statistique d'équilibre, l'intérêt se porte sur les états stationnaires. Cela signifie que ρ est diagonal dans la base qui est déterminée par l'hamiltonien $\mathcal{H}$. Par conséquent, si nous mesurons l'énergie du système, l'entropie informationnelle est effectivement $S_{\text{H}}[\rho]$. Ceci est particulièrement vrai pour l'état canonique $\rho \propto \exp(-\beta\mathcal{H})$, où elle se réduit à la définition de l'entropie thermodynamique.

Pour un état quantique pur $\rho = |\Psi\rangle\langle\Psi|$, la définition de Von-Neumann donne $S_{\text{H}}[\rho] = 0$. Cela semble impliquer qu'il manquerait une nature statistique pour un état quantique pur. Naturellement, cela n'est pas correct. Pour une mesure générale, nous avons *l'incertitude*. La définition d'entropie informationnelle quantique ne devrait assumer aucune base spéciale. Par conséquent, nous suggérons la définition la plus naturelle suivante :

$$S[\rho] \;=\; \overline{S[\rho|\mathcal{A}]} \;=\; S_0(N) + F(p_1, p_2, ...) \tag{3.3}$$

où la quantité surlignée est la moyenne de toutes les bases possibles avec la mesure uniforme (aucune base préférée) de GUE (ensemble unitaire gaussien). La deuxième égalité dans l'Eq.(3.3) (que nous allons dériver ci-dessous) indique que le résultat peut être écrit comme la somme de deux termes. Le premier terme est *l'entropie d'incertitude minimale* d'un état quantique qui est attenit par un état pur, alors que le deuxième terme donne la déviation de la pureté. Nous appellerons le deuxième terme, l'entropie statistique excessive et nous emploierons la notation

$$S_{\text{F}}[\rho] = S[\rho] - S_0(N) = F(p_1, p_2, ...) \tag{3.4}$$

De manière conceptuelle, il est significatif de se demander dans quelle mesure $S_{\text{F}}[\rho]$ est corrélée avec $S_{\text{H}}[\rho]$.

Supposons que $\rho = \text{diag}\{p_r\}$ est diagonale dans une base $\mathcal{H}$. On peut considérer toutes les bases possibles $\mathcal{A}$ comme les "rotations" unitaires de $\mathcal{H}$. Par conséquent,

$$\begin{aligned}
S &= \overline{\sum_a f\left(\sum_r p_r |\langle r|a\rangle|^2\right)}^{A} && (3.5)\\
&= \overline{\sum_s f\left(\sum_r p_r |\langle r|U|s\rangle|^2\right)}^{U} && (3.6)\\
&= \overline{Nf\left(\sum_r p_r |\langle r|\Psi\rangle|^2\right)}^{\Psi} && (3.7)\\
&= \overline{Nf\left(\sum_r p_r (x_r^2 + y_r^2)\right)}^{\text{sphere}} && (3.8)\\
&= N\int_0^\infty f(s)\ P(s)ds && (3.9)
\end{aligned}$$

où nous utilisons la notation $f(s) = -s\ln(s)$. Dans Eq.(3.5), la moyenne s'applique à toutes les bases possibles $\mathcal{A}$, tandis que dans Eq.(3.6), la moyenne s'applique à toutes les transformations unitaires possibles U. Chaque terme dans Eq.(3.6) est équivalent à la moyenne sur tous les Ψ possibles. Cela mène à Eq.(3.7). Dans Eq.(3.8), nous définissons x_r et y_r comme les parties réelles et imaginaires de $\Psi_r = \langle r|\Psi\rangle$, avec la condition de normalisation $\sum_r (x_r^2 + y_r^2) = 1$. Dans Eq.(3.9), nous introduisons la notation

$$s = \sum_r p_r |\Psi_r|^2 \tag{3.10}$$

et nous dénotons la distribution de probabilité $P(s)$.

Dans le cas d'un état mélangé de manière maximale $f(s) = \ln(N)/N$, l'entropie informationnelle est $S[\rho] = \ln(N)$ comme on pouvait s'y attendre. Si l'état n'est pas mélangé de manière maximale, alors nous avons besoin de trouver la distribution de probabilité $P(s)$. En cas d'état pur, la distribution de s bien connue [64] est

$$P(s) = (N-1)(1-s)^{N-2} \tag{3.11}$$

Alors, nous obtenons l'expression pour *"l'entropie de l'incertitude minimale"* qui dépend de N :

$$S_0(N) \;=\; \sum_{k=2}^{N} \frac{1}{k} \;\approx\; \ln(N) - (1-\gamma) + \frac{1}{2N} \tag{3.12}$$

En utilisant l'approximation asymptotique dans la dernière égalité, nous voyons que la différence entre S d'un état mélangé de manière maximale et S d'un état pur approche une valeur universelle $(1-\gamma)$, où γ est la constante d'Euler. En utilisant un langage différent, nous voyons que l'entropie statistique excessive est limitée :

$$S_{\mathrm{F}}[\rho] \;<\; 1-\gamma \tag{3.13}$$

Obtenir une expression concrète pour l'entropie statistique excessive, dûe au manque de pureté, exige encore plus d'effort. La première étape est de calculer $P(s)$, ce qui nous amène à (voir l'annexe) :

$$P(s) = (N-1) \sum_{(p_r > s)} \left[\prod_{r'(\neq r)} \frac{1}{p_r - p_{r'}} \right] (p_r - s)^{N-2} \tag{3.14}$$

La seconde étape consiste à calculer l'intégrale Eq.(3.9) en utilisant

$$\int_0^p (p-s)^{N-2} s \ln(s) ds = \frac{p^N}{N(N-1)} \left[\ln(p) - \sum_{k=2}^{n} \frac{1}{k} \right]$$

puis à employer l'identité (voir l'annexe)

$$\sum_r p_r^N \prod_{r'(\neq r)} \frac{1}{p_r - p_{r'}} \;=\; \sum_r p_r \;=\; 1 \tag{3.15}$$

De cette façon, on obtient :

$$F = -\sum_r \left[\prod_{r'(\neq r)} \frac{p_r}{p_r - p_{r'}} \right] p_r \ln(p_r) \tag{3.16}$$

On peut noter que cette expression est indépendante de N. En effet, les valeurs propres supplémentaires égales à zéro n'ont aucun effet sur le résultat. Il existe quelques cas qui représentent un intérêt tout particulier. Pour un mélange de deux états, nous obtenons

$$F = -\frac{1}{p_1 - p_2} (p_1^2 \ln(p_1) - p_2^2 \ln(p_2)) \tag{3.17}$$

Pour un mélange uniforme de n états, on obtient :

$$S_{\mathrm{F}}[\rho] \;=\; \ln(n) - \sum_{k=2}^{n} \frac{1}{k} \tag{3.18}$$

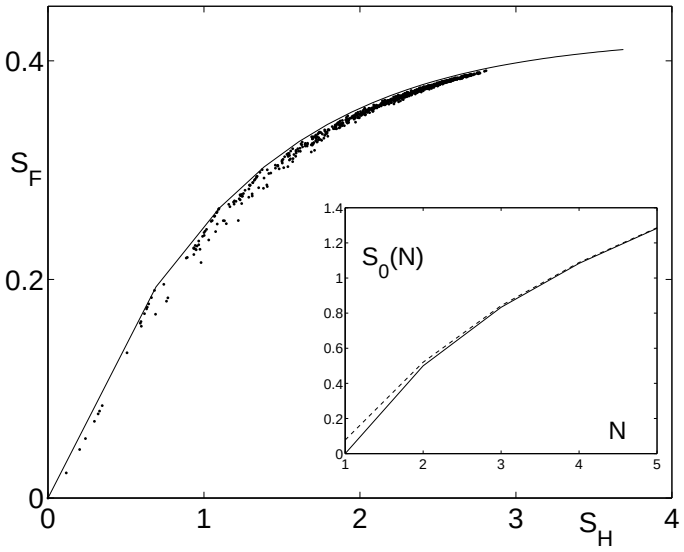


FIG. 3.1 – L'entropie informationnelle excessive d'un état quantique mélangé $S_{\rm F}$ selon l'entropie de Von-Neumann $S_{\rm H}$. La ligne solide est pour les mélanges uniformes, alors que les points sont pour les mélanges (non-uniformes) choisis de manière aléatoire. **l'encart :** L'entropie informationnelle d'un état quantique pur selon la dimension de l'espace d'Hilbert N (voir Eq.(3.12)). La ligne tirée correspond à l'approximation asymptotique.

$$S[\rho] \;=\; \ln(n) + \sum_{n<k\leq N} \frac{1}{k} \tag{3.19}$$

$S_{\rm F}[\rho]$, tout comme $S_{\rm H}[\rho]$ peut servir comme mesure de manque de pureté. La Fig.3.1 montre les résultats du calcul de $S_{\rm F}[\rho]$ selon $S_{\rm H}[\rho]$ pour un ensemble d'états représentatifs, mélanges uniformes et non-uniformes. Nous voyons qu'il y a une corrélation très forte entre ces deux mesures de pureté différente.

Notre définition de l'entropie a quelques propriétés mathématiques intéressantes. Une propriété simple est la concavité : soit avec $0 < \lambda < 1$, soit avec deux ensembles de probabilités, nous avons

$$F(\lambda p_r + (1-\lambda)q_r) \geq \lambda F(p_r) + (1-\lambda)F(q_r) \tag{3.20}$$

C'est une conséquence de la concavité de $f(s)$ dans Eq.(3.9). La concavité et la symétrie par rapport aux variables p_i impliquent que $S[\rho]$ atteigne son maximum pour les états mélangés au maximum et atteigne son minimum pour les états purs. Cette propriété est utile pour la justification des argumentations qui sont basées sur les calculs dans le "plus mauvais cas". Nous énumérons ci-dessous quelques propriétés moins évidentes qui représentent un intérêt physique.

Considérons un système dans un état ρ et son sous-système dans un état σ. Techniquement, la matrice de densité réduite σ est obtenue à partir de ρ en traçant sur les index non pertinents. Pour les considérations générales de la théorie de l'information, nous attendons d'avoir la propriété suivante :

$$S[\sigma] < S[\rho] \tag{3.21}$$

Cela signifie que la détermination de l'état de sous-système exige moins d'information. Comme on l'a déjà vu dans l'introduction, cette inégalité n'est pas vraie pour l'entropie de Von-Neumann. Par contre, elle se révèle être vraie avec notre définition $S[\rho] \geq S_0(MN) \geq S_0(2N) > \ln(N) > S[\sigma]$, où N et MN sont les dimensions de σ et de ρ respectivement.

Une autre situation physique fréquente est d'avoir un état $\rho = \sigma_{\mathrm{A}} \otimes \sigma_{\mathrm{B}}$ où σ_{A} et σ_{B} sont les états des sous-systèmes qui ont été préparés de manière indépendante. Évidemment, on a la propriété

$$S[\rho|\mathcal{A} \otimes \mathcal{B}] = S[\sigma_{\mathrm{A}}|\mathcal{A}] + S[\sigma_{\mathrm{B}}|\mathcal{B}] \tag{3.22}$$

Mais pour l'entropie informationnelle absolue, on s'attend à

$$S[\rho] \geq S[\sigma_{\mathrm{A}}] + S[\sigma_{\mathrm{B}}] \tag{3.23}$$

Si cette inégalité apparait c'est parce que certaines bases ne sont pas des "produits tensoriels externes" de la base $\mathcal{A}$ et de la base $\mathcal{B}$. Ainsi, cette inégalité reflète une plus grande incertitude quant à la détermination d'état du système combiné. On note que si notre monde était classique, nous obtiendrions une égalité ; ce qui est le cas avec l'entropie de Boltzmann et avec celle de Von-Neumann.

Afin de mieux établir Eq.(3.23), nous pouvons considérer le scénario du plus mauvais cas où N et M sont les dimensions de σ_{A} et de σ_{B} respectivement. Supposons que ces états sont les mélanges uniformes de n et m états respectivement, alors ρ sera un mélange uniforme des nm états dans la dimension NM. En utilisant Eq.(3.19) et l'inégalité

$$\begin{aligned}
\sum_{k=nm+1}^{NM} \frac{1}{k} &= \sum_{k=nm+1}^{mN} \frac{1}{k} + \sum_{k=mN+1}^{NM} \frac{1}{k} \\
&= \sum_{k_1=n+1}^{N} \sum_{l_1=0}^{m-1} \frac{1}{k_1 m - l_1} + \sum_{k_2=m+1}^{M} \sum_{l_2=0}^{N-1} \frac{1}{k_2 N - l_2} \\
&> \sum_{k=n+1}^{N} \frac{1}{k} + \sum_{k=m+1}^{M} \frac{1}{k}
\end{aligned}$$

nous pouvons confirmer que Eq.(3.23) est vraiment satisfaite.

Un cas particulier de l'inégalité de Eq.(3.23) est quand l'entropie d'incertitude minimale satisfait

$$S_0(NM) > S_0(N) + S_0(M) \tag{3.24}$$

Mais qu'en est-il de la situation avec l'entropie statistique excessive ? Notre conjecture est que

$$S_{\rm F}[\rho] \leq S_{\rm F}[\sigma_{\rm A}] + S_{\rm F}[\sigma_{\rm B}] \tag{3.25}$$

Nous pouvons encore établir cette inégalité pour les mélanges uniformes de n et m états dans les dimensions N et M respectivement : En utilisant Eq.(3.18), nous pouvons observer que

$$S_{\rm F}[\rho] - S_{\rm F}[\sigma_{\rm A}] - S_{\rm F}[\sigma_{\rm B}] = S_0(n) + S_0(m) - S_0(nm)$$

qui est négatif selon Eq.(3.24). Il est important de réaliser que Eq.(3.24) surcompense l'inégalité Eq.(3.25), ce qui amène à Eq.(3.23).

Il est bien connu que pour l'entropie de Von-Neumann, nous avons l'inégalité générale

$$S_{\rm H}[\rho] \leq S_{\rm H}[\sigma_{\rm A}] + S_{\rm H}[\sigma_{\rm B}] \tag{3.26}$$

qui est vérifiée pour toute sous-division d'un système en deux sous-systèmes (corrélés). Nous avons déjà observé (Fig.3.1) que $S_F[\rho]$ est fortement corrélé avec $S_H[\rho]$. De plus, cette corrélation est *sous-linéaire*. Il en suit que nous attendons de l'inégalité plus facile Eq.(3.25) qu'elle soit généralement vérifiée en cas de sous-systèmes corrélés.

L'effet des mesures quantiques sur l'entropie représente un intérêt particulier. Soit P_i, un ensemble complet de projecteurs orthogonaux ($\sum_i P_i = 1$). L'état obtenu après une mesure projective est $\sigma = \sum_i P_i \rho P_i$. Par conséquent, l'état du système devient plus mélangé. Cela se peut effectivement se voir à travers une augmentation de l'entropie de Von-Neumann des systèmes. Notre entropie est aussi une mesure pour le manque de pureté. Par conséquent, il est raisonnable d'attendre que $S[\sigma] \geq S[\rho]$. Nous ne pouvons pas prouver cette affirmation.

3.2 Annexe : calcul de la distribution de probabilité

En passant aux variables $s_r = x_r^2 + y_r^2$, la définition de $P(s)$ prend la forme

$$\begin{aligned} P(s) &= \left\langle \delta(s - \sum_r p_r (x_r^2 + y_r^2)) \right\rangle_{\rm sphere} \\ &= (N-1)! \int_0^\infty ds_1..ds_N \; \delta(1 - \sum_r s_r) \delta(s - \sum_r p_r s_r) \\ &= (N-1)! \int_0^\infty ds_1..ds_N \int \frac{d\omega d\nu}{(2\pi)^2} {\rm e}^{(1-\sum_r s_r)(i\nu+0) + i(s-\sum_r p_r s_r)\omega} \end{aligned}$$

où le 0 infinitésimal a été introduit pour assurer la convergence une fois l'ordre de l'intégration changé. Ainsi, après l'intégration sur $ds_1...ds_N$, nous avons

$$P(s) = (N-1)! \int \frac{d\omega d\nu}{(2\pi)^2} {\rm e}^{i\nu + i\omega s} \prod_r \frac{1}{i\omega p_r + i\nu + 0}$$

$$= \int \frac{d\omega}{2\pi} \frac{(N-1)!}{(i\omega)^{N-1}} \sum_r \mathrm{e}^{i\omega(s-p_r)} \prod_{r'(\neq r)} \frac{1}{p_{r'} - p_r}$$

On peut montrer (voir ci-dessous) qu'il n'y a aucune singularité dans l'intégrale à $\omega = 0$. Par conséquent, on peut déformer le contour de l'intégration de manière à ce que ce contour aille légèrement au-dessus du point $\omega = 0$. Alors, on peut faire l'intégrale terme par terme, ce qui mène au résultat final Eq.(3.14). Plus précisément, si $p_r < s$, le contour doit être fermé dans le demi-plan supérieur, ce qui mène au résultat égal à zéro ; par contre, si $p_r > s$, le contour doit être fermé dans le demi-plan inférieur, ce qui mène à une contribution du pôle à $\omega = 0$ différente de zéro.

Nous avons observé que la fonction à intégrer doit être non-singulière pour réaliser la manipulation ci-dessus : la singularité $1/\omega^{N-1}$ des termes individuels est annulée dans la somme sur tous r. Cette annulation peut être établie en développant l'exposant dans les puissances de ω et en employant l'identité

$$\sum_r (s - p_r)^n \prod_{r'(\neq r)} \frac{1}{p_r - p_{r'}} = 0 \qquad \text{for } n \leq (N-2)$$

Cette identité ainsi que Eq.(3.15) peuvent être prouvées par le procédé suivant :

$$\begin{aligned} \sum_r g(p_r) \prod_{k(\neq r)} \frac{1}{p_r - p_k} &= \oint \frac{dz}{2\pi i} g(z) \prod_k \frac{1}{z - p_k} \\ &= \oint \frac{dz}{2\pi i} z^{N-2} g(1/z) \prod_k \frac{1}{1 - p_k z} \end{aligned}$$

où dans la dernière étape, $z \mapsto 1/z$ est changé.

Chapitre 4

Calcul quantique de la transition d'Anderson en présence d'imperfections statiques

4.1 Algorithme quantique

Les progrès récents survenus dans le domaine du calcul quantique ont permis de montrer qu'en raison du parallélisme quantique certaines tâches peuvent être exécutées beaucoup plus rapidement sur un ordinateur quantique que sur un ordinateur classique (voir [1] ainsi que les références se trouvant à l'intérieur). L'exemple le plus connu est l'algorithme de Shor pour la factorisation des grands nombres premiers [7] qui est exponentiellement plus rapide que tous les algorithmes classiques connus. Un certain nombre d'algorithmes quantiques ont également été proposés pour simuler de façon efficace l'évolution quantique de certains hamiltoniens que cela soit ceux décrivant les systèmes à plusieurs corps [67, 68] ou les problèmes de chaos quantique [69, 19, 15]. Il a été montré dans [19] que le propagateur d'évolution d'un système possédant un régime de localisation dynamique ou de localisation d'Anderson peut être simulé de manière efficace sur un ordinateur quantique. Cependant, l'algorithme proposé [19] exige un nombre de qubits supplémentaires trop importants pour pouvoir être implémenté expérimentalement avec la première génération d'ordinateurs quantiques composés de 5 à 10 qubits.

Dans ce chapitre, nous considérons un algorithme quantique permettant de simuler la dynamique quantique dans le régime d'Anderson. Cet algorithme n'exige aucun qubit supplémentaire, utilisant les n_q qubits disponibles d'une manière optimale. La propagation d'un vecteur $N = 2^{n_q}$, sur un intervalle de temps unité, exige $O(n_q^2)$ opérations entre les portes quantiques contre $O(2^{n_q})$ opérations pour tous les algorithmes classiques connus. Grâce à ces propriétés, la transition d'Anderson peut être déjà mise en évidence sur un ordinateur de 7 à 10 qubits. Les éléments de base de l'algorithme incluent des rotations d'un qubit, des portes de phases controlées $C(\phi)$ et des opérations NOT controlées C_N. La composante primordiale de l'algorithme est la bien connue transformée de Fourier quantique (QFT) décrite dans [1]. Toutes ces opérations quantiques ont été déjà implémentées

sur des ordinateurs quantiques de 3 à 7 qubits basés sur la RMN [70, 71]. Les obstacles principaux à la détection de la transition d'Anderson dans le calcul quantique sont les effets dus à la décohérence externe [39] et ceux dus aux imperfections statiques résiduelles [42]. Les résultats obtenus pour des algorithmes quantiques fonctionnant correctement [15, 43] montrent que les imperfections statiques affectent la précision du calcul quantique d'une manière plus forte que les erreurs provoquées par le bruit aléatoire dans les portes. C'est pour cette raison que nous allons concentrer notre étude sur le cas des imperfections statiques en étudiant leur impact sur les propriétés de systèmes quantiques à proximité de la transition d'Anderson.

Pour étudier les effets des imperfections statiques dans la détermination de la transition quantique d'Anderson, nous choisissons le modèle du rotateur pulsé généralisé décrit par l'évolution unitaire de la fonction d'onde ψ

$$\bar{\psi} = \hat{U}\psi = \exp(-iV(\theta,t))\exp(-iH_0(\hat{n}))\psi \quad . \tag{4.1}$$

Ici, $\bar{\psi}$ est la nouvelle valeur de ψ après une itération, c'est-à-dire après l'application de l'opérateur unitaire $\hat{U}$, $H_0(n)$ est la phase correspondant au rotateur pulsé dans la base du moment angulaire $\hat{n} = -i\partial/\partial\theta$, le pulse (ou kick) est décrit par le potentiel $V(\theta,t)$ qui dépend de la phase du rotateur θ et du temps t mesuré en nombre de pulses (kicks), $\psi(\theta + 2\pi) = \psi(\theta)$. Pour $V(\theta,t) = k\cos\theta$ et $H_0 = Tn^2/2$, le modèle du rotateur pulsé est décrit en détail dans [31]. L'évolution donnée par (4.1) est engendrée par l'hamiltonien $H = H_0(n) + V(\theta,t)\delta_1(t)$, où $\delta_1(t)$ est une fonction δ périodique de période 1 et où (n,θ) sont des variables conjuguées. Dans ce cas, lorsque le potentiel $V(\theta,t) = -2\tan^{-1}(2k(\cos\theta+\cos\omega_1 t+\cos\omega_2 t))$ dépend du temps t d'une manière quasi-périodique, le modèle peut être exactement réduit au modèle de Lloyd tridimensionnel (3D) [34, 35]. En effet, la dépendance temporelle de $V(\theta,t)$ peut être éliminée en introduisant un espace de phase étendu en utilisant le remplacement suivant $H_0 \to H_0(n) + \omega_1 n_1 + \omega_2 n_2$. Ainsi, la dépendence linéaire par rapport aux nombres quantiques $n_{1,2}$ donne des fréquences de rotations fixes pour les phases conjuguées respectives $\theta_{1,2} = \omega_{1,2}t$. Les études approfondies publiées dans [35] montrent que ce modèle possède une transition métal-isolant d'Anderson pour $k = k_c \approx 0.5$ avec une valeur de l'exposant critique proche des valeurs trouvées dans d'autres modèles 3D de physique du solide. En suivant [36], nous allons choisir dans (4.1) $V(\theta,t) = k(1 + 0.75\cos\omega_1 t\cos\omega_2 t)\cos\theta$ avec $\omega_1 = 2\pi\lambda^{-1}$, $\omega_2 = 2\pi\lambda^{-2}$ et $\lambda = 1.3247...$, la racine réelle de l'équation cubique $x^3 - x - 1 = 0$. Les phases de rotation $H_0(n)$ sont complétement distribuées dans l'intervalle $(0, 2\pi)$. Ce modèle possède une transition d'Anderson pour $k_c \approx 1.8$ [36] avec des caractéristiques similaires à celles du modèle de Lloyd étudié dans [34, 35].

L'algorithme quantique simulant l'évolution temporelle de ce modèle est construit de la manière suivante. Les états quantiques $n = 0, ..., N-1$ sont représentés par un registre quantique de n_q qubits ainsi $N = 2^{n_q}$. L'état initial choisi, $n_0 = 0$, correspond à l'état $|00...0>$ (Le moment n peut prendre N valeurs discretes sur le cercle). La rotation de phase $U_T = \exp(-iH_0(n))$ dans la base du moment n est effectuée à l'aide d'un générateur de phases quantiques aléatoires construit à partir de deux opérateurs unitaires $U_T^{(1)}$ et $U_T^{(2)}$. L'opérateur $U_T^{(1)} = \prod_{j=1}^{n_q} e^{i\phi_j\sigma_j^z}$ effectue la rotation du qubit j

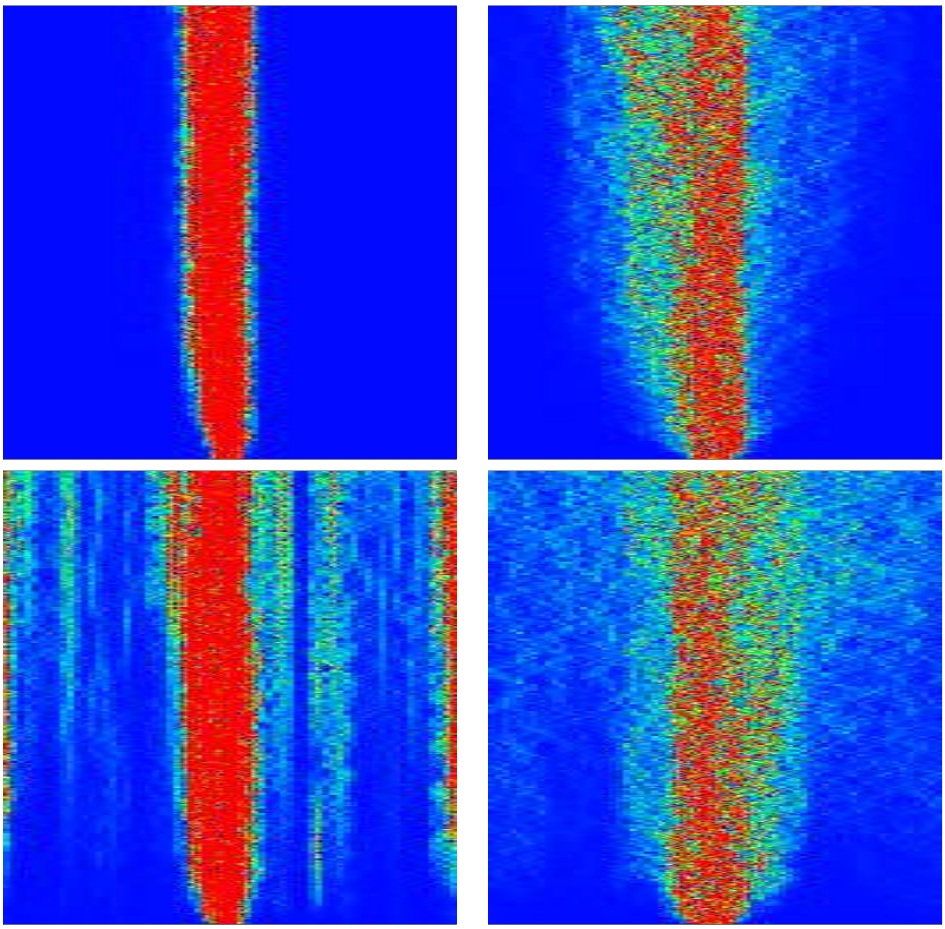


FIG. 4.1 – Evolution temporelle de la distribution de probabilité $|\psi_n|^2$ dans la phase de localisation (colonne de gauche, $k = 1.2$) et dans la phase de délocalisation (colonne de droite, $k = 2.4$) pour $n_q = 7$ qubits ($N = 2^{n_q}$), avec $0 \leq t \leq 400$ (axe vertical) et $-N/2 < n \leq N/2$ (axe horizontal) ; $k_c = 1.8$. La couleur est proportionnelle à la probabilité : bleu/noir pour zéro et rouge/blanc pour les valeurs maximales. L'intensité des imperfections statiques est $\epsilon = \mu = 0$ pour la ligne supérieure et $\epsilon = \mu = 10^{-4}$ pour la ligne inférieure.

d'une phase aléatoire ϕ_j. Ici et ci-dessous, $\sigma^x, \sigma^y, \sigma^z$ sont les matrices de Pauli. Pour améliorer l'indépendance des phases quantiques, nous appliquons alors l'opérateur $U_T^{(2)} = \prod_{k=1}^{M} C_N(i_{M-k}, j_{M-k}) \prod_{k=1}^{M} e^{i\phi'_{j_k}\sigma^z_{j_k}} C_N(i_k, j_k)$. Cette transformation est composée d'une séquence aléatoire avec M rotations de qubits $e^{i\phi'_{j_k}\sigma^z_{j_k}}$ et de portes controlled-NOT $C_N(i_k, j_k)$ suivies par la séquence inverse de portes controlled-NOT $C_N(i_{M-k}, j_{M-k})$. Ici, $C_N(i_k, j_k)$ bascule le qubit j_k si le qubit i_k est 1 ; les indices i_k, j_k et les phases ϕ'_{j_k} sont choisies aléatoirement. Le générateur de phases quantiques aléatoires $U_T = U_T^{(2)} U_T^{(1)}$ génère des phases aléatoires de plus en plus indépendantes à mesure que M croît. Nous utilisons $M \approx 2n_q$ (avec $n_q \approx 10$), ce qui selon nos tests permet de générer des phases aléatoires correctes. Cette étape implique $3M + n_q$ portes quantiques. Ensuite, l'opérateur de pulse

$U_k = \exp(-ik(t)\cos\theta)$ est simulé de la manière suivante. D'abord, à l'aide de la QFT, la fonction d'onde est amenée de la représentation du moment n vers la représentation de la phase θ avec $O(n_q^2/2)$ gates. Alors, θ peut être écrit en représentation binaire comme $\theta/2\pi = 0.a_1a_2..a_{n_q}$ avec $a_i = 0$ ou 1. Il est alors judicieux d'utiliser la notation $\theta = \pi a_1 + \bar{\theta}$ pour isoler le qubit de poids plus élevé. Ainsi, en utilisant la relation $\cos\theta = (-1)^{a_1}\cos\bar{\theta} = \sigma_1^z\cos\bar{\theta}$, l'opérateur de pulse prend la forme $U_k = e^{-ik(t)\cos\theta} = e^{-i\sigma_1^z k(t)\cos\bar{\theta}}$, où $\sigma_1^{(z,x)}$ agit sur le premier qubit. Cette opération peut être approximée avec une précision arbitraire par une séquence de portes monoqubits appliquées au premier qubit et par les opérateurs diagonaux $S^m = e^{ima_1\bar{\theta}}$. Les opérateurs S sont donnés par le produit de $n_q - 1$ portes à deux qubits, $S^m = \prod_{j=2}^{n_q} C_{1,j}(\pi m 2^{-j+1})$ où la porte de phase controllée $C_{j_1,j_2}(\phi)$ génère un déplacement de la phase $e^{i\phi}$ si les deux qubits $j_{1,2}$ sont 1. Nous introduisons alors l'opérateur unitaire $R_\gamma(\bar{\theta}) = HS^1H\ e^{-i\frac{\gamma}{2}\sigma_1^z}\ HS^{-2}H\ e^{-i\frac{\gamma}{2}\sigma_1^z}\ HS^1H$ où $H = (\sigma_1^z + \sigma_1^x)/\sqrt{2}$ est la porte de Hadamard. Cet opérateur peut-être exactement réduit sous la forme $R_\gamma(\bar{\theta}) = \cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2}\cos(2\bar{\theta}) - i\sigma_1^z\sin\gamma\cos(\bar{\theta}) + i\sigma_1^x\sin^2\frac{\gamma}{2}\sin(2\bar{\theta})$, ainsi pour γ petit nous avons $R_\gamma(\bar{\theta}) = e^{-i\sigma_1^z\gamma\cos\bar{\theta}} + i\sigma_1^x\frac{\gamma^2}{4}\sin(2\bar{\theta}) + O(\gamma^3)$. Le terme contenant γ^2 peut être éliminé en utilisant la repésentation symétrique $R_{\gamma/2}(\bar{\theta})R_{\gamma/2}(-\bar{\theta}) = HS^1H\ e^{-i\frac{\gamma}{4}\sigma_1^z}\ HS^{-2}H\ e^{-i\frac{\gamma}{2}\sigma_1^z}\ HS^2H\ e^{-i\frac{\gamma}{4}\sigma_1^z}\ HS^{-1}H = e^{-i\sigma_1^z\gamma\cos(\bar{\theta})} + O(\gamma^3)$. L'opérateur de pulse est donc donné par $U_k = (R_{\gamma/2}(\bar{\theta})R_{\gamma/2}(-\bar{\theta}))^l + O(l\gamma^3)$ où le nombre d'étapes est $l = k/\gamma$. Nous avons utilisé dans nos simulations numériques un paramètre γ petit, $\gamma = k/l \approx 0.2$. Cela correspond à $l \approx 5-10$ pour $k \sim 1-2$. Après cela, l'état est transféré dans la représentation du moment à l'aide de la QFT. Ainsi, une itération (4.1) est effectuée pour 2^{n_q} états à l'aide de n_g portes élémentaires avec $n_g = 2[k/\gamma](n_q+2)+n_q^2+6n_q+3M+9$ où $[k/\gamma]$ est la partie entière de k/γ. Cet algorithme est optimal pour le modèle du rotateur pulsé avec des valeurs modérées du paramètre k donnant des valeurs de n_g raisonnables. Tout ceci est facilement généralisable pour d dimensions.

4.2 Effets des imperfections : résultats des simulations numériques

Au travers de nos simulations numériques nous avons étudié les effets des imperfections statiques qui peuvent exister au sein d'un ordinateur quantique [42, 15, 43]. Dans ce cas, toutes les portes sont parfaites, cependant entre l'action de chaque porte l'état ψ acquiert un facteur de phase $e^{i\hat{\varphi}}$ où $\hat{\varphi} = \sum_j(\eta_j\sigma_j^z + \mu_j\sigma_j^x\sigma_{j+1}^x)$ (voir la sous-section 1.3.2, où nous avons utilisé des notations légèrement différents). Ici, les paramètres η_j et μ_j sont aléatoires avec $j = 1, ..., n_q$. Le paramètre η_j représente la déviation d'énergie statique du qubit j, $-\epsilon/2 \leq \eta_j \leq \epsilon/2$, et μ_j représente le couplage statique inter-qubit sur une chaîne circulaire, $-\mu/2 \leq \mu_j \leq \mu/2$.

Un exemple de l'évolution temporelle de la distribution de probabilié dans la représentation du moment est montré à la Fig.4.1. En-dessous de la transition de Anderson ($k < k_c$), la probabilité reste confinée proche de sa valeur initiale n_0, tandis qu'au-dessus de la transition ($k > k_c$), un étalement diffusif prend place suivant n. En comparant au calcul quantique idéal, les imperfections statiques mènent à un transfert de probabilité

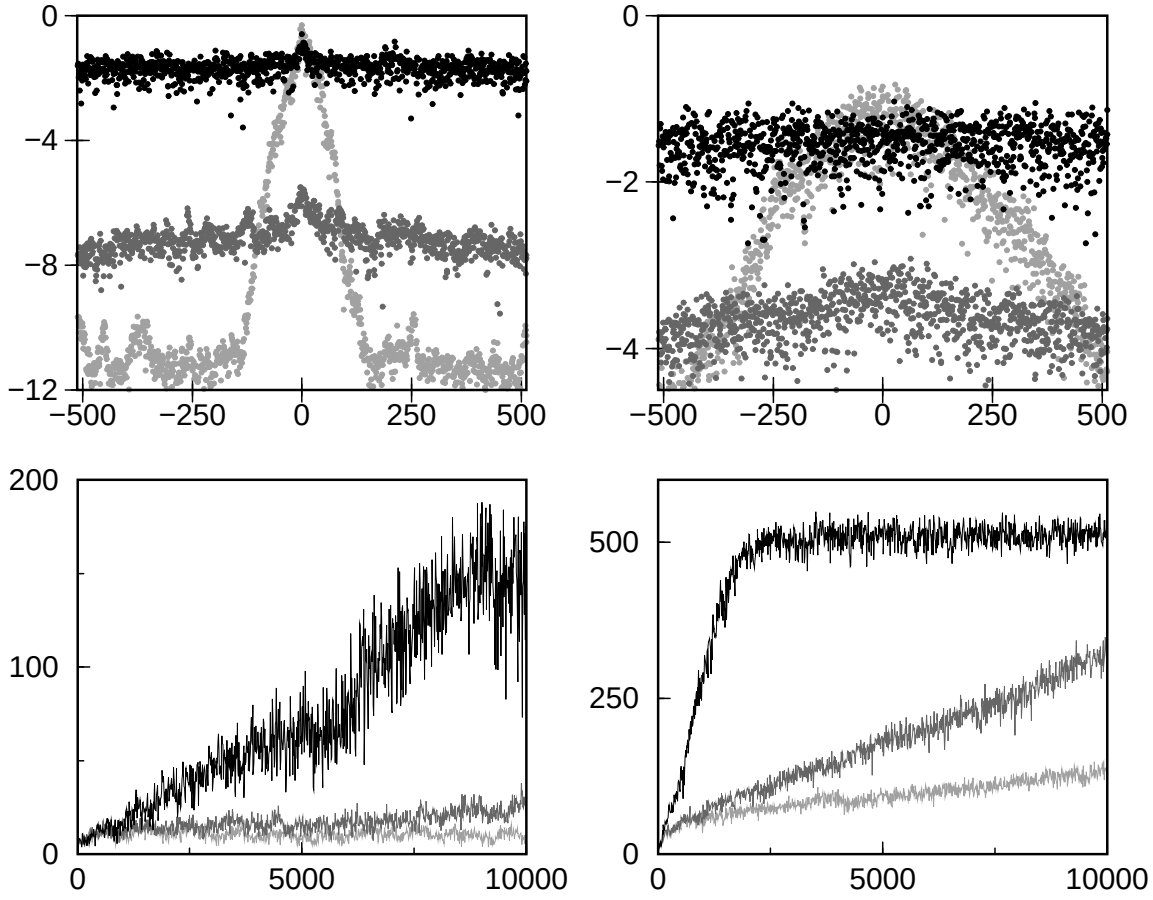


FIG. 4.2 – Ligne supérieure : logarithme de la probabilité, $\log_{10}|\psi_n|^2$, en fonction du moment n après $t = 10000$ itérations ; les courbes grises foncées sont décalées vers le bas de 5 (colonne de gauche) et 2 (colonne de droite) unités. Ligne inférieure : IPR ξ en fonction du temps t. La colonne de gauche (droite) correspond à la phase de localisation (délocalisation) pour $k = 1.2$ ($k = 2.4$). Les trois courbes correspondent à $\epsilon = 0; 2 \times 10^{-5}; 6 \times 10^{-5}$, la couleur de celles-ci changeant du gris clair au noir à mesure que ϵ croît ; $\mu = \epsilon$, $n_q = 10$.

vers des niveaux situés très loin du centre du paquet d'onde. Cet effet est lié à la structure de la QFT où une erreur dans les portes quantiques génère des harmoniques. Ainsi, les imperfections statiques créent un plateau dans la distribution de probabilité dont le niveau croît avec l'augmentation de ϵ et μ (voir Fig.4.2). Ceci mène à une diffusion artificielle du second moment de la distribution $< n^2 >=< \psi_n|(n-n_0)^2|\psi_n >$. Puisque le plateau de probabilité s'étend sur tous les N niveaux, le taux de cette diffusion croît avec n_q de manière exponentielle, les paramètres ϵ, μ étant fixés (données non montrées). Un effet similaire a été l'objet de discussion dans [72] pour le calcul quantique du rotateur pulsé en présence de bruit dans les portes. La quantité la plus appropriée pour cette étude est l'inverse du taux de participation (IPR) ξ qui est largement utilisé pour étudier les systèmes avec localisation [22, 23]. L'IPR détermine le nombre de niveaux sur lesquels la fonction d'onde est construite ($\sum_n |\psi_n|^4 = 1/\xi$). Contrairement à $< n^2 >$, l'IPR ξ reste stable en présence de bruit dans les portes pendant des temps larges au sens polynomial [72].

La variation de ξ avec le temps, ϵ et μ est montrée à la Fig.4.2. Pour des imperfections modérées, ξ reste, pendant un long intervalle de temps, proche de la valeur obtenue avec un algorithme exact. Cependant, pour de très long temps $t \geq 10^5$, ξ converge vers une valeur qui dépend de k, ϵ et μ. Un exemple typique d'un tel comportement est dépeint à la Fig.4.3. Ici, ξ passe abruptement d'une valeur petite ($\xi \sim 1$) à une valeur grande ($\xi \sim N$) et cela dans un intervalle de valeur de k étroit. Ceci est la manifestation de la transition d'Anderson, c'est-à-dire la transition d'un état localisé vers un état délocalisé. Le point critique k_c peut-être numériquement défini comme étant la valeur de k pour laquelle ξ atteint la valeur médiane de ces deux valeurs limites. Les données de la Fig.4.3 montrent que le point critique $k_c(\epsilon)$ décroît avec l'augmentation de l'intensité des imperfections. L'origine physique de cet effet est lié aux transitions additionnelles induites par les imperfections statiques qui naturellement mènent à la délocalisation pour une valeur de k plus basse comparé au calcul idéal. Une autre méthode permettant de détecter la position du point critique $k_c(\epsilon)$ en présence d'imperfections consiste à mesurer les deux qubits de plus grands poids qui codent la valeur du moment n. Après une dizaine de mesures des deux premiers qubits, nous déterminons la probabilité $W = \sum_{n=(N/4,3N/4)} |\psi_n|^2$. Pour des temps t suffisamment grand, cette probabilité passe abruptement de la valeur $W = 0$ à la valeur $W \approx 0.5$ lorsque k varie. Ceci permet de déterminer le point critique et donne des valeurs de $k_c(\epsilon)$ proche de celles obtenues avec l'IPR ξ (voir Fig.4.3).

La déviation par rapport au point critique, $\Delta k_c(\epsilon) = k_c - k_c(\epsilon)$, dépend de ϵ, μ et n_q. A partir des données de l'IPR obtenues pour plusieurs valeurs des paramètres ϵ, μ, n_q (voir Fig.4.4) nous obtenons la relation d'échelle suivante

$$\Delta k_c(\epsilon) = A\tilde{\epsilon}^{\,\alpha}, \quad \tilde{\epsilon} = \epsilon n_g \sqrt{n_q}. \tag{4.2}$$

Les données extraites des régressions linéaires nous donnent $A = 3.0$, $\alpha = 0.64$ pour $\mu = 0$ et $A = 4.8$, $\alpha = 0.68$ pour $\mu = \epsilon$. Ce résultat peut être compris utilisant les arguments suivants. D'après [15, 43], l'échelle de temps t_f, pendant laquelle la fidelité du calcul quantique est proche de l'unité, est déterminée par le paramètre $\tilde{\epsilon}$ ($t_f \sim 1/\tilde{\epsilon}$). Ainsi, l'élément de matrice effectif, entre deux états propres idéaux, induit par les imperfections

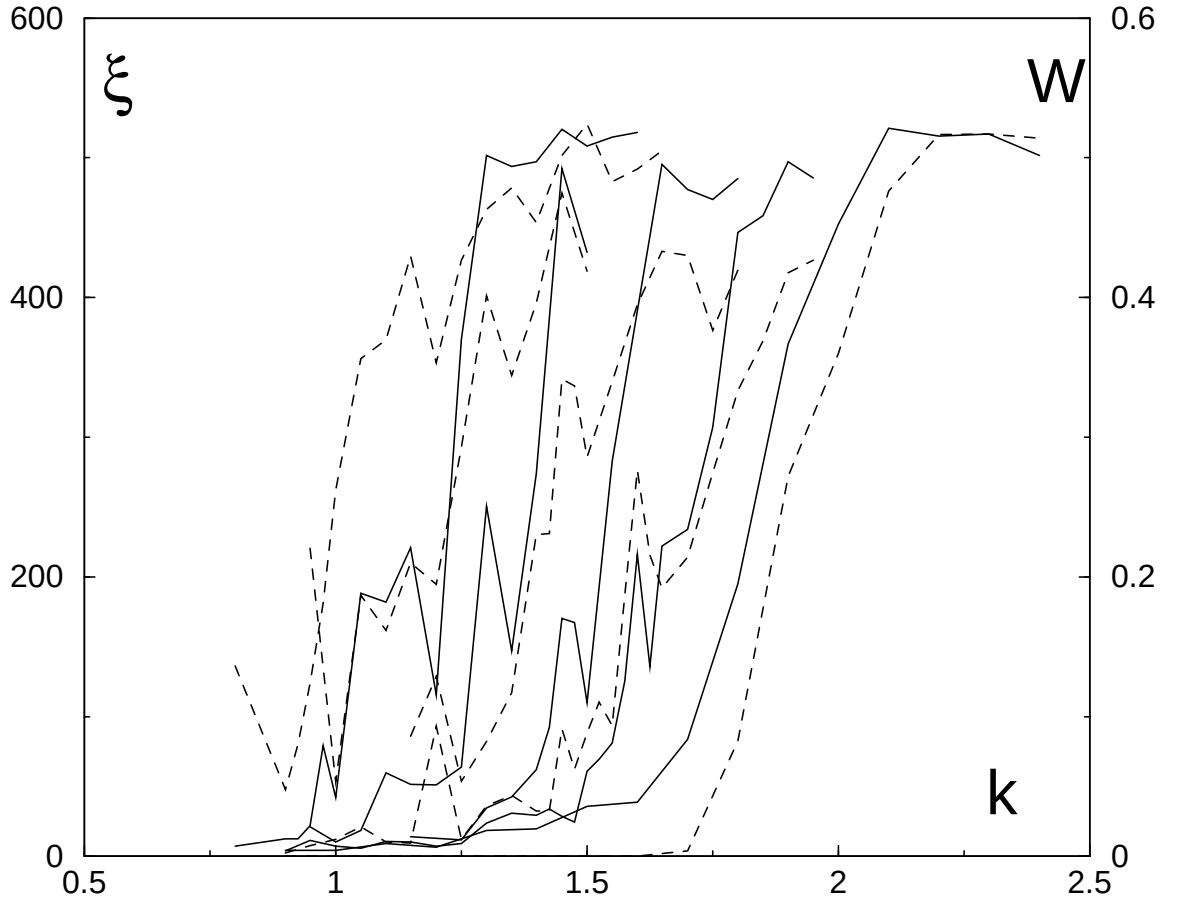


FIG. 4.3 – IPR ξ (courbes pleines, ordonnées lues sur l'axe de gauche) et probabilité d'excitation W (courbes hachurées, ordonnées lues sur l'axe de droite) en fonction de l'intensité k du pulse pour $n_q = 10$ et pour (de droite à gauche) $t \geq 10^5$, $\epsilon = 0; 10^{-5}; 2 \times 10^{-5}; 4 \times 10^{-5}; 8 \times 10^{-5}$; $\mu = 0$.

statiques peut être estimé à $U_{ef} \sim \tilde{\epsilon} Q \sim \tilde{\epsilon}/l^{\beta}$, où Q est le recouvrement typique des états propres localisés. Pour la localisation d'Anderson en dimension d, ce recouvrement peut être estimé à $Q \sim l^{-\beta}$ où $\beta = d/2$ et où l est la longueur de localisation pour l'algorithme exact (voir [18] pour le cas $d = 1$). La délocalisation induite par les imperfections survient lorsque U_{ef} excède l'écart de niveau dans un bloc de taille l ($U_{ef} > \Delta_l \sim 1/l^d$). En prenant en compte le fait que près du point critique, la longueur de délocalisation se comporte comme $l \sim \Delta k^{-\nu}$ avec $\nu \sim 1.5$ (voir [22, 34, 35, 36]), nous obtenons $\alpha = 1/(\nu(d-\beta)) = 2/\nu d$. La valeur de α obtenue donnerait une valeur raisonnable de $\nu \approx 1.0$, cependant, dans notre modèle (4.1), la situation est plus compliquée. En effet, la dynamique décrite par (4.1) est unidimensionnelle et on s'attend donc à $\beta = 1/2$ et $\nu \approx 0.6$. Cette dernière valeur diffère notablement de la valeur habituellement attendue [22, 34, 35, 36]. Cette divergence peut être due au fait que les perturbations au sein de l'algorithme donnent lieu à des transitions vers des états lointains (voir Fig.4.1) qui diminuent considérablement

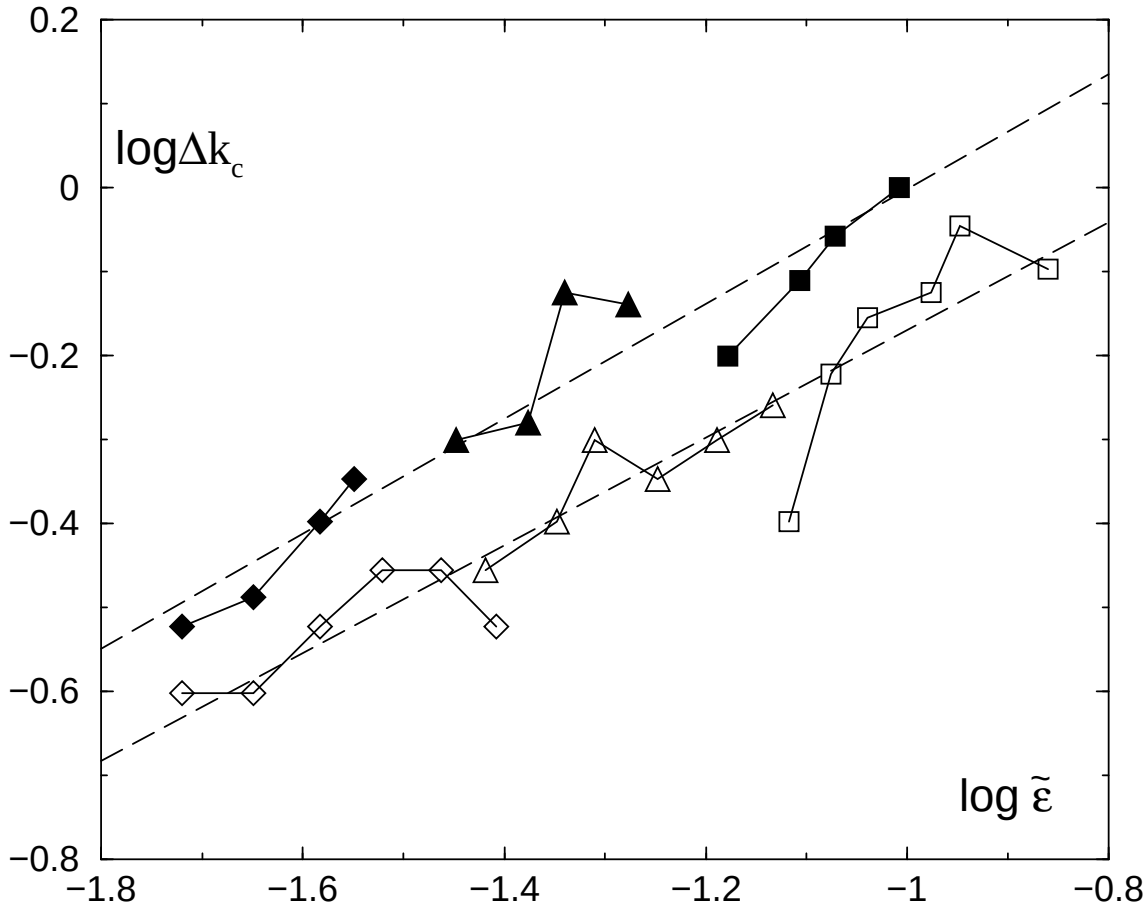


FIG. 4.4 – Déviation par rapport au point critique $\Delta k_c(\epsilon) = k_c - k_c(\epsilon)$ en fonction de l'intensité des imperfections $\tilde{\epsilon} = \epsilon n_g \sqrt{n_q}$ pour $\epsilon = 2\times10^{-5}$ (diamants), 4×10^{-5} (triangles) et 8×10^{-5} (carrés) ; les symboles ouverts/pleins correspondent respectivement à $\mu = 0$, $8 \leq n_q \leq 13$ et $\mu = \epsilon$, $8 \leq n_q \leq 11$; $k_c = 1.8$. Les lignes hachurées illustrent la relation d'échelle (4.2).

la valeur de β . Aussi, à proximité du point critique les correlations entre les éléments de matrice jouent un rôle important. Des études plus poussées seront nécessaires afin de clarifier ce point.

Finalement, nous comparons le nombre d'opérations nécessaires pour le calcul classique et quantique de la transition d'Anderson dans le cas d-dimensionnel. Pour cela, nous prenons note qu'à proximité du point critique du système réel en dimensions d, le nombre d'états croît avec le temps suivant la relation $N^d \sim t$ [22, 23, 26]. Ainsi, jusqu'au temps t, le calcul classique peut utiliser seulement N niveaux dans chaque direction, le nombre de niveaux est alors $n^d \sim t$. Les autres niveaux ne sont que très peu peuplés sur cette échelle de temps et par conséquent ils peuvent être éliminés avec confiance. Ainsi, le nombre d'opérations classiques pour t pulses peut être estimé à $n_{gcl} \sim tN^d \log^d N \sim t^2 \log^d t$. Au même moment, 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. Les caractéristiques *coarse-grained* de

la distribution de probabilité peuvent être déterminées à partir de quelques mesures sur les qubits de poids les plus élevés, à partir par exemple de W comme sur la Fig.4.3. Ainsi, même si chaque étape de (4.1) est efficace, le gain en rapidité n'est seulement que 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 $d > 2$.

Ainsi les résultats présentés dans ce chapitre montrent qu'il est possible de simuler la transition d'Anderson sur un ordinateur quantique d'une manière efficace. Des effets intéressants peuvent être vus avec 7-10 qubits, ce qui pourrait être à la portée d'expériences dans les prochaines années. Le calcul est robuste en présence de niveaux modérés d'imperfections. Ce travail correspond à l'article publié [4] (voir Article III en appendice).

Chapitre 5

Algorithme quantique de recherche de Grover en présence d'imperfections

Le calcul quantique ouvre de nouvelles perspectives et de nouvelles possibilités pour traiter de manière plus efficace les problèmes calculatoires complexes par rapport aux algorithme basés sur la logique classique [1]. Les deux plus fameux algorithmes quantiques sont l'algorithme de Shor pour la factorisation des nombres premiers [7] et l'algorithme quantique de recherche de Grover [14]. L'algorithme de Shor est exponentiellement plus rapide que n'importe quel algorithme classique connu, tandis que l'algorithme de Grover donne un gain de rapidité quadratique.

Dans les calculs quantiques réels, les portes élémentaires ne sont pas parfaites, par conséquent, il est très important d'analyser les effets que peuvent engendrer les imperfections et les erreurs quantiques sur la précision de l'algorithme. Un modèle usuel permettant de traiter les erreurs quantiques consiste à faire l'hypothèse que les angles des rotations unitaires fluctuent, aléatoirement au cours du temps, pour chaque qubit, à l'intérieur d'un petit intervalle ε proche de la valeur exacte de l'angle déterminée par l'algorithme idéal. Dans ce cas, un calcul quantique réel reste proche du calcul idéal jusqu'à un nombre de portes utilisées, $N_g \sim 1/\varepsilon^2$. Par exemple, la fidélité f du calcul, définie comme le carré du produit scalaire entre la fonction d'onde quantique de l'algorithme idéal et celle de l'algorithme perturbé, reste proche de l'unité si le nombre de portes utilisées est plus petit que N_g. Ce résultat a été établi analytiquement et numériquement dans des études approfondies de divers algorithmes quantiques [38, 39, 40, 73, 43, 41, 44].

Une autre source d'erreurs quantiques provient des imperfections internes générées par le couplage statique résiduel entre qubits et par les déviations des niveaux d'énergie qui fluctuent d'un qubit à l'autre mais restent statiques au cours du temps. Ces imperfections statiques peuvent mener à l'apparition du chaos quantique, qui modifie radicalement les propriétés de l'ordinateur quantique réel [42, 74, 75]. Les effets de ces imperfections statiques sur la précision du calcul quantique ont été étudiées sur des exemples d'algorithmes quantiques pour des modèles de dynamiques quantiques complexes [15, 4, 43, 44]. Une loi universelle, pour la décroissance de la fidélité induite par les imperfections statiques, a

été établie [44] pour les algorithmes quantiques simulant des systèmes dynamiques dans le régime du chaos quantique. Egalement, il a été montré que les effets des imperfections statiques pour les sytèmes dynamiques dans le régime intégrable n'ont pas de propriétés universelles et sont plus compliqués. Il est, par conséquent, important d'étudier les effets des imperfections statiques sur un exemple de l'algorithme bien connu de Grover. Une première tentative a été réalisée récemment [76], mais la compréhension globale du phénomène reste obscure. Ici, nous présentons une étude numérique et analytique approfondie qui établie le diagramme global de stabilité de l'opérabilité fiable de l'algorithme de Grover.

L'algorithme de Grover [14, 1] et les détails de son implémentation sont décrits à la section 1.1.3.

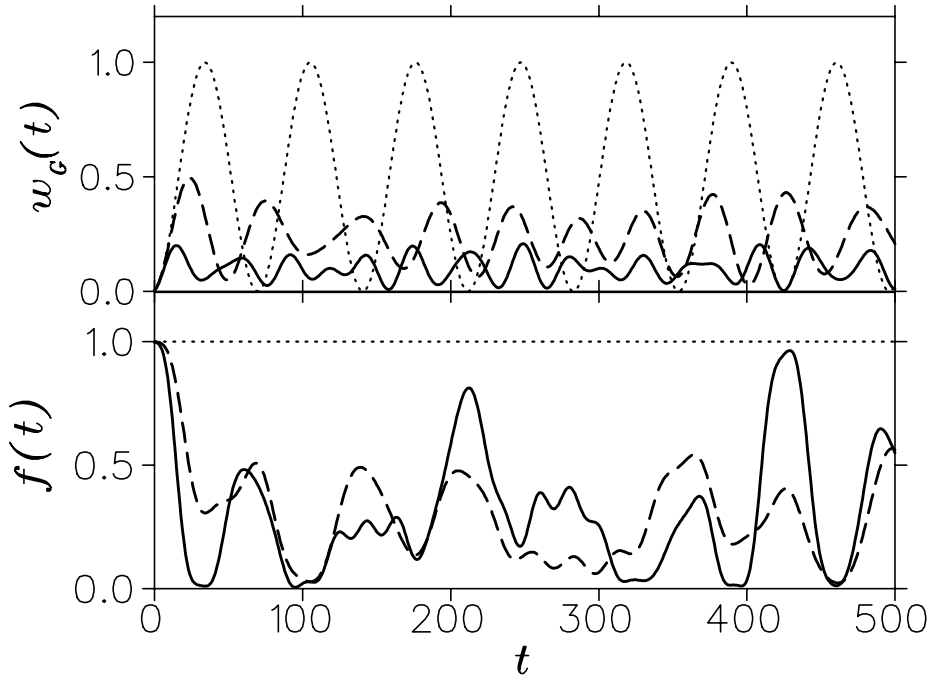


FIG. 5.1 – Probabilité d'état cherché $w_G(t)$ (panneau supérieur) et fidélité $f(t)$ (panneau inférieur) en fonction des pas d'itération t dans l'algorithme de Grover pour $n_{tot} = 12$ qubits. Les courbes pointillées montrent les résultats pour l'algorithme idéal ($\varepsilon = 0$), les courbes hachurées et pleines correspondent respectivement à des intensités d'imperfections $\varepsilon = 4 \cdot 10^{-4}$ et 10^{-3}.

Ici, nous étudions comment l'algorithme de Grover est affecté par les imperfections statiques dans le modèle introduit dans [42] et décrit à la section 1.2.2. . Un exemple typique des effets des imperfections sur la précision de l'algorithme de Grover est montré à la Fig. 5.1 pour une réalisation donnée du désordre de H_S (1.21) sur un réseau 3×4 de qubits. On peut constater clairement que les imperfections suppriment la probabilité w_G de trouver l'état cherché. w_G est donné par la somme des probabilités des états $|\tau\rangle$ et $|\tau + N\rangle$. Contrairement au cas des erreurs quantiques aléatoires dépendantes du temps, étudiées dans [73], les oscillations de la probabilité w_G ne décroissent pas avec le temps t pour le cas

d'imperfections statiques. Une autre caractéristique intéressante est la nette décroissance de la période des oscillations de Grover en comparaison avec le cas de l'algorithme idéal où $T_G = \pi/2\omega_G$. Cet effet est aussi absent dans le cas d'erreurs aléatoires. La fidélité du calcul quantique $f(t)$ possède également des oscillations non atténuées pour les longs temps. Cependant, en moyenne le maximum de la fidélité correspond au minimum de la probabilité w_G plutôt qu'à son maximum. Par conséquent, $f(t)$ n'est pas une mesure appropriée pour tester la précision de l'algorithme.

D'après [77], une représentation graphique de l'évolution dynamique de l'algorithme de Grover peut être obtenue à l'aide de la fonction de Husimi [78] (Fig.5.2). Dans cette représentation, la base de calcul x peut être considérée comme étant une coordonnée dans l'espace de représentation de la fonction d'onde $\psi(x)$ ($x = 0, \ldots, 2N-1$), tandis que la base conjuguée obtenue par transformation de Fourier correspond à la représentation du moment p ($p = -N+1, \ldots, N$). De cette façon, l'état initial de l'algorithme de Grover $|\psi_0\rangle$ donne une distribution piquée avec $p = 0$. Pour l'algorithme idéal, la probabilité totale est distribuée entre deux états $|\tau\rangle$ et $|\eta\rangle$ (voir Eq.(1.5)), ce qui donne deux lignes orthogonales dans l'espace des phases de la fonction de Husimi (voir Fig.5.2, ligne supérieure). Après une période $T_G \approx 34$, tout le poids de la probabilité est transféré sur l'état cible $|\tau\rangle$ ($w_G \approx 1$). En présence d'imperfections modérées, le basculement des qubits auxiliaires devient possible, ce qui met en jeux deux états additionnels dans la dynamique. Ainsi, la probabilité est principalement distribuée sur *quatre états* correspondant à quatre lignes droites dans l'espace des phases (Fig.5.2, ligne centrale) :

$$\begin{array}{ll} |\tau_0\rangle = |\tau\rangle & |\tau_1\rangle = |\tau + N\rangle \\ |\eta_0\rangle = |\eta\rangle & |\eta_1\rangle = \sum_{x\neq\tau}^{(0\leq x<N)} |x+N\rangle/\sqrt{N-1}. \end{array} \tag{5.1}$$

La probabilité w_4 contenue dans ces états est proche de l'unité ($w_4 = 0.998$ pour $\varepsilon = 10^{-3}$ sur la Fig.5.2). Au-dessus d'un seuil critique ε_c, cette structure simple disparaît complétement ($w_4 = 6 \cdot 10^{-4}$), et la fonction de Husimi n'est plus qu'une distribution aléatoire (Fig.5.2, ligne inférieure).

La contribution dominante de ces quatre états peut être aussi observée au travers de la densité spectrale $S(\omega)$ de la fonction d'onde $\psi_x(t)$. Cette densité est définie par $S(\omega) = \sum_x |a_x(\omega)|^2$, où $a_x(\omega) = \sum_{t=0}^{T_f} \psi_x(t) \exp(i\omega t)/\sqrt{T_f}$ et où T_f est une échelle de temps grande sur laquelle le spectre est fixé (nous avons typiquement utilisé $T_f \approx 5T_G \gg T_G$). Le diagramme de phase de la densité spectrale $S(\omega)$ dépendant de l'intensité des imperfections ε est montré à la Fig.5.3. Deux phases sont clairement présentes : pour $\varepsilon < \varepsilon_c$, le diagramme contient quatre lignes correspondant aux quatre états (5.1), tandis que pour $\varepsilon > \varepsilon_c$, ces lignes sont détruites et le spectre devient continu. Ces phases correspondent au changement qualitatif de la distribution de Husimi montrée sur la Fig.5.2.

Pour étudier la transition entre ces phases d'une manière plus quantitative, nous allons analyser comment les probabilités w_G et w_4 dépendent de l'intensité des imperfections ε pour un grand nombre de réalisation du désordre dans H_S (1.21) en changeant aussi le nombre de qubits n_{tot}. Le nombre de réalisation varie de 50 à 1000 selon les valeurs de ε et n_{tot}. Puisque la fréquence des oscillations de Grover varient fortement avec ε et le désordre, nous faisons la moyenne de w_G et w_4 sur un grand nombre d'intervalles de temps

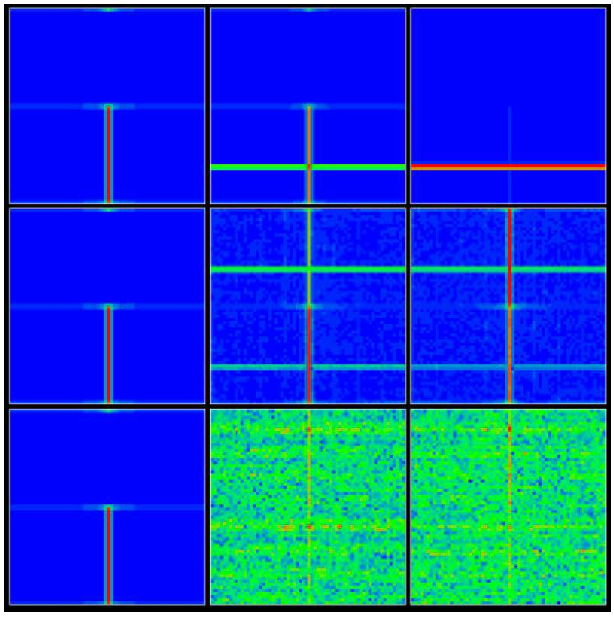


FIG. 5.2 – Evolution de la fonction de Husimi pour l'algorithme de Grover aux temps $t = 0$, 17, et 34 (de gauche à droite), et pour $\varepsilon = 0$, 0.001, et 0.008 (de haut en bas). Le réseau de qubits et la réalisation du désordre sont les même que ceux utilisés pour la Fig.5.1. L'axe vertical désigne 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).

T_f afin de supprimer les fluctuations temporelles. Les résultats obtenus sont synthétisés à la Fig.5.4. Pour une valeur fixe de n_{tot}, le comportement de $w_G(\varepsilon)$ change fortement d'une réalisation du désordre à l'autre (Fig.5.4a). Par contre, la probabilité w_4 reste proche de l'unité, se montrant insensible aux variations du désordre tant que $\varepsilon < \varepsilon_c$ (Fig.5.4b). Uniquement pour $\varepsilon > \varepsilon_c$, lorsque $w_4 \ll 1$, cette dernière devient sensible au désordre. Les probabilités moyénnées sur le désordre, $\bar{w}_G$ et $\bar{w}_4$, sont montrée aux Figs.5.4 a et b. Elles entreprennent également un changement de comportement à proximité de ε_c, ceci est le cas plus particulièrement de $\bar{w}_4$. Ces résultats confirment le fait que la transition de phase à lieu aux alentours d'un certain ε_c pour un ensemble de réalisations du désordre.

Les valeurs de ε_c peuvent être obtenues à partir de l'estimation suivante. Le taux de transition induit par les imperfections après une itération de Grover est donné par la règle d'or de Fermi : $\Gamma \sim \varepsilon^2 n_g^2 n_{tot}$, où n_{tot} apparaît en raison de la contribution aléatoire des couplages de qubits ε, tandis que le facteur n_g^2 prend en compte l'accumulation cohérente de perturbations sur les n_g portes utilisées pour une itération (voir par exemple [44]). Dans l'algorithme de Grover, les quatre états (5.1) sont séparés de tous les autres par un écart d'énergie $\Delta E \sim 1$ (cela est dû au changement de signe introduit par les opérateurs O et D). Ainsi, ces quatre états sont mélangés avec les autres pour

$$\varepsilon > \varepsilon_c \approx 1.7/(n_g\sqrt{n_{tot}}) \tag{5.2}$$

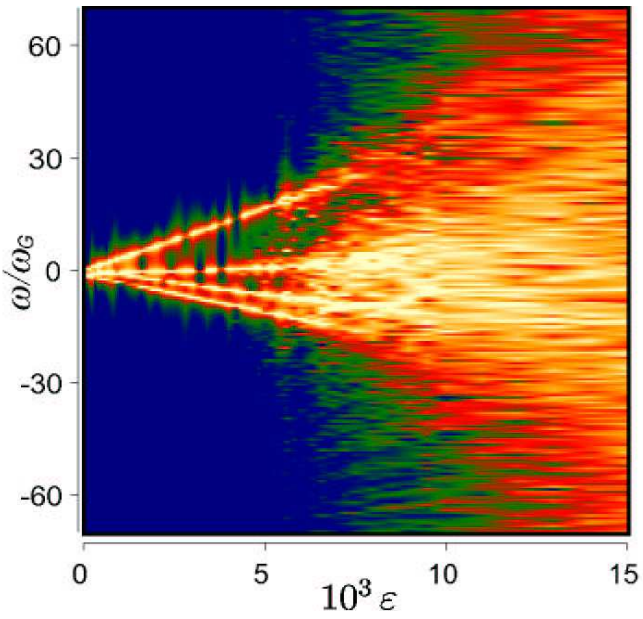


FIG. 5.3 – Diagramme de phase de la densité spectrale $S(\omega)$ en fonction de l'intensité des imperfections ε, $n_{tot} = 12$, la réalisation du désordre est la même que celle utilisée à la Fig.5.2. La couleur est proportionnelle à la densité $S(\omega)$ (jaune pour le maximum et bleu pour zéro).

avec $\Gamma > \Delta E$. Ici, le facteur numérique est obtenu à partir des données numériques. Ces résultats sont confirmés pour $\bar{w}_4$ (voir Fig.5.4d).

La variation de la probabilité de Grover $\bar{w}_G$ avec ε et n_{tot} est montrée à la Fig.5.4c. Sa dépendance par rapport aux paramètres du système peut être comprise à partir du simple modèle du rotateur avec un seul pulse. Dans ce modèle, l'action des imperfections statiques dans toutes les portes impliquées dans une itération de Grover est remplacé par un simple opérateur unitaire de pulse $U_{eff} = \exp(-iH_s n_g R)$ agissant après chaque itération. Ici, R est un facteur de renormalisation sans dimension qui prend en compte le fait que les portes ne commutent pas avec H_S. Les Figs.5.4 a et b montrent que cette approximation à un seul pulse donne une bonne description des données originales moyénnées avec $R = 0.56$. Ainsi, les effets de la normalisation jouent un rôle non négligeable et par conséquent ce modèle ne doit pas décrire la variation de probabilité pour une réalisation donnée du désordre. Cependant, la dépendance moyénnée est correctement reproduite.

Dans le régime où la dynamique de l'algorithme de Grover est dominée par le sous espace des quatre états (5.1), le modèle à un pulse peut être traité analytiquement. Les éléments de matrices du hamiltonien effectif dans cet espace sont

$$H_{eff} = \begin{pmatrix} A+a & 0 & -i\omega_G & 0 \\ 0 & A-a & 0 & -i\omega_G \\ i\omega_G & 0 & B & b \\ 0 & i\omega_G & b & B \end{pmatrix}, \tag{5.3}$$

où $A = -Rn_g \sum_{i=1}^{n_q} a_i \langle\tau|\sigma_i^{(z)}|\tau\rangle$, $B = Rn_g \sum_{i<j}^{n_q} b_{i,j} - b$, $a = -Rn_g a_{n_q+1}$ et $b = Rn_g(b_{n_q+1,n_q+2-L_x} +$

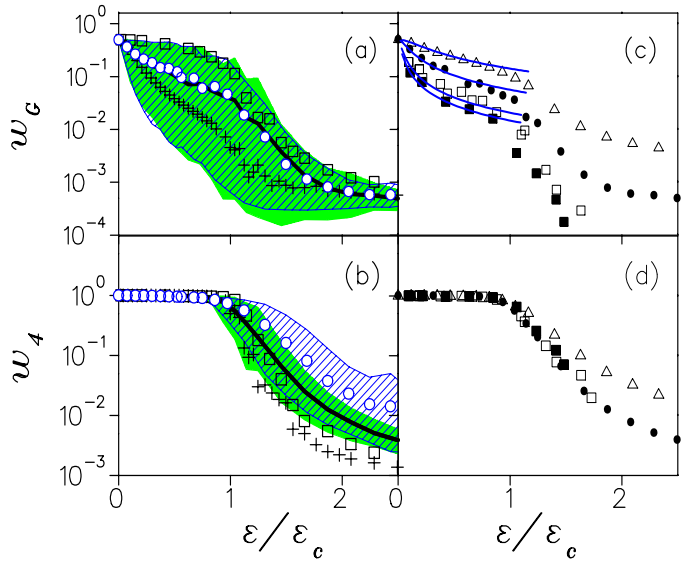


FIG. 5.4 – Probabilités w_G (a,c) et w_4 (b,d) en fonction de l'intensité des imperfections $\varepsilon/\varepsilon_c$, avec ε_c obtenu à partir de (5.2). Pour les panneaux (a,b) $n_{tot} = 12$, les carrés et les signes + désignent des données provenant de deux réalisations typiques différentes du désordre, les zones vertes/grises désignent les régions de variation de probabilité pour différentes réalisations du désordre (voir texte), les courbes en gras désignent les moyennes $\bar{w}_G$ et $\bar{w}_4$. Les zones hachurées délimitées par des très fins désignent la région de variation de probabilité du modèle à un pulse, les cercles vides désignent les données dans ce modèle avec le facteur d'échelle $R = 0.56$. Les panneaux (c,d) présentent $\bar{w}_G$ et $\bar{w}_4$ pour $n_{tot} = 9$ (triangles), 12 (cercles pleins), 15 (carrés vides) et 16 (carrés pleins). Sur le panneau (c), les courbes pleines sont données par l'Eq.(5.4).

$b_{n_q+1,L_x} + b_{n_q,n_q+1} + b_{n_q+1-L_x,n_q+1}$). Les qubits sont ordonnés sur un réseau $L_x \times L_y$, et numéroté par la formule $i = x + L_x(y-1)$, avec $x = 1, \ldots, L_x$, $y = 1, \ldots, L_y$. Dans la limite de n_q grand, les termes a, b sont plus petits que A, B d'un facteur $1/\sqrt{n_q}$ et H_{eff} esr réduit à une matrice 2×2, ce qui donne $w_G = 2\omega_G^2/[(A-B)^2 + 4\omega_G^2]$. Pour une valeur large de n_q, la difference $A - B$ possède un distribution gaussienne avec une largeur $\sigma = Rn_g\sqrt{n_q/3}\sqrt{\alpha^2 + 2\beta^2} = \varepsilon R n_g \sqrt{n_q}$. La convolution de w_G avec cette distribution donne

$$\bar{w}_G = \sqrt{\pi/2}(1 - \mathrm{erf}(\sqrt{2}\omega_G/\sigma)) \exp(2\omega_G^2/\sigma^2)\, \omega_G/\sigma. \tag{5.4}$$

Cette formule donne une bonne description des données numériques montrées à la Fig.5.4, ce qui confirme la validité du modèle à un pulse. Pour $\sigma \gg \omega_G$ et pour une réalisation typique du désordre avec $(A-B) \sim \sigma$, la fréquence des oscillations de Grover est fortement renormalisée, $\omega \approx (A-B) \sim \sigma \gg \omega_G$, et en accord avec la Fig.5.3, $\omega \sim \varepsilon/\varepsilon_c$. Dans ce cas typique, $w_G \sim \omega_G^2/\sigma^2 \ll 1$ (presque tout le poids de la probabilité se trouve sur les états $|\eta_0\rangle$,$|\eta_1\rangle$). Ainsi, le nombre total d'opérations quantiques N_{op} requisent pour la détection de l'état recherché $|\tau\rangle$, 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. [1] Par conséquent, en présence de fortes imperfections statiques, 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 $\varepsilon \sim \varepsilon_c$, il n'y a pas de gain en comparaison avec le cas classique.

Dans ce chapitre nous avons montré que l'algorithme de Grover reste robuste en présence d'imperfections statiques, cela à l'intérieur d'un domaine bien défini. Nous avons également déterminé quelles sont les influences de l'intensité des imperfections statiques sur l'efficacité de l'algorithme de Grover. Ce travail a ete publié dans [5] (voir article IV en appendice).

[1] Ici nous considérons seulement le sous-espace (5.1), une petite fuite de probabilité dans tous les autres états n'étant pas crucial parce que il sera aléatoirement distribués parmis ces $2N-4$ états.

Conclusion

Dans cette thèse, nous avons abordé certains problèmes liés au domaine de l'information quantique.

Nous avons montré l'équivalence des deux propriétés conjecturées de l'intrication de formation : son additivité et sa superadditivité forte. Les conjectures qui déclarent que l'intrication de formation et la capacité classique d'Holevo-Schumacher-Westmorland d'un canal quantique sont additives, n'ont pas été démontrées dans le cas général, mais elles sont soutenues par un certain nombre de simulations numériques et elles ont été prouvées pour certains cas particuliers. Aucun contre-exemple n'a été trouvé. On a montré dans [55], que les deux conjectures sont vraies si l'IDF a la propriété de superadditivité forte. Le but du présent travail a été d'approfondir ce raccordement en établissant le fait que la superadditivité forte de l'IDF est suivie de son additivité et que les deux conjectures sont donc équivalentes. Ce fait rend encore plus important l'étude supplémentaire de ces deux conjectures. La conjecture de superadditivité forte qui jusqu'ici a semblé plutôt spéculative, devient aussi plausible que la conjecture d'additivité. Trouver un contre-exemple à la première donnerait immédiatement un contre-exemple à la seconde. Il apparaît clairement que ce n'est pas un hasard si toutes les preuves connues de l'additivité de l'IDF pour des sous-espaces quantiques particuliers [52] sont basées sur des preuves de la conjecture de superadditivité forte pour ces sous-espaces. L'étude du problème de l'additivité de l'IDF revêt maintenant un caractère bien plus important qu'auparavant, car sa preuve fournirait automatiquement la preuve de l'additivité de la capacité d'un canal classique. La résolution du problème de l'additivité sera une des tâches les plus urgentes pour les prochaines années.

Nous avons proposé une nouvelle mesure pour l'incertitude du résultat d'une mesure quantique pour les états mélangés. Nous avons trouvé une formule explicite pour cette mesure et nous avons étudié les les plus importantes de ses propriétés. Les résultats d'une mesure quantique ont généralement une distribution de probabilité avec l'entropie de Shannon différente de zéro. Cette distribution ainsi que son entropie dépendent de la base de la mesure quantique choisie. La valeur minimale de l'entropie est donnée par l'entropie de Von-Neumann de cet état quantique. Notre proposition est de considérer la valeur moyenne de l'entropie sur toutes les bases possibles. Dans le dernier cas, l'entropie d'un état pur est généralement différente de zéro. Nous avons dérivé une expression explicite pour l'entropie informationnelle moyenne. Cette expression peut être partagée en deux parties d'une manière naturelle. La première partie donne l'entropie d'incertitude

minimale des états purs $S_0(N)$. Elle peut être associée à l' *moyenne* incertitude minimale entropique [66]. La seconde partie est l'entropie statistique excessive des mélanges $S_{\text{F}}[\rho]$. Elle peut être employée comme une mesure pour le manque de pureté des états quantiques et elle peut être fortement corrélée avec l'entropie de Von-Neumann $S_{\text{H}}[\rho]$. Elle est limitée au-dessus par $(1-\gamma)$, où γ est la constante d'Euler. L'entropie informationnelle totale $S[\rho]$, a les propriétés prévues du point de vue de la théorie de l'information. Etant donné l'élégance mathématique de la définition de l'entropie informationnelle et de ses agréables propriétés, nous aurions tout intérêt à lui trouver des applications physiques concrètes.

Nous avons considéré l'algorithme quantique de recherche dans une base de donnée non-structurée (algorithme de Grover) en présence des imperfections statiques. Nous avons montré que l'algorithme de Grover reste robuste en présence des erreurs statiques, dans le cadre d'un domaine de paramètres bien définis. Nous avons également déterminé quelles sont les influences de l'intensité des imperfections statiques sur l'efficacité de l'algorithme de Grover.

Nous avons étudié l'exécution par l'ordinateur quantique avec les imperfections statiques de la simulation du modèle de rotateur pulsé qui permet d'étudier la transition d'Anderson. Nous avons proposé un nouvel algorithme quantique pour la simulation de modèles du type du rotateur pulsé. Le rotateur pulsé est le modèle du chaos quantique le plus populaire. Notre algorithme est efficace du point de vue du nombre d'opérations et ne demande aucun qubit supplémentaire. Ensuite, nous avons étudié la stabilité de cet algorithme en présence des erreurs statiques qui représentent la source de decohérence la plus dangereuse. Ces résultats montrent que des systèmes aussi complexes que ceux qui présentent un certain chaos peuvent être simulés avec une bonne précision sur des ordinateurs quantiques réalistes, même avec un nombre modéré de qubits et ce de manière beaucoup plus efficace que sur un ordinateur classique. On peut s'attendre à ce que le progrès expérimental dans la construction des ordinateurs quantiques permettra l'implémentation des algorithmes quantiques abordés dans le présent travail ; ce qui exigera une étude encore plus approfondie des effets des imperfections statiques tout comme des autres sources de la decohérence dans les réalisations concrètes des ordinateurs quantiques.

Bibliographie

[1] M.A. Nielsen et I.L. Chuang *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2000).

[2] A.A. Pomeransky, "Strong superadditivity of the entanglement of formation follows from its additivity", Phys.Rev. A **68**, 032317 (2003), e-print quant-ph/0305056

[3] A. Stotland, A.A. Pomeransky, E. Bachmat et D. Cohen, "The information entropy of quantum mechanical states", Europhys.Lett. **67**,700 (2004), e-print quant-ph/0401021.

[4] A.A. Pomeransky, D.L. Shepelyansky, Phys. Rev. A **69**, 014302 (2004).

[5] A.A.Pomeransky, O.V.Zhirov, et D.L.Shepelyansky, "Phase diagram for the Grover algorithm with static imperfections," e-print quant-ph/0403138, accepté pour publication dans European Physical Journal D.

[6] R.P. Feynman, "Simulating physics with computers", Int. J. of Theor. Phys. **21**, Nos. 6/7 (1982).

[7] P.W.Shor, dans *Proc. 35th Annual Symposium on Foundation of Computer Science*, Ed. S.Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p.124.

[8] W.K Wootters et W.H. Zurek, Nature **299**, 802 (1982).

[9] D. Dieks, Phys. Lett. **92A**, 271 (1982).

[10] A. Barenco,*et al.*, Phys. Rev. A **52**, 3457 (1995).

[11] D.E. Knuth *The Art of Computer Programming, Volume 2 : Seminumerical Algorithms*, Addison-Wesley, Reading, MA (1981).

[12] D. Coppersmith, IBM Research Report No. RC19642 (1994).

[13] D. Deutch, unpublished (1994).

[14] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).

[15] G. Benenti, G. Casati, S. Montangero, et D.L. Shepelyansky, Phys. Rev. Lett. **87**, 227901 (2001).

[16] G. Benenti, G. Casati, S. Montangero, et D.L. Shepelyansky, Eur. Phys. J. D **20**, 293 (2002).

[17] G. Benenti, G. Casati, S. Montangero, et D.L. Shepelyansky, quant-ph/0206130.

[18] G. Benenti, G. Casati, S. Montangero, et D.L. Shepelyansky, Phys. Rev. A **67**, 052312 (2003).

[19] B. Georgeot, et D.L. Shepelyansky, Phys. Rev. Lett. **86**, 2890 (2001).

[20] P.W. Anderson, Phys. Rev. **109**, 1492 (1958).

[21] P.A. Lee et T.V. Ramakrishnan, Rev. Mod. Phys. **57**, 287 (1985).

[22] B. Kramer et A. MacKinnon, Rep. Prog. Phys. **56**, 1469 (1993).

[23] A.D. Mirlin, Phys. Rep. **326**, 259 (2000).

[24] B.I. Shklovskii, B. Shapiro, B.R. Sears, P. Lambrianides et H.B. Shore, Phys. Rev. B **47**, 11487 (1993).

[25] I.K. Zharekeshev et B. Kramer, Ann. Phys. (Leipzig) **7**, 442 (1998).

[26] T. Ohtsuki, K.Slevin et T. Kawarabayashi, Ann. Phys. (Leipzig) **8**, 655 (1999) ; Y. Asada, K. Slevin, et T. Ohtsuki, Phys. Rev. Lett. **89**, 256601 (2002).

[27] B. V. Chirikov, Phys. Rep. **52**, 263 (1990).

[28] G. Casati, B. V. Chirikov, F. M. Izraelev, et J. Ford, dans "Stochastic Behavior in Classical and Quantum Hamiltonian Systems," edité par G. Casati et J. Ford, Lecture Notes in Physics Vol. 93 (Springer, Berlin, 1979).

[29] B. V. Chirikov, F. M. Izrailev, et D. L. Shepelyansky, Sov. Sci. Rev. Sec. C **2**, 209 (1981).

[30] F. M. Izrailev et D. L. Shepelyansky, Teor. Mat. Fiz. **43**, 417 (1980) ; [Theor. Math Phys. **43**, 553 (1980)] ; Dok. Akad. Nauk SSSR **249**, 1103 (1979) ; [Sov. Phys-Dokl. **24**, 996, 1979)].

[31] F. M. Izrailev, Phys. Rep. **129**, 299 (1990) ;

[32] D. L. Shepelyansky, Phys. Rev. Lett. **56**, 677 (1986)

[33] S. Fishman, D.R. Grempel, et R.E. Prange, Phys. Rev. Lett. **49**, 509 (1982) ; Phys. Rev. A **29**, 1639 (1984).

[34] G.Casati, I.Guarneri et D.L.Shepelyansky, Phys. Rev. Lett. **62**, 345 (1989).

[35] F.Borgonovi et D.L.Shepelyansky, Physica D **109**, 24 (1997).

[36] F.Borgonovi et D.L.Shepelyansky, J. de Physique I France **6**, 287 (1996).

[37] W. H. Zurek, "Decoherence, einselection, and the quantum origins of the classical," Rev. Mod. Phys. **75**, 715 (2003).

[38] J.I. Cirac et P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[39] C.Miguel, J.P.Paz et W.H.Zurek, Phys. Rev. Lett. **78**, 3971 (1997).

[40] B. Georgeot et D.L. Shepelyansky, Phys. Rev. Lett. **86**, 5393 (2001).

[41] S. Bettelli, Phys. Rev. A **69**, 042310 (2004), et quant-ph/0310152.

[42] B.Georgeot et D.L.Shepelyansky, Phys. Rev. E **62**, 3504 (2000) ; **62**, 6366 (2000).

[43] M.Terraneo et D.L.Shepelyansky, Phys. Rev. Lett. **90**, 257902 (2003).

[44] K.M. Frahm, R. Fleckinger, et D.L. Shepelyansky, Eur. Phys. J. D **29** 139 (2004), et quant-ph/0312120.

[45] A. Einstein, B. Podolsky, et N. Rosen, "Can quantum-mechanical description of physical reality be considered complete ?", Phys. Rev. **47**, 777 (1935). Réédité dans *Quantum Theory and Measurement* (J.A. Wheeler and W.Z. Zurek, eds, Princeton University Press, 1983.

[46] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox." Physics **1**, 195 (1964). Réédité dans J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, 1987), p. 14.

[47] J. F. Clauser, M. A. Horne, A. Shimony, et R. A. Holt, Phys. Rev. Lett. **23**, 880 (1980).

[48] J.F. Clauser et A. Shimony, Rep. Prog. Phys. **41**, 1981 (1978) ; A. Aspect, P. Grangier et G. Roger, Phys. Rev. Lett. **47**, 460 (1981) ; P.G. Kwiat et. al., Phys. Rev. Lett. **75**, 4337 (1995).

[49] C.H. Bennett, D.P. DiVincenzo, J. Smolin et W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[50] V. Vedral, M.B. Plenio, M.A. Rippin et P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[51] M. Ohya et D. Petz, *Quantum Entropy and Its Use*, (Springer-Verlag 1993).

[52] G. Vidal, W. Dür et J.I. Cirac, Phys. Rev. Lett. **89**, 027901 (2002).

[53] P.M. Hayden, M. Horodecki et B.M. Terhal, J. Phys. A **34**, 6891 (2001).

[54] K.G.H. Vollbrecht et R.F. Werner, Phys. Rev. A **64**, 062307 (2001).

[55] K. Matsumoto, T. Shimono et A. Winter, "Remarks on Additivity of the Holevo Channel Capacity and of the Entanglement of Formation," Commun. Math. Phys. **246**, 427 (2004) et quant-ph/0206148 (2002).

[56] G.G. Amosov, A.S. Holevo et R.F. Werner, Problems in Information Transmission **36**, 25 (2000) et math-ph/0003002 (2000).

[57] P.W. Shor, J. Math. Phys. **43**, 4334 (2002).

[58] K.M.R. Audenaert, S.L. Braunstein, "On Strong Superadditivity of the Entanglement of Formation," Commun. Math. Phys. **246**, 443 (2004) et quant-ph/0303045 (2003).

[59] F. Benatti et H. Narnhofer, Phys. Rev. A **63**, 042306 (2001).

[60] K. Audenaert, F. Verstraete et B. De Moor, Phys. Rev. A **64**, 052304 (2001).

[61] R.T. Rockafellar, *Convex Analysis*, Princeton University Press, Princeton (1970).

[62] P.W. Shor, "Equivalence of Additivity Questions in Quantum Information Theory," Commun. Math. Phys. **246**, 453 (2004) et quant-ph/0305035 (2003).

[63] Voir Réf. [1] pour une revue détaillée et un liste de références complet. En particulier, Chapitre 11 "Entropy and Information".

[64] *Quantum Signature of Chaos*, by F. Haake (Springer, 2000). See in particular Sec. 4.8.

[65] P. Garbaczewski, cond-mat/0301044.

[66] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).

[67] S. Lloyd, Science **273**, 1073 (1996).

[68] G. Ortiz, J.E. Gubernatis, E. Knill, et R.Laflamme, Phys. Rev. A **64**, 22319 (2001).

[69] R. Schack, Phys. Rev. A **57**, 1634 (1998).

[70] Y.S. Weinstein, S. Lloyd, J. Emerson, et D.G. Cory, Phys. Rev. Lett. **89**, 157902 (2002).

[71] L.M.K.Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, et I.L. Chuang, Nature **414**, 883 (2001).

[72] P.H.Song et D.L.Shepelyansky, Phys. Rev. Lett. **86**, 2162 (2001).

[73] P.H. Song et I. Kim, Eur. Phys. J. D **23**, 299 (2003).

[74] G.P. Berman, F. Borgonovi, F.M. Izrailev, et V.I. Tsifrinovich, Phys. Rev. E **64**, 056226 (2001).

[75] G. Benenti, G. Casati, et D.L. Shepelyansky, Eur. Phys. J. D **17**, 265 (2001).

[76] D. Braun, Phys. Rev. A **65**, 042317 (2002).

[77] C. Miquel, J.P. Paz et M. Saraceno, Phys. Rev. A **65**, 062309 (2002).

[78] S.-J. Chang et K.-J. Shi, Phys. Rev. A **34**, 7 (1986).

Appendice

Article I

A.A. Pomeransky, "Strong superadditivity of the entanglement of formation follows from its additivity", Phys. Rev. A **68**, 032317 (2003).

Article II

A. Stotland, A.A. Pomeransky, E. Bachmat et D. Cohen, "The information entropy of quantum mechanical states", Europhys. Lett. **67**, 700 (2004).

Article III

A.A. Pomeransky, D.L. Shepelyansky, Phys. Rev. A **69**, 014302 (2004).

Article IV

A.A.Pomeransky, O.V.Zhirov, et D.L.Shepelyansky, "Phase diagram for the Grover algorithm with static imperfections," Eur. Phys. J. D **31**, 131 (2004).