

UNIVERSITÉ PARIS 7 – DENIS DIDEROT
UFR de Physique

THÈSE

Pour l'obtention du Diplôme de

DOCTEUR DE L'UNIVERSITÉ PARIS 7
SPÉCIALITÉ : PHYSIQUE THÉORIQUE

Présentée et soutenue publiquement par

Benjamin Lévi

le 9 novembre 2004

Titre :

**Simulation de systèmes quantiques
sur un ordinateur quantique réaliste**

Directeurs de thèse :

Bertrand GEORGEOT
Dima SHEPELYANSKY

JURY

| | |
|----------------------|-----------------------|
| Pr Gernot ALBER | Examineur |
| Dr Denis FEINBERG | Rapporteur |
| Dr Bertrand GEORGEOT | Directeur de thèse |
| Pr Philippe LAFARGE | Président du jury |
| Dr Dima SHEPELYANSKY | Co-directeur de thèse |
| Dr Dietmar WEINMANN | Rapporteur |

À Manuel

Remerciements

Je voudrais tout d'abord chaleureusement remercier Bertrand Georgeot et Dima Shepelyansky pour leur accompagnement tout au long de cette thèse. J'ai beaucoup apprécié leur disponibilité, leur implication et leur gentillesse.

Ma reconnaissance va également à Denis Feinberg et Dietmar Weinmann pour avoir accepté la lourde tâche d'être rapporteurs de ma thèse malgré un délai assez court, ainsi qu'à Philippe Lafarge et Gernot Alber pour avoir accepté de faire partie du jury.

Je remercie l'IRSAMC de m'avoir accueilli pendant ces trois années, et plus particulièrement le Laboratoire de Physique Théorique et son directeur Didier Poilblanc. Je voudrais également exprimer ma gratitude à Sylvia Scaldaferrò, Gisèle Dedieu, Nicolas Elefantis et Patrick Pérez pour leur efficacité et leur amabilité.

Merci aussi à mon école doctorale, et particulièrement Yves Charon et Agnès Feroq, de m'avoir accueilli en DEA et de m'avoir permis ensuite de partir vers le grand sud. À ce propos, merci également à l'école doctorale de physique de Toulouse de m'avoir accordé un monitorat malgré mon appartenance à une autre école.

Un grand merci également à Klaus Frahm pour les nombreuses discussions physiques ou non, à Marcello Terraneo pour m'avoir supporté dans le bureau pendant deux ans et pour s'être sacrifié pendant tout ce temps en me donnant son chocolat à la cantine, à Stefano Bettelli, magicien des temps modernes, pour sa patience et ses explications informatiques toujours limpides, et enfin à Pierre-Henri Chavanis, Leang Ming Ma et Raphaël Cherrier pour leur bonne humeur communicative.

Je tiens à saluer aussi Eleonora Bettelli, Olivier Chiappa, Catherine Armengaud, Claire Vallat, Vianney Desoutter, David Magnoux, Claudine Colnard, Fabien Mégi, Julien Sopik, Guillaume Roux, Giampaolo Cristadoro, Jae-Weon Lee, Andrei Pomeransky, José Lages, Éric Giglio et Suriyanarayanan Kothandaraman pour tous les bons moments. Que tous ceux que j'ai oublié ici me pardonnent !

Enfin, je voudrais remercier mes parents et ma soeur pour leur soutien qui dure depuis bien avant le début de cette thèse, et mon chat, animal quantique par excellence, qui n'en pense pas moins sous ses airs placides. Je les aime tous beaucoup.

Table des matières

| | | |
|----------|---|------------|
| 1 | Introduction | 9 |
| 2 | Informatique quantique | 13 |
| 2.1 | Opérations quantiques | 13 |
| 2.1.1 | Opérations sur un qubit | 13 |
| 2.1.2 | Opérations élémentaires et universalité | 16 |
| 2.1.3 | Opérations contrôlées | 17 |
| 2.2 | Transformée de Fourier quantique | 21 |
| 2.2.1 | Algorithme de la Transformée de Fourier | 21 |
| 2.2.2 | Estimation de phase | 24 |
| 2.3 | Recherche quantique | 26 |
| 2.3.1 | Algorithme de Grover | 26 |
| 2.3.2 | Amplification d'amplitude | 31 |
| 2.4 | Simulations de systèmes quantiques | 33 |
| 3 | Simulation du rotateur pulsé | 37 |
| 3.1 | Applications Quantiques : exemple du rotateur pulsé | 37 |
| 3.1.1 | Rotateur pulsé classique | 37 |
| 3.1.2 | Rotateur pulsé quantique | 47 |
| 3.1.3 | Localisation dynamique et localisation d'Anderson | 52 |
| 3.2 | Résultats sur le rotateur pulsé | 60 |
| 3.3 | Publication I | 63 |
| 4 | Simulation du Harper pulsé | 75 |
| 4.1 | Le modèle de Harper | 75 |
| 4.1.1 | Modèle de Harper | 75 |
| 4.1.2 | Modèle de Harper pulsé | 76 |
| 4.2 | Résultats sur le modèle de Harper pulsé | 78 |
| 4.3 | Publication II | 81 |
| 5 | Conclusion | 103 |

| | |
|---|------------|
| A Fonctions de Wigner et Husimi | 105 |
| A.1 Fonction de distribution générale | 105 |
| A.2 Distribution de Wigner | 107 |
| A.3 Distribution de Husimi | 111 |
| A.4 Relation entre les distributions de Wigner et de Husimi . . . | 115 |
| A.5 Distribution de Wigner discrète | 116 |
| A.6 Distribution de Husimi discrète | 119 |

Chapitre 1

Introduction

Historiquement, la première évocation du concept d'ordinateur quantique remonte à des travaux du début des années 1980, en particulier ceux de Richard Feynman [12, 34, 35]. Il s'agissait alors de répondre à la question suivante : quel type d'ordinateur est le plus adapté pour simuler un système physique quantique ? Pour qu'un tel ordinateur soit réalisable en pratique, les ressources nécessaires (taille, temps ou énergie) ne doivent pas croître exponentiellement avec la taille du système à simuler. Dans le cas d'un ordinateur classique standard, ce souhait interdit notamment de stocker les états intermédiaires de la simulation. En effet, pour un système à N corps, le nombre d'amplitudes complexes nécessaires pour caractériser complètement un état de l'espace de Hilbert croît exponentiellement avec le nombre de particules (si le nombre de niveaux par particule est fini). On peut éventuellement envisager de simuler le système quantique par un ordinateur classique probabiliste, c'est-à-dire essayer de reproduire fidèlement les résultats de n'importe quelle mesure sur le système avec les mêmes probabilités. Mais une fois encore, il s'avère que cela n'est pas possible car cela revient à utiliser un modèle à variables cachées, ce qui est en désaccord avec les données expérimentales sur la violation des inégalités de Bell. Pour simuler efficacement un système quantique, il faut donc faire appel à un ordinateur qui fonctionne lui aussi selon les lois de la mécanique quantique.

Ce concept d'ordinateur quantique fut repris en 1985 par David Deutsch [29], alors motivé par un problème d'informatique théorique : comment définir ce qui est calculable ? Le paradigme en vigueur était celui résumé laconiquement par l'hypothèse de Turing-Church forte :

Tout procédé algorithmique peut être simulé efficacement en utilisant une machine de Turing probabiliste.

Dit autrement, tous les ordinateurs sont équivalents à une machine de Turing probabiliste, et celle-ci définit ce qui est calculable ou non. Cette définition de ce qu'est un algorithme est purement heuristique, et l'objectif de Deutsch

était d'arriver à l'asseoir (elle ou une version modifiée) au moins sur des bases physiques. Comme les lois physiques fondamentales sont quantiques, il fut tout naturellement amené lui aussi à imaginer un ordinateur quantique. De fait, il exhiba un problème simple qui peut être résolu efficacement sur une telle machine, mais qui n'admet pas de solution efficace sur un ordinateur classique. Ceci met à mal l'hypothèse de Turing-Church, et suggère que les ordinateurs quantiques sont effectivement plus puissants que leurs homologues classiques.

Par la suite, ces résultats ont été repris et améliorés par d'autres. En 1994, Peter Shor a montré que le problème de la factorisation d'un entier pouvait être résolu efficacement sur un ordinateur quantique [83, 85]. Plus que toutes les autres, cette découverte a marqué le début de l'essor de l'informatique quantique. En effet la factorisation est un problème réputé difficile, dont on ne connaît pas à l'heure actuelle de solution efficace classique (certains pensent même qu'il n'en existe pas). Ce résultat remarquable a été suivi en 1996 par l'algorithme de Grover, qui permet d'effectuer une recherche dans une base de données non structurée [47, 48]. Bien que le gain en efficacité de cet algorithme soit moins spectaculaire que dans le cas de la factorisation, son vaste champ d'application en fait une méthode importante. Par delà l'étude du calcul quantique, d'autres succès concernent la cryptographie quantique et la téléportation quantique. Depuis ces travaux, le domaine de l'information quantique a attiré une très grande attention dans la communauté scientifique (pour une référence générale voir [71, 75, 89, 11]).

Comment expliquer l'avantage de l'informatique quantique sur la logique booléenne classique? La première constatation est que l'état d'un ordinateur quantique est caractérisé par un ensemble de variables continues. Cela pourrait laisser supposer qu'il s'agit là d'un ordinateur analogique. Contrairement à un ordinateur digital, un ordinateur analogique utilise une représentation physique de l'information basée sur des degrés de liberté continus. À première vue, ces calculateurs possèdent des ressources illimitées puisque des variables continues peuvent stocker une quantité d'information infinie. Le corollaire est qu'ils sont théoriquement capables de résoudre de manière efficace des problèmes jugés difficiles, semblant ainsi violer la thèse de Turing-Church. Cependant, la prise en compte du bruit inhérent à toute réalisation physique rend le nombre d'états distinguables finis, et suffit à annihiler leurs avantages dans tous les cas.

Qu'en est-il pour les ordinateurs quantique? Tout d'abord, il faut remarquer que la discrétisation des niveaux d'énergie apportée par la mécanique quantique n'implique pas que l'ordinateur soit digital. Un ordinateur digital est une machine qui représente les nombres sous la forme d'une suite de chiffre. Afin d'illustrer la différence, considérons un premier ordinateur qui

utilise les niveaux d'énergie d'un oscillateur harmonique pour représenter les différents nombres (quantique mais non digital), et un deuxième qui utilise pour cela un ensemble de n systèmes à deux niveaux (quantique digital). Pour une même taille de l'espace de Hilbert égale à 2^n , le premier doit pouvoir gérer des états dont l'énergie atteint $2^n \hbar \omega$, ce qui croît exponentiellement avec n , tandis que le second ne voit pas son énergie dépasser $n \hbar \omega$. Seule la représentation digitale de l'information permet donc d'envisager une implémentation physique réaliste. C'est pourquoi un ordinateur quantique est conçu comme un ensemble de systèmes à deux niveaux, les *qubits* (pour *quantum bit*).

Pour un ordinateur quantique constitué de qubits, la mesure du registre fournit effectivement un nombre digital (une suite de 0 et de 1), qui correspond à un des états de base. Mais lors du calcul, l'état général du registre est une superposition quelconque de ces états de base, avec des coefficients qui sont des variables continues. Comme souligné auparavant, l'ordinateur quantique se rapproche en cela des ordinateurs analogiques. Toutefois, une particularité lui permet d'éviter les écueils propres à ce genre : de manière surprenante, l'effet du bruit peut être lui aussi digitalisé. En 1996, il s'est en effet avéré qu'il était possible grâce à des codes correcteurs de rectifier un ensemble continu d'erreurs, et ceci sans même mesurer l'état du registre principal [84, 88]. De plus, il semble exister un seuil d'erreur en dessous duquel la procédure de correction corrige plus de bruit qu'elle n'en produit elle-même. Dans ces conditions, les codes correcteurs d'erreurs quantiques permettent à ces ordinateurs de garder leur efficacité même en présence d'une petite quantité de bruit.

Même si ce sont les nouveaux algorithmes destinés à résoudre des problèmes d'informatique théorique qui ont placé les ordinateurs quantiques sous les feux de la rampe, la simulation efficace des systèmes physiques quantiques reste leur tâche de prédilection, ce pour quoi ils ont été conçus à l'origine. Récemment, de nombreux algorithmes ont été proposés dans ce sens, notamment pour simuler des applications quantiques, comme l'application du bouclier ou le rotateur pulsé quantique, et en particulier par mon équipe à Toulouse. Ces modèles présentent des propriétés de chaos quantique, l'analogie quantique du chaos classique, et possèdent de nombreuses caractéristiques de systèmes complexes, comme la localisation ou l'ergodicité, et sont correctement décrits par la théorie des matrices aléatoires. De plus, le faible nombre de qubits et d'opérations élémentaires requis par ces algorithmes de simulation en font des candidats idéaux pour les ordinateurs qui seront construits dans un futur proche, pour lesquels le nombre de qubits sera restreint et la durée d'exécution limitée par un faible temps de cohérence.

En effet, expérimentalement divers systèmes ont été proposés pour essayer de réaliser un ordinateur quantique. On peut citer les pièges à ions (3 qubits à l'heure actuelle) ou les cavités QED (2 qubits). En physique du solide, les circuits quantiques supra-conducteurs à base de jonctions Josephson permettent d'encoder l'état d'un qubit dans la charge ou le flux. Mais pour l'instant, c'est dans le domaine de la résonance magnétique nucléaire que les expériences sont les plus avancées, et une factorisation a déjà été réalisée sur un ordinateur de 7 qubits. Avec cette technique, ce sont les spins nucléaires d'une molécule qui servent de support aux qubits, et l'on peut les manipuler en appliquant un champ magnétique modulé. Cependant, la résonance magnétique nucléaire en phase liquide n'est malheureusement pas utilisable à grande échelle car le signal mesuré chute exponentiellement avec le nombre de spins dans la molécule. Ainsi, il y a pour l'instant un contraste élevé entre la théorie du calcul quantique, qui s'intéresse principalement au comportement asymptotique des algorithmes pour un très grand nombre de qubits, et les expériences, qui sont pour l'instant limitées à quelques qubits. On voit donc que les algorithmes de simulation quantique qui permettent d'obtenir des résultats pertinents même sur des ordinateurs n'ayant qu'un petit nombre de qubits seront bien adaptés aux ordinateurs quantiques qui seront construits dans un futur proche.

Cependant, même si la simulation est elle-même efficace, il est important de savoir quelles quantités physiques peuvent être calculées de manière efficace. En effet, à la différence d'un ordinateur classique, on obtient à la fin du calcul une superposition d'états quantiques, et une simple mesure ne sélectionne que l'un de ces états aléatoirement. Une méthode consisterait à répéter la simulation un certain nombre de fois afin d'en déduire statistiquement les valeurs des différentes amplitudes. Mais cette façon de procéder n'est pas valable dans le cas général, puisque pour une fonction d'onde quelconque cela nécessiterait un nombre de simulations de l'ordre de la taille de l'espace de Hilbert. La conception de méthodes pour extraire efficacement des quantités physiques intéressantes est donc un point crucial. De plus, un ordinateur quantique réel ne sera pas exempt de défauts. Il peut y avoir par exemple des petites erreurs aléatoires dans l'implémentation des opérations de base ou des couplages résiduels entre les qubits même en l'absence d'opérations. Il est donc utile de connaître les effets de telles imperfections sur les résultats fournis par la simulation. Ce travail de thèse apporte des éléments de réponse à de telles questions : des algorithmes quantiques spécifiques ont été construits et analysés pour deux modèles d'application quantique, le rotateur pulsé et le Harper pulsé. Les observables mesurables ont été déterminées, et leur comportement vis-à-vis des imperfections étudié analytiquement et numériquement.

Chapitre 2

Informatique quantique

Ce chapitre présente brièvement le domaine de l'informatique quantique, ainsi que les notions de calcul quantique nécessaires à la compréhension de cette thèse. Pour une introduction plus approfondie, voir les références [11, 71, 75].

2.1 Opérations quantiques

Un algorithme quantique peut se décrire comme une suite d'opérateurs unitaires locaux élémentaires, appelés aussi portes quantiques, suivie de mesures quantiques. Le nombre d'opérations élémentaires requises rapporté à la taille des données définit la complexité de l'algorithme. Si ce nombre croît comme l'exponentielle de la taille des données, l'algorithme est dit inefficace ; il est efficace si la croissance s'effectue de manière polynomiale. Il est à noter que la complexité totale (et donc l'efficacité) doit tenir compte des mesures quantiques effectuées et de l'observable choisie. Comme mentionné dans l'introduction, le *qubit* (quantum bit) est l'objet fondamental du calcul quantique, et représente l'unité de support de l'information quantique. C'est un système quantique à 2 niveaux, appelés usuellement $|0\rangle$ et $|1\rangle$. Contrairement à un bit classique, l'état général d'un qubit est une superposition des deux états de base :

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \text{ avec } |\alpha|^2 + |\beta|^2 = 1$$

2.1.1 Opérations sur un qubit

Une opération quelconque sur un qubit est décrite par une matrice unitaire 2×2 , et peut être développée sur la base constituée de l'identité et des matrices de Pauli :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Une opération particulièrement importante est la transformation d'Hadamard

$$H = \frac{X + Z}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

La transformation d'Hadamard permet notamment de passer de la base propre de Z ($|0\rangle, |1\rangle$) à celle de X ($(|0\rangle + |1\rangle)/\sqrt{2}$, $(|0\rangle - |1\rangle)/\sqrt{2}$) et réciproquement. Les identités suivantes sont utiles pour simplifier les circuits et comprendre les algorithmes :

$$HXH = Z, \quad HYH = -Y, \quad HZH = X$$

Pour simplifier la notation des algorithmes quantiques, on utilise généralement un schéma sous forme de circuit. Dans un tel circuit, les qubits sont représentés par des lignes horizontales, et les opérateurs sont placés sur ces lignes comme sur une portée musicale, de gauche à droite. Ainsi, le circuit de la figure 2.1 porte sur deux qubits, et représente l'application de l'opérateur A sur le qubit 1, puis de l'opérateur B sur le qubit 2 et enfin de l'opérateur C à nouveau sur le qubit 1. Ce circuit est donc équivalent à l'application de l'opérateur $U = (A \otimes I)(I \otimes B)(C \otimes I)$ sur le système $|\psi\rangle_1 \otimes |\psi\rangle_2$ formé par les deux qubits.

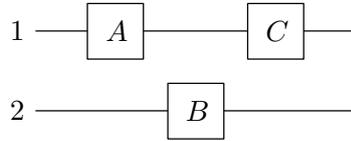


FIG. 2.1 – Exemple de circuit quantique

Dans cette notation, les opérateurs précédemment introduits sont symbolisés par les portes suivantes :

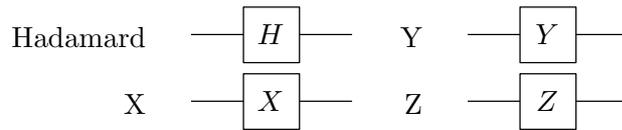


FIG. 2.2 – Noms et symboles des principales portes quantiques sur un qubit

Lorsqu'on prend l'exponentielle des matrices de Pauli, on obtient les opérateurs de rotation autour des axes x , y et z définis sur la figure 2.3

$$R_x(\theta) = e^{-i\frac{\theta}{2}X} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

On peut généraliser ces égalités en définissant l'opérateur rotation d'axe \hat{n} et d'angle θ par

$$R_{\hat{n}}(\theta) = \exp(-i\theta \hat{n} \cdot \vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z)$$

où $\vec{\sigma} = (X, Y, Z)$ et $\hat{n} = (n_x, n_y, n_z)$ est un vecteur réel de norme 1.

La raison d'une telle définition est plus évidente si on utilise la représentation de Bloch. Puisque l'état d'un qubit quelconque est décrit par la fonction d'onde $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$, et que la phase globale de $|\psi\rangle$ n'a pas d'effet observable, on peut le paramétrer par deux angles θ et φ :

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

On peut ainsi représenter l'état du système par un point (θ, φ) situé sur une sphère de rayon 1, appelée sphère de Bloch. Dans cette représentation, l'opérateur $R_{\hat{n}}(\gamma)$ effectue simplement une rotation d'un point sur la sphère de Bloch d'un angle γ autour de l'axe \hat{n} .

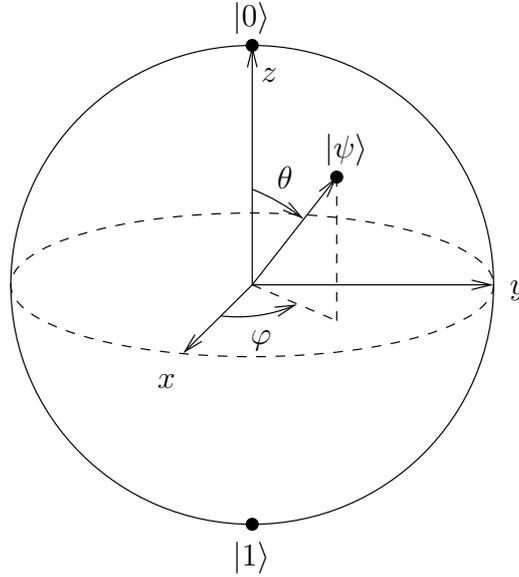


FIG. 2.3 – Sphère de Bloch

Si U est une opération unitaire sur un qubit, il existe α , β , γ et δ tels que

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \quad (2.1)$$

En effet, U étant unitaire, ses colonnes et ses lignes sont orthonormales, et on peut les paramétrer comme suit

$$U = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos \frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)} \sin \frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)} \sin \frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)} \cos \frac{\gamma}{2} \end{pmatrix}$$

Plus généralement, U peut toujours s'écrire sous la forme

$$U = e^{i\alpha} R_{\hat{n}}(\theta)$$

2.1.2 Opérations élémentaires et universalité

Pour pouvoir construire n'importe quel opérateur, il faut ajouter aux opérations sur un qubit une porte qui agit sur au moins deux qubits simultanément. La porte la plus pratique est le NON contrôlé (controlled-NOT, ou CNOT), qui agit sur deux qubits : l'un est le qubit de contrôle, l'autre la cible. Si le contrôle est dans l'état $|0\rangle$ on ne fait rien, et s'il est dans l'état $|1\rangle$ le qubit cible est inversé (on applique l'opérateur X). Dans la base naturelle $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (avec l'ordre |contrôle> \otimes |cible>), l'action de la porte CNOT est décrite par la matrice

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

Si l'on se restreint aux seuls états de la base, le CNOT est l'équivalent de la porte OU exclusif en logique booléenne, avec une recopie d'une des deux entrées pour assurer la réversibilité.

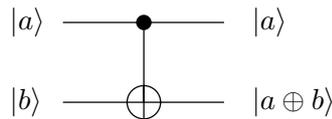


FIG. 2.4 – Symbole pour la porte controlled-NOT (CNOT). \oplus désigne l'addition binaire modulo 2.

Avec la porte CNOT et toutes les opérations sur un qubit, on dispose à présent d'un ensemble universel, c'est-à-dire que tout opérateur unitaire sur n qubits peut être implémenté exactement en composant seulement des opérations sur un qubit et des portes CNOT [30]. Il est important de noter que cette construction n'est pas forcément efficace et peut demander un nombre de portes extrêmement grand. Cependant, il existe une infinité d'opérations possibles sur un qubit ; outre la difficulté de la réalisation physique d'un tel ensemble continu d'opérations, ceci rend la correction des erreurs impossible. Il est donc préférable de disposer d'un ensemble discret de

portes, même si l'on doit pour cela se résoudre à ne construire qu'approximativement les opérations sur plusieurs qubits. Le théorème de Solovay-Kitaev [58] indique que toute opération unitaire sur un qubit peut être approximée efficacement avec une précision arbitraire à l'aide des seules portes d'Hadamard et $\frac{\pi}{8}$.

$$\text{porte } \frac{\pi}{8} : \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} = e^{i\frac{\pi}{8}} R_z \left(\frac{\pi}{4} \right)$$

On peut donc approximer à la précision voulue n'importe quel opérateur unitaire sur n qubits grâce à l'ensemble universel formé par les portes élémentaires d'Hadamard, $\frac{\pi}{8}$ et CNOT. Il est intéressant de noter que la porte $\frac{\pi}{8}$ est absolument nécessaire pour espérer tirer parti de la puissance du calcul quantique. En effet, le théorème de Gottesman-Knill [45] stipule qu'un ordinateur classique peut simuler efficacement un ordinateur quantique qui disposerait des seules portes CNOT et Hadamard. Un algorithme quantique efficace utilisant uniquement ces deux portes conduirait donc automatiquement à un algorithme classique également efficace.

Cet ensemble universel discret n'est pas unique. Par exemple, la porte de Toffoli, la porte d'Hadamard et la porte de phase forment aussi un ensemble universel. La porte de Toffoli est un NOT doublement contrôlé (fig. 2.5), c'est-à-dire que l'on effectue l'opérateur X sur le qubit cible si et seulement si les deux qubits de contrôle sont tous les deux égaux à $|1\rangle$.

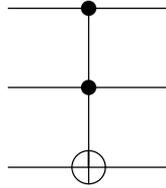


FIG. 2.5 – Porte de Toffoli

Quant à la porte de phase, c'est l'opération $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

2.1.3 Opérations contrôlées

Pour composer les algorithmes quantiques, il est pratique de disposer de portes un peu plus évoluées. Cette section est dédiée à la construction explicite des portes les plus courantes à l'aide des portes élémentaires précédentes. Ces portes seront nécessaires pour les algorithmes quantiques présentés dans cette thèse.

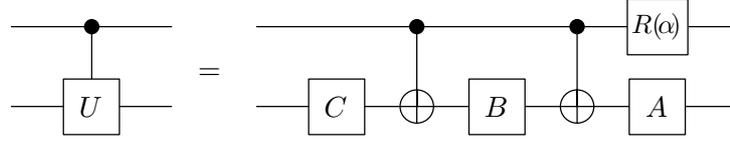


FIG. 2.6 – Construction d'un opérateur contrôlé quelconque

Armé de la porte CNOT et de toutes les opérations sur un qubit, on va construire n'importe quelle opération contrôlée sur un qubit, c'est-à-dire l'équivalent de la porte CNOT avec une opération quelconque U à la place de X sur le qubit cible. On peut pour cela partir de la décomposition (2.1) de U

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

On définit alors les opérateurs

$$\begin{aligned} A &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) \\ B &= R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta + \beta}{2}\right) \\ C &= R_z\left(\frac{\delta - \beta}{2}\right) \end{aligned}$$

On a alors

$$ABC = R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta + \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) = I$$

D'autre part

$$\begin{aligned} AXBXC &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) X R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta + \beta}{2}\right) X R_z\left(\frac{\delta - \beta}{2}\right) \\ &= R_z(\beta) R_y\left(\frac{\gamma}{2}\right) R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta + \beta}{2}\right) R_z\left(\frac{\delta - \beta}{2}\right) \\ &= R_z(\beta) R_y(\gamma) R_z(\delta) \end{aligned}$$

On a ainsi $ABC = I$ et $e^{i\alpha} AXBXC = U$. Il suffit donc d'appliquer les opérateurs A , B et C sur le qubit cible en intercalant des portes CNOT dépendantes du qubit de contrôle, comme sur la figure 2.6. La porte $R(\alpha)$ multiplie le qubit de contrôle par $e^{i\alpha}$ si celui-ci est à $|1\rangle$, et ne fait rien sinon. Ceci équivaut à appliquer la porte à deux qubits

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix}$$

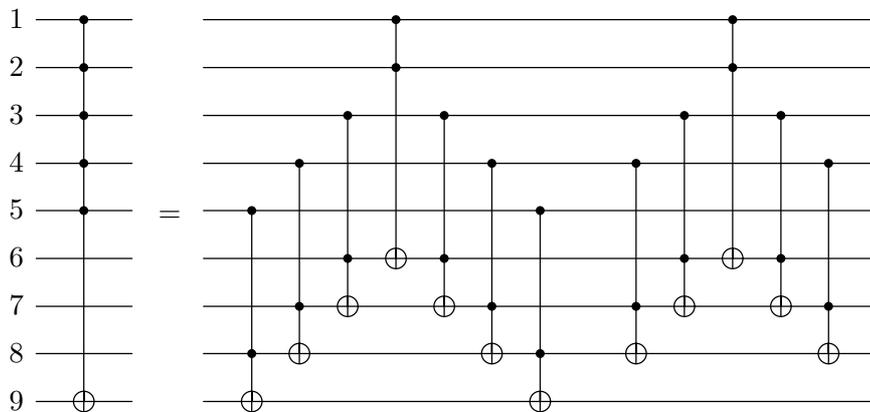


FIG. 2.7 – Construction d’un CNOT multi-contrôlé (illustré pour $n = 9$ et $m = 5$)

Un autre type de porte récurrent dans la plupart des algorithmes quantiques est l’opération contrôlée par plusieurs qubits simultanément, une généralisation de la porte précédente. On note $\wedge_n(U)$ l’opérateur U contrôlé par n qubits, c’est-à-dire qu’on applique U sur le qubit cible si et seulement si les n qubits de contrôle sont tous égaux à $|1\rangle$. Pour construire cette porte, on peut commencer par construire un CNOT multi-contrôlé [9].

Si $n \geq 5$ et $m \in 3, \dots, \lfloor n/2 \rfloor$, alors on peut construire la porte $\wedge_m(X)$ grâce au circuit de la figure 2.7, qui contient $4(m-2)$ portes de Toffoli. Dans ce circuit, considérons le premier groupe de portes. Le qubit 6 est inversé

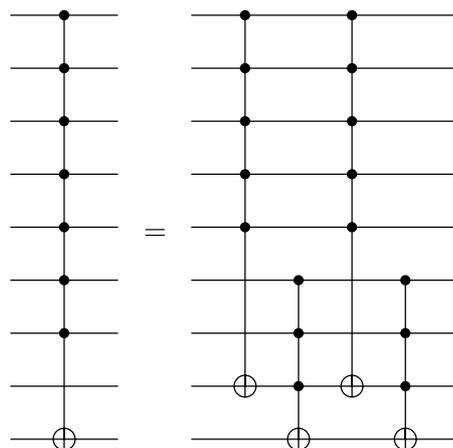


FIG. 2.8 – Construction d’un CNOT multi-contrôlé (illustré pour $n = 9$)

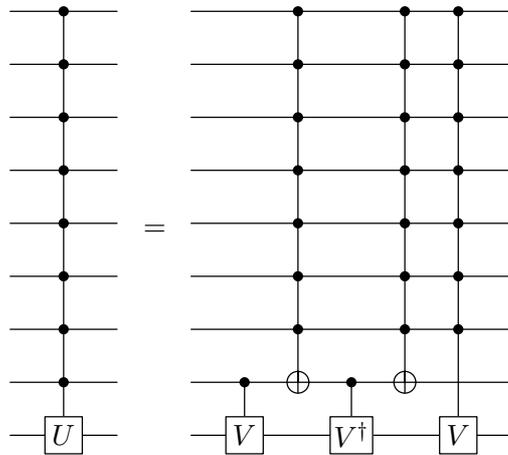


FIG. 2.9 – Construction d’une opération multi-contrôlée sur un qubit (illustré pour $n = 9$)

si et seulement si les qubits 1 et 2 sont à 1. Le qubit 7 est inversé si les 3 premiers qubits sont tous à 1, et ainsi de suite. Après le premier groupe de portes, le qubit 9 est donc inversé si et seulement si les 5 premiers qubits sont à 1, mais les qubits 6, 7 et 8 sont altérés. Pour leur rendre leurs valeurs initiales, on applique donc le second groupe de portes.

En combinant 4 portes $\wedge_m(X)$, on peut construire une porte $\wedge_{n-2}(X)$ sur n qubits grâce au circuit de la figure 2.8, ce qui fait un total de $8(n-5)$ portes de Toffoli. La construction d’une porte CNOT multi-contrôlée re-

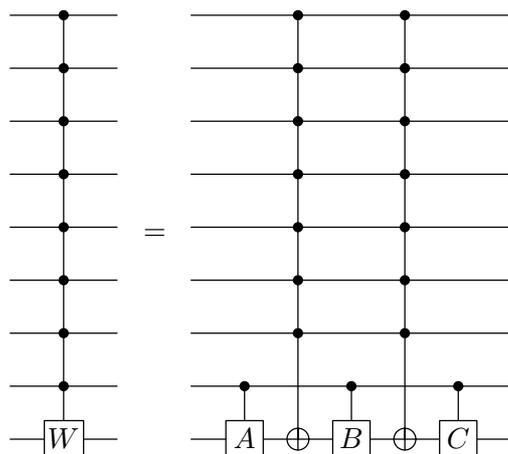


FIG. 2.10 – Construction d’une opération $SU(2)$ multi-contrôlée sur un qubit

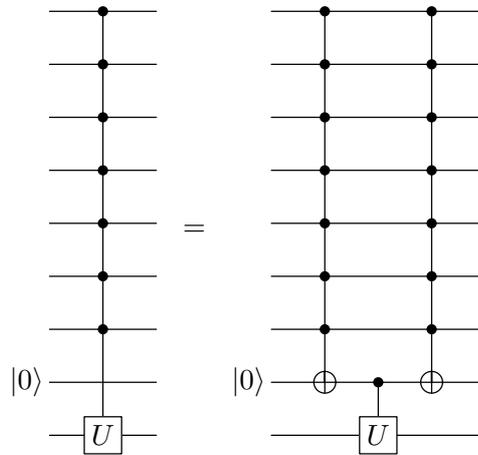


FIG. 2.11 – Construction d’une opération multi-contrôlée sur un qubit avec un qubit auxiliaire

quiert donc un nombre de portes élémentaires qui augmente linéairement avec le nombre de qubits, pourvu que l’on dispose d’un qubit auxiliaire. On peut noter également que ce qubit auxiliaire est inchangé par la porte, donc même un qubit utilisé par ailleurs peut faire l’affaire.

Grâce à la porte $\Lambda_{n-2}(X)$, on peut maintenant construire une opération U quelconque sur un qubit contrôlée par plusieurs qubits grâce au circuit de la figure 2.9, avec V tel que $V^2 = U$. Par récurrence, la construction d’une porte $\Lambda_{n-1}(U)$ requiert donc $O(n^2)$ portes élémentaires.

Cependant, dans quelques cas particuliers, la simulation de la porte $\Lambda_{n-1}(U)$ peut être linéaire en n . C’est le cas par exemple si $U \in SU(2)$, avec le circuit de la figure 2.10 (cette construction est similaire à celle de la figure 2.6, avec $\alpha = 0$, ce qui correspond bien à un opérateur de $SU(2)$).

Si l’on s’octroie un qubit auxiliaire, on peut également simuler une porte $\Lambda_{n-1}(U)$ de façon linéaire, avec un U quelconque (fig. 2.11). Mais contrairement au cas du circuit 2.8, le qubit auxiliaire doit rester dans l’état $|0\rangle$; il n’est donc pas possible de le réutiliser ailleurs.

2.2 Transformée de Fourier quantique

2.2.1 Algorithme de la Transformée de Fourier

À l’aide des portes définies précédemment, on est à présent en mesure de construire des algorithmes quantiques évolués. Honneur à la transformée de

Fourier quantique, qui est utilisée dans de nombreux algorithmes, dont ceux de cette thèse. La transformée de Fourier discrète d'un vecteur complexe x_0, \dots, x_{N-1} est définie par

$$\tilde{x}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}}$$

De la même manière, on définit la transformée de Fourier quantique (TFQ) [28, 83] par son action sur les vecteurs de la base orthonormale $|0\rangle, \dots, |N-1\rangle$

$$|j\rangle \xrightarrow{TFQ} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle$$

L'équivalence avec la transformée de Fourier discrète est visible lorsqu'on applique la transformée de Fourier quantique à une superposition d'états

$$\sum_{j=0}^{N-1} x_j |j\rangle \mapsto \sum_{k=0}^{N-1} \tilde{x}_k |k\rangle$$

Même si l'unitarité d'une telle transformation n'est pas évidente au premier abord, on peut la décomposer en une série de transformations unitaires élémentaires. On suppose dans la suite que $N = 2^n$; cette hypothèse n'est à vrai dire pas très restrictive car elle est généralement faite aussi dans le cas de la transformée de Fourier discrète (l'algorithme de la transformée de Fourier rapide ne marche que pour N de la forme a^b). Le calcul s'effectue donc sur les vecteurs de base $|0\rangle, \dots, |2^n - 1\rangle$, et on note $j_1 j_2 \dots j_n$ la représentation binaire de j (ou $j = j_1 2^{n-1} + \dots + j_n 2^0$), et $0.j_l j_{l+1} \dots j_m$ la fraction binaire $j_l/2 + j_{l+1}/4 + \dots + j_m/2^{m-l+1}$.

On peut alors factoriser la transformation de Fourier quantique ainsi

$$\begin{aligned} |j\rangle &\mapsto \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \\ &= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i j (\sum_{l=1}^n k_l 2^{-l})} |k_1 \dots k_n\rangle \\ &= \frac{1}{2^{n/2}} \sum_{k_1=0}^1 \dots \sum_{k_n=0}^1 \bigotimes_{l=1}^n e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\ &= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left[\sum_{k_l=0}^1 e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \\ &= \frac{1}{2^{n/2}} \bigotimes_{l=1}^n \left(|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right) \end{aligned}$$

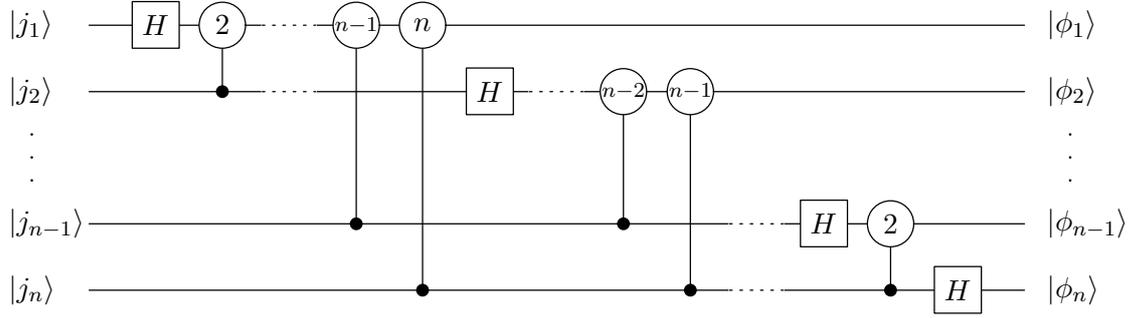


FIG. 2.12 – Circuit de la transformée de Fourier quantique

$$= \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) \quad (2.2)$$

Cette décomposition permet de concevoir aisément un circuit pour la transformée de Fourier quantique, comme celui de la figure 2.12, où

$$\text{---} \bigcirc k \text{---} \quad \text{représente l'opération} \quad \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{pmatrix}$$

Pour comprendre le fonctionnement de ce circuit, suivons son action sur $|j\rangle = |j_1 \dots j_n\rangle$. La première porte de Hadamard donne

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle \right) |j_2 \dots j_n\rangle$$

Puis, la première rotation contrôlée ajoute un bit de phase supplémentaire suivant l'état de $|j_2\rangle$

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2} |1\rangle \right) |j_2 \dots j_n\rangle$$

Et ainsi de suite jusqu'à la rotation n

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) |j_2 \dots j_n\rangle$$

De même, la deuxième série de porte de Hadamard et de rotations contrôlées conduisent à l'état

$$\frac{1}{2} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_2 \dots j_n} |1\rangle \right) |j_3 \dots j_n\rangle$$

À la fin du circuit, nous obtenons donc l'état

$$\begin{aligned} & |\phi_1\rangle \otimes |\phi_2\rangle \otimes \dots \otimes |\phi_{n-1}\rangle \otimes |\phi_n\rangle \\ &= \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle \right) \left(|0\rangle + e^{2\pi i 0 \cdot j_2 \dots j_n} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle \right) \end{aligned}$$

Ceci n'est rien d'autre que la transformée de Fourier quantique de $|j\rangle$ (2.2) où l'ordre des qubits a été inversé (la transformée exacte serait $|\phi_n\rangle \otimes |\phi_{n-1}\rangle \otimes \dots \otimes |\phi_2\rangle \otimes |\phi_1\rangle$). On peut remettre les qubits dans le bon ordre en appliquant $n/2$ portes d'échange, comme celle de la figure 2.13. Cependant, on peut faire l'économie de cette étape en redéfinissant simplement les rôles des qubits, et en inversant donc systématiquement toutes les portes à venir. Cela peut être fait automatiquement par l'ordinateur classique qui pilote l'évolution de l'ordinateur quantique.

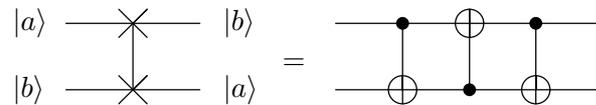


FIG. 2.13 – Circuit de la porte d'échange

Ce circuit contient $n(n+1)/2$ portes quantiques, et est donc un moyen efficace de calculer la transformée de Fourier discrète d'un vecteur. En comparaison, l'algorithme classique de transformée de Fourier rapide demande $O(n2^n)$ opérations, ce qui est exponentiellement plus lent. Cependant, on ne peut pas utiliser cet algorithme pour calculer naïvement la transformée de Fourier discrète d'une série de données. Si le calcul est en effet exponentiellement plus efficace, l'extraction du résultat complet de la mémoire quantique demanderait elle un nombre exponentiel de mesures. La transformée de Fourier quantique n'est pas un algorithme en elle-même, elle doit être incluse dans un algorithme quantique à même d'utiliser simultanément toutes les composantes du résultat, comme dans l'estimation de phase, l'algorithme de factorisation de Shor ou les algorithmes construits dans cette thèse.

2.2.2 Estimation de phase

Comme dit ci-dessus, la transformée de Fourier quantique est très puissante, mais ce n'est pas vraiment un algorithme en soi. Elle est en général utilisée au sein d'autres algorithmes qui tirent parti de ses spécificités. Le plus célèbre est sans doute l'estimation de phase [57]. Supposons qu'un opérateur unitaire U , que l'on sait construire efficacement, a un vecteur propre $|u\rangle$ avec la valeur propre $e^{i2\pi\varphi}$. Le but de cet algorithme est d'estimer la valeur de φ . Pour cela, on fait deux hypothèses :

- on est capable de construire au préalable le vecteur propre $|u\rangle$ dont on veut déterminer la valeur propre, ou tout du moins un état initial qui a une projection importante sur $|u\rangle$
- on peut effectuer l'opération U^{2^j} pour tout $j \geq 0$, et ce en un temps qui n'augmente pas exponentiellement avec j

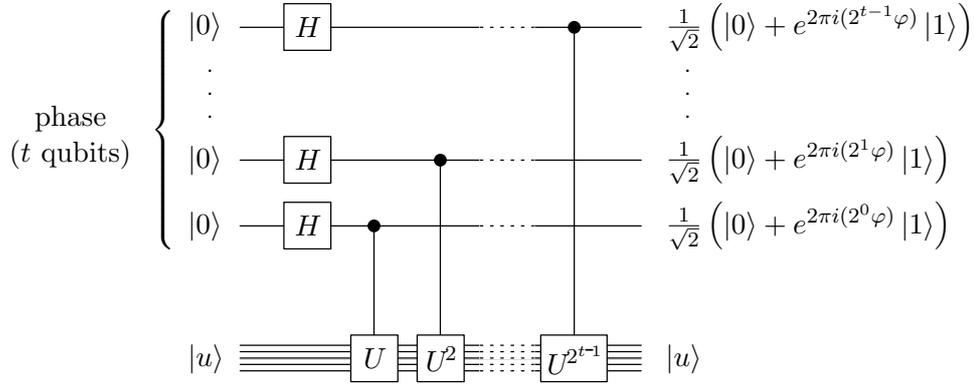


FIG. 2.14 – Circuit quantique pour l'estimation de phase

La seconde hypothèse est très contraignante, puisque même si l'on sait appliquer U de manière efficace, rien ne garantit qu'il en soit de même pour U^{2^j} . Par exemple la méthode qui consisterait à itérer 2^j fois l'opérateur U demande un nombre d'opérations qui croît exponentiellement avec j . L'algorithme d'estimation de phase n'est donc utile que dans les cas particuliers où cette construction efficace est possible.

Deux registres vont être utilisés : un premier registre de t qubits initialement mis à $|0\rangle$, qui va accueillir l'estimation de φ à la fin du calcul, et un deuxième registre qui contient le vecteur propre $|u\rangle$. L'algorithme se décompose en deux phases. On applique en premier lieu le circuit de la figure 2.14. La série de transformations d'Hadamard permettent d'obtenir l'état

$$\frac{1}{2^{t/2}} (|0\rangle + |1\rangle) (|0\rangle + |1\rangle) \dots (|0\rangle + |1\rangle) \otimes |u\rangle$$

Puis l'application d'une suite de puissances de l'opérateur U sur le second registre contrôlée par le premier registre conduit à l'état

$$\begin{aligned} \frac{1}{2^{t/2}} (|0\rangle + U^{2^{t-1}} |1\rangle) (|0\rangle + U^{2^{t-2}} |1\rangle) \dots (|0\rangle + U^{2^0} |1\rangle) \otimes |u\rangle \\ = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} |k\rangle \otimes U^k |u\rangle \\ = \left(\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i k \varphi} |k\rangle \right) \otimes |u\rangle \end{aligned}$$

La deuxième phase de l'algorithme consiste à appliquer une transformée de Fourier quantique inverse sur le premier registre (celle-ci est obtenue en inversant l'ordre des portes du circuit 2.12). Puis on termine en mesurant simplement le premier registre dans la base naturelle.

En effet, l'état du premier registre obtenu à la fin de la première phase est de la forme $\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} f(k) |k\rangle$ avec $f(k) = e^{2\pi i k \varphi}$. Une transformée de Fourier inverse continue de f donnerait

$$\int_{-\infty}^{\infty} f(x) e^{-2\pi i x \nu} dx = \int_{-\infty}^{\infty} e^{-2\pi i x (\nu - \varphi)} dx = \delta(\nu - \varphi)$$

On voit donc intuitivement que la transformée de Fourier quantique inverse (discrète) va conduire à un état dont la mesure donne une valeur proche de φ avec une forte probabilité. Quantitativement, appelons b l'entier compris entre 0 et $2^t - 1$ tel que $b/2^t$ soit la meilleure approximation de φ inférieure à φ . Supposons que le résultat de la mesure finale du premier registre est m , et soit e un entier positif. La probabilité pour que m soit proche de b à e près peut être majorée (voir par exemple [71])

$$p(|m - b| > e) \leq \frac{1}{2(e - 1)} \quad (2.3)$$

Supposons qu'on désire une approximation de φ exacte à n bits ($n \leq t$), c'est-à-dire avec une précision de 2^{-n} . On choisit donc $e = 2^{t-n} - 1$, et d'après (2.3), la probabilité d'obtenir une approximation de φ avec cette précision est d'au moins $1 - 1/2(2^{t-n} - 2)$. Pour avoir une précision de n bits sur φ avec une probabilité d'au moins $1 - \varepsilon$, il faut ainsi prendre

$$t = n + \left\lceil \log_2 \left(2 + \frac{1}{2\varepsilon} \right) \right\rceil$$

où $\lceil \cdot \rceil$ désigne l'arrondi à l'entier supérieur.

Une application spectaculaire de l'estimation de phase est l'algorithme de Shor [83, 85]. En effet, la factorisation d'un entier N peut être réduite au problème de trouver la période de la fonction $f(x) = a^x \bmod N$, où $a < N$ est choisi aléatoirement et n'a pas de facteur commun avec N . Ceci peut être fait en appliquant l'algorithme d'estimation de phase à l'opérateur U tel que

$$U |y\rangle = |ay \bmod N\rangle$$

Cela est possible car les puissances de U sont constructibles de manière efficace, et car le vecteur propre auquel on applique l'algorithme ne dépend pas de a ni de N .

2.3 Recherche quantique

2.3.1 Algorithme de Grover

Un autre algorithme illustre est celui de Grover [47, 48]. Supposons que l'on dispose d'une liste de N éléments, et que l'on veuille en trouver un

qui réponde à certains critères. Si la liste ne possède pas de structure particulière (par exemple si les éléments y sont rangés aléatoirement), alors aucun algorithme classique ne peut faire mieux que de regarder les éléments un par un jusqu'à trouver le bon. Cette méthode de recherche rudimentaire mais néanmoins optimale requiert en moyenne $N/2$ opérations, soit $O(N)$. Remarquablement, il existe un algorithme de recherche *quantique* (appelé algorithme de Grover) qui permet d'effectuer la même recherche en $O(\sqrt{N})$ opérations.

Pour formuler ce problème plus précisément, on introduit une fonction $f(x)$ qui vaut 1 si x est l'un des éléments recherchés et 0 sinon. On suppose de plus que $N = 2^n$ et qu'il y a exactement M éléments qui correspondent aux critères de la recherche, avec $0 \leq M \ll N$. Classiquement, la recherche se réduit alors à trouver l'un des M éléments x qui vérifient $f(x) = 1$.

Afin de pouvoir formuler les deux algorithmes de la même manière, on suppose qu'on dispose également d'un *oracle* quantique O : on soumet à cette boîte noire un état $|x\rangle$ accompagné d'un qubit auxiliaire $|a\rangle$, et celle-ci nous révèle par l'intermédiaire du qubit auxiliaire si $|x\rangle$ fait parti des éléments recherchés ou non. Plus précisément, l'oracle O effectue l'opération quantique

$$|x\rangle |a\rangle \longrightarrow |x\rangle |a \oplus f(x)\rangle$$

Si l'on applique l'oracle à l'état $|x\rangle|0\rangle$, il suffit de mesurer ensuite le qubit auxiliaire pour déterminer si x est une des solutions recherchées, auquel cas le résultat de la mesure sera 1. Dans le cas de l'algorithme de Grover, il est cependant plus astucieux d'appliquer l'oracle avec un qubit auxiliaire dans l'état $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. On effectue ainsi la transformation

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \longrightarrow (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Comme le qubit auxiliaire n'est pas modifié, on l'omettra par la suite :

$$|x\rangle \longrightarrow (-1)^{f(x)} |x\rangle$$

On ne se préoccupe pas pour l'instant de savoir comment est constitué l'oracle, on se contente juste de supposer qu'il est possible de le construire efficacement. Cependant, on suppose également que l'appel à l'oracle est le facteur limitant de l'algorithme, l'étape qui coûte le plus. Grâce à cette hypothèse, l'efficacité de l'algorithme sera évaluée simplement comme le nombre d'appels nécessaires à l'oracle. On peut remarquer que cela était déjà le cas classiquement, puisqu'on a considéré la vérification d'un élément comme une opération élémentaire.

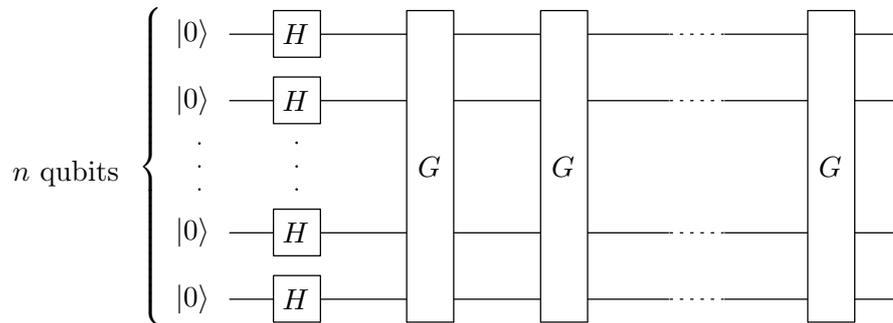


FIG. 2.15 – Circuit quantique pour l'algorithme de Grover

L'algorithme proprement dit est représenté sur la figure 2.15. On commence par construire une superposition uniforme $|\psi\rangle$ de tous les états grâce à la transformation $H^{\otimes n}$ appliquée à $|0\dots 0\rangle$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

Grâce à l'application répétée de l'opérateur de Grover G , l'amplitude de probabilité des états recherchés est ensuite augmentée progressivement, pendant que celle des autres est diminuée. Si l'on mesure le registre quantique à la fin de cet algorithme, on trouvera ainsi avec une forte probabilité l'une des solutions à notre problème de recherche.

L'opérateur de Grover se décompose en 4 étapes :

1. application de l'oracle O
2. transformation d'Hadamard $H^{\otimes n}$
3. application d'une phase de -1 sur tous les états de l'ordinateur sauf $|0\rangle$, soit l'opération $P = 2|0\rangle\langle 0| - I$
4. transformation d'Hadamard $H^{\otimes n}$

L'effet combiné des 3 dernières étapes peut se résumer dans l'opération

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

Une itération de Grover peut donc s'écrire

$$G = (2|\psi\rangle\langle\psi| - I)O$$

Le mécanisme de cet algorithme s'explique élégamment à l'aide d'une représentation géométrique. Appelons S l'ensemble des éléments x qui satisfont aux critères de la recherche, et \bar{S} son complémentaire. On définit les

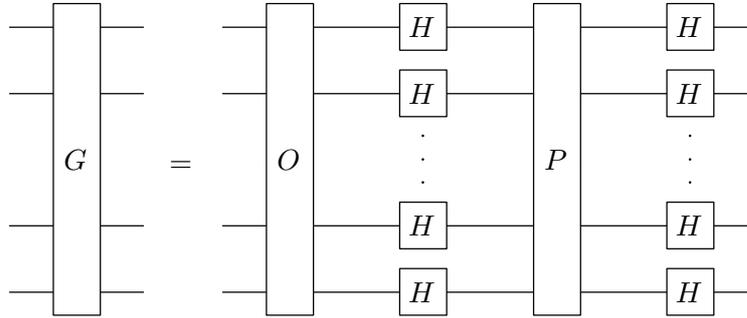


FIG. 2.16 – Circuit quantique pour une itération de Grover

états $|\alpha\rangle$ et $|\beta\rangle$

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \bar{S}} |x\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle$$

Dans le plan $(|\alpha\rangle, |\beta\rangle)$, l'itération de Grover prend une forme très simple. En effet, l'état initial du calcul $|\psi\rangle$ peut être réexprimé en fonction de ces vecteurs

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$$

$$= \cos\left(\frac{\theta}{2}\right) |\alpha\rangle + \sin\left(\frac{\theta}{2}\right) |\beta\rangle$$

De plus, l'oracle O multiplie tous les états de S par -1 et laisse ceux de \bar{S} invariants. Il s'agit donc tout simplement d'une réflexion par rapport au vecteur $|\alpha\rangle$ dans le plan $(|\alpha\rangle, |\beta\rangle)$. De même, $2|\psi\rangle\langle\psi| - I$ est une réflexion par rapport au vecteur $|\psi\rangle$. L'action de G , qui est la composée de deux réflexions, est donc finalement une rotation dans le plan $(|\alpha\rangle, |\beta\rangle)$, d'un angle égal à θ (le double de l'angle entre $|\alpha\rangle$ et $|\psi\rangle$). Toutes ces opérations sont représentées sur la figure 2.17, en partant d'un état quelconque $|\varphi\rangle$.

L'état obtenu après k applications de l'itération de Grover G est donc la rotation de $|\psi\rangle$ d'un angle $k\theta$ dans le plan $(|\alpha\rangle, |\beta\rangle)$

$$G^k |\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right) |\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right) |\beta\rangle$$

L'objectif de l'algorithme étant d'augmenter l'amplitude de probabilité des états $|x\rangle$ tels que $x \in S$, on cherche en fait à se rapprocher le plus possible du vecteur $|\beta\rangle$. Quel est le nombre r d'itérations nécessaires pour atteindre

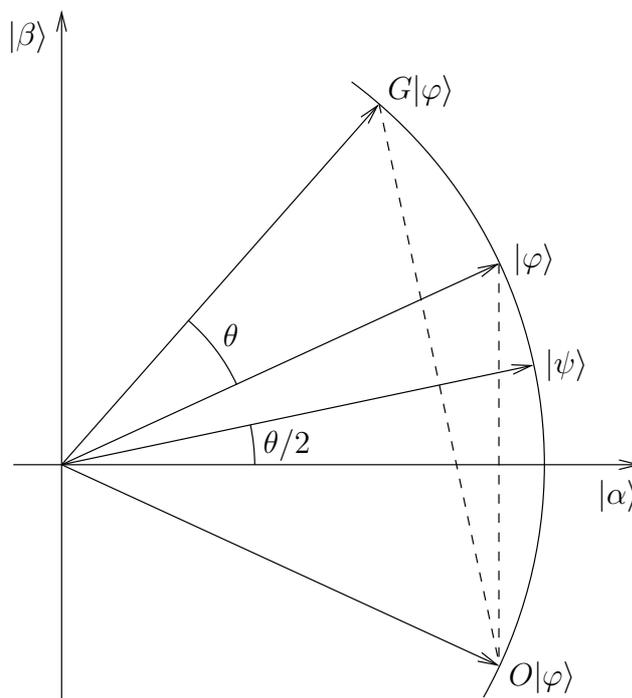


FIG. 2.17 – Interprétation géométrique de l'algorithme de Grover

ce but ? On veut $G^r |\psi\rangle \approx |\beta\rangle$, donc on doit choisir r tel que $(r + \frac{1}{2})\theta$ soit le plus proche possible de $\frac{\pi}{2}$, soit

$$r = \left[\frac{\pi}{2\theta} - \frac{1}{2} \right] = \left\lfloor \frac{\pi}{2\theta} \right\rfloor$$

où $[]$ représente l'entier le plus proche, et $\lfloor \rfloor$ le plus grand entier inférieur ou égal. Comme

$$\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}} \leq \frac{\theta}{2}$$

On obtient une borne supérieure pour l'efficacité de l'algorithme

$$r \leq \frac{\pi}{4} \sqrt{\frac{N}{M}} = O(\sqrt{N})$$

Par ailleurs, il a été démontré que cette efficacité en $O(\sqrt{N})$ était optimale [13, 16]. C'est-à-dire que tout algorithme quantique qui consiste en une succession d'opérations unitaires et d'appels à l'oracle nécessite au moins $O(\sqrt{N})$ appels pour réussir avec une forte probabilité. Bien que le gain ne soit pas aussi important que dans le cas de l'algorithme de Shor, l'intérêt de cet algorithme n'en est pas moindre puisqu'il est très versatile. En effet, un

grand nombre de problèmes mathématiques peuvent être formulés comme la recherche d'une solution devant satisfaire les critères d'un oracle. Cela inclut notamment tous les problèmes NP, qui peuvent être durs à résoudre, mais dont on peut vérifier les solutions facilement. Pour cette classe de problèmes, l'algorithme de Grover permet d'obtenir un gain de vitesse quadratique de manière systématique. Cependant, comme le gain n'est pas exponentiel mais seulement polynomial, cela ne suffit pas à changer la classe de complexité de ces problèmes. Il faut noter enfin que le gain quadratique de Grover est prouvé, ce qui n'est pas le cas du gain exponentiel de Shor, puisqu'il peut éventuellement exister un algorithme classique efficace de factorisation encore non découvert.

2.3.2 Amplification d'amplitude

L'algorithme de Grover peut être généralisé sous une forme intéressante [17, 18]. Cette extension est utilisée dans la deuxième publication de cette thèse. Supposons que l'espace de Hilbert de l'ordinateur se décompose comme la somme directe de deux sous-espaces H_0 et H_1

$$H = H_0 \oplus H_1$$

À la fin d'un certain calcul représenté par l'opérateur unitaire A , l'ordinateur quantique se trouve dans un état $|\psi\rangle = A|0\rangle$. Si $|\psi_0\rangle$ et $|\psi_1\rangle$ sont respectivement les projections de $|\psi\rangle$ sur H_0 et H_1

$$|\psi\rangle = |\psi_0\rangle + |\psi_1\rangle$$

Or, pour une raison particulière seule la composante de $|\psi\rangle$ qui se trouve dans H_1 nous intéresse. Par exemple, dans le cas où la probabilité totale $a = \langle\psi_1|\psi_1\rangle$ de mesurer la fonction d'onde $|\psi\rangle$ dans un état de H_1 est faible, il est très inefficace de déterminer l'expression de $|\psi_1\rangle$ dans la base naturelle par une mesure directe. On va donc chercher à augmenter l'amplitude de $|\psi_1\rangle$ tout en diminuant celle de $|\psi_0\rangle$ afin d'obtenir un état qui soit entièrement compris dans H_1 .

Pour cela, on utilise une version modifiée de l'algorithme de Grover. Le processus d'amplification est réalisé en appliquant itérativement à l'état $|\psi\rangle$ l'opérateur

$$Q = APA^\dagger O$$

De même que précédemment, P est un opérateur qui multiplie tous les états par -1 sauf $|0\rangle$, et O est un oracle qui applique une phase de -1 également à tous les états qui sont inclus dans H_1

$$|x\rangle \longrightarrow \begin{cases} -|x\rangle & \text{si } |x\rangle \in H_1 \\ |x\rangle & \text{si } |x\rangle \in H_0 \end{cases}$$

Q est donc la composition de la réflexion d'axe $|\psi\rangle\langle\psi|$

$$APA^\dagger = A(2|0\rangle\langle 0| - I)A^\dagger = 2|\psi\rangle\langle\psi| - I$$

et de la réflexion d'axe $|\psi_0\rangle\langle\psi_0|$

$$O = 2|\psi_0\rangle\langle\psi_0| - I$$

De manière analogue à l'itération de Grover, Q a pour effet de tourner le vecteur $|\psi\rangle$ dans le plan $(|\psi_0\rangle, |\psi_1\rangle)$ d'un angle θ défini par

$$\sin^2\left(\frac{\theta}{2}\right) = \langle\psi|\psi_1\rangle = a$$

Après k itérations de Q sur $|\psi\rangle$, l'état obtenu est

$$Q^k|\psi\rangle = \frac{1}{\sqrt{1-a}} \cos\left(\frac{2k+1}{2}\theta\right)|\psi_0\rangle + \frac{1}{\sqrt{a}} \sin\left(\frac{2k+1}{2}\theta\right)|\psi_1\rangle \quad (2.4)$$

Pour avoir l'amplitude de $|\psi_1\rangle$ la plus grande possible, on doit choisir un nombre d'itérations

$$r = \left\lfloor \frac{\pi}{2\theta} \right\rfloor \approx \frac{\pi}{4\sqrt{a}}$$

la dernière approximation étant valable si a est faible, ce qui est généralement le cas puisqu'on cherche précisément à l'amplifier.

Illustrons l'utilité de cet algorithme sur un exemple. Prenons un registre de 5 qubits dont les états de base représentent des positions variant de 0 à $2^5 - 1 = 31$. L'algorithme A appliqué à ce registre délivre une fonction d'onde $|\psi\rangle$, dont seule la partie qui est située près de l'origine est digne d'intérêt. On choisit donc arbitrairement d'amplifier la fonction d'onde entre les positions 0 et $2^2 - 1 = 3$. Ceci est réalisé en appliquant l'algorithme présenté ci-dessus, avec l'oracle O de la figure 2.18. Celui-ci ajoute une phase de -1 si les 3 qubits de poids fort sont tous à 0, ce qui correspond bien aux états $|x\rangle$ avec x entre 0 et 3. La construction de telles portes multi-contrôlées est détaillée dans la section (2.1.3).

Un aspect assez gênant de cet algorithme est qu'il nécessite la connaissance préalable de a pour fonctionner. Il est possible d'obtenir une estimation de a grâce une utilisation subtile de la transformée de Fourier quantique. Cependant, de tels raffinements ne sont la plupart du temps pas nécessaires. En effet, il s'agit généralement d'amplifier un petit sous-espace ($a \ll 1$) afin de pouvoir mesurer avec une bonne probabilité les amplitudes relatives des états qui y sont contenus. Pour cela, obtenir un état $|\varphi\rangle$ tel que $\langle\varphi_1|\varphi_1\rangle \sim 1$ est suffisant. Si l'on regarde l'équation (2.4), on voit qu'en prenant un k

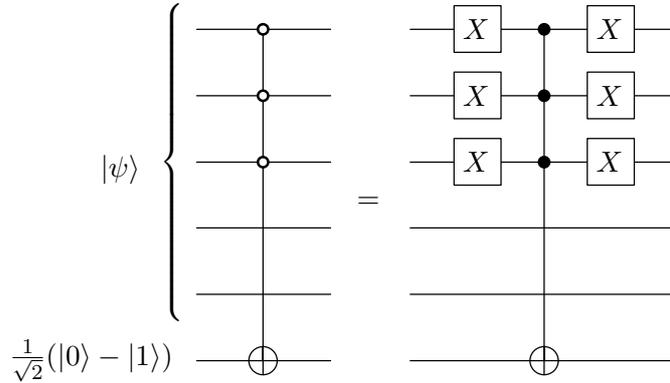


FIG. 2.18 – Exemple d’oracle pour l’algorithme d’amplification d’amplitude

au hasard, mais toutefois assez grand pour que $\frac{2k+1}{2}\theta \gg \pi$, alors on peut considérer que

$$Q^k |\psi\rangle = \frac{1}{\sqrt{1-a}} \cos(\gamma) |\psi_0\rangle + \frac{1}{\sqrt{a}} \sin(\gamma) |\psi_1\rangle$$

avec γ un angle tiré de manière aléatoire et uniforme entre 0 et 2π . Dans ce cas, la probabilité de réussite de l’algorithme est de $\langle \sin^2(\gamma) \rangle = \frac{1}{2}$. Si le k choisi au hasard n’est pas assez grand, on peut atteindre de manière efficace le régime en question en doublant la valeur de k à chaque échec de l’algorithme.

2.4 Simulations de systèmes quantiques

Cette dernière partie est consacrée plus spécifiquement à la simulation des systèmes quantiques. Comme mentionné dans l’introduction, les ordinateurs quantiques seraient très utiles pour simuler l’évolution dynamique de systèmes quantiques. Par exemple dans le cas d’un problème quantique à N corps, la taille de l’espace de Hilbert augmente exponentiellement avec N mais le nombre de qubits nécessaire pour simuler ce système croît seulement comme N . L’idée originale remonte à Feynman, mais celui-ci n’avait proposé aucun exemple précis. Depuis, de nombreux algorithmes ont été conçus, notamment pour la simulation de systèmes quantiques à N corps [68, 1, 72] et la simulation de systèmes de spins [66, 87].

Prenons comme illustration une méthode générale pour simuler un système quantique à temps continu qui a été développée dans [95, 99]. Considérons le mouvement d’une particule quantique à une dimension. Il est régi par l’équation de Schrödinger

$$i\hbar \frac{\partial}{\partial t} \psi(x, t) = H\psi(x, t)$$

où le hamiltonien est donné par

$$H = H_0 + V(x) \quad \text{avec} \quad H_0 = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2}$$

H_0 est la partie responsable de l'évolution libre du système, et $V(x)$ est un potentiel à une dimension. Supposons que l'on désire simuler l'évolution de $\psi(x, t)$ sur un ordinateur quantique de n qubits. Tout d'abord, si le système n'est pas naturellement quantifié, il faut procéder à une discrétisation de la variable continue x . Cela revient à borner l'espace accessible, et à découper celui-ci en 2^n intervalles, représentés chacun par un des 2^n états de l'espace de Hilbert de l'ordinateur. On supposera maintenant pour simplifier que le système est déjà quantifié (c'est le cas des modèles qui seront étudiés dans les chapitres suivants).

Pour intégrer l'équation de Schrödinger, on discrétise l'évolution en temps également. En effet, pour deux opérateurs A et B quelconques on peut décomposer l'opérateur d'évolution grâce à la formule de Trotter :

$$\lim_{n \rightarrow \infty} \left(e^{iAt/n} e^{iBt/n} \right)^n = e^{i(A+B)t}$$

Considérons un intervalle de temps ε ; l'état de la fonction d'onde à l'instant $t + \varepsilon$ est donné en fonction de celui au temps t par

$$\psi(x, t + \varepsilon) = e^{-\frac{i}{\hbar}[H_0+V(x)]\varepsilon} \psi(x, t)$$

Comme H_0 et $V(x)$ ne commutent pas, on doit utiliser un développement approché pour construire l'opérateur du membre de droite

$$e^{i(A+B)\Delta t} = e^{iA\Delta t} e^{iB\Delta t} + O(\Delta t^2)$$

On peut noter au passage qu'il existe aussi un autre développement à peine plus compliqué qui permet d'approximer $e^{i(A+B)\Delta t}$ à l'ordre 3 en Δt

$$e^{i(A+B)\Delta t} = e^{iA\Delta t/2} e^{iB\Delta t} e^{iA\Delta t/2} + O(\Delta t^3)$$

Si ε est suffisamment petit, on peut écrire

$$e^{-\frac{i}{\hbar}[H_0+V(x)]\varepsilon} \approx e^{-\frac{i}{\hbar}H_0\varepsilon} e^{-\frac{i}{\hbar}V(x)\varepsilon} \quad (2.5)$$

Pour implémenter ces opérateurs, on utilise la transformée de Fourier quantique. Si F est l'opérateur de transformée de Fourier, la variable k conjuguée de x est telle que $-i\frac{\partial}{\partial x} = F^\dagger k F$. Comme $p = \hbar k$, le premier opérateur de 2.5 peut s'écrire

$$e^{-\frac{i}{\hbar}H_0\varepsilon} = F^\dagger e^{\frac{i}{\hbar}\left(\frac{\hbar^2 k^2}{2m}\right)\varepsilon} F$$

On peut ainsi simuler l'évolution du système de la façon suivante : on découpe la durée t de la simulation en s tranches ε ($t = s\varepsilon$). Pour obtenir la fonction d'onde $\psi(x, t)$, il suffit alors d'appliquer s fois l'opérateur

$$F^\dagger e^{\frac{i}{\hbar} \left(\frac{\hbar^2 k^2}{2m} \right) \varepsilon} F e^{-\frac{i}{\hbar} V(x) \varepsilon}$$

L'opérateur $e^{-\frac{i}{\hbar} V(x) \varepsilon}$ est diagonal dans la représentation x . Grâce à la transformée de Fourier F , on passe en représentation k , où l'opérateur d'évolution libre est à son tour diagonal. On termine le cycle en appliquant l'opérateur $F^\dagger = F^{-1}$ pour revenir en représentation x .

La principale difficulté est ainsi de construire une transformation unitaire diagonale du type

$$|x\rangle \longmapsto e^{if(x)} |x\rangle$$

où f est une fonction quelconque. Il existe une méthode générale pour construire ce type d'opérateur diagonal, mais elle est assez gourmande en qubits. Dans les chapitres suivants, des méthodes qui tirent parti de la forme particulière de f seront présentées. Bien sûr, ce type d'algorithme ne donne qu'une méthode pour simuler le système, et la complexité réside aussi dans la manière de mesurer et d'extraire de l'information de la fonction d'onde finale.

Une famille de systèmes qui se prêtent bien à la simulation par des ordinateurs quantiques est celle des applications quantiques. Plusieurs algorithmes ont déjà été développés pour différents modèles issus du chaos quantique. On peut citer l'application du boulanger [78], qui a déjà été implémentée sur 3 qubits en utilisant la résonance magnétique nucléaire [94], ainsi que le rotateur pulsé [43] et l'application en dents de scie [10]. Le calcul de quantités physiques intéressantes dans les modèles dynamiques a aussi été abordé dans [32, 31]. Dans une optique voisine, il existe aussi des algorithmes quantiques permettant de simuler des systèmes chaotiques classiques [44].

Dans cette thèse, nous expliciterons et développerons des algorithmes mieux adaptés aux applications pulsées (comme le rotateur pulsé ou le modèle de Harper pulsé). Nous discuterons également l'extraction d'informations à partir de tels algorithmes.

Chapitre 3

Simulation du rotateur pulsé

3.1 Applications Quantiques : exemple du rotateur pulsé

3.1.1 Rotateur pulsé classique

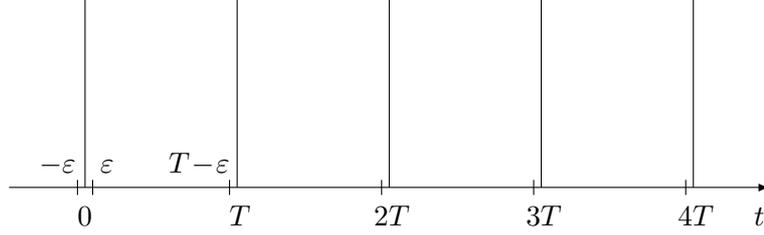
Pour étudier le chaos dynamique, il est intéressant de disposer d'un modèle simple qui soit aisé à simuler, mais qui reproduise néanmoins les caractéristiques essentielles. Si on prend un système dynamique dont l'hamiltonien ne dépend pas explicitement du temps, alors il faut au moins 2 degrés de liberté pour voir apparaître un comportement chaotique (un système à un seul degré de liberté est intégrable si l'énergie est conservée). Une autre solution est de choisir un système à un seul degré de liberté, mais dépendant du temps. Parmi ces systèmes, une classe de modèles très étudiée [26] est celui des applications pulsées, définies par le Hamiltonien

$$H(q, p, t) = H_0(p) + V(q) \sum_{m=-\infty}^{\infty} \delta(t - mT) \quad (3.1)$$

dont le comportement est régi par les équations du mouvement classiques

$$\dot{q} = \frac{\partial H}{\partial p}, \quad \dot{p} = -\frac{\partial H}{\partial q}$$

Le système évolue donc librement selon $H_0(p)$, mais subit périodiquement des perturbations externes de potentiel $V(q)$, sous la forme d'impulsions infiniment courtes. Pour étudier ce modèle, on se ramène à une application discrète en ne considérant l'état du système qu'aux instants qui précèdent immédiatement les impulsions (c'est-à-dire les temps de la forme $mT - \varepsilon$, avec ε infinitésimal).



On peut alors écrire l'état du système (\bar{q}, \bar{p}) à l'instant $(m+1)T - \varepsilon$ en fonction de (q, p) , l'état à l'instant précédent $mT - \varepsilon$. Cette relation ne dépend pas de m à cause de la périodicité en temps de H , donc on prendra $m = 0$ pour simplifier le calcul. De plus, on peut remarquer que p est constant entre ε et $T - \varepsilon$.

$$\begin{aligned}
 \bar{p} - p &= \int_{-\varepsilon}^{T-\varepsilon} \dot{p} \, dt \\
 &= \int_{-\varepsilon}^{T-\varepsilon} -V'(q) \sum_m \delta(t - mT) \, dt \\
 &= \int_{-\varepsilon}^{\varepsilon} -V'(q) \delta(t) \, dt = -V'(q) \\
 \bar{q} - q &= \int_{-\varepsilon}^{T-\varepsilon} \dot{q} \, dt \\
 &= \int_{-\varepsilon}^{T-\varepsilon} H'_0(p) \, dt = H'_0(p(\varepsilon)) T = H'_0(\bar{p}) T
 \end{aligned}$$

$$\begin{cases} \bar{p} = p - V'(q) \\ \bar{q} = q + TH'_0(\bar{p}) \end{cases} \quad (3.2)$$

Pour calculer l'état du système à n'importe quel instant $mT - \varepsilon$, il suffit donc d'itérer cette application m fois à partir de l'état initial.

Une autre façon de construire l'application (3.2) est de partir non pas d'un système à un degré de liberté dépendant du temps comme (3.1) mais d'un système conservatif adéquat à 2 degrés de liberté, et de restreindre l'étude aux instants où l'un des paramètres passe par une valeur donnée (sections de Poincaré). À cause de la conservation de l'énergie, la variété sur laquelle s'effectue le mouvement est alors bien une surface dans l'espace des phases.

Un cas particulier très populaire de cette classe de modèles est celui du rotateur pulsé (aussi appelé application standard ou application de Chirikov [24, 25]). On suppose que (q, p) sont des variables d'angle et de moment cinétique (θ, p) , et on choisit un hamiltonien d'évolution libre de la forme

$H_0(p) = \frac{p^2}{2}$ et un potentiel $V(\theta) = k \cos(\theta)$ ($k \geq 0$), ce qui donne l'hamiltonien

$$H(\theta, p, t) = \frac{p^2}{2} + k \cos(\theta) \sum_m \delta(t - mT) \quad (3.3)$$

et l'application

$$\begin{cases} \bar{p} &= p + k \sin(\theta) \\ \bar{\theta} &= \theta + T\bar{p} \bmod 2\pi \end{cases} \quad (3.4)$$

Malgré sa simplicité apparente, cette application possède de nombreuses propriétés et est utilisée pour modéliser des systèmes physiques très variés. Par exemple, le mouvement d'une comète autour du Soleil perturbé par Jupiter, ou le mouvement d'une particule chargée dans un piège magnétique peuvent tous deux être décrits par l'application standard.

Puisque θ est un angle, la topologie de l'espace des phases est cylindrique. De plus, l'application est périodique en p , de période $\frac{2\pi}{T}$. On peut donc se contenter d'étudier l'espace des phases sur une seule cellule de $2\pi \times \frac{2\pi}{T}$ (fig. 3.1).

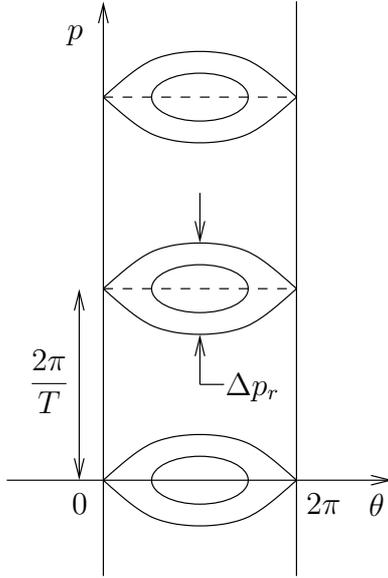


FIG. 3.1 – Représentation schématique de l'espace des phases du rotateur pulsé. Les courbes représentent quelques trajectoires appartenant aux résonances principales, de largeur Δp_r .

Si l'on effectue le changement de variable $x = \frac{\theta}{2\pi}$ et $y = \frac{Tp}{2\pi}$, alors l'application (3.4) peut se réécrire sous la forme

$$\begin{cases} \bar{y} &= y + \frac{K}{2\pi} \sin(2\pi x) \\ \bar{x} &= x + \bar{y} \end{cases} \quad (3.5)$$

On voit donc que la dynamique du système est complètement déterminée par le seul paramètre $K = kT$, en plus bien sûr des conditions initiales. Avec

ces nouvelles variables, une cellule dans l'espace des phases est paramétrée par x et y variant entre 0 et 1.

Pour $K = 0$, le système est intégrable (y est une quantité conservée), et le mouvement d'un point s'effectue le long de lignes à y constant, qui sont des tores à une dimension [77]. Toutes les orbites pour lesquelles $y_0 = \frac{N}{M}$ (avec N et M entiers premiers entre eux) sont périodiques de période M . Autrement dit, si on réécrit l'application (3.5) comme l'action d'un opérateur R

$$\begin{pmatrix} y_{m+1} \\ x_{m+1} \end{pmatrix} = R \begin{pmatrix} y_m \\ x_m \end{pmatrix}$$

alors tous les points pour lesquels $y_0 = \frac{N}{M}$ sont des points fixes de R^M . Si y_0 est irrationnel, alors l'orbite ne se répète jamais et parcourt la ligne $y = y_0$ dans son intégralité au cours du temps. On peut définir une quantité appelée nombre d'enroulement par l'écart moyen entre deux valeurs successives de x sur une orbite

$$w = \lim_{m \rightarrow \infty} \frac{x_m - x_0}{m}$$

Pour $K = 0$, le nombre d'enroulement est simplement $w = y_0$. Cette définition va permettre de caractériser les orbites, périodiques ou non, pour $K \neq 0$. On appelle les orbites périodiques de nombre d'enroulement $w = \frac{N}{M}$ des cycles d'ordre M . Le mouvement d'un point sur cette orbite est dit résonnant.

Lorsque l'on ajoute la perturbation ($K \neq 0$), l'application cesse d'être intégrable, et l'interaction entre les résonances non linéaires conduit à l'apparition du chaos. Kolmogorov, Arnol'd et Moser (appelés affectueusement KAM) ont développé une théorie perturbative en K qui peut être appliquée aux régions non résonantes de l'espace des phases sous certaines conditions de régularité du potentiel V [60, 77]. Ces conditions étant vérifiées par l'application standard, sa transition vers le chaos sera orchestrée selon le théorème KAM.

Dès que $K > 0$, les tores dont le nombre d'enroulement est rationnel se transforment instantanément en des chaînes d'îlots intégrables. Ce phénomène s'explique par le fait que le comportement général de l'application standard est alors essentiellement gouverné par le flot près des points fixes. Supposons que (x_f, y_f) soit un point fixe de R^M

$$\begin{pmatrix} y_f \\ x_f \end{pmatrix} = R^M \begin{pmatrix} y_f \\ x_f \end{pmatrix}$$

On linéarise alors l'application (3.5) autour de ce point, en posant $x_i =$

$x_f + \delta x_i$ et $y_i = y_f + \delta y_i$

$$\begin{pmatrix} \delta y_M \\ \delta x_M \end{pmatrix} = \nabla R^M \begin{pmatrix} \delta y_0 \\ \delta x_0 \end{pmatrix}$$

avec

$$\nabla R^M = \begin{pmatrix} \frac{\partial y_M}{\partial y_0} & \frac{\partial y_M}{\partial x_0} \\ \frac{\partial x_M}{\partial y_0} & \frac{\partial x_M}{\partial x_0} \end{pmatrix}$$

Les deux valeurs propres λ_1 et λ_2 de ∇R^M déterminent le type de flot aux alentours du point fixe. Comme l'application R préserve les surfaces, $\det(\nabla R^M) = \lambda_1 \lambda_2 = 1$. Deux cas peuvent se présenter :

- λ_1 et λ_2 sont complexes de module 1, le flot est alors elliptique
- λ_1 et λ_2 sont réelles, le flot est alors hyperbolique

À cause de la direction du flot aux environs des points fixes, deux points d'un même type ne peuvent pas être contigus dans l'espace des phases. De plus, si P_f est un point fixe de R^M , alors $RP_f, R^2P_f, \dots, R^{M-1}P_f$ le sont aussi. Pour chaque nombre d'enroulement $w = \frac{N}{M}$, on aura donc deux cycles d'ordre M entrelacés, l'un elliptique et l'autre hyperbolique, du moins tant que K n'est pas trop grand.

Prenons comme exemple le cycle d'ordre 1, qui admet comme points fixes $(0, 0)$ et $(\frac{1}{2}, 0)$. En linéarisant R près de ces points on obtient

$$\begin{pmatrix} \delta y_1 \\ \delta x_1 \end{pmatrix} = \begin{pmatrix} 1 & k \cos(2\pi x_f) \\ T & 1 + kT \cos(2\pi x_f) \end{pmatrix} \begin{pmatrix} \delta y_0 \\ \delta x_0 \end{pmatrix}$$

Les valeurs propres locales de cette application linéarisée sont alors

$$\lambda_{\pm} = \frac{2 + K \cos(2\pi x_f)}{2} \pm \sqrt{K \cos(2\pi x_f) \left(1 + \frac{K \cos(2\pi x_f)}{4}\right)}$$

Pour $x_f = 0$, λ_+ et λ_- sont réelles avec $\lambda_+ > 1$, donc le flot autour du point $(0, 0)$ va être hyperbolique, comme représenté sur la figure 3.2. En $x_f = \frac{1}{2}$, λ_+ et λ_- sont complexes de module 1, et le flux est elliptique autour de ce point.

Pour $K > 0$, les cycles d'ordre M sont donc des chaînes de M îlots chacune. Sur la figure 3.3, pour $K = 0,5$, on peut voir par exemple tous les cycles jusqu'à l'ordre 5. Le chaos commence à se développer le long des séparatrices, et notamment autour des points fixes hyperboliques. Les tores dont le nombre d'enroulement est irrationnel ont eux un comportement totalement différent. D'après le théorème KAM, ces tores, appelés judicieusement tores KAM, sont préservés en présence d'une faible perturbation. En effet, le destin de ces tores est dicté par le comportement des

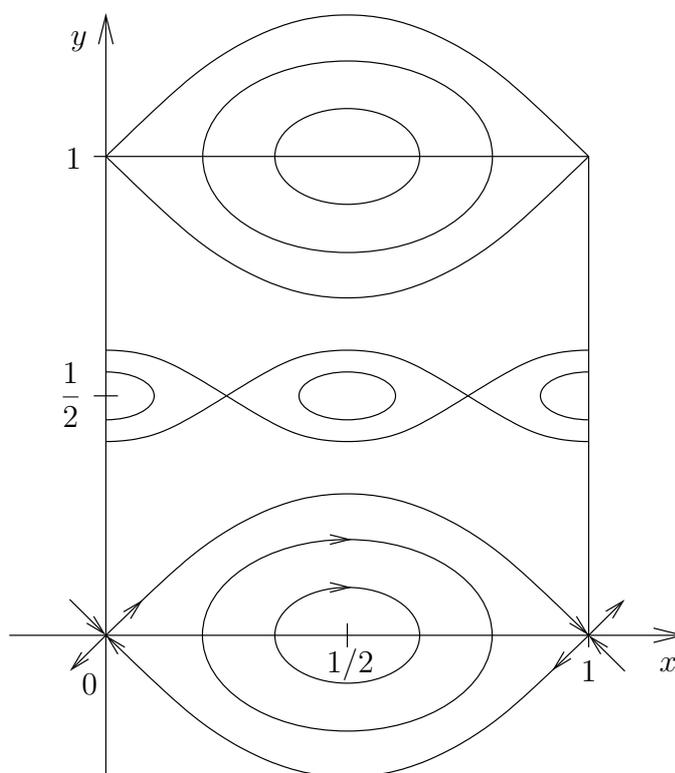


FIG. 3.2 – Résonances d'ordre 1 et 2 du rotateur pulsé.

chaînes d'îlots qui les joutent. Chaque tore KAM est bordé par une infinité d'orbites périodiques, dont l'influence va être d'autant plus grande que celles-ci seront proches dans l'espace des phases. À ce titre, les orbites les plus prépondérantes sont celles dont le nombre d'enroulement est une approximation rationnelle de celui du tore KAM considéré. Cependant, la largeur de ces chaînes de résonances décroît fortement lorsque l'ordre M du cycle augmente. En d'autres termes, plus les résonances sont proches du tore, plus leur largeur est faible. Selon le théorème KAM, ces deux effets se compensent et la somme des largeurs converge. Ceci explique pourquoi les tores KAM peuvent survivre même pour $K \neq 0$. Lorsque K augmente, ils sont tout d'abord simplement déformés par les résonances voisines, puis à terme rompus lorsque celles-ci deviennent trop importantes.

Le nombre d'enroulement w d'un tore KAM peut s'écrire sous la forme d'une fraction continue

$$w = [a_0, a_1, a_2, a_3, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

avec a_i entier et $a_i \geq 1 \forall i \geq 1$ (si on se restreint à une seule cellule de l'espace des phases, $a_0 = 0$). On peut alors obtenir une bonne approximation rationnelle de w en tronquant ce développement à un ordre donné (ce qui revient à prendre un des coefficient $a_i = \infty$). Plus précisément, si $w = [a_0, a_1, a_2, \dots]$, alors les approximants rationnels $\frac{N_i}{M_i}$ donnés par $\frac{N_i}{M_i} = [a_0, a_1, \dots, a_i, \infty]$ sont les meilleurs qui existent, c'est-à-dire que

$$\left| w - \frac{N}{M} \right| \geq \left| w - \frac{N_i}{M_i} \right| \quad \forall M, N \text{ avec } M < M_{i+1}$$

Ainsi, on peut étudier un tore KAM de nombre d'enroulement w en construisant la suite des orbites périodiques de nombres d'enroulement $\frac{N_i}{M_i}$ qui convergent vers ce tore. Comme la largeur de leurs résonances décroît lorsque M_i augmente, le tore KAM peut rester intact pour de faibles valeurs de K malgré la présence d'orbites périodiques arbitrairement proches.

Lorsque l'on augmente K , les tores KAM vont donc être détruits les uns après les autres par l'expansion des résonances voisines. Sur la figure 3.3, on peut voir par exemple pour $K = 0,8$ que l'espace des phases est constitué de zones chaotiques constellées d'îlots intégrables, et séparées les unes des autres par les tores KAM encore intacts. Il existe une valeur critique de K , K_c , au-delà de laquelle tous les tores KAM sont détruits et les zones chaotiques communiquent toutes entre elles. Les derniers tores à être détruits sont ceux dont les nombres d'enroulement (irrationnels) sont les plus difficiles à approximer par des rationnels. C'est le cas des deux tores $w = \frac{1}{\varphi}$ et $w = 1 - \frac{1}{\varphi}$, où φ est le nombre d'or, défini par

$$\varphi = [1, 1, 1, \dots, 1, \dots] = \frac{1 + \sqrt{5}}{2}$$

Comme tous les coefficients du développement sont des 1, la convergence des approximants rationnels vers φ est très lente. Les zones de résonance les plus proches de ces deux tores vont être d'ordre très élevé, et leur finesse va rendre la destruction des tores beaucoup plus difficile. Ils sont encore visibles sur la figure 3.3 pour $K = 0,9716 \approx K_c$; pour cette valeur de K , tous les autres tores KAM ont été détruits.

Enfin, lorsque $K > K_c$, l'espace des phases est constitué d'une mer chaotique parsemée d'îlots intégrables, dont la taille se réduit au fur et à mesure que K augmente. Un point situé initialement dans la zone chaotique peut traverser librement tout l'espace des phases dans la direction des moments, ce qui était interdit avant par la présence des tores KAM. En effet, aucune trajectoire ne peut franchir les courbes invariantes correspondant à des orbites périodiques.

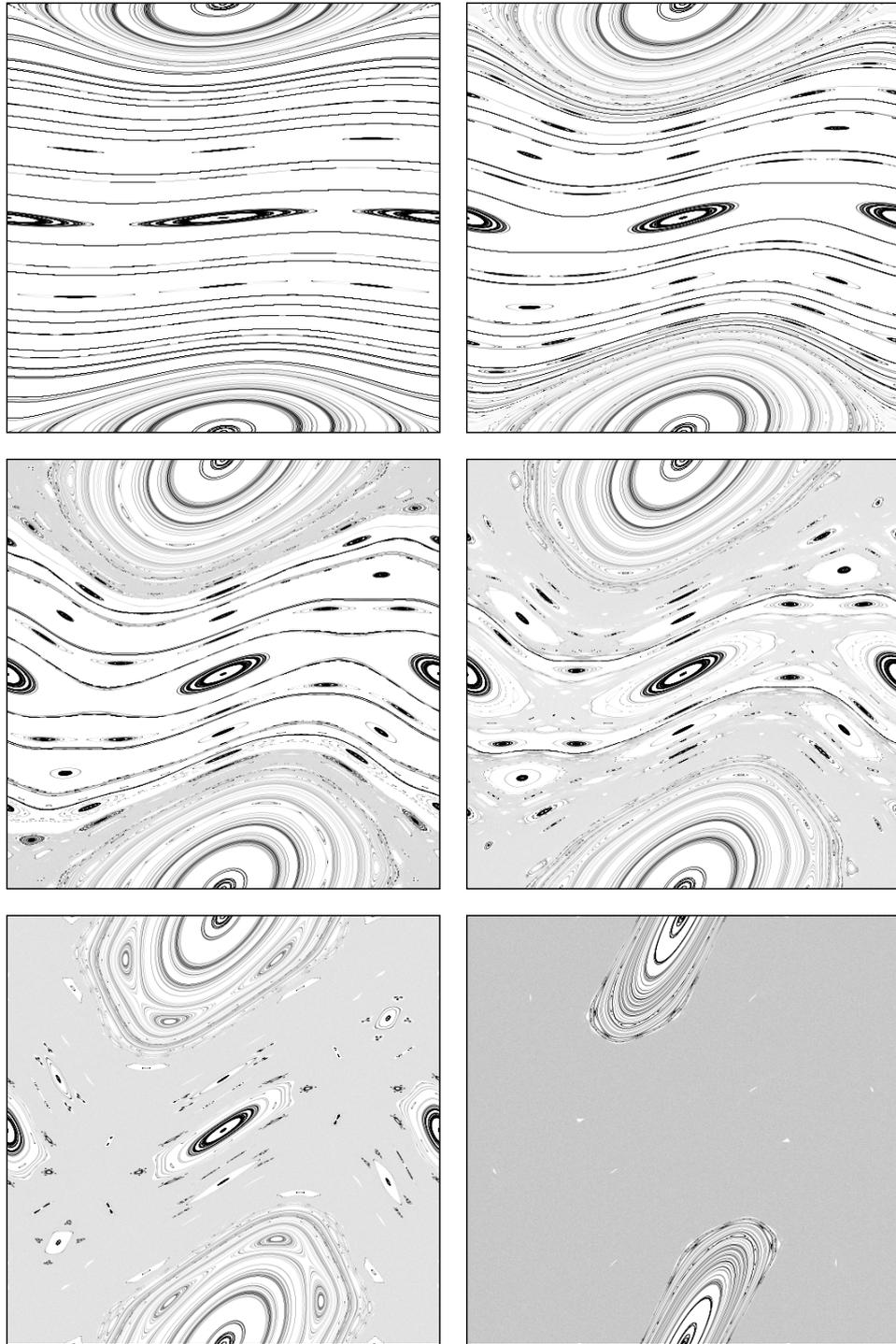


FIG. 3.3 – Espace des phases du rotateur pulsé, pour $K = 0,2$, $K = 0,5$, $K = 0,8$, $K = 0,9716$, $K = 1,3$ et $K = 3,0$ (les courbes correspondent à des trajectoires périodiques, et les zones grises à des trajectoires chaotiques).

Pour déterminer la valeur de K_c , on peut commencer par analyser la résonance principale, d'ordre 1. Si $K = kT$ est faible, alors $|\bar{p} - p| \ll 1$ et $|\bar{\theta} - \theta| \ll 1$, et l'équation aux différences (3.4) peut être vue comme une équation aux dérivées partielles découlant de l'hamiltonien

$$H_r(\theta, p) = \frac{p^2}{2} + \frac{k}{T} \cos \theta$$

Dans ces conditions, le système est équivalent à un pendule simple. La résonance est alors délimitée dans l'espace des phases par une trajectoire particulière, appelée séparatrice, qui sépare les trajectoires liées (oscillations autour du point $(\pi, 0)$) des trajectoires libres. La largeur maximale de la résonance, atteinte pour $\theta = \pi$, est telle que $H_r(0, 0) = H_r(\pi, \frac{\Delta p_r}{2})$, d'où

$$\Delta p_r = 4\sqrt{\frac{k}{T}}$$

Ce régime perturbatif, où les résonances sont supposées ne pas interagir entre elles, va nécessairement prendre fin lorsque la résonance principale va entrer en contact avec celle de la cellule du dessus, comme on peut le voir sur la figure 3.1, c'est-à-dire lorsque

$$\Delta p_r \approx \frac{2\pi}{T}$$

Ce critère de recouvrement des résonances (appelé aussi "critère de Chirikov" [23, 26]) donne la valeur $K_c = \frac{\pi^2}{4} \approx 2,5$, soit seulement le bon ordre de grandeur (la valeur exacte est $K_c \approx 0,9716354$). L'écart est principalement dû à la négligence des résonances d'ordre supérieur. Par exemple sur la figure 3.2, la prise en compte de la résonance d'ordre 2 donne une valeur de K_c inférieure à 2,5, car le recouvrement des résonances intervient plus tôt.

Lorsque $K > K_c$, un système situé dans la zone chaotique peut accéder librement à tout l'espace des phases. Pour étudier le comportement statistique des trajectoires, on se place tout d'abord dans la limite $K \gg K_c$, où la mer chaotique est totalement répandue et les récifs intégrables marginaux. Dans ce cas $|\bar{\theta} - \theta| \gg 2\pi$, ce qui permet de faire une approximation de phase aléatoire, qui consiste à supposer que les valeurs successives de θ_i sont aléatoires et réparties uniformément sur $[0, 2\pi]$. D'après les équations (3.4), le système effectue alors une marche aléatoire en p , ce qui correspond à un comportement diffusif dans la direction des moments cinétiques.

$$\langle (p_t - p_0)^2 \rangle = D_p t \quad (3.6)$$

La constante de diffusion D_p peut être calculée simplement comme suit, où $\langle \dots \rangle$ désigne une moyenne uniforme de chaque couple (θ_i, p_i) sur tout

l'espace des phases

$$\langle \dots \rangle = \prod_i \lim_{p' \rightarrow \infty} \frac{1}{2p'} \int_{-p'}^{p'} dp_i \frac{1}{2\pi} \int_0^{2\pi} d\theta_i \dots$$

$$\begin{aligned} D_p &= \frac{1}{m} \langle (p_m - p_0)^2 \rangle \\ &= \frac{1}{m} \sum_{i,j=0}^{m-1} \langle (p_{i+1} - p_i)(p_{j+1} - p_j) \rangle \\ &= \frac{k^2}{m} \sum_{i,j=0}^{m-1} \langle \sin \theta_i \sin \theta_j \rangle \end{aligned}$$

Si on suppose que deux valeurs de θ successives sont complètement décorréélées, alors $\langle \sin \theta_i \sin \theta_j \rangle = \delta_{i,j} \langle \sin^2 \theta_i \rangle$ et

$$D_p = \frac{k^2}{2}$$

Ceci est une bonne approximation dans la limite $K \rightarrow \infty$. Si on prend en compte les corrélations entre θ_i et θ_j pour $j \neq i$, on doit apporter quelques corrections à cette formule. Ces corrélations décroissant très vite lorsque $|j - i|$ augmente, on peut se limiter au premier ordre non nul. De plus, par symétrie $\langle \sin \theta_i \sin \theta_j \rangle$ ne dépend que de $|j - i|$, donc on utilisera pour simplifier les notations $\bar{\theta}$ pour l'itéré de θ , et $\underline{\theta}$ pour l'antécédent de θ .

$$\begin{aligned} \langle \sin \bar{\theta} \sin \theta \rangle &= \langle \sin(\theta + Tp + K \sin \theta) \sin \theta \rangle \\ &= \frac{1}{2} \langle \cos(Tp + K \sin \theta) \rangle - \frac{1}{2} \langle \cos(\theta + Tp + K \sin \theta) \rangle \\ &= 0 \end{aligned}$$

$$\begin{aligned} \langle \sin \bar{\theta} \sin \underline{\theta} \rangle &= \frac{1}{2} \langle \cos(\bar{\theta} - \underline{\theta}) - \cos(\bar{\theta} + \underline{\theta}) \rangle \\ &= \frac{1}{2} \langle \cos(T(p + \bar{p})) - \cos(2\theta + T(\bar{p} - p)) \rangle \\ &= \frac{1}{2} \underbrace{\langle \cos(2Tp + K \sin \theta) \rangle}_0 - \frac{1}{2} \underbrace{\langle \cos(2\theta + K \sin \theta) \rangle}_{J_2(K)} \end{aligned}$$

où J_2 est une fonction de Bessel. Cela conduit à la constante de diffusion [65]

$$D_p \approx \frac{k^2}{2} (1 - 2J_2(K))$$

Empiriquement, on constate que cette formule est une bonne approximation de D_p pour $K > 5$.

Pour K légèrement supérieur à $K_c \approx 0,97$, ces approximations sont mises à mal par les fragments des tores KAM. Chaque tore est détruit pour une certaine valeur critique de K . Au dessus de cette valeur, la barrière continue que formait le tore est amputée de tous les segments recouverts par les résonances des orbites périodiques voisines. Ces segments sont d'autant plus petits que l'orbite est d'ordre élevé. Les restes du tore KAM forment ainsi un ensemble de Cantor, appelé fort à propos *Cantores* (*Cantorus* en anglais). Malgré leurs perforations, les Cantores représentent tout de même des obstacles sérieux à la diffusion, surtout lorsque K est à peine supérieur à la valeur critique. Pour $K_c < K < 5$, la constante de diffusion peut être approximée par [26]

$$D_p \approx \frac{(K - K_c)^3}{3T^2}$$

3.1.2 Rotateur pulsé quantique

La version quantique du rotateur pulsé s'obtient en appliquant le principe de correspondance de Bohr à l'hamiltonien de départ (3.3) :

$$H(\hat{\theta}, \hat{p}, t) = \frac{\hat{p}^2}{2} + k \cos(\hat{\theta}) \sum_m \delta(t - mT) \quad (3.7)$$

où $\hat{p} = -i\hbar \frac{\partial}{\partial \theta}$ est l'opérateur moment cinétique. Comme son homologue classique, le rotateur pulsé quantique est un modèle simple mais très riche, qui peut décrire de nombreux systèmes physiques [19, 26, 54, 81]. Il modélise par exemple l'ionisation d'un atome de Rydberg par un champ électrique monochromatique uniforme [20, 59], et la localisation d'Anderson en physique du solide [36, 46], qui sera développée plus loin. Le rotateur pulsé quantique a été réalisé expérimentalement avec des atomes de césium ultrafroids dans une onde lumineuse stationnaire proche de la résonance, pulsée périodiquement. Les effets de la localisation dynamique, du bruit extérieur et de la décohérence ont pu ainsi être étudiés expérimentalement [2, 70].

La fonction d'onde du rotateur $|\psi(t)\rangle$ vérifie l'équation de Schrödinger dépendante du temps

$$i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = H(\hat{\theta}, \hat{p}, t) |\psi(t)\rangle$$

On peut résoudre formellement cette équation en introduisant l'opérateur d'évolution $U(t, t_0)$ tel que

$$|\psi(t)\rangle = U(t, t_0) |\psi(t_0)\rangle$$

avec

$$U(t, t_0) = \exp\left(-\frac{i}{\hbar} \int_{t_0}^t H(\hat{\theta}, \hat{p}, t) dt\right)$$

L'équivalent quantique de l'application standard classique est obtenu en ne considérant que les états $|\psi(mT)\rangle$ du système juste avant les impulsions $|\psi(mT)\rangle = \lim_{\varepsilon \rightarrow 0} |\psi(mT - \varepsilon)\rangle$. On peut alors passer de l'état $|\psi(mT)\rangle$ à l'état suivant $|\psi((m+1)T)\rangle$ par application de l'opérateur de Floquet U_F [90]

$$|\psi((m+1)T)\rangle = U_F |\psi(mT)\rangle$$

où U_F est défini par

$$U_F = \lim_{\varepsilon \rightarrow 0} U(T - \varepsilon, -\varepsilon)$$

$$\begin{aligned} U(T - \varepsilon, -\varepsilon) &= U(T - \varepsilon, \varepsilon) U(\varepsilon, -\varepsilon) \\ &= \exp\left(-\frac{i}{\hbar} \int_{\varepsilon}^{T-\varepsilon} \frac{\hat{p}^2}{2} dt\right) \exp\left(-\frac{i}{\hbar} \int_{-\varepsilon}^{\varepsilon} \frac{\hat{p}^2}{2} + k \cos \hat{\theta} \delta(t) dt\right) \\ &= \exp\left(-\frac{i}{\hbar} \frac{\hat{p}^2}{2} (T - 2\varepsilon)\right) \exp\left(-\frac{i}{\hbar} \left(\frac{\hat{p}^2}{2} 2\varepsilon + k \cos \hat{\theta}\right)\right) \end{aligned}$$

On arrive ainsi à une forme simple de l'opération d'évolution entre deux états successifs

$$U_F = \exp\left(-\frac{i}{\hbar} \frac{T \hat{p}^2}{2}\right) \exp\left(-\frac{i}{\hbar} k \cos \hat{\theta}\right) \quad (3.8)$$

Il faut noter que, bien que l'hamiltonien d'évolution libre et l'hamiltonien responsable des impulsions ne commutent pas, U_F s'écrit sous la forme d'un produit entre un opérateur qui ne dépend que de $\hat{\theta}$ et un opérateur qui ne dépend que de \hat{p} . C'est la brièveté des impulsions qui permet d'obtenir une expression analytique pour l'opérateur d'évolution, et incidemment la séparation entre les phases d'évolution libre et les phases d'impulsions. C'est l'un des grands avantages des modèles pulsés.

L'hamiltonien $H(\hat{\theta}, \hat{p}, t)$ est invariant par translation dans le temps de T . On peut donc trouver une base propre commune à H et à l'opérateur de translation dans le temps T_T . D'après le théorème de Floquet (analogue du théorème de Bloch pour les systèmes périodiques en temps et non pas spatialement), si $|\psi_n(t)\rangle$ est un de ces vecteurs propres communs

$$|\psi_n(t)\rangle = e^{-i\omega_n t} |u_n(t)\rangle$$

avec $|u_n(t)\rangle$ périodique : $|u_n(t+T)\rangle = |u_n(t)\rangle$.

$$\begin{aligned} U_F |\psi_n(t)\rangle = |\psi_n(t+T)\rangle &= e^{-i\omega_n(t+T)} |u_n(t+T)\rangle \\ &= e^{-i\omega_n T} e^{-i\omega_n t} |u_n(t)\rangle \\ &= e^{-i\omega_n T} |\psi_n(t)\rangle \end{aligned}$$

U_F a donc pour valeurs propres $e^{-i\omega_n T}$. Si H était indépendant du temps, avec pour énergies propres E_n , U_F aurait pour valeurs propres $e^{-i\frac{E_n}{\hbar}T}$. Par analogie, les $\hbar\omega_n$ sont appelées des *quasi-énergies*. Comme la phase de Floquet $\omega_n T$ n'est définie que modulo 2π , ces quasi-énergies ne sont définies qu'à un multiple de $\frac{2\pi\hbar}{T}$ près.

Soit $|p\rangle$ les vecteurs propres de l'opérateur moment cinétique $\hat{p} = -i\hbar\frac{\partial}{\partial\theta}$. Ces vecteurs ont pour représentation dans la base $|\theta\rangle$

$$\langle\theta|p\rangle = \frac{1}{\sqrt{2\pi\hbar}} e^{\frac{i}{\hbar}p\theta}$$

On peut donc passer de la représentation de $|\psi\rangle$ dans la base $|\theta\rangle$ à celle dans la base $|p\rangle$ par une simple transformée de Fourier

$$\begin{aligned} \langle p|\psi\rangle &= \int \langle p|\theta\rangle \langle\theta|\psi\rangle d\theta \\ &= \frac{1}{\sqrt{2\pi\hbar}} \int e^{-\frac{i}{\hbar}p\theta} \langle\theta|\psi\rangle d\theta \end{aligned}$$

Or $\langle\theta+2\pi|\psi\rangle = \langle\theta|\psi\rangle$, donc le moment cinétique p est quantifié : $\langle p|\psi\rangle$ est non nul pour $p = n\hbar$, avec n entier. On peut alors définir une autre base $|n\rangle = \sqrt{\hbar}|p\rangle$, telle que $\hat{p}|n\rangle = n\hbar|n\rangle$. L'expression de $|n\rangle$ dans la base $|\theta\rangle$ est donnée par

$$\langle\theta|n\rangle = \frac{1}{\sqrt{2\pi}} e^{in\theta}$$

Cependant, $\langle n|\psi\rangle$ étant quantifiée, il est plus pratique de travailler avec les coefficients de Fourier $\psi_m^{(n)}$ tels que

$$\langle n|\psi\rangle = \sum_{m=-\infty}^{+\infty} \psi_m^{(n)} \delta(n-m)$$

Le passage entre la représentation $|\theta\rangle$ et la représentation $|n\rangle$ se fait alors par simple développement en série de Fourier

$$\psi_n^{(n)} = \frac{1}{\sqrt{2\pi}} \int_0^{2\pi} e^{-in\theta} \langle\theta|\psi\rangle d\theta \quad (3.9)$$

$$\langle\theta|\psi\rangle = \frac{1}{\sqrt{2\pi}} \sum_{n=-\infty}^{+\infty} e^{in\theta} \psi_n^{(n)} \quad (3.10)$$

Si l'on introduit l'opérateur $\hat{n} = -i\frac{\partial}{\partial\theta}$ tel que $\hat{n}|n\rangle = n|n\rangle$, U_F devient :

$$U_F = \exp\left(-i\hbar T\frac{\hat{n}^2}{2}\right) \exp\left(-i\frac{K}{\hbar T} \cos\hat{\theta}\right) \quad (3.11)$$

avec toujours $K = kT$. Mais contrairement au rotateur pulsé classique, le système dépend cette fois de deux paramètres, K et $\hbar T$. K détermine entièrement le comportement du système dans la limite semi-classique, et \hbar gouverne les spécificités quantiques si on choisit $T = 1$, ce qui sera dorénavant le cas.

On peut écrire (3.11) sous forme de matrice dans la base $|n\rangle$

$$\begin{aligned} \langle n|U_F|m\rangle &= \exp\left(-i\hbar\frac{n^2}{2}\right) \langle n|\exp\left(-\frac{i}{\hbar}K \cos\hat{\theta}\right)|m\rangle \\ &= \exp\left(-i\hbar\frac{n^2}{2}\right) \iint d\theta d\theta' \langle n|\theta'\rangle \langle \theta'|\exp\left(-\frac{i}{\hbar}K \cos\hat{\theta}\right)|\theta\rangle \langle \theta|m\rangle \\ &= \exp\left(-i\hbar\frac{n^2}{2}\right) \frac{1}{2\pi} \iint d\theta d\theta' e^{i(m\theta-n\theta')} \exp\left(-\frac{i}{\hbar}K \cos\theta\right) \delta(\theta-\theta') \\ &= \exp\left(-i\hbar\frac{n^2}{2}\right) \frac{1}{2\pi} \int d\theta e^{i(m-n)\theta} \exp\left(-\frac{i}{\hbar}K \cos\theta\right) \\ &= \exp\left(-i\hbar\frac{n^2}{2}\right) (-i)^{m-n} J_{m-n}\left(\frac{K}{\hbar}\right) \end{aligned} \quad (3.12)$$

où J_{m-n} est une fonction de Bessel. L'opérateur d'impulsion ne dépend que de $(m-n)$; de plus, la valeur de $J_{m-n}\left(\frac{K}{\hbar}\right)$ décroît vite lorsque $|m-n|$ augmente. $\langle n|U_F|m\rangle$ est donc une matrice de bande, avec des éléments importants seulement près de la diagonale.

Dans la pratique, pour simuler le rotateur pulsé quantique sur un ordinateur fini (classique ou quantique), il est nécessaire de clore également l'espace des phases dans la direction des moments. Pour effectuer cette fermeture, on choisit la condition aux limites périodique $\langle p+2\pi\alpha|\psi\rangle = \langle p|\psi\rangle$, ce qui donne à l'espace des phases la topologie d'un tore. Dans l'espace des phases classique, une cellule a une dimension de 2π dans la direction p (avec $T = 1$). Lorsque α est entier, ce nombre représente donc simplement le nombre de cellules choisies (par exemple $\alpha = 2$ sur la figure 3.4). D'autre part, comme $p = n\hbar$, $2\pi\alpha$ doit être un multiple entier de \hbar pour pouvoir assurer la périodicité de $\langle p|\psi\rangle$. On appelle $N = \frac{2\pi\alpha}{\hbar}$ le nombre d'états de l'espace de Hilbert ainsi construit.

La périodisation de l'espace des phases en p provoque à son tour une quantification de $\langle \theta | \psi \rangle$, qui devient non nulle seulement pour $\theta = \frac{2\pi}{N} \Theta$, avec Θ entier. On introduit la nouvelle base $|\Theta\rangle = \sqrt{\frac{2\pi}{N}} |\theta\rangle$ telle que $\hat{\theta} |\Theta\rangle = \frac{2\pi}{N} \Theta |\Theta\rangle$. Sa relation à la base $|n\rangle$ est donnée par

$$\langle \Theta | n \rangle = \frac{1}{\sqrt{N}} e^{i2\pi \frac{\Theta n}{N}}$$

De la même manière que les $\psi_m^{(n)}$, on définit les coefficients de Fourier $\psi_m^{(\Theta)}$ tels que

$$\langle \Theta | \psi \rangle = \sum_{m=-\infty}^{+\infty} \psi_m^{(\Theta)} \delta(\Theta - m)$$

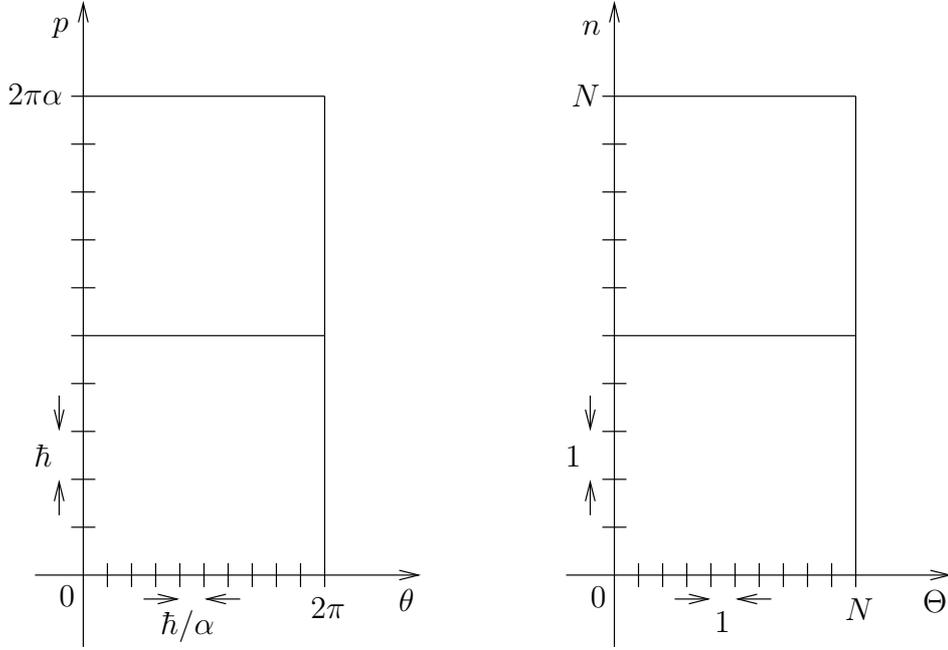


FIG. 3.4 – Discretisation de l'espace des phases du rotateur pulsé quantique, dans les coordonnées (θ, p) et (Θ, n)

On peut alors entièrement spécifier $|\psi\rangle$ grâce à N nombres complexes, qui sont soit les $\psi_m^{(\Theta)}$ dans la base $|\Theta\rangle$, soit les $\psi_m^{(n)}$ dans la base $|n\rangle$. Le passage d'une base à l'autre s'effectue facilement grâce à une Transformée de Fourier discrète, directe de la base $|n\rangle$ vers la base $|\Theta\rangle$ et inverse dans l'autre sens

$$\psi_{\Theta}^{(\Theta)} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{i2\pi \frac{\Theta n}{N}} \psi_n^{(n)} \quad (3.13)$$

$$\psi_n^{(n)} = \frac{1}{\sqrt{N}} \sum_{\Theta=0}^{N-1} e^{-i2\pi \frac{\Theta n}{N}} \psi_{\Theta}^{(\Theta)} \quad (3.14)$$

La Transformée de Fourier rapide permet d'ailleurs, grâce à ces relations de changement de base, d'appliquer U_F de façon plus efficace qu'avec l'expression (3.12).

3.1.3 Localisation dynamique et localisation d'Anderson

Comme dans le cas classique, on va maintenant étudier la diffusion du moment cinétique. De ce point de vue, le rotateur pulsé quantique a un comportement radicalement différent suivant que \hbar est ou non une fraction rationnelle de 4π [26, 77]. Supposons pour commencer que $\hbar = 4\pi$; alors l'opérateur U_F devient diagonal dans la base $|\theta\rangle$

$$U_F = e^{-i \frac{K}{4\pi} \cos \hat{\theta}}$$

On met à l'instant initial le rotateur dans l'état $n = 0$ ($\psi_m^{(n)}(0) = \delta_{m0}$), ce qui, traduit dans la base $|\theta\rangle$, donne l'état initial $\langle \theta | \psi(0) \rangle = \frac{1}{2\pi}$. Après un temps t , qui correspond à l'application de t impulsions puisque $T = 1$,

$$\langle \theta | \psi(t) \rangle = \langle \theta | U_F^t | \psi(0) \rangle = \frac{1}{2\pi} e^{-i \frac{Kt}{4\pi} \cos \theta}$$

On peut alors calculer le second moment de la distribution en moment cinétique par

$$\begin{aligned} \langle \hat{n}^2 \rangle &= \langle \psi | \hat{n}^2 | \psi \rangle \\ &= \int_0^{2\pi} \langle \psi | \theta \rangle \langle \theta | \hat{n}^2 | \psi \rangle d\theta \\ &= \frac{1}{2\pi} \int_0^{2\pi} e^{i \frac{Kt}{4\pi} \cos \theta} \left(-\frac{\partial^2}{\partial \theta^2} \right) e^{-i \frac{Kt}{4\pi} \cos \theta} d\theta \\ &= \frac{1}{2\pi} \int_0^{2\pi} \left(-i \frac{Kt}{4\pi} \cos \theta + \frac{K^2 t^2}{(4\pi)^2} \sin^2 \theta \right) d\theta \\ &= \frac{K^2 t^2}{(4\pi)^3} \end{aligned}$$

On voit que $\langle \hat{n}^2 \rangle$, et donc l'énergie moyenne du rotateur, augmente quadratiquement avec le temps. Plus généralement, cette croissance quadratique de l'énergie, appelée résonance quantique, intervient aussi pour n'importe quelle valeur rationnelle de $\frac{\hbar}{4\pi}$, excepté $\frac{1}{2}$ (fig. 3.5).

Lorsque $\frac{\hbar}{4\pi}$ n'est pas rationnel, le comportement du moment cinétique est tout autre. Pour les petits temps, l'énergie commence par croître linéairement

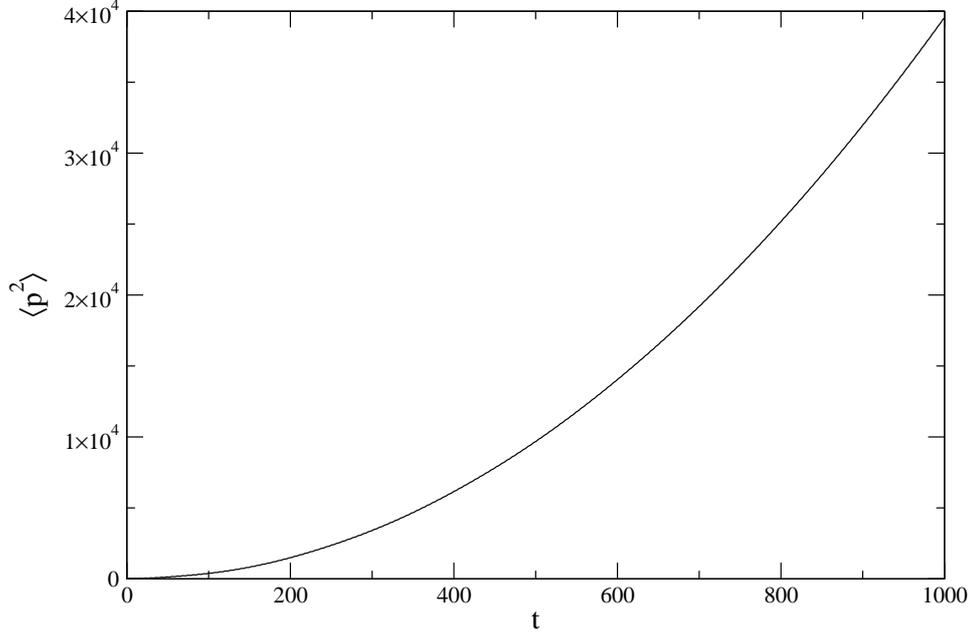


FIG. 3.5 – Croissance quadratique de l'énergie du rotateur pour $\hbar = 4\pi \times \frac{2}{5}$ et $K = 5$.

avec le temps, en suivant la même loi que pour le rotateur pulsé classique. Par contre, aux temps longs $\langle \hat{n}^2 \rangle$ cesse d'augmenter et devient stationnaire, comme on peut le voir sur la figure 3.6. À cet instant, la fonction d'onde est localisée : son extension dans l'espace de Hilbert est limitée à une petite zone de taille l (appelée longueur de localisation) autour de son point de départ, et elle décroît exponentiellement lorsque l'on s'en écarte (fig. 3.7)

$$\psi_m^{(n)} = \frac{1}{2l} e^{-\frac{|m|}{l}}$$

Si on reprend par exemple la condition initiale $\psi_m^{(n)}(0) = \delta_{m0}$, alors

$$\begin{aligned} \langle \hat{n}^2 \rangle &= \langle \psi(0) | U_F^{\dagger t} \hat{n}^2 U_F^t | \psi(0) \rangle \\ &= \sum_n n^2 (U_F^t)_{n0} (U_F^t)_{n0}^* \end{aligned} \quad (3.15)$$

On peut diagonaliser U_F grâce à une transformation unitaire V

$$(U_F)_{nm} = \sum_k e^{-i\phi_k} V_{kn}^* V_{km}$$

où les ϕ_k sont les phases de Floquet. En remplaçant dans (3.15), on obtient

$$\langle \hat{n}^2 \rangle = \sum_{n,k,k'} n^2 e^{it(\phi_{k'} - \phi_k)} V_{kn}^* V_{k'0} V_{k'0}^* V_{k'n} \quad (3.16)$$

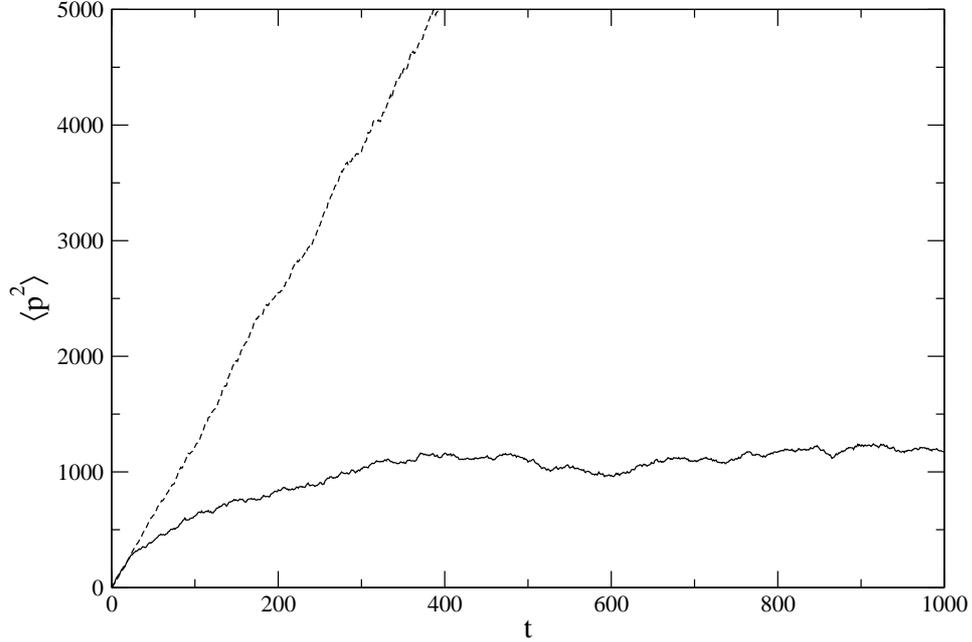


FIG. 3.6 – L'énergie du rotateur tend vers un état stationnaire pour $\hbar = \frac{2}{5}$ et $K = 5$. La courbe en pointillés correspond à la diffusion classique, et celle en trait plein à la localisation quantique avec $p = n\hbar$.

Comme U_F est une matrice de bande, la matrice de changement de base V l'est aussi, ce qui restreint la somme dans (3.16) à approximativement l termes non nuls. Les phases de Floquet étant a priori réparties uniformément sur le cercle, la différence de phase $(\phi_{k'} - \phi_k)$ est en moyenne de l'ordre de $\Delta\phi = \frac{2\pi}{l}$. Cet écart moyen entre quasi-énergies conduit au temps de Heisenberg $t_H \sim \frac{1}{\Delta\phi} \sim l$, qui est le temps pour lequel le système commence à sentir les effets de la discrétisation du spectre. Pour $t \ll t_H$, le système se comporte comme son pendant classique et le second moment diffuse normalement. Mais pour $t \gg t_H$, le facteur de phase dans (3.16) oscille rapidement, et tous les termes pour lesquels $k \neq k'$ s'annulent. On a alors

$$\langle \hat{n}^2 \rangle = \sum_{n,k} n^2 |V_{kn}|^2 |V_{k0}|^2 \quad (3.17)$$

qui ne dépend plus de t , et la diffusion s'arrête.

La localisation intervient donc pour $t \sim l$. D'autre part, comme la somme dans l'expression (3.17) ne court que sur un domaine de taille l , n^2 ne peut valoir au maximum que l^2 , et $\langle \hat{n}^2 \rangle \sim l^2$. Or, jusqu'à $t \sim l$ le système diffuse classiquement selon la loi (3.6), donc $\langle \hat{n}^2 \rangle \sim D_p l$. En rapprochant les deux expressions pour $\langle \hat{n}^2 \rangle$, on obtient la relation trouvée par Chirikov, Izrailev

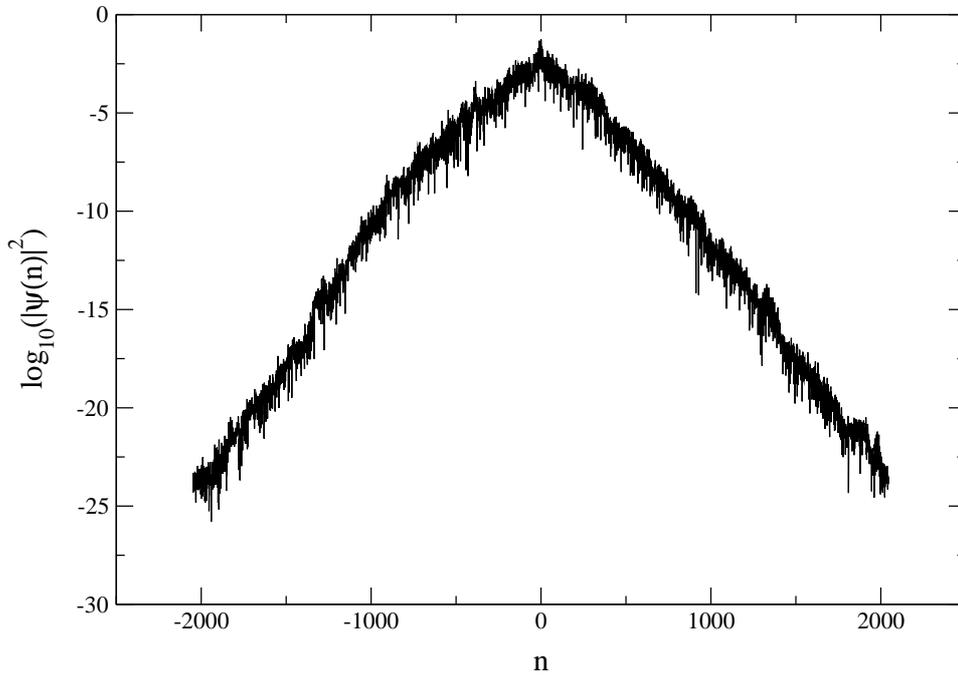


FIG. 3.7 – Localisation de la fonction d'onde du rotateur dans l'espace des moments pour $\hbar = \frac{2}{5}$ et $K = 5$, après 1000 itérations, avec un état initial concentré en $n = 0$.

et Shepelyansky [27, 80, 81]

$$l \sim D_p$$

La longueur de localisation quantique est proportionnelle au coefficient de diffusion classique. Numériquement, on trouve $l = \frac{1}{2}D_p$. La constante de proportionnalité a pu être établie analytiquement dans le cadre d'autres modèles, comme le modèle de Lloyd pour lequel le potentiel des perturbations est donné par

$$V(\theta) = V_0 \arctan(E - 2k \cos \theta)$$

Un dernier point digne d'intérêt peut être abordé par la question suivante : comment peut-on simuler numériquement la localisation du rotateur pulsé quantique, qui intervient pour une valeur irrationnelle de $\frac{\hbar}{4\pi}$, alors que les ordinateurs ne peuvent manipuler essentiellement que des nombres rationnels ? La solution de ce paradoxe apparent tient dans le comportement des résonances quantiques aux hautes harmoniques, c'est-à-dire pour $\frac{\hbar}{4\pi} = \frac{p}{q}$ avec $q \gg 1$. D'après l'équation (3.11), la perturbation est alors de période q et les états propres satisfont le théorème de Bloch

$$\psi(n + q) = \psi(n)e^{iq\gamma}$$

Le module de la fonction propre a ainsi une période de q . D'autre part, celle-ci doit être localisée au sein de chaque période si $l \ll q$. En effet, d'après le principe d'incertitude, la structure fine du spectre n'a aucune influence sur le mouvement pour des échelles de temps courtes, et une petite imprécision sur la valeur de $\frac{\hbar}{4\pi}$ ne doit pas induire un changement de comportement important, même si l'on passe d'une valeur rationnelle à une valeur irrationnelle. De fait, le recouvrement entre les états propres diminue exponentiellement avec le paramètre $q/l \gg 1$. Ainsi, l'énergie suit bien une loi de croissance quadratique

$$E(t) \sim r(q)t^2$$

mais son taux de croissance $r(q)$, qui est lié au taux de transition entre états, est d'autant plus faible que le dénominateur q est grand

$$r(q) \approx \left(\frac{K}{2}\right)^2 e^{-\frac{q}{2\pi l}}$$

On peut définir un temps caractéristique t_q pour lequel la loi de croissance quadratique donne une énergie comparable à celle de l'état localisé $E(t_q) \sim l^2$, soit

$$t_q \sim e^{\frac{q}{4\pi l}} \sqrt{l}$$

Tant que $t \ll t_q$, les états propres restent localisés. Comme t_q augmente exponentiellement avec le dénominateur q , le régime de croissance quadratique devient très vite inobservable pour les hautes harmoniques.

Le phénomène de localisation est présent également dans un modèle célèbre issu de la matière condensée, le modèle d'Anderson [3]. Celui-ci est utilisé pour étudier le comportement d'un électron sur un réseau cristallin désordonné. À une dimension, l'hamiltonien d'un tel système est donné par

$$H = -\frac{\hbar^2}{2m} \frac{d^2}{dx^2} + V(x)$$

où $V(x)$ est le potentiel créé par un réseau d'atomes régulièrement espacés d'une distance d . Pour résoudre l'équation de Schrödinger, on fait l'hypothèse de fort couplage : l'électron interagit fortement avec un seul atome à la fois, ce qui permet de développer sa fonction d'onde sur la base des fonctions propres monoatomiques $\psi_0(x - nd)$

$$\psi(x) = \sum_n a_n \psi_0(x - nd)$$

avec un recouvrement négligeable entre les sites

$$\int \psi_0^*(x - nd) \psi_0(x - md) dx = \delta_{nm}$$

Si $\psi(x)$ est une fonction propre de H , on obtient

$$\sum_{k \neq n} W_{nk} a_k + E_n^0 a_n = E a_n \quad (3.18)$$

avec

$$\begin{aligned} E_n^0 &= \int \psi_0^*(x - nd) H \psi_0(x - nd) dx \\ W_{nk} &= \int \psi_0^*(x - nd) H \psi_0(x - kd) dx \end{aligned}$$

Si le potentiel V est périodique, alors E_n^0 est indépendant de n , et W_{nk} ne dépend que de $(n - k)$. On retombe alors sur le modèle standard de la conduction dans les solides, avec un spectre sous forme de bandes. Le modèle d'Anderson consiste à prendre un potentiel V non plus périodique mais perturbé par un désordre aléatoire, provoqué par exemple par des défauts dans l'agencement cristallin ou par des impuretés. Pour ce faire, on peut introduire soit un désordre dans les liaisons, auquel cas les W_{kn} sont aléatoires de site en site alors que les E_n^0 restent constants, soit un désordre sur site, en prenant des énergies de site E_n^0 aléatoires et en gardant les W_{kn} constants.

Prenons le cas d'un désordre de site, en se restreignant à une interaction avec les plus proches voisins. L'équation (3.18) devient

$$W a_{n+1} + W a_{n-1} + E_n^0 a_n = E a_n$$

On peut la réécrire sous la forme matricielle

$$\begin{pmatrix} a_{n+1} \\ a_n \end{pmatrix} = T_n \begin{pmatrix} a_n \\ a_{n-1} \end{pmatrix}$$

où T_n est la matrice de transfert donnée par

$$T_n = \begin{pmatrix} (E - E_n^0)/W & -1 \\ 1 & 0 \end{pmatrix}$$

Si l'on considère une chaîne de N sites, l'état du bout de la chaîne peut être obtenu à partir de celui du début en appliquant plusieurs fois la matrice de transfert

$$\begin{pmatrix} a_{N+1} \\ a_N \end{pmatrix} = T_N T_{N-1} \dots T_2 T_1 \begin{pmatrix} a_1 \\ a_0 \end{pmatrix}$$

Comme les matrices T_n ont un déterminant de module 1, on peut (sous certaines conditions) leur appliquer le théorème de Furstenberg [39]

$$\lim_{N \rightarrow \infty} \frac{1}{N} \ln \text{Tr}(T_N T_{N-1} \dots T_2 T_1) = \gamma > 0$$

D'après ce théorème, loin du site de départ ($|N| \rightarrow \infty$) la matrice $T_N T_{N-1} \dots T_2 T_1$ possède les deux valeurs propres $\exp(\pm N\gamma)$. Pour éviter une croissance exponentielle de la fonction d'onde dans l'une ou l'autre direction, il faut choisir des valeurs particulières de a_0 , a_1 et E . Les énergies propres du modèle d'Anderson ne forment ainsi pas un continuum et constituent un spectre discret. La fonction d'onde de l'électron est alors localisée exponentiellement de part et d'autre du site de départ, avec une longueur de localisation $\frac{1}{\gamma}$ [49, 77, 90]. On peut remarquer que le système est localisé quelle que soit l'intensité du désordre, mais ceci n'est valable qu'en dimension 1. Pour un système de dimension 3 ou plus, il existe un seuil de désordre en dessous duquel la localisation n'a pas lieu. La dimension 2 est un cas marginal pour lequel tous les états sont localisés, mais la longueur de localisation peut être extrêmement grande. On voit donc que les électrons diffusent classiquement mais sont localisés quantiquement ce qui correspond physiquement à un isolant. La compréhension de ces modèles a valu le prix Nobel (1977) à P. W. Anderson [3]. Ce domaine est encore étudié à l'heure actuelle, en particulier l'effet des interactions a donné lieu à de nombreuses publications récentes [82, 53, 15, 37, 93, 92].

Grâce à quelques manipulations, le modèle du rotateur pulsé quantique peut être reformulé d'une manière analogue au modèle d'Anderson présenté ci-dessus [36, 46]. On peut écrire l'opérateur de Floquet (3.11) sous la forme (avec toujours $T = 1$)

$$\hat{U}_F = \exp\left(-i\frac{H_0(\hat{n})}{\hbar}\right) \exp\left(-i\frac{V(\hat{\theta})}{\hbar}\right)$$

On suppose que $\psi^{(n)}$ est la représentation dans la base $|n\rangle$ d'un vecteur propre $|\psi\rangle$ de \hat{U}_F avec la phase propre ϕ

$$U_F \psi^{(n)} = e^{-iH_0(n)/\hbar} e^{-iV(\theta)/\hbar} \psi^{(n)} = e^{-i\phi} \psi^{(n)}$$

$$\text{avec } \psi^{(n)} = \begin{pmatrix} \vdots \\ \psi_k^{(n)} \\ \vdots \end{pmatrix}$$

En faisant la substitution

$$e^{-iV(\theta)/\hbar} = \frac{1 + iW(\theta)}{1 - iW(\theta)}$$

$$\text{où } W(\theta) = -\tan \frac{V(\theta)}{2\hbar}$$

L'équation aux valeurs propres devient

$$\frac{1 + iW(\theta)}{1 - iW(\theta)} \psi^{(n)} = e^{i(H_0/\hbar - \phi)} \psi^{(n)}$$

ou

$$(1 - e^{i(H_0/\hbar - \phi)})\psi^{(n)} + iW(1 + e^{i(H_0/\hbar - \phi)})\psi^{(n)} = 0$$

On introduit le nouveau vecteur propre $\bar{\psi}^{(n)}$

$$\bar{\psi}^{(n)} = (1 + e^{i(H_0/\hbar - \phi)})\psi^{(n)}$$

Ce qui donne l'équation

$$\frac{1 - e^{i(H_0/\hbar - \phi)}}{1 + e^{i(H_0/\hbar - \phi)}}\bar{\psi}^{(n)} + iW\bar{\psi}^{(n)} = 0$$

ou

$$\tan\left(\frac{\phi - H_0/\hbar}{2}\right)\bar{\psi}^{(n)} + W\bar{\psi}^{(n)} = 0$$

Grâce aux relations de changement de représentation (3.9) et (3.10), on peut enfin réécrire cette dernière équation comme

$$\sum_{k \neq n} W_{n-k}\bar{\psi}_k^{(n)} + E_n^0\bar{\psi}_n^{(n)} = E\bar{\psi}_n^{(n)} \quad (3.19)$$

où les énergies de liaison W_n sont les coefficients de Fourier de $W(\theta)$

$$W_n = \frac{1}{2\pi} \int_0^{2\pi} W(\theta)e^{-in\theta} d\theta$$

et les énergies E_n^0 et E sont données par

$$E_n^0 = \tan\left(\frac{\phi - H_0(n)/\hbar}{2}\right)$$

et

$$E = -W_0$$

Si on la compare à (3.18), on voit que l'équation (3.19) correspond bien au modèle d'Anderson avec un désordre sur site (les énergies de liaisons W_{nk} dépendent en effet seulement de la différence $(n - k)$). L'obtention de la formulation (3.19) ne dépendant pas explicitement de H_0 et V , cette correspondance entre la localisation dynamique quantique et la localisation d'Anderson est valable aussi pour tous les modèles pulsés en général. La seule différence avec le modèle d'Anderson réside dans le fait que les coefficients E_n^0 ne sont pas statistiquement aléatoires, mais seulement pseudo-aléatoires. De la même manière que pour l'étude de la diffusion, on suppose que $\frac{\hbar}{4\pi}$ est un nombre irrationnel β . Alors, en prenant $\phi = 0$ pour simplifier, les énergies de site sont données par

$$E_n^0 = -\tan\left(\frac{\hbar n^2}{4}\right) = -\tan(\pi\beta n^2)$$

Comme β est irrationnel, un théorème de Weyl implique que $\beta n^2 \bmod 1$ est uniformément réparti sur $[0, 1]$. Les énergies E_n^0 ont alors pour distribution de probabilité

$$p(E) = \frac{1}{\pi} \frac{1}{1 + E^2}$$

Il subsiste malgré tout quelques corrélations qui trahissent la nature pseudo-aléatoire des énergies de site, mais cela ne suffit pas à détruire la localisation.

3.2 Résultats sur le rotateur pulsé

Ce modèle incontournable du chaos quantique fait l'objet de l'étude de la publication I ci-après. Il peut être simulé efficacement sur un ordinateur quantique grâce à un algorithme découvert par Georgeot et Shepelyansky [43]. Les détails de cet algorithme sont rappelés dans la publication I. Les premières études des effets des imperfections sur ce modèle sont dues à Song et Shepelyansky [86]. Il est important d'identifier des observables mesurables sur un ordinateur quantique une fois la simulation effectuée, et également de voir comment ces observables sont affectées par les imperfections inhérentes à toute implémentation réaliste. Le but de I est d'étudier précisément un ensemble aussi large que possible d'observables et de voir l'effet d'erreurs effectuées pendant le calcul sur ces observables.

Le modèle d'imperfections étudié ici est celui des erreurs dynamiques. On considère que dans une implémentation physique réaliste d'un ordinateur quantique la précision finie du contrôle conduit à appliquer des portes quantiques imparfaites. Chaque instance d'une porte quantique élémentaire est ainsi légèrement éloignée de sa valeur idéale, tout en restant unitaire.

Illustrons l'effet d'un bruit unitaire aléatoire sur une porte simple : la porte d'Hadamard. Celle-ci peut s'écrire comme $H = \hat{n}_0 \cdot \vec{\sigma}$ avec

$$\hat{n}_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \text{et} \quad \vec{\sigma} = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

À chaque application de H , celle-ci est remplacée par la porte voisine $H' = \hat{n} \cdot \vec{\sigma}$, où \hat{n} est un vecteur unitaire qui fait un angle β avec \hat{n}_0 . L'angle β est tiré aléatoirement à chaque application, de manière uniforme entre 0 et $\varepsilon\pi$. ε représente ainsi l'amplitude des imperfections.

Pour effectuer la transformée de Fourier quantique et l'opérateur d'évolution libre, les seules portes nécessaires sont la porte d'Hadamard et la porte de phase contrôlée. Cette porte à deux qubits est également sujette

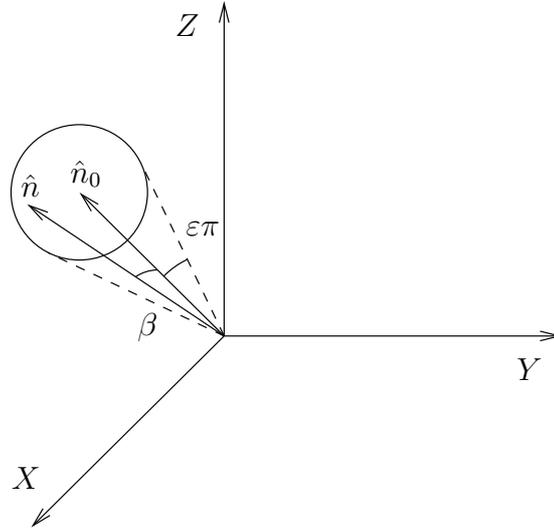


FIG. 3.8 – Modèle d’erreur dynamique pour la porte d’Hadamard.

au bruit unitaire, mais le modèle retenu ici est plus simple :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix} \text{ est remplacé par } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i(\alpha+\beta)} \end{pmatrix}$$

avec toujours une distribution aléatoire uniforme entre 0 et $\varepsilon\pi$ pour β . Ce type d’imperfection ne couple pas les états de la base naturelle entre eux, mais les autres types de porte s’en chargeront (comme la porte d’Hadamard). Cette simplification du modèle par rapport à celui qui consisterait à tirer une porte aléatoirement dans $U(4)$ ne change donc pas qualitativement le comportement de l’algorithme. Une autre approximation concerne l’opérateur $\exp\left(-i\frac{K}{\hbar}\cos\hat{\theta}\right)$. Celui-ci a été systématiquement appliqué exactement (sans erreur) lors de la simulation du rotateur pulsé par l’algorithme quantique.

Différents types d’observables ont été envisagés. Tout d’abord, la longueur de localisation est mesurable facilement sur un ordinateur quantique, puisque le nombre de mesures nécessaires pour déterminer l’état du système est alors assez réduit par rapport à la taille de l’espace de Hilbert. Numériquement, elle peut être obtenue à partir de quantités comme le second moment ou l’IPR (inverse participation ratio). La fidélité est aussi une grandeur très utilisée pour caractériser la proximité d’un état réel à un état idéal. Les lois qui régissent sa décroissance en fonction du temps sont très étudiées par ailleurs. Un autre phénomène intéressant est l’effet tunnel assisté par le

chaos [22]. Si le système est placé à l'intérieur d'un îlot intégrable, il peut éventuellement passer par effet tunnel vers un autre îlot. Ce processus est normalement d'autant plus lent que les deux îlots sont éloignés, mais la mer chaotique séparant les deux peut l'accélérer. Enfin, les distributions de Wigner ou d'Husimi (voir appendice A) sont très utiles car elles permettent une comparaison directe de la dynamique avec espace des phases classique. Elles sont de plus abondamment étudiées en calcul quantique, et il existe des algorithmes [69] pour mesurer un point particulier du pseudo-espace des phases de manière efficace.

Dans la publication I ci-après [64], l'effet d'un bruit unitaire dans les portes quantiques a été étudié analytiquement et numériquement sur des réalisations allant jusqu'à 20 qubits. On montre ainsi que toutes les quantités n'ont pas le même comportement face au bruit. La très grande sensibilité au bruit de quelques quantités, comme le second moment de la distribution de probabilité, ou les transitions par effet tunnel à travers des courbes invariantes, a été mise en évidence. Plus précisément, l'échelle de temps au bout de laquelle ces quantités commencent à être affectées augmente exponentiellement avec le nombre de qubits. Cependant, d'autres quantités comme la fidélité ou la distribution de Wigner sont robustes, c'est-à-dire que leur temps caractéristique augmente seulement polynomialement avec l'intensité du bruit et la taille du registre. Ces résultats impliquent que de telles quantités peuvent être calculées de manière fiable en présence d'un bruit modéré.

3.3 Publication I

Quantum computing of quantum chaos in the kicked rotator model
B. Lévi, B. Georgeot and D. L. Shepelyansky
Phys. Rev. E. **67**, 046220 (2003)
quant-ph/0210154

Chapitre 4

Simulation du Harper pulsé

4.1 Le modèle de Harper

4.1.1 Modèle de Harper

L'équation de Harper a été introduite en 1955 comme modèle approché pour des électrons en champ cristallin bidimensionnel plongés dans un champ magnétique [50]. Plusieurs approximations importantes sont nécessaires pour l'établir. Tout d'abord, on se restreint à l'étude d'une seule bande de Bloch, par exemple celle qui contient l'énergie de Fermi et dans laquelle se trouvent les électrons de conduction. L'approximation suivante consiste à postuler une forme d'énergie de bande $E(\vec{k})$ dérivant d'un couplage fort (\vec{k} est le quasi-moment défini modulo le réseau réciproque). La périodicité de $E(\vec{k})$ en \vec{k} permet alors de développer l'énergie en série de Fourier. Pour un réseau carré de maille a , et en se restreignant au premier ordre, on obtient

$$E(\vec{k}) = K \cos(k_x a) + L \cos(k_y a)$$

Ce réseau cristallin bidimensionnel est alors plongé dans un champ magnétique uniforme perpendiculaire B (dérivant par exemple du potentiel-vecteur $\vec{A} = (0, Bx, 0)$). Pour tenir compte de ce champ magnétique, on effectue la substitution de Peierls : on remplace $\hbar\vec{k}$ dans l'expression de l'énergie ci-dessus par $\vec{\Pi} = \vec{p} - e\vec{A}$, pour obtenir un opérateur que l'on traite comme un hamiltonien effectif.

$$H = K \cos\left(\frac{\Pi_x}{\hbar} a\right) + L \cos\left(\frac{\Pi_y}{\hbar} a\right)$$

En présence du champ magnétique, Π_x et Π_y ne commutent plus

$$\begin{aligned} [\Pi_x, \Pi_y] &= -[p_x, eA_y] + [p_y, eA_x] \\ &= i\hbar e \left(\frac{\partial A_y}{\partial x} - \frac{\partial A_x}{\partial y} \right) \\ &= i\hbar e B \end{aligned}$$

On peut réécrire le hamiltonien en fonction de $\kappa_x = \frac{\Pi_x}{\hbar}a$ et $\kappa_y = \frac{\Pi_y}{\hbar}a$

$$H = K \cos \kappa_x + L \cos \kappa_y \quad (4.1)$$

avec la relation de commutation

$$[\kappa_x, \kappa_y] = i \frac{e}{\hbar} B a^2 = 2\pi i \alpha$$

La quantité sans dimension $\alpha = \frac{\phi}{\phi_0}$ représente simplement le rapport entre le flux magnétique à travers une maille du réseau $\phi = B a^2$ et le quantum de flux $\phi_0 = \frac{h}{e}$.

La relation de commutation entre κ_x et κ_y est formellement équivalente à la relation de commutation canonique $[\hat{q}, \hat{p}] = i\hbar = 2\pi i \alpha$ avec $\alpha = \frac{\hbar}{2\pi}$. On peut donc transposer (4.1) à un système à une dimension, avec un hamiltonien fonction des deux variables conjuguées \hat{q} et \hat{p} . On obtient ainsi le hamiltonien de Harper [50, 7, 8, 33, 40, 97]

$$H = K \cos \hat{q} + L \cos \hat{p} \quad (4.2)$$

La forme du spectre de (4.2) dépend de la rationalité de α . Pour $\alpha = \frac{r}{s}$, le spectre est composé de s bandes, mais pour α irrationnel, les valeurs propres forment un ensemble de Cantor. Si l'on trace la structure de bande en fonction de α , on obtient la figure bien connue du papillon de Hofstadter [52] (fig. 4.1).

La longueur de maille typique d'un réseau cristallin est de l'ordre de 0,2 nm. Comme $\alpha = \frac{eBa^2}{h}$, la réalisation expérimentale du papillon de Hofstadter requièrerait un champ de 10^5 T, ce qui est bien au-delà des limites techniques actuelles. Cependant, en augmentant la taille de la maille grâce à des super-réseaux artificiels, il est possible d'observer les effets de la commensurabilité sur la magnétoconductance [79].

4.1.2 Modèle de Harper pulsé

Classiquement, le hamiltonien de Harper est toujours intégrable

$$H = K \cos q + L \cos p$$

Afin d'introduire un peu de diversité et une once de chaos, on définit le modèle de Harper pulsé de manière analogue au rotateur pulsé

$$H = L \cos p + K \cos q \sum_{m=-\infty}^{\infty} \delta(t - m)$$

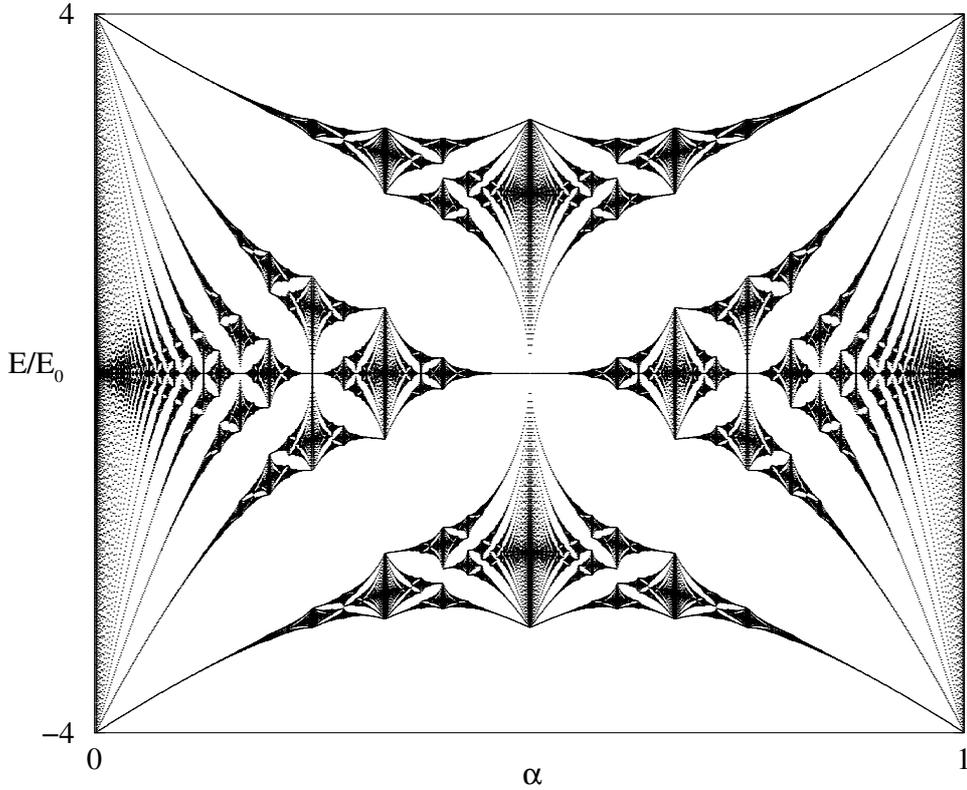


FIG. 4.1 – Papillon de Hofstadter pour un réseau symétrique en x et y , avec $K = L = 2E_0$ (figure obtenue par diagonalisation de (4.3) avec $K = L = 10^{-3}$).

En ne considérant l'état du système qu'aux temps t entiers, on obtient l'application correspondante

$$\begin{cases} \bar{p} = p + K \sin q \\ \bar{q} = q - L \sin \bar{p} \end{cases}$$

De même que pour le rotateur pulsé quantique, la quantification du modèle de Harper donne un opérateur d'évolution qui s'écrit comme le produit de deux opérateurs fonctions respectivement de \hat{q} et de \hat{p}

$$\hat{U} = \exp\left(-i\frac{L}{\hbar} \cos \hat{p}\right) \exp\left(-i\frac{K}{\hbar} \cos \hat{q}\right) \quad (4.3)$$

Un certain nombre de nouvelles propriétés peuvent être remarquées. Tout d'abord, pour des faibles valeurs de $K = L$, l'espace des phases est majoritairement intégrable, à l'exception d'une mince couche chaotique qui entoure les îlots principaux. Ce réseau stochastique ("stochastic web") traverse l'espace des phases de part en part, et est à l'origine de phénomènes de transport

particuliers. Ce type de réseau a été très étudié dans la littérature. Pour des valeurs plus fortes de K et L , on assiste à des transitions entre états localisés et états délocalisés selon les valeurs des paramètres [4, 5, 6, 14, 56, 61, 67, 76]. Cependant, contrairement au modèle avec transition d'Anderson étudié dans [74], les états propres ne possèdent pas tous le même seuil de délocalisation. Dès lors, on peut avoir pour certains régimes de paramètres des états “mixtes” qui sont des superpositions d'états localisés et d'états délocalisés. La délocalisation du système global se fait donc de manière très graduelle contrairement au modèle d'Anderson, et également au rotateur pulsé où il n'y a pas de transition. Dans la phase délocalisée, le système peut présenter une diffusion normale ou anormale suivant la valeur des paramètres. Les transitions entre ces types de diffusion ne sont pas encore complètement élucidées à l'heure actuelle.

4.2 Résultats sur le modèle de Harper pulsé

Comme nous venons de le voir, le modèle de Harper pulsé présente de nombreuses propriétés originales. Sa forme est représentative d'un grand nombre de modèles d'applications pulsées. Pour cette raison, il est possible de le simuler grâce à la même méthode que celle employée pour le rotateur pulsé quantique [43]. Cependant celle-ci est longue et coûteuse en qubits. Existe-t-il d'autres algorithmes plus économes, en acceptant éventuellement des solutions approchés ? Ici aussi se pose le problème de l'extraction d'informations à partir de la fonction d'onde finale : quelles quantités peut-on mesurer précisément, et avec quel gain par rapport à une simulation classique ? Enfin, le modèle d'erreur étudié ici diffère de celui du chapitre précédent ; on suppose maintenant la présence d'imperfections statiques internes. Les interactions entre qubits, qui sont nécessaires pour construire les portes à deux qubits, ne pourront vraisemblablement pas être éliminées totalement lorsque celles-ci ne sont plus désirées. Ces imperfections statiques ne résultent pas d'une interaction avec l'extérieur, mais simplement d'un couplage résiduel entre les qubits de l'ordinateur quantique. Leurs effets peuvent être importants, et de nature différente de ceux provoqués par les erreurs dynamiques.

Ce type d'imperfection a déjà été étudié par Georgeot et Shepelyansky [42, 41]. Au-dessus d'un certain seuil critique de couplage interqubits, le chaos quantique apparaît, conduisant à l'ergodicité des états propres de l'ordinateur. Dans ce régime, les qubits ne sont plus indépendants et l'opérabilité de l'ordinateur est fortement compromise. Cependant, le seuil de chaos décroît seulement linéairement avec le nombre de qubits, ce qui ménage une plage de paramètres relativement large dans laquelle le bon fonctionnement est possible. Dans cette étude, il s'agissait toutefois d'un ordinateur au repos, ne faisant pas tourner d'algorithme. Il est intéressant de connaître

l'effet des erreurs sur un ordinateur en fonctionnement typique, d'autant plus que le modèle simulé ici possède un comportement très riche. De plus, des résultats précédents sur d'autres modèles suggèrent que ce type d'imperfection statique a des conséquences plus graves qu'un bruit unitaire dans les portes quantiques.

On suppose que les portes quantiques sont appliquées instantanément, mais qu'entre deux portes successives le système évolue pendant τ_g suivant l'hamiltonien

$$H_e = \sum_{i=0}^{n_q-1} (\Delta_0 + \delta_i) Z_i + \sum_{i=0}^{n_q-1} J_i X_i X_{i+1}$$

où la deuxième somme porte sur toutes les paires de qubits voisins sur une chaîne circulaire. La différence d'énergie entre les deux états d'un qubit est égale à la valeur moyenne Δ_0 , à laquelle s'ajoute une quantité aléatoire δ_i , comprise entre $-\frac{\delta}{2}$ et $\frac{\delta}{2}$. De même, les couplages J_i (répartis aléatoirement et uniformément dans l'intervalle $[-\frac{J}{2}, \frac{J}{2}]$) représentent l'interaction statique résiduelle entre les qubits. Contrairement aux erreurs dynamiques, les imperfections statiques sont supposées être caractéristiques de l'ordinateur quantique considéré, donc le jeu de δ_i et J_i ne varie pas au cours du calcul. Ce modèle d'erreur est la version la plus simple de l'hamiltonien d'Heisenberg qui permette d'obtenir des effets non triviaux.

Comme Δ_0 est constant et identique pour tous les qubits, son effet est simple et peut être compensé facilement. L'hamiltonien effectif utilisé pour simuler les erreurs est alors

$$H_e = \sum_{i=0}^{n_q-1} \delta_i Z_i + \sum_{i=0}^{n_q-1} J_i X_i X_{i+1}$$

De plus, on choisit $\delta = J$; l'amplitude des erreurs est alors gouvernée par le paramètre $\varepsilon = \delta\tau_g = J\tau_g$.

Dans la publication II ci-après [63], trois algorithmes quantiques différents sont présentés et analysés, permettant de simuler efficacement l'opérateur d'évolution du modèle de Harper pulsé avec des précisions et des besoins en ressources différents. En plus de la méthode exacte déjà mentionnée dans le cas du rotateur pulsé quantique, nous avons aussi exploré une autre approche où la dynamique n'est simulée qu'approximativement, mais où aucun qubit supplémentaire n'est requis. Deux méthodes de ce type ont été étudiées, l'une mettant en jeu un découpage en temps de l'opérateur d'évolution, l'autre l'approximant avec des polynômes.

Selon les paramètres choisis, le système est presque intégrable, localisé, ou partiellement délocalisé. Dans chaque cas, nous identifions les quantités

concernant le transport ou le spectre qui peuvent être obtenues plus efficacement sur un ordinateur quantique que sur un ordinateur classique. Dans la plupart des cas, un gain polynomial est obtenu, quadratique ou moins suivant le régime considéré.

Nous présentons également les effets des imperfections statiques sur les quantités choisies, et montrons que selon le jeu de paramètres des comportements très différents sont observés. Quelques quantités, comme la distribution de Husimi, la longueur de localisation ou le spectre, peuvent être obtenues de manière fiable avec des niveaux modérés d'imperfections, tandis que d'autres sont exponentiellement sensibles à leur amplitude. En particulier, le seuil d'imperfection pour la délocalisation devient exponentiellement faible dans le régime partiellement délocalisé. Ceci signifie que contrairement à l'étude [74] sur la transition d'Anderson, le point de transition calculé en présence d'imperfections se déplace exponentiellement vite lorsque l'on augmente l'amplitude des erreurs. Nos résultats montrent qu'un comportement intéressant peut être observé avec seulement 7 ou 8 qubits, et peut être mesuré de manière fiable en présence d'un taux modéré d'imperfections internes.

4.3 Publication II

Quantum computation of a complex system : The kicked Harper model

B. Lévi and B. Georgeot

Phys. Rev. E. **70**, 056218 (2004)

quant-ph/0409028

Chapitre 5

Conclusion

Cette étude montre qu'une dynamique complexe peut être simulée de manière fiable et efficace sur un ordinateur quantique réaliste. Des algorithmes quantiques ont été présentés pour simuler des modèles importants du chaos quantique, ayant des applications en physique atomique et physique du solide, le rotateur pulsé quantique et le modèle de Harper pulsé. Les méthodes employées se généralisent à toute une classe de modèles, les applications pulsées. Les effets de petites erreurs unitaires ou d'imperfections statiques sur ces modèles ont été caractérisés. Il a été ainsi mis en évidence que certaines quantités physiques sont robustes face à des imperfections modérées, alors que d'autres y sont très sensibles. Le comportement de ces quantités en présence d'erreur dépend également du jeu de paramètres considéré. De même, selon le régime des quantités physiques peuvent être extraites efficacement, avec un gain au moins polynomial par rapport à une simulation sur un ordinateur classique.

La plupart des algorithmes présentés ici sont très économes, applicables avec un petit nombre de qubits, et demandant un nombre de portes qui varie polynomialement avec la taille du registre. Ils sont donc bien adaptés pour une implémentation expérimentale dans les prochaines années. La résonance magnétique nucléaire permet déjà de manipuler quelques qubits, ce qui a permis de réaliser par exemple l'application du boulanger quantique [94]. Un sujet non abordé dans cette thèse est d'augmenter la protection de la fonction d'onde par des codes correcteurs d'erreur [71, 84, 88]. Cependant, même s'ils sont asymptotiquement assez efficaces les codes correcteurs quantiques usuels sont très gourmands en nombre de qubits. On peut toutefois minimiser les effets cohérents des erreurs statiques en utilisant la méthode Pauli-Random-Error-Correction, récemment introduite dans [55]. L'avantage de cette procédure est qu'elle ne demande pas de qubit supplémentaire pour fonctionner. Enfin, un travail a été commencé pour établir les expressions analytiques des lois de variation de quelques quantités dans le régime chao-

tique. En effet, dans ce régime l'ergodicité permet d'appliquer la théorie des matrices aléatoires et d'obtenir ces quantités comme des moyennes sur des ensembles particuliers de matrices [38].

Le calcul quantique est un domaine récent en plein développement, et d'autres études seront nécessaires pour connaître précisément son champ d'application et son efficacité.

Annexe A

Fonctions de Wigner et Husimi

Pour une particule quantique, le principe d'incertitude d'Heisenberg interdit l'existence d'une véritable distribution de probabilité dans l'espace des phases. On ne peut en effet pas définir la probabilité qu'une particule ait une position q et une quantité de mouvement p puisque ces deux quantités ne peuvent pas avoir simultanément des valeurs bien définies. Néanmoins, il est possible de concevoir différentes distributions de pseudo-probabilité qui possèdent des propriétés proches de celles d'une distribution de probabilité classique [51, 62, 91, 96]. Bien entendu, aucune de ces distributions ne les possède toutes, mais le physicien avisé pourra toujours choisir à son gré celle qui lui semble la plus appropriée selon ses contraintes. Ces distributions se montrent particulièrement utiles lorsqu'il s'agit de mener à bien des calculs semi-classique, par exemple lorsqu'un système quantique interagit avec un autre système décrit classiquement. Ceci leur ouvre des champs d'application assez divers, tels que la mécanique statistique des systèmes quantiques hors d'équilibre, ou l'optique quantique. Elles peuvent être également plus facilement comparées qu'une fonction d'onde à la distribution de probabilité classique dans l'espace des phases.

A.1 Fonction de distribution générale

Considérons une particule quantique décrite par une matrice densité $\hat{\rho}$, et l'on s'intéresse à la valeur moyenne d'une observable représentée par un opérateur fonction de la position et de la quantité de mouvement $\hat{O}(\hat{q}, \hat{p})$

$$\langle \hat{O} \rangle = \text{Tr} \{ \hat{\rho} \hat{O} \}$$

Par analogie avec la mécanique classique, on cherche à exprimer cette valeur moyenne comme une moyenne sur tout l'espace des phases d'une certaine

forme scalaire $O(q, p)$ de l'opérateur \hat{O} multipliée par une pseudo-probabilité de présence $P(q, p)$ de la particule en ce point

$$\langle \hat{O}(\hat{q}, \hat{p}) \rangle = \iint dq dp O(q, p) P(q, p) \quad (\text{A.1})$$

Pour donner un sens à cette expression, il faut bien sûr préciser comment obtenir O et P en fonction de \hat{O} et \hat{p} respectivement. L'approche naïve qui consiste à remplacer directement \hat{q} et \hat{p} par q et p dans l'expression de $\hat{O}(\hat{q}, \hat{p})$ conduit malheureusement à une impasse. Prenons par exemple deux fonctions f_1 et f_2

$$\begin{aligned} f_1(\hat{q}, \hat{p}) &= \hat{p}\hat{q}^2\hat{p} \\ f_2(\hat{q}, \hat{p}) &= \frac{1}{2}(\hat{p}^2\hat{q}^2 + \hat{q}^2\hat{p}^2) + \hbar^2 \end{aligned}$$

On a bien $f_1(\hat{q}, \hat{p}) = f_2(\hat{q}, \hat{p})$, mais $f_1(q, p) \neq f_2(q, p)$. Deux opérateurs identiques peuvent donc conduire par ce procédé à des fonctions scalaires différentes, et réciproquement, deux opérateurs différents peuvent correspondre à la même fonction scalaire.

Il faut donc définir une règle de correspondance qui associe de manière univoque une fonction $A(q, p)$ et un opérateur $\hat{O}(\hat{q}, \hat{p})$. Pour ce faire, on commence par développer $O(q, p)$ en une intégrale de Fourier

$$O(q, p) = \iint d\xi d\eta \omega(\xi, \eta) e^{i(\xi q + \eta p)} \quad (\text{A.2})$$

Le problème se réduit alors à choisir l'opérateur qui correspond à la fonction particulière $e^{i(\xi q + \eta p)}$. Cela revient à choisir la façon dont on doit ordonner q et p dans le développement de Taylor de $e^{i(\xi q + \eta p)}$ avant de les remplacer par \hat{q} et \hat{p} . Par exemple, un premier choix peut être de placer tous les q à gauche et les p à droite

$$e^{i(\xi q + \eta p)} \longleftrightarrow e^{i\xi\hat{q}} e^{i\eta\hat{p}}$$

C'est l'ordre standard. L'ordre anti-standard (qui conduit à la distribution de Kirkwood) consiste à faire exactement l'inverse, c'est-à-dire placer tous les p avant les q

$$e^{i(\xi q + \eta p)} \longleftrightarrow e^{i\eta\hat{p}} e^{i\xi\hat{q}}$$

Un cas particulièrement important est l'ordre de Weyl, qui sera développé plus loin

$$e^{i(\xi q + \eta p)} \longleftrightarrow e^{i(\xi\hat{q} + \eta\hat{p})}$$

Dans la suite, on se restreindra à une relation de correspondance de la forme

$$e^{i(\xi q + \eta p)} \longleftrightarrow e^{i(\xi\hat{q} + \eta\hat{p})} f(\xi, \eta)$$

Cette forme simple englobe des cas assez variés : l'ordre de Weyl bien sûr, mais également les ordres standards et anti-standard, ainsi que les ordres normal et anti-normal qui seront définis plus tard. Avec cette relation de correspondance, l'opérateur \hat{O} s'exprime comme

$$\hat{O}(\hat{q}, \hat{p}) = \iint d\xi d\eta \omega(\xi, \eta) e^{i(\xi\hat{q} + \eta\hat{p})} f(\xi, \eta) \quad (\text{A.3})$$

On est alors en mesure de définir la fonction de distribution $P_f(q, p)$ par

$$\text{Tr} \left\{ \hat{\rho}(\hat{q}, \hat{p}) e^{i(\xi\hat{q} + \eta\hat{p})} f(\xi, \eta) \right\} = \iint dq dp e^{i(\xi q + \eta p)} P_f(q, p) \quad (\text{A.4})$$

ou

$$P_f(q, p) = \frac{1}{4\pi^2} \iint d\xi d\eta \text{Tr} \left\{ \hat{\rho}(\hat{q}, \hat{p}) e^{i(\xi\hat{q} + \eta\hat{p})} f(\xi, \eta) \right\} e^{-i(\xi q + \eta p)} \quad (\text{A.5})$$

Comme f ne dépend pas de $\hat{\rho}$, cette fonction de distribution a l'avantage d'être bilinéaire en la fonction d'onde. On peut en effet concevoir d'autres définitions qui ne possèdent pas cette propriété, comme par exemple $|\psi(q)|^2 |\psi(p)|^2$. En appliquant (A.2) et (A.3) sur les membres de droite et de gauche de (A.4), on obtient ainsi une expression analogue à celle souhaitée pour calculer la valeur moyenne (A.1)

$$\text{Tr} \left\{ \hat{\rho} \hat{O} \right\} = \iint dq dp O(q, p) P_f(q, p)$$

avec \hat{O} et O liés par la relation de correspondance énoncée plus haut.

Enfin, il est souvent pratique d'écrire la distribution P_f comme la valeur moyenne d'un opérateur $\hat{A}_f(q, p)$, connu sous le nom d'opérateur point de l'espace des phases (phase space point operator), ou opérateur de Fano.

$$P_f(q, p) = \text{Tr} \left\{ \hat{\rho} \hat{A}_f(q, p) \right\} \quad (\text{A.6})$$

D'après (A.5), \hat{A}_f est donné par la formule générale

$$\hat{A}_f(q, p) = \frac{1}{4\pi^2} \iint d\xi d\eta e^{i(\xi\hat{q} + \eta\hat{p})} f(\xi, \eta) e^{-i(\xi q + \eta p)} \quad (\text{A.7})$$

A.2 Distribution de Wigner

Dans le cas de la distribution de Wigner, on choisit l'ordre de Weyl

$$e^{i(\xi q + \eta p)} \longleftrightarrow e^{i(\xi\hat{q} + \eta\hat{p})}$$

ou, de manière équivalente, on choisit la fonction f particulière $f_W(\xi, \eta) = 1$. D'après le théorème de Baker-Hausdorff, si deux opérateurs \hat{A} et \hat{B} commutent avec leur commutateur $[\hat{A}, \hat{B}]$, alors

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}}e^{\hat{B}}e^{-\frac{1}{2}[\hat{A}, \hat{B}]}$$

Comme $[\hat{q}, \hat{p}] = i\hbar$, on peut réécrire $\exp(i(\xi\hat{q} + \eta\hat{p}))$ sous la forme

$$e^{i(\xi\hat{q}+\eta\hat{p})} = e^{i\frac{\eta}{2}\hat{p}}e^{i\xi\hat{q}}e^{i\frac{\eta}{2}\hat{p}} \quad (\text{A.8})$$

De plus, on a

$$e^{i\eta\hat{p}}|q\rangle = |q - \eta\hbar\rangle \quad (\text{A.9})$$

Grâce à ces deux identités, on a

$$\begin{aligned} \text{Tr} \left\{ \hat{\rho} e^{i(\xi\hat{q}+\eta\hat{p})} \right\} &= \iint dq dq' \langle q | \hat{\rho} | q' \rangle \langle q' | e^{i(\xi\hat{q}+\eta\hat{p})} | q \rangle \\ &= \iint dq dq' \langle q | \hat{\rho} | q' \rangle \left\langle q' + \frac{\eta}{2}\hbar \left| q - \frac{\eta}{2}\hbar \right. \right\rangle e^{i\xi(q - \frac{\eta}{2}\hbar)} \\ &= \int dq' \left\langle q' + \frac{\eta}{2}\hbar \left| \hat{\rho} \left| q' - \frac{\eta}{2}\hbar \right. \right. \right\rangle e^{i\xi q'} \end{aligned}$$

D'après (A.5), la distribution de Wigner a donc pour expression

$$\begin{aligned} P_W(q, p) &= \frac{1}{4\pi^2} \iint d\xi d\eta \text{Tr} \left\{ \hat{\rho} e^{i(\xi\hat{q}+\eta\hat{p})} \right\} e^{-i(\xi q + \eta p)} \\ &= \frac{1}{4\pi^2} \iiint d\xi d\eta dq' \left\langle q' + \frac{\eta}{2}\hbar \left| \hat{\rho} \left| q' - \frac{\eta}{2}\hbar \right. \right. \right\rangle e^{i\xi(q' - q)} e^{-i\eta p} \end{aligned}$$

Soit

$$P_W(q, p) = \frac{1}{2\pi} \int d\eta \left\langle q + \frac{\eta}{2}\hbar \left| \hat{\rho} \left| q - \frac{\eta}{2}\hbar \right. \right. \right\rangle e^{-i\eta p} \quad (\text{A.10})$$

On peut remarquer que $P_W^*(q, p) = P_W(q, p)$, donc la distribution de Wigner est réelle. Par contre, elle peut prendre des valeurs négatives, comme on le verra plus tard. Dans le cas d'un état pur, c'est-à-dire lorsque $\hat{\rho} = |\psi\rangle\langle\psi|$, on a

$$P_W(q, p) = \frac{1}{2\pi} \int d\eta e^{-i\eta p} \psi^* \left(q - \frac{\eta}{2}\hbar \right) \psi \left(q + \frac{\eta}{2}\hbar \right)$$

En utilisant l'inégalité de Cauchy-Schwarz, on voit que

$$\begin{aligned} |P_W(q, p)| &= \frac{1}{\pi\hbar} \left| \int dx e^{-2i\frac{px}{\hbar}} \psi^*(q-x) \psi(q+x) \right| \\ &\leq \frac{1}{\pi\hbar} \left\| e^{-2i\frac{px}{\hbar}} \psi^*(q-x) \right\| \|\psi(q+x)\| \end{aligned}$$

Soit, pour un état pur

$$|P_W(q, p)| \leq \frac{1}{\pi\hbar}$$

Cette inégalité est aussi valable dans le cas d'un état mixte, puisqu'il suffit d'appliquer le même raisonnement à

$$\hat{\rho} = \sum_i p_i |\psi_i\rangle \langle \psi_i| \quad \text{avec } 0 \leq p_i \leq 1 \text{ et } \sum_i p_i = 1$$

On va maintenant établir certaines propriétés particulièrement utiles de l'opérateur point de l'espace des phases correspondant à la distribution de Wigner. D'après (A.7)

$$\hat{A}_W(q, p) = \frac{1}{4\pi^2} \iint d\xi d\eta e^{i(\xi\hat{q} + \eta\hat{p})} e^{-i(\xi q + \eta p)}$$

En utilisant (A.8) et (A.9), on montre que

$$\begin{aligned} & \text{Tr} \left\{ \hat{A}_W(q, p) \hat{A}_W(q', p') \right\} \\ &= \frac{1}{(2\pi)^4} \iiint d\xi d\xi' d\eta d\eta' dq'' e^{-i(\xi q + \eta p)} e^{-i(\xi' q' + \eta' p')} \\ & \quad \times \left\langle q'' \left| e^{i\frac{\xi}{2}\hat{q}} e^{i\eta\hat{p}} e^{i\frac{\xi'}{2}\hat{q}} e^{i\eta'\hat{p}} e^{i\frac{\xi'}{2}\hat{q}} \right| q'' \right\rangle \\ &= \frac{1}{(2\pi)^4} \iiint d\xi d\xi' d\eta d\eta' dq'' e^{-i(\xi q + \eta p)} e^{-i(\xi' q' + \eta' p')} \\ & \quad \times e^{i\frac{\xi}{2}q''} e^{i\frac{\xi+\xi'}{2}(q'' - \eta'\hbar)} e^{i\frac{\xi'}{2}q''} \delta[(\eta + \eta')\hbar] \\ &= \frac{1}{(2\pi)^4 \hbar} \iiint d\xi d\xi' d\eta dq'' e^{-i(\xi q + \eta p)} e^{-i(\xi' q' - \eta p')} e^{i(\xi + \xi')q''} e^{i\frac{\xi+\xi'}{2}\eta\hbar} \\ &= \frac{1}{2\pi\hbar(2\pi)^2} \iiint d\xi d\xi' d\eta e^{-i(\xi q + \eta p)} e^{-i(\xi' q' - \eta p')} e^{i\frac{\xi+\xi'}{2}\eta\hbar} \delta(\xi + \xi') \\ &= \frac{1}{2\pi\hbar(2\pi)^2} \iint d\xi d\eta e^{-i\xi(q-q')} e^{-i\eta(p-p')} \end{aligned}$$

D'où la relation

$$\text{Tr} \left\{ \hat{A}_W(q, p) \hat{A}_W(q', p') \right\} = \frac{1}{2\pi\hbar} \delta(q - q') \delta(p - p') \quad (\text{A.11})$$

Les $\hat{A}_W(q, p)$ sont donc un ensemble d'opérateurs orthogonaux. D'autre part, on peut montrer qu'ils forment également une base complète, c'est-à-dire que tout opérateur hermitien peut s'écrire comme une combinaison linéaire des \hat{A}_W .

$$\hat{O} = 2\pi\hbar \int dq dp \text{Tr} \left\{ \hat{O} \hat{A}_W(q, p) \right\} \hat{A}_W(q, p)$$

Dans le cas particulier de l'opérateur densité, les coefficients sont tout simplement les valeurs de la fonction de Wigner en chaque point

$$\hat{\rho} = 2\pi\hbar \int dq dp P_W(q, p) \hat{A}_W(q, p)$$

Dans la base des positions, les A_W ont pour expression

$$\begin{aligned}
\langle q' | \hat{A}_W(q, p) | q'' \rangle &= \frac{1}{4\pi^2} \iint d\xi d\eta \langle q' | e^{i\frac{\eta}{2}\hat{p}} e^{i\xi\hat{q}} e^{i\frac{\eta}{2}\hat{p}} | q'' \rangle e^{-i(\xi q + \eta p)} \\
&= \frac{1}{4\pi^2} \iint d\xi d\eta \delta(q' - q'' + \eta\hbar) e^{i\xi(q'' - \frac{\eta}{2}\hbar)} e^{-i(\xi q + \eta p)} \\
&= \frac{1}{4\pi^2\hbar} \int d\xi e^{i\xi\left(\frac{q'+q''}{2} - q\right)} e^{i\frac{p}{\hbar}(q' - q'')} \\
&= \frac{1}{2\pi\hbar} \delta\left(q - \frac{q' + q''}{2}\right) e^{i\frac{p}{\hbar}(q' - q'')} \tag{A.12}
\end{aligned}$$

De même, dans la base des impulsions

$$\langle p' | \hat{A}_W(q, p) | p'' \rangle = \frac{1}{2\pi\hbar} \delta\left(p - \frac{p' + p''}{2}\right) e^{-i\frac{q}{\hbar}(p' - p'')}$$

On peut exprimer $A_W(q, p)$ d'une autre manière assez élégante en introduisant l'opérateur de translation continue

$$\hat{D}(q, p) = e^{-\frac{i}{\hbar}(q\hat{p} - p\hat{q})} \tag{A.13}$$

et l'opérateur de réflexion dans l'espace des $|q\rangle$

$$\hat{R}|q\rangle = |-q\rangle$$

On a

$$\begin{aligned}
\langle q' | \hat{D}(q, p) \hat{R} \hat{D}^\dagger(q, p) | q'' \rangle &= \langle q' | e^{\frac{i}{\hbar}p\hat{q}} e^{-\frac{i}{\hbar}q\hat{p}} \hat{R} e^{\frac{i}{\hbar}q\hat{p}} e^{-\frac{i}{\hbar}p\hat{q}} | q'' \rangle \\
&= e^{\frac{i}{\hbar}p(q' - q'')} \langle q' - q | \hat{R} | q'' - q \rangle \\
&= \frac{1}{2} e^{\frac{i}{\hbar}p(q' - q'')} \delta\left(q - \frac{q' + q''}{2}\right)
\end{aligned}$$

En comparant cette dernière expression avec (A.12), on constate que

$$\hat{A}(q, p) = \frac{1}{\pi\hbar} \hat{D}(q, p) \hat{R} \hat{D}^\dagger(q, p) \tag{A.14}$$

La distribution de Wigner peut être vue comme la valeur moyenne d'un opérateur de réflexion translaté.

La fonction de Wigner peut être comparée à une fonction de distribution classique. C'est une fonction réelle, qui vérifie

$$\iint dq dp P_W(q, p) = \text{Tr} \{ \hat{\rho} \hat{I} \} = 1$$

De plus,

$$\int dq \hat{A}_W(q, p) = \frac{1}{2\pi} \int d\eta e^{i\eta(\hat{p} - p)} = |p\rangle\langle p|$$

et

$$\int dp \hat{A}_W(q, p) = |q\rangle\langle q|$$

donc la distribution de Wigner donne des probabilités marginales correctes

$$\begin{aligned} \int dp P_W(q, p) &= \langle q | \hat{\rho} | q \rangle \\ \int dq P_W(q, p) &= \langle p | \hat{\rho} | p \rangle \end{aligned}$$

On peut même montrer que

$$\int dq dp \delta(a_1 q + a_2 p - a_3) P_W(q, p) = \langle a_3 | \hat{\rho} | a_3 \rangle$$

où $|a_3\rangle$ est le vecteur propre de l'opérateur $a_1 \hat{q} + a_2 \hat{p}$ avec la valeur propre a_3 . Dit autrement, l'intégrale de la fonction de Wigner selon une ligne quelconque de l'espace des phases, définie par $a_1 q + a_2 p = a_3$, est égale à la densité de probabilité qu'une mesure de l'observable $a_1 \hat{q} + a_2 \hat{p}$ donne le résultat a_3 .

Le produit scalaire entre deux états $\hat{\rho}_1$ et $\hat{\rho}_2$ peut être calculé grâce à leurs distributions de Wigner

$$\text{Tr} \{ \hat{\rho}_1 \hat{\rho}_2 \} = 2\pi\hbar \iint dq dp P_{W1}(q, p) P_{W2}(q, p) \quad (\text{A.15})$$

On peut remarquer que si $\hat{\rho}_1$ et $\hat{\rho}_2$ sont orthogonaux, alors

$$\iint dq dp P_{W1}(q, p) P_{W2}(q, p) = 0$$

Pour que cette égalité soit vérifiée, les distributions de Wigner doivent pouvoir prendre des valeurs négatives, ce qui les distingue de vraies distributions de probabilité classique. Les seuls états dont la fonction de Wigner est partout positive sont les états cohérents, avec une distribution gaussienne. Cependant, même si le système est initialement dans un état cohérent, son évolution ultérieure va invariablement conduire à un autre type d'état si le hamiltonien n'est pas quadratique. Plus généralement, on peut montrer qu'il n'existe pas de fonction de distribution bilinéaire partout positive qui donne des probabilités marginales correctes. A condition d'accepter de perdre certaines propriétés incompatibles, on peut néanmoins construire une fonction partout positive : la distribution de Husimi, qui fait l'objet de la section suivante.

A.3 Distribution de Husimi

Supposons pour commencer que le système est un oscillateur harmonique de masse m et de fréquence ω . Les ordres normal et anti-normal sont alors

définis à l'aide des opérateurs annihilation et création

$$\begin{aligned}\hat{a} &= \frac{1}{\sqrt{2\hbar m\omega}} (m\omega\hat{q} + i\hat{p}) \\ \hat{a}^\dagger &= \frac{1}{\sqrt{2\hbar m\omega}} (m\omega\hat{q} - i\hat{p})\end{aligned}$$

Si on réécrit l'opérateur $\hat{A}(\hat{q}, \hat{p})$ en fonction de \hat{a} et \hat{a}^\dagger , l'ordre normal consiste à placer tous les \hat{a}^\dagger à gauche et les \hat{a} à droite. Dans le formalisme précédent, cela revient à prendre comme relation de correspondance

$$e^{i(\xi q + \eta p)} \longleftrightarrow e^{z\hat{a}^\dagger} e^{-z^*\hat{a}}$$

avec

$$z = i\xi\sqrt{\frac{\hbar}{2m\omega}} - \eta\sqrt{\frac{\hbar m\omega}{2}} \quad (\text{A.16})$$

ou bien encore choisir comme fonction f

$$f_N(\xi, \eta) = e^{\hbar\xi^2/(4m\omega) + \hbar m\omega\eta^2/4} = e^{\frac{|z|^2}{2}} \quad (\text{A.17})$$

L'ordre anti-normal, quant à lui, consiste à placer les \hat{a} avant les \hat{a}^\dagger , soit la règle de correspondance

$$e^{i(\xi q + \eta p)} \longleftrightarrow e^{-z^*\hat{a}} e^{z\hat{a}^\dagger}$$

ou la fonction

$$f_{AN}(\xi, \eta) = e^{-\hbar\xi^2/(4m\omega) - \hbar m\omega\eta^2/4} = e^{-\frac{|z|^2}{2}} \quad (\text{A.18})$$

Tout ceci peut s'appliquer également à la description d'un champ électromagnétique, puisqu'il est mathématiquement équivalent à un oscillateur harmonique de masse $m = 1$. Les distributions issues des ordres normal et anti-normal sont de ce fait très utilisées en optique quantique, respectivement sous le nom de fonction P et fonction Q . L'état du champ électromagnétique y est représenté dans un pseudo-espace des phases, où la position q et la quantité de mouvement p sont remplacées par les deux quadratures du champ.

Si le système considéré n'est pas un oscillateur harmonique ni un champ électromagnétique, il reste possible de définir les deux opérateurs \hat{a} et \hat{a}^\dagger en choisissant arbitrairement le paramètre $m\omega$. On peut ainsi généraliser les ordres normal et anti-normal à n'importe quel système. La distribution de Husimi est construite à partir de cet ordre anti-normal généralisé, et dépend donc d'un paramètre libre dont le rôle sera éclairci par la suite.

En insérant dans l'équation (A.5) le choix de l'ordre anti-normal

$$e^{i(\xi\hat{q}+\eta\hat{p})} f_{AN}(\xi, \eta) = e^{-z^* \hat{a}} e^{z \hat{a}^\dagger}$$

on obtient l'expression dans l'espace des phases (q, p) de la distribution de Husimi

$$P_H(q, p) = \frac{1}{4\pi^2} \iint d\xi d\eta \operatorname{Tr} \left\{ \hat{\rho} e^{-z^* \hat{a}} e^{z \hat{a}^\dagger} \right\} e^{-i(\xi q + \eta p)} \quad (\text{A.19})$$

Cependant, dans ce cas précis il est plus naturel d'exprimer la distribution de Husimi dans l'espace complexe α , l'espace des phases des états cohérents. Un état cohérent $|\alpha\rangle$ est défini par

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

où les $|n\rangle$ sont les vecteurs propres de l'opérateur $\hat{N} = \hat{a}^\dagger \hat{a}$ et α est complexe. Les états cohérents sont les vecteurs propres de l'opérateur annihilation : $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. Ils ne sont pas orthogonaux, mais forment néanmoins une base complète. En effet, en adoptant la convention $d^2\alpha = d(\operatorname{Re} \alpha) d(\operatorname{Im} \alpha)$, et en posant $\alpha = r e^{i\theta}$ tel que $d^2\alpha = r dr d\theta$

$$\begin{aligned} \int d^2\alpha |\alpha\rangle \langle\alpha| &= \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} \frac{|m\rangle \langle n|}{\sqrt{m!n!}} \int_0^\infty dr e^{-r^2} r^{m+n+1} \int_0^{2\pi} d\theta e^{i(m-n)\theta} \\ &= 2\pi \sum_{n=0}^{\infty} \frac{|n\rangle \langle n|}{n!} \underbrace{\int_0^\infty dr e^{-r^2} r^{2n+1}}_{\frac{n!}{2}} = \pi \hat{I} \end{aligned}$$

D'où on peut développer l'opérateur identité sur la base des $|\alpha\rangle$

$$\hat{I} = \frac{1}{\pi} \int d^2\alpha |\alpha\rangle \langle\alpha| \quad (\text{A.20})$$

Pour exprimer P_H dans l'espace des α , on effectue le changement de variable

$$\alpha = \frac{1}{\sqrt{2\hbar m\omega}} (m\omega q + ip) \quad (\text{A.21})$$

Comme $d^2\alpha = \frac{1}{2\hbar} dq dp$ et, par normalisation

$$\iint dq dp P_H(q, p) = \iint d^2\alpha P_H(\alpha) = \operatorname{Tr}(\hat{\rho}) = 1$$

on a $P_H(\alpha) = 2\hbar P_H(q, p)$.

En utilisant (A.21) et (A.16), on peut alors réécrire (A.19), en remarquant que $d^2z = \frac{\hbar}{2} d\xi d\eta$

$$P_H(\alpha) = \frac{1}{\pi^2} \iint d^2z \operatorname{Tr} \left\{ \hat{\rho} e^{-z^* \hat{a}} e^{z \hat{a}^\dagger} \right\} e^{z^* \alpha - z \alpha^*}$$

Soit

$$\operatorname{Tr} \left\{ \hat{\rho} e^{-z^* \hat{a}} e^{z \hat{a}^\dagger} \right\} = \iint d^2\alpha e^{z \alpha^* - z^* \alpha} P_H(\alpha)$$

Par ailleurs, en insérant (A.20) dans le membre de gauche de cette équation on obtient

$$\operatorname{Tr} \left\{ \hat{\rho} e^{-z^* \hat{a}} \hat{I} e^{z \hat{a}^\dagger} \right\} = \frac{1}{\pi} \iint d^2\alpha e^{z \alpha^* - z^* \alpha} \langle \alpha | \hat{\rho} | \alpha \rangle$$

En comparant ces deux dernière équation, on en déduit

$$P_H(\alpha) = \frac{1}{\pi} \langle \alpha | \hat{\rho} | \alpha \rangle$$

Pour un état mixte quelconque

$$\hat{\rho} = \sum_i p_i |\psi_i\rangle \langle \psi_i| \text{ avec } 0 \leq p_i \leq 1$$

On a

$$P_H(\alpha) = \frac{1}{\pi} \sum_i p_i |\langle \alpha | \psi \rangle|^2$$

On en tire l'inégalité suivante

$$0 \leq P_H(\alpha) \leq \frac{1}{\pi}$$

En passant dans l'espace des phases standard (q, p) , P_H a pour expression

$$P_H(q, p) = \frac{1}{2\pi\hbar} \langle \alpha_{q,p} | \hat{\rho} | \alpha_{q,p} \rangle \quad (\text{A.22})$$

avec

$$0 \leq P_H(q, p) \leq \frac{1}{2\pi\hbar}$$

Ici, $|\alpha_{q,p}\rangle$ désigne l'état cohérent centré en q et en p , soit l'état $|\alpha\rangle$ avec $\alpha = \frac{1}{\sqrt{2\hbar m\omega}}(m\omega q + ip)$. Dans la représentation des positions, $|\alpha_{q,p}\rangle$ a pour expression

$$\langle x | \alpha_{q,p} \rangle = \alpha_{q,p}(x) = \left(\frac{m\omega}{\pi\hbar} \right)^{\frac{1}{4}} e^{-\frac{m\omega}{2\hbar}(x-q)^2} e^{i\frac{px}{\hbar}}$$

D'où, pour un état pur $\hat{\rho} = |\psi\rangle \langle \psi|$

$$P_H(q, p) = \frac{1}{2\pi\hbar} \left| \int dx \alpha_{q,p}^*(x) \psi(x) \right|^2$$

On peut constater que la distribution de Husimi est réelle (comme la distribution de Wigner), mais surtout partout positive. Cela lui permet d'être plus facilement comparée à une distribution de probabilité classique. Néanmoins, elle n'en partage pas toutes les propriétés ; par exemple, les probabilités marginales, qui étaient exactes dans le cas de la fonction de Wigner, ne le sont plus.

Dans le cas de la distribution de Husimi, l'opérateur point de l'espace des phases prend une expression très simple. D'après (A.22)

$$P_H(q, p) = \text{Tr} \left\{ \hat{\rho} \frac{1}{2\pi\hbar} |\alpha_{q,p}\rangle \langle \alpha_{q,p}| \right\}$$

Ce qui donne l'opérateur

$$\hat{A}_H(q, p) = \frac{1}{2\pi\hbar} |\alpha_{q,p}\rangle \langle \alpha_{q,p}|$$

Par contre, contrairement au cas de la distribution de Wigner, ces opérateurs ne sont pas orthogonaux entre eux

$$\begin{aligned} \text{Tr} \left\{ \hat{A}_H(q, p) \hat{A}_H(q', p') \right\} &= \frac{1}{(2\pi\hbar)^2} |\langle \alpha_{q,p} | \alpha_{q',p'} \rangle|^2 \\ &= \frac{1}{(2\pi\hbar)^2} e^{-|\alpha_{q,p} - \alpha_{q',p'}|^2} \end{aligned}$$

A.4 Relation entre les distributions de Wigner et de Husimi

La distribution de Husimi peut également être construite à partir de la distribution de Wigner en lissant celle-ci par une gaussienne. En effet, si l'on revient à la définition (A.5)

$$\begin{aligned} P_H(q, p) &= \frac{1}{4\pi^2} \iint d\xi d\eta \text{Tr} \left\{ \hat{\rho}(\hat{q}, \hat{p}) e^{i(\xi\hat{q} + \eta\hat{p})} f_H(\xi, \eta) \right\} e^{-i(\xi q + \eta p)} \\ &= \frac{1}{4\pi^2} \iint d\xi d\eta \text{Tr} \left\{ \hat{\rho}(\hat{q}, \hat{p}) e^{i(\xi\hat{q} + \eta\hat{p})} f_W(\xi, \eta) \right\} \frac{f_H(\xi, \eta)}{f_W(\xi, \eta)} e^{-i(\xi q + \eta p)} \end{aligned}$$

avec $f_W(\xi, \eta) = 1$ et $f_{AN}(\xi, \eta) = e^{-\hbar\xi^2/(4m\omega) - \hbar m\omega\eta^2/4}$. Or, d'après (A.4)

$$\text{Tr} \left\{ \hat{\rho} e^{i(\xi\hat{q} + \eta\hat{p})} f_W(\xi, \eta) \right\} = \iint dq' dp' e^{i(\xi q' + \eta p')} P_W(q', p')$$

D'où

$$P_H(q, p) = \iint dq' dp' g(q' - q, p' - p) P_W(q', p')$$

avec

$$g(q, p) = \frac{1}{4\pi^2} \iint d\xi d\eta e^{i(\xi q + \eta p)} \frac{f_H(\xi, \eta)}{f_W(\xi, \eta)}$$

On en déduit

$$P_H(q, p) = \frac{1}{\pi\hbar} \iint dq' dp' e^{-\frac{m\omega}{\hbar}(q'-q)^2 - \frac{1}{\hbar m\omega}(p'-p)^2} P_W(q', p') \quad (\text{A.23})$$

La distribution de Husimi n'est donc rien d'autre que le lissage de la distribution de Wigner par une gaussienne pour éliminer les fluctuations rapides. La gaussienne utilisée correspond à un paquet d'onde d'incertitude minimale, c'est-à-dire que ses écarts-type σ_q et σ_p vérifient $\sigma_q\sigma_p = \frac{\hbar}{2}$ (car $\sigma_q^2 = \frac{\hbar}{2m\omega}$ et $\sigma_p^2 = \frac{\hbar m\omega}{2}$). En fait, on peut montrer que le lissage gaussien de la distribution de Wigner donne des fonctions partout positives dès que $\sigma_q\sigma_p \geq \frac{\hbar}{2}$. Il faut remarquer en outre qu'aucune information essentielle n'est perdue lors de cette opération, puisque l'on peut reconstruire exactement la fonction d'onde à partir de la distribution de Husimi.

A.5 Distribution de Wigner discrète

On cherche maintenant à trouver l'équivalent de la distribution de Wigner continue pour un espace de Hilbert discret et fini [21, 69, 98]. Pour cela, on commence par introduire la base $|n\rangle$ (avec n variant de 0 à $N-1$), que l'on identifie arbitrairement comme la base des positions. Pour s'accommoder de la taille finie N de l'espace de Hilbert, on choisit des conditions aux limites périodiques $|n+N\rangle = |n\rangle$. L'interprétation de la base $|n\rangle$ comme celle d'une position est purement formelle et peut parfaitement ne pas correspondre à une observable physique. Par exemple dans le cas d'un ordinateur quantique, on peut choisir la base naturelle qui ne correspond pas à une position dans une implémentation réelle. On introduit également la base des moments conjugués $|k\rangle$, avec $k = 0, \dots, N-1$, qui s'obtient à partir de la base $|n\rangle$ par

$$|k\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{i2\pi \frac{nk}{N}} |n\rangle$$

Ainsi, comme dans le cas continu, la position et le moment sont reliés par une transformée de Fourier. Par contre, les opérateurs position et moment que l'on pourrait définir par $\hat{Q} = \sum_n n |n\rangle\langle n|$ et $\hat{P} = \sum_k k |k\rangle\langle k|$ ne sont plus canoniquement conjugués. Leur commutateur n'est en effet pas proportionnel à l'identité, et l'on peut montrer plus généralement qu'il est impossible de trouver deux opérateurs qui vérifient cette propriété dans un espace de Hilbert de dimension finie. Il est donc plus judicieux de définir la distribution de Wigner discrète à l'aide des opérateurs de translation. Avant de les aborder, il est important de remarquer que la taille de l'espace de Hilbert est reliée à une constante de Planck effective. Si l'on considère un système continu dont la position et le moment sont tous deux périodiques de période 2π , alors seul un nombre fini N d'états ont une amplitude non nulle, et l'on peut les indexer par n et k : $q = 2\pi \frac{n}{N}$ et $p = 2\pi \frac{k}{N}$ (voir page 50 et figure

3.4). Or, comme q est 2π -périodique, on a également $p = k\hbar$, ce qui donne $N = \frac{2\pi}{\hbar}$. N joue donc le rôle de l'inverse d'une constante de Planck, et la limite de grand N correspond à une limite semi-classique.

Une fois les bases des positions et des moments définies, on peut construire les opérateurs de translation. Même si la notion de translation infinitésimale n'a ici pas de sens, on peut néanmoins définir les opérateurs de translation finie \hat{U} et \hat{V} , qui génèrent des translations finies en position et en moment respectivement.

$$\begin{aligned}\hat{U}^m |n\rangle &= |n+m\rangle & \hat{V}^m |k\rangle &= |k+m\rangle \\ \hat{U}^m |k\rangle &= e^{-i2\pi\frac{mk}{N}} |k\rangle & \hat{V}^m |n\rangle &= e^{i2\pi\frac{mn}{N}} |n\rangle\end{aligned}$$

Ces opérateurs vérifient la relation de commutation

$$\hat{V}^p \hat{U}^q = \hat{U}^q \hat{V}^p e^{i2\pi\frac{qp}{N}} \quad (\text{A.24})$$

À l'aide de ces opérateurs, on est en mesure de trouver un équivalent discret à l'opérateur de translation continue dans l'espace des phases (A.13)

$$\hat{D}(q, p) = e^{-\frac{i}{\hbar}(q\hat{p}-p\hat{q})} = e^{-i\frac{qp}{\hbar}} e^{i\frac{p\hat{q}}{\hbar}} e^{i\frac{p\hat{q}}{2\hbar}}$$

En identifiant les opérateurs de déplacement correspondants, on définit l'analogue discret de $\hat{D}(q, p)$ par

$$\hat{T}(q, p) = \hat{U}^q \hat{V}^p e^{i\pi\frac{qp}{N}} \quad (\text{A.25})$$

On définit enfin un dernier opérateur \hat{R} , qui agit comme une réflexion dans la base des positions (ou des moments), selon $\hat{R}|n\rangle = |-n\rangle$. Il vérifie les lois de commutation suivantes avec les opérateurs de translation

$$\begin{aligned}\hat{U}\hat{R} &= \hat{R}\hat{U}^{-1} \\ \hat{V}\hat{R} &= \hat{R}\hat{V}^{-1}\end{aligned}$$

Pour construire une fonction de Wigner discrète, le plus simple est de trouver une version discrète de l'opérateur point de l'espace des phases $\hat{A}(q, p)$. On cherche donc une base de l'espace des opérateurs hermitiens; comme l'espace de Hilbert est de dimension N , une telle base doit avoir N^2 éléments. Par analogie avec l'expression (A.14) pour $\hat{A}(q, p)$ dans le cas continu, on peut être tenté de définir l'opérateur équivalent dans le cas discret par

$$\hat{A}(q, p) = \frac{2}{N} \hat{T}(q, p) \hat{R} \hat{T}^\dagger(q, p)$$

Cet opérateur est bien hermitien par construction. Cependant, la base ainsi construite n'est pas assez grande. Pour le voir, on réécrit \hat{A} en utilisant la relation de commutation (A.24)

$$\hat{A}(q, p) = \frac{1}{N} \hat{U}^{2q} \hat{R} \hat{V}^{-2p} e^{i4\pi\frac{qp}{N}}$$

Comme \hat{U} et \hat{V} sont des opérateurs cycliques de période N , on a la relation $\hat{A}(q + \frac{N}{2}, p) = \hat{A}(q, p)$ et de même pour p . Cela signifie que lorsque q et p varient entre 0 et $N - 1$, seulement $\frac{N}{2} \times \frac{N}{2} = \frac{N^2}{4}$ opérateurs indépendants sont engendrés.

Pour résoudre ce problème, il suffit de définir les opérateurs point de l'espace des phases sur un réseau deux fois plus grand ($2N \times 2N$) afin d'obtenir $4N^2$ opérateurs, dont N^2 indépendants. On adopte ainsi la définition suivante, avec q et p variant entre 0 et $2N - 1$

$$\hat{A}(q, p) = \frac{1}{2N} \hat{U}^q \hat{R} \hat{V}^{-p} e^{i\pi \frac{qp}{N}} \quad (\text{A.26})$$

On peut montrer aisément que

$$\hat{A}(q + \sigma_q N, p + \sigma_p N) = \hat{A}(q, p) (-1)^{\sigma_p q + \sigma_q p + \sigma_q \sigma_p N}$$

avec $\sigma_q, \sigma_p = 0, 1$. Cela signifie que les N^2 opérateurs correspondant au sous-réseau $q, p = 0, \dots, N$ de l'espace des phases déterminent tous les autres. D'autre part, les $\hat{A}(q, p)$ forment une base complète de ce sous-réseau. En effet, on a

$$\text{Tr} \left\{ \hat{A}(q, p) \hat{A}(q', p') \right\} = \frac{1}{4N} \delta_N(q' - q) \delta_N(p' - p) \quad (\text{A.27})$$

avec q, q', p et p' variant entre 0 et N , et $\delta_N(q) = \frac{1}{N} \sum_{n=0}^{N-1} e^{i2\pi q n/N}$ est la fonction delta périodique qui est nulle sauf si $q = 0 \pmod{N}$.

On peut maintenant définir la fonction de Wigner discrète par

$$P_W(q, p) = \text{Tr} \left\{ \hat{A}(q, p) \hat{\rho} \right\} \quad (\text{A.28})$$

avec $q, p = 0, \dots, N$. De la même manière que les $\hat{A}(q, p)$ ne sont pas tous indépendants, la fonction de Wigner discrète obéit à la relation

$$P_W(q + \sigma_q N, p + \sigma_p N) = P_W(q, p) (-1)^{\sigma_p q + \sigma_q p + \sigma_q \sigma_p N}$$

Comme les opérateurs \hat{A} forment une base du premier sous-réseau $N \times N$, on peut inverser la définition (A.28) et développer la matrice densité sur cette base

$$\begin{aligned} \hat{\rho} &= 4N \sum_{q,p=0}^{N-1} P_W(q, p) \hat{A}(q, p) \\ &= N \sum_{q,p=0}^{2N-1} P_W(q, p) \hat{A}(q, p) \end{aligned}$$

La dernière égalité est obtenue en remarquant que les contributions provenant des 4 réseaux $N \times N$ sont identiques.

La distribution de Wigner discrète ainsi définie possède les mêmes propriétés que la distribution continue. En effet, W est réel car \hat{A} est hermitien par construction. De plus, d'après (A.27) on a

$$\text{Tr} \{ \hat{\rho}_1 \hat{\rho}_2 \} = N \sum_{q,p=0}^{2N-1} P_{W_1}(q,p) P_{W_2}(q,p)$$

Enfin, on peut montrer qu'on obtient les probabilités marginales correctes en sommant la fonction de Wigner selon q ou p

$$\begin{aligned} \sum_{q=0}^{2N-1} P_W(q,p) &= \langle p | \hat{\rho} | p \rangle \\ \sum_{p=0}^{2N-1} P_W(q,p) &= \langle q | \hat{\rho} | q \rangle \end{aligned}$$

A.6 Distribution de Husimi discrète

De même, on peut trouver un équivalent discret à la fonction de Husimi [73]. Dans le cas discret avec des conditions aux limites périodiques, l'état cohérent centré en $(0,0)$ s'écrit

$$|\alpha_{0,0}\rangle = \gamma \sum_{n=0}^{N-1} \sum_{j=-\infty}^{\infty} e^{-\frac{\pi\omega}{N}(Nj+n)^2} |n\rangle$$

(on a pris ici $m = 1$). Le facteur de normalisation γ n'a pas d'expression générale simple, mais pour N grand, le recouvrement entre les différentes gaussiennes devient rapidement très faible, et on peut alors approximer γ avec une bonne précision par

$$\gamma = \sqrt[4]{\frac{2\omega}{N}}$$

On obtient les autres états cohérents centrés en (q,p) grâce à l'opérateur de translation finie (A.25)

$$\begin{aligned} |\alpha_{q,p}\rangle &= \hat{T}(q,p) |\alpha_{0,0}\rangle \\ &= \gamma \sum_{n=0}^{N-1} \sum_{j=-\infty}^{\infty} e^{-\frac{\pi\omega}{N}(Nj+n-q)^2} e^{-i\frac{2\pi}{N}p(\frac{q}{2}-n)} |n\rangle \end{aligned}$$

De la même manière que dans le cas continu, la distribution de Husimi discrète est alors définie par

$$P_H(q,p) = \frac{1}{N} \text{Tr} \{ |\alpha_{q,p}\rangle \langle \alpha_{q,p} | \hat{\rho} \} \quad (\text{A.29})$$

Pour un état pur $\hat{\rho} = |\psi\rangle\langle\psi|$, cela donne (avec $|\psi\rangle$ exprimée dans la représentation des positions)

$$P_H(q, p) = \sqrt{\frac{2\omega}{N^3}} \left| \sum_{j=-\infty}^{\infty} \sum_{n=0}^{N-1} \psi(n) e^{-\frac{\pi\omega}{N}(Nj+n-q)^2} e^{i\frac{2\pi}{N}pn} \right|^2$$

Le facteur ω peut être interprété simplement comme le rapport $\frac{\Delta_p}{\Delta_q}$ entre l'extension de l'état cohérent selon p et selon q , avec Δ_q et Δ_p exprimés en nombre d'états. Les écarts-types σ_q et σ_p définis page 116, qui sont exprimés en unités d'espace des phases, s'obtiennent à partir des précédents par $\sigma_q = \frac{2\pi c_q}{N} \Delta_q$ et $\sigma_p = \frac{2\pi c_p}{N} \Delta_p$ (on suppose ici que l'espace des phases a pour extension $2\pi c_q \times 2\pi c_p$). Si $c_q = c_p$, alors $\omega = \frac{\Delta_p}{\Delta_q} = \frac{\sigma_p}{\sigma_q}$, comme c'est le cas pour le choix usuel $2\pi \times 2\pi$. Dans le cas contraire, on a $\omega = \frac{\sigma_p c_q}{\sigma_q c_p}$. Si l'on souhaite avoir un paquet d'onde symétrique dans une cellule $2\pi \times 2\pi$ de l'espace des phases ($\sigma_p = \sigma_q$), on doit donc prendre $\omega = \frac{c_q}{c_p}$ (voir par exemple la figure A.1).

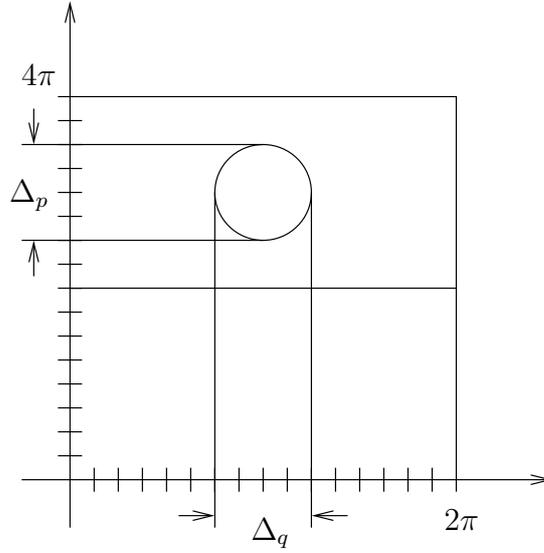


FIG. A.1 – État cohérent dans un espace des phases $2\pi \times 4\pi$. Ici, $\omega = \frac{\Delta_p}{\Delta_q} = 1$ mais $\frac{\sigma_p}{\sigma_q} = 2$.

Bibliographie

- [1] D. S. Abrams et S. Lloyd. *Simulation of many-body fermi systems on a universal quantum computer*. Phys. Rev. Lett. **79**, 2586–2589 (1997).
- [2] H. Ammann, R. Gray, I. Shvarchuck et N. Christensen. *Quantum delta-kicked rotor : Experimental observation of decoherence*. Phys. Rev. Lett. **80**, 4111 (1998).
- [3] P. W. Anderson. *Absence of diffusion in certain random lattices*. Phys. Rev. **109**, 1492–1505 (1958).
- [4] R. Artuso, F. Borgonovi, I. Guarneri, L. Rebuzzini et G. Casati. Phys. Rev. Lett. **69**, 3302 (1992).
- [5] R. Artuso, F. Borgonovi, I. Guarneri, L. Rebuzzini et G. Casati. Int. Jour. Mod. Phys. B **8**, 207 (1994).
- [6] R. Artuso, G. Casati et D. L. Shepelyansky. Phys. Rev. Lett. **68**, 3826 (1992).
- [7] A. Barelli, J. Bellissard et R. Rammal. J. Phys. France **51**, 2167 (1990).
- [8] A. Barelli et C. Kref. J. Phys. I France **1**, 1229 (1991).
- [9] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin et H. Weinfurter. *Elementary gates for quantum computation*. Phys. Rev. A **52**, 3457–3467 (1995), quant-ph/9503016.
- [10] G. Benenti, G. Casati, S. Montangero et D. L. Shepelyansky. *Efficient quantum computing of complex dynamics*. Phys. Rev. Lett. **87**, 227901 (2001).
- [11] G. Benenti, G. Casati et G. Strini. *Principles of Quantum Computation and Information*. World Scientific (2004).
- [12] P. Benioff. *Quantum mechanical models of turing machines that dissipate no energy*. Phys. Rev. Lett. **48**, 1581–1585 (1982).
- [13] C. H. Bennett, E. Bernstein, G. Brassard et U. Vazirani. *Strengths and weaknesses of quantum computing*. SIAM J. Comput. **26**, 1510–1523 (1997), quant-ph/9701001.
- [14] F. Borgonovi et D. L. Shepelyansky. Europhysics Letters **29**, 117 (1995).

- [15] F. Borgonovi et D. L. Shepelyansky. *Enhancement of localization length for two interacting kicked rotators*. Nonlinearity **8**, 877 (1995).
- [16] M. Boyer, G. Brassard, P. Høyer et A. Tapp. *Tight bounds on quantum searching*. Fortsch. Phys. **46**, 493–505 (1998).
- [17] G. Brassard et P. Høyer. Dans *Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems*, pages 12–23. IEEE Computer Society, Los Alamitos, CA (1997).
- [18] G. Brassard, P. Høyer, M. Mosca et A. Tapp. Dans Jr. S. J. Lomonaco et H. E. Brandt, éditeurs, *Quantum Computation and Quantum Information : A Millennium Volume* (2002), AMS, Contemporary Mathematics Series Vol. 305, quant-ph/0005055.
- [19] G. Casati, B. V. Chirikov, J. Ford et F. M. Izrailev. Lecture Notes in Physics **93**, 334 (1979).
- [20] G. Casati, I. Guarneri et D. L. Shepelyansky. IEEE Jour. of Quant. Elect. **24**, 1420 (1988).
- [21] S. Chang et K. Shi. *Evolution and exact eigenstates of a resonant quantum system*. Phys. Rev. A **34**, 7–22 (1986).
- [22] A. D. Chepelianskii et D. L. Shepelyansky. *Simulation of chaos-assisted tunneling in a semiclassical regime on existing quantum computers*. Phys. Rev. Lett. **66**, 054301 (2002).
- [23] B. V. Chirikov. At. Energ. **6**, 630 (1959), [Engl. Trans., J. Nucl. Energy Part C : Plasma Phys. **1**, 253 (1960)].
- [24] B. V. Chirikov. *Research concerning the theory of nonlinear resonance and stochasticity*. Preprint N 267, Institute of Nuclear Physics, Novosibirsk (1969), [Engl. Trans., CERN Trans. 71-40 (1971)].
- [25] B. V. Chirikov. *A universal instability of many-dimensional oscillator systems*. Physics Reports **52**, 263–379 (1979).
- [26] B. V. Chirikov. *Time-dependent quantum systems*. Dans M.-J. Gianoni, A. Voros et J. Zinn-Justin, éditeurs, *Chaos and Quantum Physics*, pages 443–545. North-Holland (1989), Les Houches Summer School Lectures, Session LII, 1989.
- [27] B. V. Chirikov, F. M. Izrailev et D. L. Shepelyansky. *Dynamical stochasticity in classical and quantum mechanics*. Sov. Sci. Rev. C **2**, 209 (1981).
- [28] D. Coppersmith. *An approximate fourier transform useful in quantum factoring*. IBM Research Report RC 19642 (1994).
- [29] D. Deutsch. *Quantum theory, the church-turing principle and the universal quantum computer*. Proc. R. Soc. Lond. A **400**, 97 (1985).
- [30] D. P. DiVincenzo. *Two-bit gates are universal for quantum computation*. Phys. Rev. A **51**, 1015–1022 (1995).

- [31] J. Emerson, S. Lloyd, D. Poulin et D. Cory. *Estimation of the local density of states on a quantum computer*. Phys. Rev. A **69**, 050305 (2004).
- [32] J. Emerson, Y. S. Weinstein, S. Lloyd et D. G. Cory. *Fidelity decay as an efficient indicator of quantum chaos*. Phys. Rev. Lett. **89**, 284102 (2002).
- [33] S. N. Evangelou et J.-L. Pichard. Phys. Rev. Lett. **84**, 1643 (2000).
- [34] R. P. Feynman. *Simulating physics with computers*. Int. J. Theor. Phys. **21**, 467–488 (1982).
- [35] R. P. Feynman. *Quantum mechanical computers*. Found. Phys. **16**, 507–531 (1986).
- [36] S. Fishman, D. R. Grempel et R. E. Prange. *Chaos, quantum recurrences, and anderson localization*. Phys. Rev. Lett. **49**, 509–512 (1982).
- [37] K. Frahm, A. Müller-Groeling, J.-L. Pichard et D. Weinmann. *Scaling in interaction-assisted coherent transport*. Europhys. Lett. **31**, 169 (1995).
- [38] K. M. Frahm, R. Fleckinger et D. L. Shepelyansky. *Quantum chaos and random matrix theory for fidelity decay in quantum computations with static imperfections*. Eur. Phys. J. D **29**, 139–155 (2004).
- [39] H. Furstenberg. Trans. Ann. Math. Soc. **108**, 377 (1963).
- [40] T. Geisel, R. Ketzmerick et G. Petschel. Phys. Rev. Lett. **66**, 1651 (1991).
- [41] B. Georgeot et D. L. Shepelyansky. *Emergence of quantum chaos in the quantum computer core and how to manage it*. Phys. Rev. E **62**, 6366–6375 (2000).
- [42] B. Georgeot et D. L. Shepelyansky. *Quantum chaos border for quantum computing*. Phys. Rev. E **62**, 3504–3507 (2000).
- [43] B. Georgeot et D. L. Shepelyansky. *Exponential gain in quantum computing of quantum chaos and localization*. Phys. Rev. Lett. **86**, 2890 (2001).
- [44] B. Georgeot et D. L. Shepelyansky. *Stable quantum computation of unstable classical chaos*. Phys. Rev. Lett. **85**, 5393 (2001).
- [45] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. Thèse de Doctorat, California Institute of Technology, Pasadena (1997), quant-ph/9705052.
- [46] D. R. Grempel, R. E. Prange et S. Fishman. *Quantum dynamics of a nonintegrable system*. Phys. Rev. A **29**, 1639–1647 (1984).
- [47] L. K. Grover. *A fast quantum mechanical algorithm for database search*. Dans *Proc. of the 28th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 212–219 (1996).

- [48] L. K. Grover. *Quantum mechanics helps in searching for a needle in a haystack*. Phys. Rev. Lett. **79**, 325–328 (1997).
- [49] F. Haake. *Quantum Signatures of Chaos*. Springer (1992).
- [50] P. G. Harper. *Single band motion of conduction electrons in a uniform magnetic field*. Proc. Phys. Soc. A **68**, 874–878 (1955).
- [51] M. Hillery, R. F. O’Connell, M. O. Scully et E. P. Wigner. *Distribution functions in physics : Fundamentals*. Physics Reports **106**, 121–167 (1984).
- [52] D. R. Hofstadter. *Energy levels and wave functions of bloch electrons in rational and irrational magnetic fields*. Phys. Rev. B **14**, 2239–2249 (1976).
- [53] Y. Imry. *Coherent propagation of two interacting particles in a random potential*. Europhys. Lett. **30**, 405 (1995).
- [54] F. M. Izrailev. *Simple models of quantum chaos : spectrum and eigenfunctions*. Physics Reports **196**, 299–392 (1990).
- [55] O. Kern, G. Alber et D. L. Shepelyansky. *Quantum error correction of coherent errors by randomization* (2004), quant-ph/0407262.
- [56] R. Ketzmerick, K. Kruse et T. Geisel. Phys. Rev. Lett. **80**, 137 (1998).
- [57] A. Y. Kitaev. *Quantum measurements and the abelian stabilizer problem* (1995), quant-ph/9511026.
- [58] A. Y. Kitaev. *Quantum computations : algorithms and error correction*. Russ. Math. Surv. **52**, 1191–1249 (1997).
- [59] P. M. Koch et K. A. H. van Leeuwen. Phys. Rep. **255**, 289 (1995).
- [60] A. N. Kolmogorov. Dokl. Akad. Nauk. SSSR **98**, 527 (1954).
- [61] P. Leboeuf, J. Kurchan, M. Feingold et D. P. Arovav. Phys. Rev. Lett. **65**, 3076 (1990).
- [62] H.-W. Lee. *Theory and application of the quantum phase-space distribution functions*. Physics Reports **259**, 147–211 (1995).
- [63] B. Lévi et B. Georgeot. *Quantum computation of a complex system : The kicked Harper model*. Phys. Rev. E **70**, 056218 (2004), quant-ph/0409028.
- [64] B. Lévi, B. Georgeot et D. L. Shepelyansky. *Quantum computing of quantum chaos in the kicked rotator model*. Phys. Rev. E **67**, 046220 (2003), quant-ph/0210154.
- [65] A. Lichtenberg et M. Lieberman. *Regular and Chaotic Dynamics*. Springer, New York (1992).
- [66] D. A. Lidar et O. Biham. *Simulating ising spin glasses on a quantum computer*. Phys. Rev. E **56**, 3661–3681 (1997).
- [67] R. Lima et D. L. Shepelyansky. Phys. Rev. Lett. **67**, 1377 (1991).

- [68] S. Lloyd. *Universal quantum simulators*. Science **273**, 1073 (1996).
- [69] C. Miquel, J. P. Paz et M. Saraceno. *Quantum computers in phase space*. Phys. Rev. A **65**, 062309 (2002).
- [70] F. L. Moore, J. C. Robinson, C. F. Bharucha, B. Sundaram et M. G. Raizen. *Atom optics realization of the quantum delta-kicked rotor*. Phys. Rev. Lett. **75**, 4598 (1995).
- [71] M. A. Nielsen et I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York (2000).
- [72] G. Ortiz, J. E. Gubernatis, E. Knill et R. Laflamme. *Quantum algorithms for fermionic simulations*. Phys. Rev. A **64**, 022319 (2001).
- [73] J. P. Paz, A. J. Roncaglia et M. Saraceno. *Quantum algorithms for phase-space tomography*. Phys. Rev. A **69**, 032312 (2004).
- [74] A. A. Pomeransky et D. L. Shepelyansky. *Quantum computation of the anderson transition in the presence of imperfections*. Phys. Rev. A **69**, 014302 (2004).
- [75] J. Preskill. *Quantum Computation and Information*. California Institute of Technology (1998), <http://www.theory.caltech.edu/people/preskill/ph229/>.
- [76] T. Prosen, I. I. Satija et N. Shah. Phys. Rev. Lett. **87**, 066601 (2001).
- [77] L. E. Reichl. *The Transition to Chaos*. Springer-Verlag (1992).
- [78] R. Schack. *Using a quantum computer to investigate quantum chaos*. Phys. Rev. A **57**, 1634 (1998).
- [79] T. Schlösser, K. Ensslin, J. P. Kotthaus et M. Holland. *Experimental observation of an artificial bandstructure in lateral superlattices*. Dans Montambaux Martin et Trân Thanh Vân, éditeurs, *Correlated Fermions and Transport in Mesoscopic Systems*, page 423. Frontières (1996).
- [80] D. L. Shepelyansky. *Localization of quasienergy eigenfunctions in action space*. Phys. Rev. Lett. **56**, 677 (1986).
- [81] D. L. Shepelyansky. *Localization of diffusive excitation in multi-level systems*. Physica D **28**, 103 (1987).
- [82] D. L. Shepelyansky. *Coherent propagation of two interacting particles in a random potential*. Phys. Rev. Lett. **73**, 2607–2610 (1994).
- [83] P. W. Shor. *Algorithms for quantum computation : discrete logarithms and factoring*. Dans *Proc. of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134 (1994).
- [84] P. W. Shor. *Scheme for reducing decoherence in quantum computer memory*. Phys. Rev. A **52**, 2493 (1995).
- [85] P. W. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM J. Comput. **26**, 1484–1509 (1997), quant-ph/9508027.

- [86] P. H. Song et D. L. Shepelyansky. *Quantum computing of quantum chaos and imperfection effects*. Phys. Rev. Lett. **86**, 2162–2165 (2001).
- [87] A. Sørensen et K. Mølmer. *Spin-spin interaction and spin squeezing in an optical lattice*. Phys. Rev. Lett. **83**, 2274–2277 (1999).
- [88] A. M. Steane. *Error correcting codes in quantum theory*. Phys. Rev. Lett. **77**, 793 (1996).
- [89] A. M. Steane. *Quantum computing*. Rep. Prog. Phys. **61**, 117 (1998).
- [90] H.-J. Stöckmann. *Quantum Chaos, an introduction*. Cambridge University Press (1999).
- [91] V. I. Tatarskii. *The wigner representation of quantum mechanics*. Sov. Phys. Usp. **26**, 311–327 (1983).
- [92] F. von Oppen, T. Wettig et J. Müller. *Interaction-induced delocalization of two particles in a random potential : Scaling properties*. Phys. Rev. Lett. **76**, 491–494 (1996).
- [93] D. Weinmann, A. Müller-Groeling, J.-L. Pichard et K. Frahm. *$h/2e$ oscillations for correlated electron pairs in disordered mesoscopic rings*. Phys. Rev. Lett. **75**, 1598–1601 (1995).
- [94] Y. S. Weinstein, S. Lloyd, J. Emerson et D. G. Cory. *Experimental implementation of the quantum baker's map*. Phys. Rev. Lett. **89**, 157902 (2002).
- [95] S. Wiesner. *Simulations of many-body quantum systems by a quantum computer* (1996), quant-ph/9603028.
- [96] E. Wigner. *On the quantum correction for thermodynamic equilibrium*. Phys. Rev. **40**, 749–759 (1932).
- [97] M. Wilkinson et R. J. Kay. Phys. Rev. Lett. **76**, 1896 (1996).
- [98] W. K. Wootters. *A wigner-function formulation of finite-state quantum mechanics*. Annals of Physics **176**, 1–21 (1987).
- [99] C. Zalka. *Efficient simulation of quantum systems by quantum computers*. Fortschr. Phys. **46**, 877 (1998).