

Université de Montréal

**Évolution des systèmes quantiques ouverts :  
décohérence et informatique quantique**

par  
Olivier Landon-Cardinal

Département de physique  
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures  
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)  
en physique

Août, 2009

© Olivier Landon-Cardinal, 2009.



Université de Montréal  
Faculté des études supérieures

Ce mémoire intitulé

**Évolution des systèmes quantiques ouverts :  
décohérence et informatique quantique**

présenté par

Olivier Landon-Cardinal

a été évalué par un jury composé des personnes suivantes :

Manu Paranjape,	président-rapporteur
Richard MacKenzie,	directeur de recherche
Gilles Brassard,	codirecteur
Michel Côté,	membre du jury.

Mémoire accepté le 26 novembre 2009



## RÉSUMÉ

L'informatique quantique, brièvement introduite au chapitre 1, exploite les corrélations quantiques et en particulier l'intrication. Ces corrélations sont difficiles à maintenir car un système quantique n'est habituellement pas fermé, mais en interaction avec son environnement. Le traitement formel d'un système quantique *ouvert* requiert des outils spécifiques, introduits au chapitre 2. En utilisant ces notions, nous montrerons au chapitre 3 que l'interaction entre le système et son environnement aura pour effet de privilégier certains états, qualifiés de quasi-classiques, suggérant ainsi l'émergence d'un monde classique à partir d'un monde quantique. De plus, l'intrication qui se crée entre le système et son environnement détruira la cohérence d'une superposition d'états quasi-classiques. Il s'agit du phénomène de *décohérence* dont les mécanismes seront mis en évidence dans notre étude originale d'un gyroscope quantique au chapitre 4. Nous montrerons qu'une particule de grand spin servant à mesurer le moment angulaire d'électrons perd sa cohérence en un temps très court par rapport au temps caractéristique de relaxation. Afin de protéger la cohérence d'un système, essentielle pour l'informatique quantique, plusieurs techniques de protection ont été développées. Nous les rappellerons brièvement en début de chapitre 5, avant d'introduire une approche originale qui consiste à *préparer l'environnement*. Notre étude [47] nous permet de caractériser l'existence d'états initiaux de l'environnement permettant une évolution sans décohérence du système dans une gamme de modèles où le système interagit avec un environnement présentant une dynamique propre.

**Mots clés :** Décohérence, système quantique ouvert, informatique quantique, transition quantique-classique.



## ABSTRACT

Quantum information processing, briefly introduced in Chapter 1, relies on quantum correlations, namely on entanglement. Those correlations are difficult to maintain since a typical quantum system is not closed, but interacting with its environment. The analysis of an open quantum system requires specific tools which we introduce in Chapter 2. Using these concepts, we show in Chapter 3 that the interaction between the system and its environment will distinguish certain quasi-classical states, suggesting the emergence of a classical world from a quantum one. Furthermore, the entanglement created between the system and its environment will destroy the coherence of a superposition of such quasi-classical states. This phenomenon of decoherence exhibits mechanisms which we highlight in our original study of a quantum gyroscope in chapter 4. We demonstrate that a particle with large spin, used to measure the angular momentum of electrons, loses its coherence on a timescale much shorter than the characteristic timescale of relaxation. To protect the coherence of a system, essential to quantum information processing, several techniques have been developed. We briefly review them at the beginning of Chapter 5, before introducing a novel approach based on the preparation of the environment. Our analysis [47] characterizes the existence of initial states of the environment allowing for decoherence-free evolution of the system in a large class of models in which the system interacts with a dynamical environment.

**Keywords:** Decoherence, open quantum system, quantum information, quantum-to-classical transition.



# TABLE DES MATIÈRES

RÉSUMÉ	v
ABSTRACT	vii
TABLE DES MATIÈRES	ix
LISTE DES FIGURES	xv
NOTATION	xvii
DÉDICACE	xix
REMERCIEMENTS	xxi
AVANT-PROPOS	xxiii
<b>1 Physique et informatique quantiques</b>	<b>1</b>
1.1 Rappels de mécanique quantique . . . . .	2
1.2 Notions d'informatique quantique . . . . .	6
1.2.1 Qubit . . . . .	6
1.2.1.1 État d'un qubit . . . . .	7
1.2.1.2 Mesure d'un qubit . . . . .	8
1.2.1.3 Portes quantiques . . . . .	9
1.2.2 Registre quantique . . . . .	10
1.2.2.1 Intrication . . . . .	11
1.2.2.2 État à $n$ qubits . . . . .	12
1.3 Algorithmes quantiques . . . . .	13
1.3.1 Circuits quantiques . . . . .	13
1.3.1.1 Oracle . . . . .	14
1.3.1.2 Parallélisme quantique . . . . .	15
1.3.1.3 Interférence quantique . . . . .	15

1.3.2	Algorithme de Grover . . . . .	16
1.3.2.1	Opérateurs de l'algorithme de Grover . . . . .	16
1.3.2.2	Description de l'algorithme . . . . .	17
1.3.3	Remarques sur le calcul quantique . . . . .	18
<b>2</b>	<b>Système quantique ouvert</b>	<b>21</b>
2.1	Opérateur densité . . . . .	22
2.1.1	Cas pur . . . . .	22
2.1.2	Intrication et trace partielle . . . . .	23
2.1.3	État quantique . . . . .	27
2.1.3.1	Définition formelle . . . . .	27
2.1.3.2	État à 1 qubit : boule de Bloch . . . . .	27
2.1.3.3	Interprétations . . . . .	29
2.2	Mesure généralisée et superopérateur . . . . .	33
2.2.1	Mesure généralisée . . . . .	34
2.2.1.1	Observable sur un grand système . . . . .	34
2.2.1.2	POVM . . . . .	34
2.2.2	Superopérateur . . . . .	36
2.2.2.1	Évolution unitaire sur un grand système . . . . .	36
2.2.2.2	Canal à amortissement de phase . . . . .	39
<b>3</b>	<b>Théorie de la décohérence</b>	<b>45</b>
3.1	Transition quantique-classique . . . . .	46
3.1.1	Limite quantique-classique . . . . .	46
3.1.2	Problème de la mesure . . . . .	48
3.1.2.1	Mesure quantique . . . . .	48
3.1.2.2	Base privilégiée et unicité du résultat . . . . .	50
3.1.3	Intrication et importance de l'environnement . . . . .	54
3.2	Modèles de décohérence . . . . .	57
3.2.1	Modèle de Żurek . . . . .	57
3.2.1.1	Description du modèle . . . . .	57
3.2.1.2	Évolution dans le temps . . . . .	59

3.2.1.3	Opérateur densité réduit de $\mathcal{S}$ . . . . .	60
3.2.1.4	Caractéristiques générales . . . . .	65
3.2.1.5	Évolution propre du système . . . . .	66
3.2.2	Autres modèles . . . . .	67
3.3	Rôles de l'environnement . . . . .	68
3.3.1	Supersélection induite par l'environnement . . . . .	68
3.3.1.1	Mesure étendue de von Neumann . . . . .	68
3.3.1.2	Limite de la mesure quantique . . . . .	69
3.3.1.3	Limite quantique de la décohérence . . . . .	71
3.3.1.4	Cas intermédiaires . . . . .	71
3.3.2	Décohérence induite par l'environnement . . . . .	72
3.3.3	Environnement en tant que témoin . . . . .	75
<b>4</b>	<b>Gyroscope quantique</b> . . . . .	<b>77</b>
4.1	Motivation . . . . .	77
4.2	Gyroscope quantique . . . . .	78
4.2.1	Systèmes en présence . . . . .	79
4.2.2	Mesure induite sur la particule . . . . .	80
4.3	Évolution du gyroscope . . . . .	81
4.3.1	Canal quantique . . . . .	82
4.3.2	Interaction de Heisenberg . . . . .	82
4.3.3	Équivalence des modèles . . . . .	83
4.4	Régime quasi-classique . . . . .	86
4.4.1	Choix des axes . . . . .	86
4.4.2	Évolution quasi-classique . . . . .	87
4.4.2.1	État cohérent . . . . .	87
4.4.2.2	Équations du mouvement . . . . .	89
4.4.3	Superposition d'états cohérents . . . . .	90
<b>5</b>	<b>Lutte contre la décohérence</b> . . . . .	<b>93</b>
5.1	Décohérence et calcul quantique . . . . .	93
5.1.1	Décohérence et interférométrie . . . . .	93

5.1.2	Algorithme de Grover avec décohérence . . . . .	95
5.1.2.1	Modèle d'erreur . . . . .	95
5.1.2.2	Impact sur l'algorithme de Grover . . . . .	95
5.2	Différentes stratégies possibles . . . . .	96
5.2.1	Correction d'erreur . . . . .	97
5.2.2	Prévention de la décohérence . . . . .	97
5.2.2.1	Espace protégé de la décohérence . . . . .	97
5.2.2.2	Contrôle quantique . . . . .	99
5.3	Préparation de l'environnement . . . . .	99
5.3.1	Motivation . . . . .	100
5.3.2	Modèles étudiés . . . . .	101
5.3.3	États initiaux . . . . .	102
5.3.3.1	Condition d'existence . . . . .	102
5.3.3.2	Rareté . . . . .	104
5.3.4	Perturbation due à la dynamique de l'environnement . . . . .	107
5.3.5	Préparation imparfaite de l'environnement . . . . .	109
5.3.6	Contrôle imparfait de l'environnement . . . . .	110
<b>6</b>	<b>Conclusion</b>	<b>115</b>
	<b>BIBLIOGRAPHIE</b>	<b>117</b>
<b>A</b>	<b>Algorithmes à la physicienne</b>	<b>xxv</b>
A.1	Oracle hamiltonien . . . . .	xxv
A.2	Algorithme hamiltonien . . . . .	xxvi
<b>B</b>	<b>Téléportation quantique</b>	<b>xxix</b>
B.1	Partage d'intrication . . . . .	xxix
B.2	Mesure de Bell chez Alice . . . . .	xxx
B.3	Signal classique et correction . . . . .	xxxix
<b>C</b>	<b>Mesure généralisée</b>	<b>xxxiii</b>

<b>D</b>	<b>Equation pilote</b>	<b>xxxvii</b>
D.1	Approximation de Born-Markov . . . . .	xxxvii
D.1.1	Mouvement brownien quantique . . . . .	xxxix
D.2	Équation de Lindblad . . . . .	xl
<b>E</b>	<b>Correction d’erreur</b>	<b>xliii</b>
E.1	Correction d’erreur classique . . . . .	xliii
E.2	Correction d’erreur quantique . . . . .	xliv
E.2.1	Numérisation de l’erreur . . . . .	xliv
E.2.2	Code à 3 qubits . . . . .	xlv
E.2.3	Calcul robuste et théorème-seuil . . . . .	xlvi



## LISTE DES FIGURES

1.1	Sphère de Bloch . . . . .	8
1.2	Portes quantique . . . . .	14
1.3	Oracle ou boîte noire . . . . .	14
2.1	Boule de Bloch . . . . .	28
2.2	Action du canal à amortissement de phase . . . . .	43
3.1	Expérience des fentes de Young avec détecteur . . . . .	55
3.2	Modèle de Żurek . . . . .	57
3.3	Évolution d'un état dans la boule de Bloch . . . . .	63
3.4	Simulation numérique de l'évolution du facteur de cohérence	64
3.5	Représentation simplifiée des domaines . . . . .	65
3.6	Alternative pour résoudre un modèle . . . . .	67
4.1	Choix des axes . . . . .	87
4.2	Évolution numérique de $\langle \alpha   \mathcal{E} ( \alpha\rangle\langle\beta = 0 )  \beta = 0\rangle$ . . . . .	91
4.3	Simulation numérique de l'évolution de l'opérateur $\chi$ . . . . .	92
5.1	Modèle de décohérence avec environnement dynamique ( $n = 5$ )	108
5.2	Résultats numériques . . . . .	112
B.1	Partage d'intrication . . . . .	xxx
B.2	Représentation en circuit du protocole de téléportation . . . . .	xxxi



## NOTATION

$\mathbb{N}$	Ensemble des entiers naturels (contient 0)
$\mathbb{N}^*$	Ensemble des entiers naturels privé de 0
$\mathbb{Q}$	Ensemble des rationnels
$\mathbb{R}$	Ensemble des nombres réels
$\mathbb{R}^+$	Ensemble des nombres réels positifs $\mathbb{R}^+ = \{\lambda \in \mathbb{R} \mid \lambda \geq 0\}$
$\mathbb{R}^*$	Ensemble des nombres réels privé de 0
$\mathbb{C}$	Ensemble des nombres complexes
$i$	Nombre complexe tel que $i^2 = -1$
$[[a; b]]$	Intervalle entier entre $a$ et $b$
$[a; b]$	Intervalle réel entre $a \in \mathbb{R}$ et $b \in \mathbb{R}$
$\alpha^*$	Conjugué de $\alpha$
$ \alpha $	Module de $\alpha \in \mathbb{C}$
$\mathcal{H}^A$	Espace de Hilbert associé au système $A$
$ \psi\rangle$	Ket : vecteur d'un espace de Hilbert
$\langle\psi $	Bra : forme linéaire continue sur un espace de Hilbert
$\   \psi\rangle \ $	Norme hermitienne du vecteur $\psi$
$\mathcal{L}(\mathcal{H})$	Ensemble des opérateurs linéaires de $\mathcal{H}$ dans $\mathcal{H}$
$\mathcal{D}(\mathcal{H})$	Ensemble des opérateurs densité sur $\mathcal{H}$
$\text{Vect}\{ \psi_k\rangle\}$	Espace vectoriel engendré par les combinaisons linéaires des vecteurs $\{ \psi_k\rangle\}$
$\text{Ker}A$	Espace vectoriel des vecteurs que l'opérateur linéaire $A$ envoie sur le vecteur nul. $\text{Ker}A = \{ \psi\rangle \mid A \psi\rangle = 0\}$
Erf	Fonction erreur définie par $\text{Erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$



À tous ceux qui m'ont soutenu et n'ont  
jamais cessé de croire en moi, même dans mes moments de doute.



## REMERCIEMENTS

L'heure est maintenant venue de remercier celles et ceux qui m'ont accompagné au cours de cette maîtrise. Mes premiers remerciements vont à mon directeur, Richard, et mon codirecteur, Gilles. Merci tout d'abord d'avoir couru le risque de prendre un étudiant au parcours un peu étrange qui tenait à travailler dans le domaine de l'informatique quantique. Merci ensuite de m'avoir appris tant de choses au cours des deux dernières années. Merci finalement de m'avoir aidé à faire mes premières armes dans le monde de la recherche, en particulier en me permettant de participer à de nombreuses conférences et ateliers.

Merci aussi à tous les joyeux lurones et luronnes du LITQ de participer à la joyeuse ambiance qui règne dans ce laboratoire et aussi d'avoir tenté d'inculquer des bases d'informatique à un incorrigible physicien. Merci aux amis qui ont partagé mon passage au labo : Adrien, David, Frédéric, Hugue et Michaël; à ces compagnons de route qui ont fini avant moi : Anne, Sébastien et Éric; à tous ces camarades de passage, collègues et professeurs que j'ai cotôyé de près ou de loin. Merci aussi à mes camarades physiciens, en particulier Heinz et Louis, qui m'ont rappelé la beauté de la physique afin de ne pas laisser le "côté obscur" de l'informatique s'emparer complètement de moi.

L'argent étant le nerf de la guerre, j'aimerais reconnaître ici l'appui financier du département de physique et du CRSNG qui m'ont permis de me consacrer à temps plein sur mon travail de maîtrise durant ces deux années.

En dernier lieu, je ne saurais jamais assez remercier tous mes proches, famille et amis, qui me soutiennent dans mon projet, tout en me rappelant qu'il y a pleins de belles choses en dehors du monde de la recherche. Une pensée toute spéciale à mon père qui m'a non seulement aidé à maintes reprises à me relever mais m'a aussi transmis, au moins partiellement, son savoir-faire en recherche. Merci enfin à celle qui partage mes peines et surtout mes joies, Laureen.



## AVANT-PROPOS

L'informatique quantique est un domaine de recherche à la jonction de l'informatique et de la physique qui étudie les possibilités nouvelles de traitement de l'information offertes par la mécanique quantique. Du point de vue d'un physicien, il s'agit d'étudier des systèmes physiques non pas seulement en terme des grandeurs physiques habituelles telles que l'énergie, mais aussi en terme de transfert d'information. Ce domaine pluridisciplinaire permet donc à un physicien d'explorer de nouveaux horizons et propose de mettre à profit les aspects les plus étranges de la mécanique quantique, par exemple l'intrication. Au-delà de la potentielle mise au point expérimentale d'un ordinateur quantique, ce domaine pose des questions fondamentales sur notre compréhension même de la physique quantique.

La décohérence est non seulement un problème théorique, mais aussi le problème central qui retarde la réalisation expérimentale d'un ordinateur quantique. En effet, la décohérence entraîne une fragilité extrême des corrélations quantiques essentielles au calcul quantique. Il est donc nécessaire de mieux comprendre la décohérence pour mieux lutter contre ses effets. La décohérence suggère également des mécanismes permettant l'émergence de propriétés classiques pour des systèmes fondamentalement quantiques.

Ce projet de maîtrise s'est articulé autour de deux axes principaux. Le premier consiste à étudier la décohérence d'un gyroscope quantique. Il s'agit d'un modèle jouet qui permet de mettre en évidence les propriétés générales de la théorie de la décohérence. Le second est la proposition d'une nouvelle méthode afin de lutter contre la décohérence : préparer l'état de l'environnement afin de permettre au système d'évoluer sans perdre de cohérence. Cette idée, *a priori* farfelue, a germé à la lecture des articles fondateurs de la théorie de la décohérence qui mentionnent l'existence de tels états mais les rejettent aussitôt comme étant "négligeables". J'ai voulu en avoir le cœur net et le principal apport original de ce travail de maîtrise est d'avoir exploré à fond l'existence et l'intérêt de ces états particuliers.



# Chapitre 1

## Physique et informatique quantiques

*Is information the key?*

–Gilles Brassard, article inaugural de *Nature Physics* [18]

Les objectifs de ce chapitre sont multiples. Il s’agit dans un premier temps de réinterpréter les postulats de la mécanique quantique en les évaluant du point de vue de l’information. Ceci nous amènera à évoquer plusieurs points problématiques qui seront abordés en détail dans les chapitres suivants, en particulier la description d’un sous-système d’un système intriqué. Dans un second temps, nous introduirons les bases de l’informatique quantique afin de montrer l’importance du principe de superposition (qui donne naissance au parallélisme quantique) et de la cohérence (qui permet l’interférence). L’objectif n’est pas d’être exhaustif dans notre introduction à l’informatique quantique, mais plutôt de présenter les notions essentielles de ce domaine de recherche pluridisciplinaire, à la rencontre de la physique quantique et de l’informatique. Cette introduction sera entièrement axée sur une approche théorique qui n’accorde certainement pas tout le mérite qui leur revient aux expérimentateurs œuvrant dans le domaine. Pour un tour d’horizon des implémentations expérimentales de l’informatique quantique, voir [53].

## 1.1 Rappels de mécanique quantique

Nous allons rapidement rappeler ici les postulats simplifiés de la mécanique quantique en suivant la présentation qui en est donnée dans l'ouvrage de C. Cohen-Tannoudji, B. Diu et F. Lalœ [25]. Pour chacun des postulats, une discussion critique suivra.

Le premier postulat définit comment la mécanique quantique décrit un système physique.

**Postulat** [Description de l'état d'un système] À un instant  $t_0$ , l'état d'un système physique est défini par un ket  $|\psi(t_0)\rangle$  appartenant à un espace de Hilbert  $\mathcal{H}$ .

La description de l'état quantique d'un système repose donc sur la notion d'espace de Hilbert qui est un espace vectoriel complexe, muni d'un produit hermitien noté  $\langle \dots | \dots \rangle$  et complet pour la norme issue du produit hermitien. Dans toute la suite, nous utiliserons les notions de kets (vecteurs de l'espace  $\mathcal{H}$ ) et de bras (forme linéaire continue sur  $\mathcal{H}$ ) introduites par Dirac.

Ce postulat pose problème dans le cas où un système physique est constitué de plusieurs sous-systèmes. En effet, dans ce cas, même si l'état du système peut être décrit par un ket, il peut être impossible de décrire l'état de chacun des sous-systèmes par un ket. Un tel phénomène est appelé intrication : nous reviendrons en détail sur cette notion en section 1.2.2.1. Par contre, même si l'état d'un système ne peut être décrit par un ket, il est toujours possible d'agrandir le système considéré en lui adjoignant un autre système physique, habituellement désigné comme son environnement, afin que le système global soit décrit par un ket<sup>1</sup> (voir section 2.1.3.3).

**Postulat** [Principe de correspondance] Toute grandeur physique mesurable  $\mathcal{O}$  est décrite par une observable  $O$ .

Ce postulat s'intéresse à la description d'une grandeur physique. Il s'agissait d'un problème essentiel au début de la mécanique quantique puisque les phy-

---

<sup>1</sup>L'existence de cet environnement en tant qu'objet physique ou comme abstraction mathématique reste sujette à interprétation.

siciens voulaient savoir comment décrire les grandeurs physiques habituelles (position, vitesse, énergie. . .) dans le formalisme quantique.

Rappelons qu'une observable est un opérateur auto-adjoint. Nous ne nous attarderons pas à cette notion délicate qui nécessite l'introduction d'un formalisme qui nous sera inutile par la suite. Pour les lecteurs intéressés à en savoir plus sur le formalisme mathématique de la mécanique quantique, nous suggérons toutefois l'ouvrage [3] qui constitue une bonne introduction. Nous allons immédiatement nous placer en dimension finie qui sera dorénavant le cadre de ce mémoire, sauf mention explicite du contraire. En dimension finie, les notions d'opérateur auto-adjoint et d'opérateur hermitien coïncident. L'opérateur  $\dagger$  est alors défini par la transconjugaison, c'est-à-dire que la représentation matricielle de  $O^\dagger$  s'obtient à partir de celle de  $O$  grâce à la relation  $O_{ij}^\dagger = (O_{ji})^*$ . Un opérateur hermitien est alors un opérateur linéaire  $O$  qui vérifie  $O^\dagger = O$ . Le théorème spectral affirme qu'un tel l'opérateur  $O$  est diagonalisable, que ces valeurs propres sont réelles et que les vecteurs propres correspondant à des valeurs propres différentes sont orthogonaux.

La notion d'observable, incontournable en physique, est liée à la notion de mesure projective ou mesure de von Neumann. En effet, grâce au théorème spectral, tout observable  $O$  peut être décomposé sous la forme

$$O = \sum_{\lambda \in \text{Sp}(O)} \lambda \Pi_\lambda \quad (1.1)$$

où  $\text{Sp}(O)$  sont les valeurs propres de  $O$  et  $\Pi_\lambda$  est le projecteur sur le sous-espace propre associé à  $\lambda$ , qui peut être dégénéré<sup>2</sup>. Cette décomposition permet de mieux comprendre les prochains postulats qui concernent la mesure d'une grandeur physique.

**Postulat** [Principe de quantification] La mesure de la grandeur physique  $\mathcal{O}$  ne donne comme résultat qu'une valeur propre de l'observable  $O$ .

---

<sup>2</sup>Un sous-espace propre est dit dégénéré s'il est de dimension  $k > 1$ . Dans ce cas, le projecteur sur ce sous-espace s'écrit  $\Pi = \sum_i |u_i\rangle\langle u_i|$  où  $\{|u_i\rangle\}_{i \in \llbracket 1; k \rrbracket}$  est une famille orthonormale du sous-espace.

**Postulat** [Règle de Born] Quand on mesure la grandeur physique  $\mathcal{O}$  sur un système dans l'état  $|\psi(t)\rangle$ , la probabilité  $\mathcal{P}(\lambda)$  d'obtenir la valeur propre  $\lambda$  est donné par

$$\mathcal{P}(\lambda) = \langle \psi(t) | \Pi_\lambda | \psi(t) \rangle. \quad (1.2)$$

**Postulat** [Réduction du paquet d'onde] L'état du système immédiatement après la mesure de  $\mathcal{A}$  est la projection (normalisée) de  $|\psi(t)\rangle$  sur le sous-espace propre associé à la valeur propre résultant de la mesure :

$$\frac{1}{\sqrt{\mathcal{P}(\lambda)}} \Pi_\lambda |\psi(t)\rangle. \quad (1.3)$$

Ce postulat peut sembler étrange puisqu'une mesure a souvent pour effet de détruire l'objet physique mesuré. Par exemple, la mesure de la polarisation d'un photon détruit habituellement ce photon. En informatique quantique, l'opération de pseudo-mesure (effectuée dans la base de mesure) permet de contourner ce problème en ajoutant un système auxiliaire. Les deux systèmes sont alors fortement corrélés et une mesure sur le système ancillaire va révéler l'information tout en laissant le système original dans l'état (1.3).

Finalement, le dernier postulat gouverne l'évolution de l'état du système grâce à l'équation de Schrödinger<sup>3</sup>.

**Postulat** [Équation d'évolution] L'évolution dans le temps de l'état  $|\psi(t)\rangle$  est donnée par l'équation de Schrödinger

$$i \frac{d}{dt} |\psi(t)\rangle = H(t) |\psi(t)\rangle \quad (1.4)$$

où  $H(t)$  est l'opérateur hamiltonien, qui est l'observable associée à l'énergie totale du système.

Le caractère hermitien de  $H(t)$  implique l'unitarité de l'opérateur d'évolu-

---

<sup>3</sup>L'équation de Schrödinger n'est valable que dans le cadre non-relativiste. Sauf mention explicite, nous nous plaçons dans le cadre de la mécanique quantique non-relativiste pour tout le reste du mémoire.

tion. Rappelons qu'un opérateur linéaire  $O$  est dit unitaire s'il est inversible et que son inverse est son transconjugué, autrement dit

$$OO^\dagger = \mathbf{1}. \quad (1.5)$$

En dimension finie, un opérateur linéaire  $O$  vérifiant (1.5) est inversible<sup>4</sup>.

Souvent, nous nous intéresserons à l'évolution d'un état quantique sur une durée finie  $t$ . Nous cherchons donc à exprimer l'opérateur d'évolution  $U(t)$  qui décrit la transition entre  $|\psi(0)\rangle$  et  $|\psi(t)\rangle$

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle.$$

L'équation de Schrödinger montre que la norme de  $|\psi(t)\rangle$  se conserve, ce qui est une conséquence directe du caractère hermitien du hamiltonien  $H(t)$

$$\begin{aligned} \frac{d}{dt} (\langle\psi(t)|\psi(t)\rangle) &= \frac{d\langle\psi(t)|}{dt} |\psi(t)\rangle + \langle\psi(t)| \frac{d|\psi(t)\rangle}{dt} \\ &= i\langle\psi(t)|H^\dagger|\psi(t)\rangle - i\langle\psi(t)|H|\psi(t)\rangle \\ &= 0. \end{aligned}$$

Cette conservation de la norme entraîne l'unitarité de l'opérateur d'évolution puisque la relation suivante doit être vérifiée pour tout état initial  $|\psi(0)\rangle$  :

$$\langle\psi(t)|\psi(t)\rangle = \langle\psi(0)|U^\dagger U|\psi(0)\rangle.$$

Ainsi, l'opérateur d'évolution  $U(t)$  vérifie la relation d'unitarité (1.5).

L'opérateur d'évolution est la solution de l'équation différentielle  $i\frac{d}{dt}U(t) = H(t)U(t)$  avec condition initiale  $U(0) = \mathbf{1}$ . Dans le cas particulier où l'hamiltonien ne dépend pas du temps, l'opérateur d'évolution est simplement donné par

$$U(t) = e^{-iHt}.$$

---

<sup>4</sup>En dimension infinie, un opérateur linéaire  $O$  peut être inversible à droite, c.-à-d. tel qu'il existe  $\tilde{O}$  qui vérifie  $O\tilde{O} = \mathbf{1}$ , sans pour autant être inversible à gauche.

Nous verrons dans la suite que les informaticiens quantiques préfèrent raisonner en termes d'opérateurs unitaires plutôt qu'en termes d'hamiltoniens. Notons aussi au passage qu'une évolution hamiltonienne maintient l'entropie et implique donc une préservation de l'information.

## 1.2 Notions d'informatique quantique

Nous introduirons ici les notions de base d'informatique quantique en nous restreignant à ce qui est strictement nécessaire pour la suite de ce mémoire. Pour une introduction plus complète, l'ouvrage de référence dans le domaine est celui de Nielsen et Chuang [54]. Les notes de cours de John Preskill, physicien théorique à CalTech, constituent aussi une bonne introduction [62] et sont disponibles à l'adresse suivante <http://www.theory.caltech.edu/~preskill/ph229/#lecture>.

Finalement, de nombreux ouvrages sont apparus dans les dernières années, dont voici une liste non-exhaustive [11, 43, 45, 50].

### 1.2.1 Qubit

Le qubit (pour *quantum binary digit*) est l'unité de base de l'informatique quantique. Il s'agit d'un système quantique à deux niveaux, c'est-à-dire évoluant dans un espace de Hilbert à deux dimensions. Dans ce mémoire, le qubit sera traité comme un objet mathématique. En particulier, nous ne nous intéresserons pas au support physique du qubit. Mentionnons toutefois, pour fixer les idées, que la polarisation d'un photon ou le spin d'un électron constituent des qubits.

### 1.2.1.1 État d'un qubit

L'état d'un qubit peut<sup>5</sup> être représenté par un vecteur dans un espace de Hilbert  $\mathcal{H}$ . De plus, ce vecteur doit être normalisé de telle façon que sa norme soit égale à 1. En choisissant une base orthonormale notée  $\{|0\rangle, |1\rangle\}$  qui sera dorénavant appelée *base de calcul*, l'état d'un qubit s'écrit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1.6)$$

où  $\alpha$  et  $\beta$  sont des nombres complexes qui vérifient  $|\alpha|^2 + |\beta|^2 = 1$  (condition normalisée).

Or, nous savons que les états quantiques ne sont définis qu'à une phase globale près puisque aucune mesure ne permet de distinguer  $|\psi\rangle$  et  $e^{i\theta}|\psi\rangle$  selon la règle de Born. Il est donc possible de choisir la phase afin que  $\langle\psi|0\rangle$  soit réel afin d'obtenir :

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \quad (1.7)$$

où  $\theta \in [0; \pi]$  et  $\phi \in [0; \pi]$ . Cette écriture donne lieu à une interprétation géométrique où l'état d'un qubit sera représenté par un point sur une sphère : la *sphère de Bloch* (figure 1.1). Dans cette représentation, l'angle  $\theta$  est la colatitude et l'angle  $\phi$  la longitude d'un point de la sphère unité. En particulier, les états  $|0\rangle$  et  $|1\rangle$  sont respectivement représentés par le pôle Nord et le pôle Sud. La visualisation sur la sphère de Bloch permet de rendre plus tangible l'état d'un qubit.

La sphère de Bloch permet aussi de visualiser la norme du produit scalaire entre deux états. Plus précisément, elle permet de visualiser l'angle  $\gamma \in [0; \frac{\pi}{2}]$  entre deux états  $|\psi\rangle$  et  $|\phi\rangle$  qui est défini par

$$\cos\gamma = |\langle\psi|\phi\rangle|.$$

---

<sup>5</sup>Ceci n'est possible que si le qubit est dans un état *pur*. Pour des raisons pédagogiques, dans tout ce chapitre, nous nous restreindrons à des états purs. Le chapitre 2 reviendra en grand détail sur cette notion.

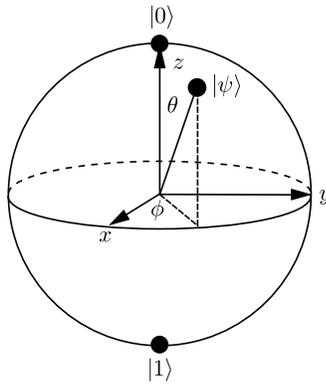


Figure 1.1 – Sphère de Bloch

En effet, l'angle géométrique entre les vecteurs normalisés représentant  $|\psi\rangle$  et  $|\phi\rangle$  sur la sphère de Bloch est le double de l'angle  $\gamma$  dans l'espace de Hilbert<sup>6</sup>. En particulier, deux états sont orthogonaux si et seulement s'ils correspondent à des points aux antipodes l'un de l'autre.

Notons finalement que les informaticiens quantiques ont une caractérisation très intéressante de l'orthogonalité en terme d'information : deux états sont orthogonaux si et seulement s'il existe une mesure permettant de les distinguer à tout coup et avec certitude. Pour un physicien, cela revient à dire qu'à deux états orthogonaux correspond toujours un observable et ce dernier permettra de distinguer les deux états. Le cas de l'orthogonalité n'est qu'un exemple particulier du travail important effectué sur la notion de distinguabilité.

### 1.2.1.2 Mesure d'un qubit

Une question intéressante est de déterminer la quantité d'information contenue dans un qubit. Puisque l'état d'un qubit est déterminé par la donnée de deux nombres réels, un qubit semble contenir autant d'information que ces deux nombres. Il ne faut toutefois pas perdre de vue que la mesure d'un qubit par un observable quelconque n'a que deux issues possibles

<sup>6</sup>Cette propriété est liée au fait que le groupe  $SU(2)$  est un recouvrement double du groupe  $SO(3)$

et ne fournira donc qu'un bit (classique) d'information<sup>7</sup>. En informatique quantique, le qubit est généralement mesuré dans la base de calcul.

**Proposition 1.1.** *Un qubit dans l'état donné par l'équation 1.6 est mesuré dans l'état  $|0\rangle$  avec probabilité  $|\alpha|^2$  et dans l'état  $|1\rangle$  avec probabilité  $|\beta|^2$ .*

Cette mesure correspond simplement à un observable dont la décomposition spectrale se ferait sur la base de calcul. Une mesure dans une base quelconque peut toujours se faire en appliquant d'abord la matrice correspondant au passage de cette base vers la base de calcul puis en mesurant dans la base de calcul.

### 1.2.1.3 Portes quantiques

L'évolution après mesure est un cas très important mais néanmoins particulier de l'évolution d'un qubit. Toute autre évolution d'un qubit est donnée par un opérateur d'évolution  $U$  qui est unitaire. Une façon intéressante de caractériser un opérateur unitaire est d'exiger qu'il préserve le produit scalaire  $\langle \psi | U^\dagger U | \phi \rangle = \langle \psi | \phi \rangle$ , ce qui équivaut à ce qu'il envoie une base orthonormale sur une autre base orthonormale. Ainsi, un opérateur unitaire maintient la distinguabilité de deux états quantiques.

En informatique quantique, la notion d'opérateur d'évolution sera remplacée par celle de porte quantique. Ces portes décrivent le passage d'un état quantique en entrée à un autre état quantique en sortie. Les matrices de Pauli constituent des exemples de portes quantiques à un qubit. Dans la suite de ce mémoire, elles seront notées de plusieurs façons et parfois regroupées dans un vecteur  $\sigma = (\sigma_1, \sigma_2, \sigma_3)$  où

$$\sigma_1 = \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \sigma_y = Y = iXZ \quad \sigma_3 = \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

---

<sup>7</sup>Ce raisonnement n'est plus valable si la mesure effectuée sur le qubit n'est pas une mesure projective, mais plutôt une mesure généralisée. Toutefois, le théorème de Holevo affirme que la transmission d'un qubit entre deux parties initialement non intriquées ne fournit pas plus de un bit d'information classique.

Introduisons aussi la porte de Hadamard notée traditionnellement  $H$ , mais que nous noterons  $\mathbb{H}$  afin d'éviter toute confusion avec l'opérateur hamiltonien. La porte de Hadamard transforme les états de la base de calcul en des superpositions de même amplitude de ces états avec une phase bien définie :

$$\mathbb{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (1.8)$$

$$\mathbb{H}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \quad (1.9)$$

La représentation de la porte de Hadamard sous forme matricielle dans la base de calcul est

$$\mathbb{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (1.10)$$

et son expression dans une base quelconque est obtenue par linéarité.

## 1.2.2 Registre quantique

Maintenant que nous savons décrire l'état d'un qubit, intéressons-nous au cas de deux qubits. Nous allons voir que plusieurs phénomènes extrêmement différents apparaissent alors. Le passage d'un qubit à deux qubits est donc un excellent exemple de phénomène émergent, idée souvent résumée par la formule de P.W. Anderson : "more is different" [2].

Avant d'aller plus loin, nous allons devoir introduire le formalisme permettant de représenter l'état d'un système physique composé de plusieurs sous-systèmes. Nous allons raisonner sur deux qubits, mais la construction est très générale. Soient deux qubits distinguables étiquetés  $A$  et  $B$ . À chacun des qubits est associé un espace de Hilbert  $\mathcal{H}$  de dimension 2. L'espace de Hilbert associé au système physique constitué des deux qubits sera le produit tensoriel  $\mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$  qui sera donc de dimension  $4 = 2 \times 2$ . La base de calcul associée à cet espace est donnée par le produit tensoriel des bases de calcul associées aux qubits  $A$  et  $B$ . La base de calcul à deux

qubits est donc  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  où  $|00\rangle$  est une notation condensée qui signifie que le qubit  $A$  est dans l'état  $|0\rangle$  et que le qubit  $B$  est dans l'état  $|0\rangle$ , autrement dit  $|00\rangle \equiv |0\rangle^A \otimes |0\rangle^B$ . L'état de deux qubits est donc un état normalisé de la forme

$$|\Gamma\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle. \quad (1.11)$$

### 1.2.2.1 Intrication

Une question essentielle est de déterminer si un état à deux qubits  $|\Gamma\rangle$  peut être mis sous la forme d'un produit tensoriel d'états à un qubit.

**Définition 1.2.** Un état à deux qubits  $|\Gamma\rangle \in \mathcal{H}^{AB} = \mathcal{H}^A \otimes \mathcal{H}^B$  est dit *séparable* s'il existe deux états à un qubit  $|\psi^A\rangle \in \mathcal{H}^A$  et  $|\psi^B\rangle \in \mathcal{H}^B$  tels que  $|\Gamma\rangle = |\psi^A\rangle \otimes |\psi^B\rangle$ . Un état non séparable est dit *intriqué*.

Autrement dit, un état est séparable si chacun de ses sous-systèmes est dans un état bien défini. Au contraire, l'intrication concerne un état à deux qubits qui est bien défini sans que l'on puisse associer un état à chacun des qubits qui le constituent. Au passage, notons que la notion d'intrication est liée à la division du système en plusieurs sous-systèmes. Or, il est facile d'exhiber des états qui ne sont pas séparables. Par exemple, les états suivants, communément appelés paires EPR ou états de Bell<sup>8</sup>, sont intriqués (et forment une base orthonormale) :

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{\sqrt{2}}|10\rangle \quad (1.12)$$

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{\sqrt{2}}|11\rangle. \quad (1.13)$$

Les états intriqués sont intéressants à plusieurs égards. En particulier, en effectuant des mesures sur chacun des qubits d'une paire EPR, il est possible d'obtenir des corrélations qui ne peuvent être reproduites par aucune théorie à variable cachée locale, résultat théorique prouvé par John Bell [10]. Cette

---

<sup>8</sup>en référence aux articles de A. Einstein, B. Podolsky et N. Rosen [30] et de J.S. Bell [10]

découverte a par la suite donné naissance à plusieurs inégalités (dites de Bell) qui contraignent les corrélations locales et peuvent être violées par la mécanique quantique. Citons en particulier l'inégalité CHSH qui a été proposée en 1969 [23] et dont la violation a été vérifiée expérimentalement en 1982 [5]. Ces corrélations *non-locales* font l'objet de plusieurs recherches à l'heure actuelle.

### 1.2.2.2 État à $n$ qubits

Finalement, nous allons être appelés à utiliser dans la suite des états à  $n$  qubits où  $n$  peut être arbitrairement grand. Dans ce cas, l'espace de Hilbert associé sera de taille  $N = 2^n$ . Un état à  $n$  qubits sera habituellement représenté dans la base de calcul constitué des états  $|x\rangle$  où  $x$  est la représentation binaire d'un nombre entre 0 et  $2^n - 1$ . Ainsi, un état à  $n$  qubits sera de la forme

$$|\Gamma\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \quad (1.14)$$

Comme nous l'avons déjà mentionné, tout opérateur d'évolution sur un qubit est un opérateur unitaire  $U$ . Plus généralement, un opérateur d'évolution sur un état à  $n$  qubits est un opérateur unitaire sur un espace de Hilbert de dimension  $N = 2^n$ . Il est possible de montrer que n'importe quelle porte unitaire à  $n$  qubits peut être engendrée par le produit tensoriel et la composition de certains sous-ensembles de portes à 1 et 2 qubits. En fait, il suffit d'une seule porte à 2 qubits et de portes à 1 qubit pour obtenir cette universalité. La porte à 2 qubits est nécessaire afin de créer de l'intrication, ce qui ne peut pas être fait par le produit tensoriel de portes à 1 qubit. La porte à 2 qubits la plus utilisée est appelée CNOT. Son expression dans la base de calcul est

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Ainsi, son effet sur les états de la base de calcul consiste à prendre la négation du second qubit quand le premier qubit est dans l'état  $|1\rangle$  et à ne rien faire si celui-ci est dans l'état  $|0\rangle$ . Son action sur un état quelconque est ensuite obtenu par linéarité.

## 1.3 Algorithmes quantiques

Nous allons brièvement introduire le modèle des circuits quantiques avant de présenter l'algorithme de Grover. Il ne s'agit que d'un exemple particulier d'algorithme quantique, mais il utilise plusieurs des éléments clés qui constituent les algorithmes quantiques connus à ce jour. De plus, notre objectif n'est pas de donner une revue exhaustive des algorithmes quantiques, mais plutôt d'avoir un exemple type afin de montrer dans la suite du mémoire l'effet catastrophique de la décohérence sur un calcul quantique. Le modèle des circuits quantiques, largement utilisé par la communauté informatique, n'est pas très naturelle pour un physicien<sup>9</sup>. Nous incluons en annexe A la présentation d'un autre point de vue, peut-être plus conforme à l'intuition d'un physicien et qui a permis de développer de nouveaux algorithmes.

### 1.3.1 Circuits quantiques

Dans un circuit quantique, chaque *fil quantique* correspond à un qubit. Celui-ci évoluera sous l'action de différentes *portes quantiques* (voir figure 1.2) représentant des opérateurs unitaires sur un ou des qubits.

Il est important de noter que le produit tensoriel et la composition d'opérateurs unitaires est encore un opérateur unitaire. Ainsi, durant l'exécution d'un algorithme quantique, un registre de  $n$  qubits préparé dans un état initial  $|0\rangle^{\otimes n}$  va évoluer sous l'action d'un opérateur unitaire qui se décompose en produits tensoriels et en composition de  $m$  portes quantiques à 1 ou 2 qubits. En fin d'exécution, une mesure projective sera effectuée afin d'ex-

---

<sup>9</sup>Pourtant, ce modèle a été introduit par le physicien David Deutsch !

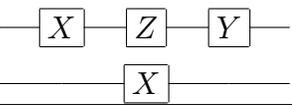
	$\mathbb{H} \otimes \mathbf{1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$
	$YZX \otimes X = i\mathbf{1} \otimes X = i \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
	<p>CNOT</p>

Figure 1.2 – Portes quantique

traire une information classique. Nous allons maintenant décrire en détail les différentes étapes d’un algorithme quantique.

### 1.3.1.1 Oracle

Plusieurs problèmes quantiques font intervenir un oracle, c’est-à-dire une boîte noire qui évalue une fonction. Dans ce qui va suivre, nous allons nous restreindre à une fonction de  $n$  bits dans 1 bit, c.-à-d.  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ . Ainsi, aux composants précédents d’un circuit quantique, nous rajoutons une porte unitaire notée  $\mathcal{C}$  dont l’action dans la base de calcul est de transformer  $|x\rangle \otimes |b\rangle$  en  $|x\rangle \otimes |b \oplus f(x)\rangle$  où  $\oplus$  est l’addition modulo 2 (voir figure 1.3). De façon équivalente, nous nous donnerons une opération unitaire  $U_f$  qui inscrit l’action de  $f$  sur l’entrée classique  $x \in \{0, 1\}^n$  dans la phase en transformant  $|x\rangle$  en  $(-1)^{f(x)}|x\rangle$  (voir figure 1.3).



Figure 1.3 – Oracle ou boîte noire

### 1.3.1.2 Parallélisme quantique

Un des outils essentiels des algorithmes quantiques repose sur la linéarité de la mécanique quantique. Classiquement, chaque appel à l'oracle ne calcule que l'image  $f(x)$  d'une seule entrée  $x$ . Par contre, un oracle quantique peut être appelé en superposition. Un algorithme quantique utilise typiquement une superposition de même amplitude des entrées classiques

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle. \quad (1.15)$$

Cette superposition est obtenue simplement en initialisant chacun des  $n$  qubits dans l'état  $|0\rangle$  puis en appliquant une porte de Hadamard sur chacun d'entre eux. L'action de l'oracle sur une telle entrée permet d'obtenir, par linéarité, l'action de la fonction  $f$  sur chacun des  $N$  entrées classiques

$$\mathcal{C}|s\rangle|0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle \quad (1.16)$$

$$U_f|s\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle. \quad (1.17)$$

### 1.3.1.3 Interférence quantique

Le calcul quantique semble disposer d'une immense puissance de parallélisation. Toutefois, la mesure du registre de  $n$  qubits ne fournit qu'une sortie classique  $x \in \{0,1\}^n$  ne contenant que  $n$  bits classiques d'information. Une idée (naïve) serait de cloner l'état (1.16) afin de pouvoir extraire plus d'information. Or, Żurek et Wootters ont montré que la linéarité de la mécanique quantique interdit le clonage de l'information quantique [75]. Ce résultat est fondamental dans la distinction entre information classique et quantique.

L'état 1.16 obtenu, l'interférométrie est utilisée pour ne garder que l'information pertinente, qui sera révélée par la mesure. Un ordinateur quantique est donc un gigantesque interféromètre et l'interférométrie est sans doute l'étape la plus délicate dans le développement d'algorithmes quantiques.

### 1.3.2 Algorithme de Grover

Afin de mettre en oeuvre les notions introduites précédemment, intéressons-nous au problème qui consiste à chercher un élément particulier dans une liste dépourvue de structure.

#### Problème

Soit  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  tel que  $\exists! w \in \{0, 1\}^n$  tel que  $f(w) = 1$ .

Déterminer  $w \in \{0, 1\}^n$  parmi les  $N = 2^n$  possibilités.

D'un point de vue informatique, il s'agit d'un problème pour lequel la fonction  $f$  est calculée par un oracle, notion introduite en 1.3.1.1. Ainsi, la fonction  $f$  n'est connue qu'à travers des appels à cet oracle. Classiquement, le nombre moyen d'appels à l'oracle nécessaires afin de déterminer  $w$  vaut  $N/2$ . Autrement dit, le nombre d'appels est proportionnel à  $N$  et grandit donc linéairement avec la taille du problème. En 1996, L. Grover a exhibé un algorithme quantique permettant de déterminer  $w$  avec un nombre d'appels à l'oracle proportionnel à  $\sqrt{N}$  [38].

#### 1.3.2.1 Opérateurs de l'algorithme de Grover

Cet algorithme repose sur l'utilisation de deux opérateurs unitaires. Un de ces deux opérateurs n'est autre que l'opérateur unitaire  $U_f$  correspondant à l'oracle. Dans le cas simple où  $w$  est unique, cet opérateur se réécrit sous la forme

$$U_f = \mathbf{1} - 2|w\rangle\langle w|. \quad (1.18)$$

Insistons sur le fait qu'il n'est pas nécessaire de construire  $U_f$ , qui est donné par une boîte noire. Par contre, la structure de  $U_f$  est connue, dans la mesure où il est connu que  $U_f$  est de la forme de (1.18) *sans que la valeur de  $w \in \{0, 1\}^n$  ne soit connue.*<sup>10</sup>

---

<sup>10</sup>Par exemple, supposons que nous disposions de  $N = 2^n$  ions dont un et un seul dans son état excité alors que les autres sont dans leur état fondamental. L'interaction entre un électron et un des ions durant une durée fixée  $\tau$  va permettre de distinguer l'ion excité des autres. En effet, le fait que l'ion soit excité introduit une différence d'énergie  $\Delta E$  qui se traduit par un déphasage  $e^{-i\Delta E\tau}$ .

L'autre opérateur correspond à l'inversion par rapport à la moyenne. Il n'est pas défini directement dans la base de calcul, mais plutôt introduit dans sa base propre avant de le ramener dans la base de calcul. Soit l'opérateur

$$P : |x\rangle \mapsto \begin{cases} |x\rangle & \text{si } x = 0^n \\ -|x\rangle & \text{sinon.} \end{cases}$$

qui se réécrit  $P = 2|0\rangle\langle 0| - \mathbf{1}$ . L'opérateur d'inversion par rapport à la moyenne est défini par

$$U_D = \mathbb{H}^{\otimes n} P \mathbb{H}^{\otimes n} \quad (1.19)$$

où  $\mathbb{H}$  est la porte de Hadamard. L'opérateur d'inversion par rapport à la moyenne  $U_D$  se réécrit

$$U_D = 2|s\rangle\langle s| - \mathbf{1}. \quad (1.20)$$

Dans l'algorithme de Grover, une itération est définie par  $U_D U_f$ .

### 1.3.2.2 Description de l'algorithme

La première étape de l'algorithme consiste à initialiser les  $n$  qubits dans l'état  $|0\rangle^{\otimes n}$ . Cette étape est cruciale afin de pouvoir effectuer un calcul quantique. Expérimentalement, pouvoir initialiser un système quantique dans un état bien déterminé est hautement non-trivial. Une fois cet état initialisé, l'application de portes de Hadamard sur chacun des qubits permet d'obtenir l'état  $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$ .

Le cœur de l'algorithme consiste à effectuer  $m$  itérations de Grover, c'est-à-dire d'appliquer  $m$  fois l'opérateur  $U_D U_f$ . Ainsi, nous nous intéressons à l'état  $|\psi_i\rangle$  en sortie de la  $i$ ème itérations de Grover. Mathématiquement, nous étudions donc la suite  $\{|\psi_i\rangle\}_{i \in \llbracket 0; m \rrbracket}$  définie par

$$\begin{cases} |\psi_0\rangle = |s\rangle \\ |\psi_{i+1}\rangle = U_D U_f |\psi_i\rangle. \end{cases}$$

L'analyse mathématique de l'algorithme se fait simplement dans le sous-espace engendré par  $|w\rangle$  et  $\sum_{x \neq w} |x\rangle$  puisque pour tout  $i$ , l'état  $|\psi_i\rangle$  évolue dans ce sous-espace et s'exprime donc sous la forme

$$|\psi_i\rangle = k_i |w\rangle + \ell_i \sum_{x \neq w} |x\rangle.$$

L'objectif est alors de minimiser  $\ell_i$ . Un calcul simple<sup>11</sup> montre que

$$|\psi_{i+1}\rangle = \left( \frac{N-2}{N} k_i + \frac{2(N-1)}{N} \ell_i \right) |w\rangle + \left( -\frac{2}{N} k_i + \frac{N-2}{N} \ell_i \right) \sum_{x \neq w} |x\rangle.$$

Ceci définit les relations de récurrence de deux suites réelles  $\{k_i\}$  et  $\{\ell_i\}$  dont la solution est

$$\begin{cases} k_i = \sin((2i+1)\theta) \\ \ell_i = \frac{1}{\sqrt{N-1}} \cos((2i+1)\theta) \end{cases}$$

où  $\theta \in ]0; \frac{\pi}{2}]$  est défini par  $\sin^2 \theta = \frac{1}{N}$ . En se souvenant que  $m$  est restreint à être un entier, la valeur optimale de  $m$  est  $\tilde{m} = \left\lfloor \frac{\pi}{4} \sqrt{N} \right\rfloor$  afin que  $|\psi_{\tilde{m}}\rangle$  soit très proche de  $|w\rangle$ , c'est-à-dire qu'une mesure dans la base de calcul de l'état quantique obtenu après  $\tilde{m}$  itérations fournit  $w \in \{0, 1\}^n$  avec grande probabilité. La probabilité de mesurer un autre état que  $|w\rangle$  est alors inférieure à  $1/N$ .

### 1.3.3 Remarques sur le calcul quantique

Contrairement à certaines idées répandues, rien ne prouve à l'heure actuelle la supériorité théorique du calcul quantique par rapport au calcul classique. En effet, nous savons seulement que par rapport à certains oracles, le calcul quantique est plus puissant (cas de Grover) et que certains algo-

---

<sup>11</sup>L'approche utilisée ici reprend celle du cours "Introduction à l'informatique quantique" enseigné par Gilles Brassard à l'Université de Montréal. Son approche est reprise dans un livre à paraître [17].

rithmes quantiques sont plus efficaces que le meilleur algorithme classique *connu* (cas des algorithmes de Shor [69] et NAND tree [34]). Un autre bémol est lié au nombre limité d’algorithmes quantiques qui ont été découverts jusqu’à maintenant. Cet état de fait est sans doute lié à la difficulté de trouver des problèmes pour lesquels l’algorithmique quantique apporte un avantage par rapport à l’algorithmique classique. Pour une discussion intéressante sur ce dernier point, lire l’article de Peter Shor [70].

## Algorithmes quantiques et décohérence

L’exemple de l’algorithme de Grover a mis en évidence deux phénomènes cruciaux : le parallélisme et l’interférence quantiques. Le parallélisme est intimement lié à la linéarité de la mécanique quantique. Cette linéarité se manifeste par le principe de superposition et par la linéarité de l’évolution. En particulier, le principe de superposition affirme que si  $|\psi_1\rangle$  et  $|\psi_2\rangle$  sont des états possibles du système alors toute combinaison linéaire  $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$  est aussi un état possible (à la normalisation près). Il traite donc sur un pied d’égalité tous les états possibles du système. Or, nous allons montrer que l’interaction du système avec son environnement induit des règles de super-sélection qui privilégient certains états. En particulier, cela aura pour effet de détruire la cohérence d’une superposition d’états arbitraires avec toutes les conséquences dramatiques que cela entraîne pour le calcul quantique. En effet, une fois la cohérence éliminée ou à tout le moins réduite, le processus d’interférence sera alors inefficace puisque les corrélations quantiques auront été converties en corrélations classiques.

Le prochain chapitre va introduire les outils nécessaires à la description d’un système quantique en interaction avec son environnement. En particulier, nous y montrerons qu’un sous-système ne peut pas toujours être décrit par un vecteur d’état dans l’espace de Hilbert et que la notion de ket doit être généralisée à celle d’opérateur densité.



# Chapitre 2

## Systeme quantique ouvert

Comme nous l'avons vu dans le chapitre 1, un système quantique, dont l'état est décrit par un vecteur de l'espace de Hilbert, peut être constitué de plusieurs sous-systèmes intriqués les uns par rapport aux autres. Dans ce cas, il n'est pas possible de décrire l'état de ces sous-systèmes par un vecteur dans leurs espaces de Hilbert respectifs. Il faut alors faire appel à la notion d'*opérateur densité*.

Une fois capable de décrire l'état d'un sous-système, nous nous intéresserons à la description d'une évolution quantique du système global, mais *du point de vue du sous-système*. Cette description fera intervenir la notion de superopérateur ou canal quantique qui décrit l'évolution d'un opérateur densité. De plus, nous nous attarderons à la description d'une mesure effectuée sur le système global, toujours du point de vue du sous-système. Ceci nous amènera à introduire la notion de POVM qui généralise les mesures projectives.

Équipés de ce formalisme, il nous sera alors possible de s'attaquer à la théorie de la décohérence dont l'intérêt, voire même la nécessité, seront mis en évidence dans le prochain chapitre.

## 2.1 Opérateur densité

### 2.1.1 Cas pur

Ce paragraphe s'inspire du cours « Cohérence quantique et dissipation » enseigné par Jean Dalibard à l'École Normale Supérieure, rue d'Ulm à Paris. Les notes [27] de ce cours sont disponibles à l'adresse suivante [http://www.phys.ens.fr/~dalibard/Notes\\_de\\_cours/magistere\\_2006.pdf](http://www.phys.ens.fr/~dalibard/Notes_de_cours/magistere_2006.pdf).

Soit un système dont l'état est décrit par un vecteur  $|\psi\rangle \in \mathcal{H}$ . Il est également possible de décrire l'état par le projecteur associé à ce vecteur, qui n'est autre que  $\rho = |\psi\rangle\langle\psi|$ . Ceci peut paraître superflu, mais notons que cette description a déjà l'avantage d'éliminer la phase globale puisque pour toute phase  $\phi$ , les états  $e^{i\phi}|\psi\rangle$  seront tous associés au même projecteur. Il est maintenant possible de reformuler les postulats concernant la mesure et l'évolution d'un système physique en termes d'opérateur densité.

Soit  $O$  une observable dont la décomposition spectrale est  $O = \sum_{\lambda} \lambda \Pi_{\lambda}$ . La probabilité de mesurer  $\lambda$  est donnée par  $\mathcal{P}(\lambda) = \sum_k |\langle\phi_k|\psi\rangle|^2$  où  $\{|\phi_k\rangle\}$  est une famille orthonormale formant une base du sous-espace propre associé à  $\lambda$ . Or, cette probabilité se réécrit simplement  $\mathcal{P}(\lambda) = \sum_k \langle\phi_k|\psi\rangle\langle\psi|\phi_k\rangle = \sum_k \langle\phi_k|\rho|\phi_k\rangle = \text{Tr}\Pi_{\lambda}\rho$ . Ainsi, la probabilité de mesurer  $\lambda$  est donnée par

$$\mathcal{P}(\lambda) = \text{Tr}\Pi_{\lambda}\rho. \quad (2.1)$$

En particulier, l'espérance de la mesure de  $\mathcal{O}$  est

$$\langle\mathcal{O}\rangle = \text{Tr}\rho\mathcal{O}.$$

Finalement, l'état du système après mesure de la valeur propre  $\lambda$  est

$$\rho = \frac{1}{\mathcal{P}(\lambda)}\Pi_{\lambda}\rho\Pi_{\lambda}. \quad (2.2)$$

Ainsi, l'utilisation de l'opérateur densité est tout particulièrement adaptée

à la description d'une mesure quantique.

Qu'en est-il de l'équation d'évolution? Soit  $H(t)$  l'hamiltonien du système. Calculons la variation infinitésimale de  $\rho$

$$\begin{aligned} i\frac{d\rho}{dt} &= i\frac{d|\psi\rangle\langle\psi|}{dt} + i|\psi\rangle\frac{d\langle\psi|}{dt} \\ &= H|\psi\rangle\langle\psi| - |\psi\rangle\langle\psi|H^\dagger \\ &= [H, \rho]. \end{aligned}$$

Ainsi, l'équation de Schrödinger se réécrit simplement

$$i\frac{d}{dt}\rho(t) = [H(t), \rho(t)]. \quad (2.3)$$

Si  $U(t)$  est l'opérateur d'évolution tel que  $|\psi(t)\rangle = U(t)|\psi(0)\rangle$ , alors

$$\rho(t) = U\rho(0)U^\dagger.$$

Nous voyons donc que les postulats habituels de la mécanique quantique se réexpriment facilement en terme de l'opérateur densité. Pour les vecteurs d'état, la structure d'espace vectoriel mène à la notion de superposition. Est-il possible de donner un sens à une combinaison linéaire de projecteurs?

### 2.1.2 Intrication et trace partielle

Nous avons vu en (1.2.2.1) qu'un système est dit intriqué lorsqu'il n'est pas possible de décrire l'état de chacun des sous-systèmes par un vecteur d'état dans l'espace de Hilbert. Est-il toutefois possible de donner une description partielle de l'état d'un tel sous-système?

Supposons que nous ayons entre les mains une moitié de paire EPR. Le résultat d'une mesure sur notre moitié sera très fortement corrélé avec le résultat obtenu sur l'autre moitié. Or, il est concevable que l'autre moitié nous soit, à toute fin pratique, inaccessible. D'où la question suivante : comment décrire l'état d'un sous-système intriqué si l'on se restreint à des mesures lo-

cales sur ce sous-système sans avoir accès au reste du système intriqué? La réponse à cette question fera naturellement intervenir la notion d'opérateur densité réduit et fournira un sens physique à cet objet.

Soit un système divisé en deux sous-systèmes désignés par  $A$  et  $B$ . Un tel système sera dorénavant qualifié de *biparti*. L'espace de Hilbert associé à ce système s'écrit  $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^B$  et supposons que son état initial soit  $|\psi^{AB}\rangle = \sum_{ik} c_{ik} |i^A\rangle \otimes |k^B\rangle$  où  $\{|i^A\rangle\}_{i \in I}$  et  $\{|k^B\rangle\}_{k \in K}$  sont des bases orthonormales de  $\mathcal{H}^A$  et  $\mathcal{H}^B$ . Son opérateur densité s'écrit donc

$$\rho^{AB} = \sum_{ijkl} c_{ik} c_{jl}^* |i^A\rangle \langle j^A| \otimes |k^B\rangle \langle l^B|. \quad (2.4)$$

Supposons maintenant que seul le sous-système  $A$  soit accessible, c.-à-d. qu'il nous est donc seulement possible d'effectuer une mesure sur  $A$ . Une telle mesure sera décrite par une observable de la forme  $O^A \otimes \mathbf{1}^B$ . La probabilité de mesurer une valeur propre  $\lambda$  de  $O_A$  est alors

$$\begin{aligned} \mathcal{P}(\lambda) &= \text{Tr} [(\Pi_\lambda^A \otimes \mathbf{1}^B) \rho^{AB}] \\ &\stackrel{(2.4)}{=} \sum_{ijkl} c_{ik} c_{jl}^* \text{Tr} [\Pi_\lambda^A |i^A\rangle \langle j^A| \otimes |k^B\rangle \langle l^B|] \\ &= \sum_{ijkl} c_{ik} c_{jl}^* \text{Tr} [\Pi_\lambda^A |i^A\rangle \langle j^A|] \text{Tr} [|k^B\rangle \langle l^B|] \\ &= \text{Tr} \left[ \Pi_\lambda^A \left( \sum_{ijkl} c_{ik} c_{jl}^* \delta_{kl} |i^A\rangle \langle j^A| \right) \right] \\ &= \text{Tr} [\Pi_\lambda^A \rho^A]. \end{aligned} \quad (2.5)$$

Ainsi, la probabilité de mesure ne dépend que d'un opérateur sur  $\mathcal{H}^A$ , noté  $\rho^A$ , qui est obtenu grâce à une opération linéaire dite de *trace partielle* qui est définie par

$$\text{Tr}_B : \begin{array}{ccc} \mathcal{L}(\mathcal{H}^A \otimes \mathcal{H}^B) & \rightarrow & \mathcal{L}(\mathcal{H}^A) \\ |\phi^A\rangle \langle \xi^A| \otimes |\varphi^B\rangle \langle \chi^B| & \mapsto & \langle \chi^B | \varphi^B \rangle |\phi^A\rangle \langle \xi^A|. \end{array} \quad (2.6)$$

L'opérateur densité réduit  $\rho^A = \text{Tr}_B \rho^{AB}$ , appelé *trace partielle de  $\rho^{AB}$  sur  $B$* , contient donc toute l'information qui peut être extraite par mesure sur le sous-système  $A$ . En ce sens, cet opérateur représente l'état du sous-système  $A$  pour un observateur qui n'a pas accès au sous-système  $B$ .<sup>1</sup>

Le résultat que nous venons de démontrer peut être généralisé grâce au lemme suivant, qui nous sera fort utile dans la suite :

**Lemme 2.1.** *Soit un système biparti  $AB$  dans l'état  $\rho^{AB}$ . Pour tout opérateur linéaire  $O^A$  agissant sur le sous-système  $A$ , on a*

$$\text{Tr}_B [(O^A \otimes \mathbf{1}^B) \rho^{AB}] = O^A \text{Tr}_B [\rho^{AB}]. \quad (2.7)$$

*Démonstration.* Par linéarité, il suffit de montrer le résultat pour  $\rho^{AB}$  de la forme  $\rho^{AB} = |\psi^A\rangle\langle\phi^A| \otimes |\xi^B\rangle\langle\chi^B|$ . On a alors

$$\begin{aligned} \text{Tr}_B [(O^A \otimes \mathbf{1}^B) \rho^{AB}] &= \text{Tr}_B [(O^A \otimes \mathbf{1}^B) (|\psi^A\rangle\langle\phi^A| \otimes |\xi^B\rangle\langle\chi^B|)] \\ &= \text{Tr}_B [(O^A |\psi^A\rangle\langle\phi^A|) \otimes (|\xi^B\rangle\langle\chi^B|)] \\ &= (O^A |\psi^A\rangle\langle\phi^A|) \langle\chi^B|\xi^B\rangle \\ &= O^A (\langle\chi^B|\xi^B\rangle |\psi^A\rangle\langle\phi^A|) \\ &= O^A \text{Tr}_B [\rho^{AB}]. \end{aligned}$$

□

Ce résultat signifie que, *du point de vue du sous-système  $A$* , l'application de  $O^A$  n'agissant que sur  $A$  suivie de la perte du système  $B$  est équivalente à la perte du sous-système  $B$  suivie de l'application de  $O^A$  sur  $A$ .

Attardons-nous aux propriétés d'un opérateur densité réduit.

1.  $\rho^A$  est hermitien car

$$(\rho^A)^\dagger = \left( \sum_{ijk} c_{ik} c_{jk}^* |i^A\rangle\langle j^A| \right)^\dagger = \sum_{ijk} c_{ik}^* c_{jk} |j^A\rangle\langle i^A| = \text{Tr}_B (\rho^{AB})^\dagger = \rho^A.$$

<sup>1</sup>Pour un opérateur linéaire  $O$  défini sur  $\mathcal{H}^A$ , la trace partielle de  $O$  sur  $A$  correspond à la définition habituelle de la trace, autrement dit  $\text{Tr}_A O = \text{Tr} O$ .

Autrement dit,  $(\text{Tr}_B [\rho^{AB}])^\dagger = \text{Tr}_B [(\rho^{AB})^\dagger]$ .

2. Sa trace vaut 1 car

$$\text{Tr}_A \sum_{ijk} c_{ik} c_{jk}^* |i^A\rangle \langle j^A| = \sum_{ik} |c_{ik}|^2 = \text{Tr}_{AB} \rho^{AB} = 1.$$

Autrement dit,  $\text{Tr}_A [\text{Tr}_B [\rho^{AB}]] = \text{Tr}_{AB} [\rho^{AB}]$ .

3.  $\rho^A$  est positif<sup>2</sup> car pour tout vecteur  $|\psi^A\rangle \in \mathcal{H}^A$

$$\begin{aligned} \langle \psi^A | \rho^A | \psi^A \rangle &= \text{Tr}_A [|\psi^A\rangle \langle \psi^A | \rho^A] \\ &= \text{Tr}_{AB} [(|\psi^A\rangle \langle \psi^A | \otimes \mathbf{1}^B) \rho^{AB}] \stackrel{(2.5)}{\geq} 0. \end{aligned}$$

Le postulat selon lequel tout système quantique est décrit par un vecteur d'état dans l'espace de Hilbert n'est pas cohérent si on accepte qu'un sous-système d'un système quantique est lui-même un système quantique. En effet, dès que le système quantique est dans un état intriqué par rapport à ses sous-systèmes, l'état de ces derniers est en général décrit par un opérateur densité qui ne correspond pas à un vecteur d'état. Schrodinger, dès 1935, affirmait que « la caractérisation complète d'un système n'implique pas la caractérisation de chacune de ses parties ».<sup>3</sup> Par exemple, soient deux qubits dans un état singulet  $|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$  dont l'opérateur densité est

$$\rho^{AB} = |\Psi^-\rangle \langle \Psi^-| = \frac{1}{2}|01\rangle \langle 01| - \frac{1}{2}|01\rangle \langle 10| - \frac{1}{2}|10\rangle \langle 01| + \frac{1}{2}|10\rangle \langle 10|$$

L'état de l'un des deux qubits est décrit par un opérateur densité

$$\rho^A = \text{Tr}_B \rho^{AB} = \frac{1}{2}|0\rangle \langle 0| + \frac{1}{2}|1\rangle \langle 1| \quad (2.8)$$

Cet opérateur densité n'est clairement pas un projecteur car  $\rho^2 \neq \rho$ .

<sup>2</sup>Nous suivons ici la terminologie française selon laquelle un réel  $a$  est *positif* s'il vérifie  $a \geq 0$  et *négatif* s'il vérifie  $a \leq 0$ .

<sup>3</sup>Traduction libre de l'auteur à partir de la traduction de l'allemand à l'anglais réalisée par John D. Trimmer [71] à partir de l'article original de Schrodinger [68].

### 2.1.3 État quantique

La discussion précédente a montré, qu'en général, l'état d'un système quantique ne peut pas être décrit par un ket dans un espace de Hilbert, mais seulement par un opérateur densité. Un tel état est appelé *état mixte*<sup>4</sup> ou *état mélangé* en raison de l'interprétation qui peut être donnée de ces états. Au contraire, les états décrits par un ket sont nommés *états purs*. Donnons maintenant une définition formelle à la notion d'état quantique.

#### 2.1.3.1 Définition formelle

**Définition 2.2.** [État quantique] L'état quantique d'un système quantique auquel correspond un espace de Hilbert  $\mathcal{H}$  est décrit par un opérateur densité  $\rho$ , c'est-à-dire un opérateur linéaire de  $\mathcal{H}$  dans lui-même qui vérifie les propriétés suivantes

1.  $\rho$  est hermitien, c.-à-d.  $\rho^\dagger = \rho$ .
2.  $\text{Tr}\rho = 1$ .
3.  $\rho$  est positif, c.-à-d. pour tout  $|\psi\rangle$  dans  $\mathcal{H}$   $\langle\psi|\rho|\psi\rangle \geq 0$ .

L'ensemble des opérateurs densité sur un espace de Hilbert  $\mathcal{H}$  est noté  $\mathcal{D}(\mathcal{H})$ .

Cette définition est cohérente avec les propriétés auxquelles obéit un opérateur densité réduit obtenu par trace partielle. Nous allons d'ailleurs voir qu'un système dans un état mixte peut toujours être vu comme un sous-système d'un système plus grand dans un état pur.

#### 2.1.3.2 État à 1 qubit : boule de Bloch

Dans le cas d'un qubit, un état peut être représenté graphiquement. Notons qu'un état pour un qubit est décrit par un opérateur densité  $\rho$  sur un espace de Hilbert à deux dimensions, que nous confondrons avec son expression dans la base de calcul. La matrice  $\rho$  est hermitienne et peut donc

---

<sup>4</sup>L'emploi de ce terme va malheureusement (à l'heure actuelle) à l'encontre de l'usage courant en français.

être décomposée sur la base constituée de l'identité et des trois matrices de Pauli. Or, les trois matrices de Pauli sont de trace nulle et  $\rho$  doit être de trace unité. Donc, la décomposition de  $\rho$  est de la forme

$$\rho = \frac{1}{2} \left( \mathbf{1} + \sum_{i=1}^3 p_i \sigma_i \right). \quad (2.9)$$

De plus,  $\rho$  est une matrice positive. La somme de ses valeurs propres vaut 1 (car  $\text{Tr}\rho = 1$ ). Il faut et il suffit donc d'imposer que le produit des valeurs propres soit positif pour que  $\rho$  le soit. Or, le produit des valeurs propres de  $\rho$  est son déterminant qui vaut

$$\det\rho = \frac{1}{4} (1 - \|\mathbf{p}\|^2).$$

Ainsi,  $\rho$  est un opérateur densité à 1 qubit si et seulement si  $\rho$  a une décomposition du type de (2.9) avec un vecteur  $\mathbf{p} = (p_1, p_2, p_3)$  qui est de norme inférieure à 1. De plus, un calcul immédiat montre que

$$\rho^2 = \frac{1}{4} (1 + \|\mathbf{p}\|^2) \mathbf{1} + \frac{1}{2} \mathbf{p} \cdot \boldsymbol{\sigma}$$

qui permet de conclure qu'un état est pur si et seulement si  $\|\mathbf{p}\| = 1$ . Or, nous savons que les états purs à un qubit peuvent être représentés sur la *sphère* de Bloch. Il est alors cohérent de représenter un état *quelconque* par un point de la *boule* de Bloch (voir figure 2.1), repéré par le vecteur  $\mathbf{p}$ .

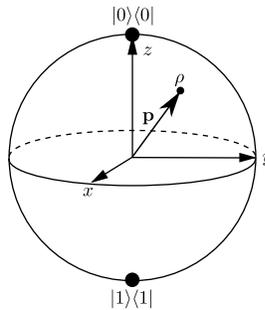


Figure 2.1 – Boule de Bloch

### 2.1.3.3 Interprétations

Comment interpréter l'état d'un système quantique décrit par un opérateur densité? Un élément de réponse est donné par le théorème de décomposition spectrale qui permet d'écrire tout opérateur densité de la façon suivante

$$\rho = \sum_x p_x |\psi_x\rangle\langle\psi_x| \quad (2.10)$$

où les  $p_x$  sont des nombres réels et les  $|\psi_x\rangle$  forment une famille orthonormée. De plus, la positivité montre que  $\forall x p_x \geq 0$  et la normalisation impose  $\sum_x p_x = 1$ . Ces propriétés suggèrent fortement une interprétation des facteurs  $p_x$  en terme de probabilité. Nous allons proposer deux interprétations possibles : l'une est liée à un manque d'information accessible à l'observateur qui décrit l'état quantique tandis que dans l'autre, l'état du système global est parfaitement connu, mais l'observateur n'a accès qu'à un sous-système. Nous verrons que les deux interprétations sont équivalentes en raison de la possibilité de *purifier* un état mixte.

**Mélange statistique et manque d'information** Un système quantique dont l'état est mixte peut être interprété comme un mélange statistique d'états purs  $\{(|\psi_k\rangle, p_k)\}$  où

$$\forall k p_k \in [0; 1] \quad \text{et} \quad \sum_k p_k = 1,$$

c'est-à-dire un système dans un état pur qui est  $|\psi_k\rangle$  avec probabilité  $p_k$ . Dans ce cas, il existe une incertitude sur l'état initial qui se traduit par une description en tant que somme pondérée d'états purs. L'incertitude sur un tel état est habituellement quantifiée par l'entropie de von Neumann.

**Définition 2.3.** L'entropie de von Neumann d'un système quantique dans l'état  $\rho$  est donnée par

$$S(\rho) \equiv -\text{Tr} [\rho \log_2 \rho]. \quad (2.11)$$

Un calcul immédiat montre que si  $\rho$  a pour valeurs propres  $\{p_x\}$ , son entropie de von Neumann vaut

$$S(\rho) = - \sum_x p_x \log_2 p_x. \quad (2.12)$$

**Proposition 2.4.** *Pour un système quantique de dimension  $N$ , l'entropie de von Neumann vaut 0 pour un état pur et atteint son maximum  $\log_2 N$  pour l'état dit complètement mélangé  $\frac{1}{N}\mathbf{1}$ .*

Un qubit dans l'état complètement mélangé est un qubit qui, lorsque mesuré par n'importe quelle observable, fournira n'importe quelle valeur propre de façon équiprobable. Ainsi, seul, il ne contient aucune information utile.

Une description en terme de mélange statistique intervient par exemple lorsqu'un qubit dans l'état pur  $|\psi\rangle$  a été mesuré par rapport à l'observable  $O = \sum \lambda_k |\phi_k\rangle\langle\phi_k|$ , mais que le résultat de la mesure n'est pas connu. L'état sera alors décrit par

$$\rho = \sum_k |\langle\psi|\phi_k\rangle|^2 |\phi_k\rangle\langle\phi_k|. \quad (2.13)$$

Une telle description est très différente d'une superposition linéaire des  $|\phi_k\rangle$  car dans le cas de l'opérateur densité, il n'y a aucune cohérence de phase entre les  $|\phi_k\rangle$  alors que ces phases sont bien définies pour une superposition.

Notons qu'un opérateur densité  $\rho$  correspond à l'état de plusieurs mélanges statistiques et que ces mélanges statistiques sont donc indistinguables. Par exemple, l'état complètement mélangé à deux qubits  $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$  correspond au mélange statistique  $\{(|0\rangle, \frac{1}{2}), (|1\rangle, \frac{1}{2})\}$  mais aussi à tous les mélanges statistiques  $\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}$  où  $|\psi\rangle$  est un état pur à 1 qubit auquel est appliqué les matrices de Pauli  $X$  et  $Z$ .

Vérifions ce résultat en prenant  $|\psi\rangle = a|0\rangle + b|1\rangle$

$$\begin{aligned}
\rho &= \frac{1}{4}|\psi\rangle\langle\psi| + \frac{1}{4}X|\psi\rangle\langle\psi|X + \frac{1}{4}Z|\psi\rangle\langle\psi|Z + \frac{1}{4}XZ|\psi\rangle\langle\psi|ZX \\
&= \frac{1}{4} \begin{pmatrix} |a|^2 & a^*b \\ ab^* & |b|^2 \end{pmatrix} + \frac{1}{4} \begin{pmatrix} |b|^2 & ab^* \\ a^*b & |a|^2 \end{pmatrix} \\
&\quad + \frac{1}{4} \begin{pmatrix} |a|^2 & -a^*b \\ -ab^* & |b|^2 \end{pmatrix} + \frac{1}{4} \begin{pmatrix} |b|^2 & -ab^* \\ -a^*b & |a|^2 \end{pmatrix} \\
&= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned} \tag{2.14}$$

Finalement, notons que pour un état pur, la décomposition de l'opérateur densité est unique. Ceci justifie le terme *pur* puisqu'il n'y a aucune incertitude sur l'état. D'un point de vue géométrique, les états purs correspondent aux points extrémaux de l'ensemble des opérateurs densité.

**Système intriqué et purifications** Un système quantique dont l'état est mixte peut toujours être considéré comme un sous-système d'un système plus grand qui est dans un état pur. Ainsi, partant d'un système  $A$  dont l'état est donné par  $\rho^A$ , il est toujours possible de lui adjoindre un système de référence noté  $R$  de telle façon que le système  $AR$  soit dans un état pur  $|\Psi^{AR}\rangle$  et que  $\rho^A = \text{Tr}_R|\Psi^{AR}\rangle\langle\Psi^{AR}|$ . Un tel état est appelé une *purification de*  $\rho^A$ . Une méthode permettant d'obtenir une purification consiste à calculer la décomposition spectrale de  $\rho^A = \sum_k p_k |\psi_k^A\rangle\langle\psi_k^A|$ , puis de considérer l'état

$$|\Psi^{AR}\rangle = \sum_k \sqrt{p_k} |\psi_k^A\rangle \otimes |k^R\rangle \tag{2.15}$$

où  $\{|k^R\rangle\}$  est une famille orthonormée de  $\mathcal{H}^R$ . La trace partielle sur  $R$  fournit un opérateur densité réduit

$$\rho^A = \sum_k p_k |\psi_k^A\rangle\langle\psi_k^A|. \tag{2.16}$$

Ainsi, tout mélange statistique peut être interprété comme un sous-système d'un système qui est dans un état pur. Ainsi, la connaissance limitée de l'observateur est due au fait qu'il n'a accès qu'à un sous-système intriqué d'un système global dont l'état *global* est parfaitement déterminé. Une question métaphysique est alors de savoir si le système de référence  $R$  existe au-delà de la construction mathématique que nous avons présentée.

**Lien entre les deux interprétations** Les deux interprétations reposent sur des hypothèses distinctes : la première suppose une indétermination de l'état du système alors que la seconde postule que le système est intriqué avec un autre système auquel il n'est pas possible d'avoir accès. Nous allons montrer que la seconde interprétation mène à la première. En fait, les deux interprétations sont équivalentes si on accepte que la mesure est la seule source d'indétermination en mécanique quantique.

Afin de discuter d'un système qui se décompose en deux sous-systèmes  $A$  et  $B$ , il est très pratique d'introduire deux personnages nommés Alice et Bob, en accord avec la tradition des informaticiens<sup>5</sup>. Chacun détient un des deux sous-systèmes quantiques. Soient donc Alice et Bob qui possèdent chacun une partie d'un système dans un état intriqué  $|\Psi\rangle$

$$|\Psi\rangle = \sum_{ij} \sqrt{p_{ij}} |i^A\rangle |j^B\rangle. \quad (2.17)$$

où  $\{|i^A\rangle\}_{i \in I}$  et  $\{|j^B\rangle\}_{j \in J}$  sont des familles orthonormées. Alice et Bob connaissent tous les deux l'état  $|\Psi\rangle$  qu'ils partagent. Alice cherche maintenant à décrire l'état  $\rho^A$  de son sous-système. Elle peut le calculer directement en effectuant une trace partielle sur  $B$ .

Elle peut aussi faire le raisonnement suivant :

Si Bob mesure son système dans la base  $\{|j^B\rangle\}$  et qu'il obtient  $j_0$ , mon état (non-normalisé) sera alors  $|\phi_{j_0}\rangle = \sum_i \sqrt{p_{ij_0}} |i^A\rangle$ . La

---

<sup>5</sup>Le physicien David Mermin a affirmé qu'une des contributions fondamentales de l'informatique à la physique au sens large est l'introduction d'Alice et Bob!

probabilité pour Bob d'obtenir  $j_0$  est  $\mathcal{P}_{j_0} = \sum_i p_{ij_0}$ . Or, je ne connais pas le résultat de la mesure de Bob donc mon système sera un mélange statistique  $\left\{ \left( \mathcal{P}_{j_0}, \frac{1}{\sqrt{\mathcal{P}_{j_0}}} |\phi_{j_0}\rangle \right) \right\}_{j_0 \in J}$ , c.-à-d. un mélange statistique pondéré où  $j_0$  peut prendre n'importe quelle valeur dans  $J$ .

Faut-il vraiment que Bob mesure son système pour que cette description soit correcte du point de vue d'Alice? Si c'était le cas, autrement dit si le fait que Bob ait mesuré son système entraîne une différence mesurable chez Alice, Alice pourrait déterminer instantanément si Bob a effectué une mesure et ce indépendamment de la distance entre eux. Autrement dit, Bob pourrait envoyer un signal à Alice aussi rapidement qu'il le désire. Afin d'éviter ce paradoxe, *il faut que la description de l'état d'Alice comme un mélange statistique soit correcte indépendamment du fait que Bob ait mesuré (et en particulier de la base de mesure qu'il aurait utilisé).*

Ainsi, l'intrication est une source d'incertitude pour un observateur qui n'a pas accès à une partie du système intriqué. En admettant que la seule source fondamentale d'incertitude soit liée à la mesure, les deux interprétations d'un opérateur densité sont alors réconciliées.

La notion d'opérateur densité réduit trouve une application dans la compréhension du protocole de téléportation quantique, décrit en annexe B.

## 2.2 Mesure généralisée et superopérateur

La section (2.1) a montré que l'état d'un système quantique est généralement donné non pas par un vecteur d'état dans l'espace de Hilbert, mais plutôt par un opérateur densité. Les postulats de la mécanique quantique réécrit en (2.1.1) restent valables pour un état mixte.

Toutefois, ces postulats ne permettent pas de décrire l'évolution d'un sous-système quantique faisant partie d'un système quantique plus grand évoluant sous l'action d'une mesure ou d'une évolution unitaire. Nous allons donc introduire la notion de mesure généralisée et celle de superopérateur.

## 2.2.1 Mesure généralisée

### 2.2.1.1 Observable sur un grand système

Soit un système quantique  $A$  dont l'état est décrit par un opérateur densité  $\rho$ . Nous cherchons à obtenir de l'information sur ce système quantique. Au lieu de mesurer sur  $A$ , il est possible d'adjoindre à  $A$  un système auxiliaire  $R$ , qualifié d'*ancillaire* dans le jargon de l'informatique quantique, puis de mesurer le système conjoint. Une telle mesure est appelée *mesure généralisée*. Nous allons voir que dans ce cas, la mesure résultante sur le sous-système  $A$  n'est pas toujours décrite par une mesure projective.

### 2.2.1.2 POVM

Pour décrire une mesure généralisée, nous nous plaçons dans l'espace de Hilbert  $\mathcal{H} = \mathcal{H}^A \otimes \mathcal{H}^R$ . Nous allons mesurer le système conjoint grâce à une observable  $O \in \mathcal{L}(\mathcal{H})$  dont la décomposition spectrale est

$$O = \sum_{\lambda} \lambda \Pi_{\lambda}. \quad (2.18)$$

L'état initial du système  $AR$  est

$$\rho^{AR} = \rho^A \otimes \rho^R \quad (2.19)$$

puisque les deux systèmes ne sont pas intriqués initialement. La probabilité  $\mathcal{P}(\lambda)$  de mesurer la valeur propre  $\lambda$  est

$$\begin{aligned} \mathcal{P}(\lambda) &= \text{Tr}_{AR} [\Pi_{\lambda} \rho^{AR}] \\ &= \text{Tr}_A [\text{Tr}_R [(\rho^A \otimes \mathbf{1}^R) (\mathbf{1}^A \otimes \rho^R) \Pi_{\lambda}]] \\ &\stackrel{\text{Lemme 2.1}}{=} \text{Tr}_A [\rho^A \text{Tr}_R [(\mathbf{1}^A \otimes \rho^R) \Pi_{\lambda}]] \\ &= \text{Tr}_A [\rho^A E_{\lambda}] \end{aligned} \quad (2.20)$$

et prend donc la même forme que l'équation (2.1) où le projecteur a été remplacé par un opérateur linéaire sur  $\mathcal{H}^A$  défini par

$$E_\lambda = \text{Tr}_R [(\mathbf{1}^A \otimes \rho^R) \Pi_\lambda]. \quad (2.21)$$

Quels sont les propriétés vérifiées par un tel opérateur ?

1.  $E_\lambda$  est hermitien.

$$\begin{aligned} E_\lambda^\dagger &= (\text{Tr}_R [(\mathbf{1}^A \otimes \rho^R) \Pi_\lambda])^\dagger \\ &= \text{Tr}_R [(\mathbf{1}^A \otimes \rho^R) \Pi_\lambda]^\dagger \\ &= E_\lambda. \end{aligned} \quad (2.22)$$

2.  $E_\lambda$  est positif.

$$\begin{aligned} \langle \psi^A | E_\lambda | \psi^A \rangle &= \text{Tr}_A [|\psi^A\rangle\langle\psi^A| E_\lambda] \\ &= \text{Tr}_{AR} [\Pi_\lambda (|\psi^A\rangle\langle\psi^A| \otimes \rho^R)] \geq 0. \end{aligned} \quad (2.23)$$

3. Les  $\{E_\lambda\}$  vérifient la relation de fermeture  $\sum_\lambda E_\lambda = \mathbf{1}^A$ .

$$\begin{aligned} \sum_\lambda E_\lambda &= \sum_\lambda \text{Tr}_R [(\mathbf{1}^A \otimes \rho^R) \Pi_\lambda] \\ &= \text{Tr}_R \left[ (\mathbf{1}^A \otimes \rho^R) \sum_\lambda \Pi_\lambda \right] \\ &= \text{Tr}_R [(\mathbf{1}^A \otimes \rho^R) \mathbf{1}^{AR}] \\ &= \mathbf{1}^A. \end{aligned} \quad (2.24)$$

Ainsi, alors qu'une mesure projective est définie par un ensemble de projecteurs  $\{\Pi_\lambda\}$  donné par la décomposition spectrale de l'observable, une mesure généralisée est définie par un ensemble  $\{E_\lambda\}$  d'opérateurs hermitiens. Une telle mesure est nommée POVM (*Positive Operator Valued Measure*) dans le jargon de l'informatique quantique. Un exemple de situation où une telle mesure généralisée est utile est donné en annexe C.

En conclusion de cette section sur les mesures généralisées, énonçons sans démonstration un résultat qui présente une réciproque à notre approche. Nous avons introduit les POVM en tant que formalisme décrivant une mesure effectuée sur un système augmenté d'un système ancillaire. Un théorème [35] nommé d'après le mathématicien russe M.A. Naimark (parfois orthographié Neumark) indique que tout POVM sur un espace de Hilbert  $\mathcal{H}$  peut être vu comme une mesure projective sur un espace de Hilbert plus grand.

### 2.2.2 Superopérateur

Dans cette section, nous allons chercher à décrire l'évolution quantique d'un sous-système qui fait partie d'un plus grand système qui évolue de façon unitaire. Nous allons voir que l'évolution induite sur le sous-système n'est pas unitaire mais doit respecter plusieurs contraintes afin de toujours envoyer un état quantique valable vers un autre état quantique valable. Ainsi, une telle évolution sera décrite par un opérateur linéaire  $\mathcal{N}$  sur l'espace des opérateurs densité  $\mathcal{D}(\mathcal{H}^A)$ .  $\mathcal{N}$  est couramment appelé superopérateur puisqu'il s'agit d'un opérateur linéaire agissant sur des opérateurs linéaires.

#### 2.2.2.1 Évolution unitaire sur un grand système

Soit un système  $\mathcal{S}$  qui nous intéresse. Habituellement, ce système n'est pas fermé, mais en interaction avec un grand nombre de degrés de liberté qui constituent son environnement  $\mathcal{E}$ . Initialement, supposons que le système et l'environnement ne soient pas intriqués. L'état initial est donc de la forme

$$\rho^{S\mathcal{E}} = \rho^S \otimes |\xi^{\mathcal{E}}\rangle\langle\xi^{\mathcal{E}}| \quad (2.25)$$

où l'environnement peut être pris dans un état pur sans perte de généralité.

Le système  $\mathcal{SE}$  étant en interaction, il va évoluer de façon unitaire et aboutir à l'état global

$$U\rho^{S\mathcal{E}}U^\dagger = U(\rho^S \otimes |\xi^{\mathcal{E}}\rangle\langle\xi^{\mathcal{E}}|)U^\dagger. \quad (2.26)$$

Toutefois, si l'opérateur  $U$  n'est pas séparable, l'évolution du sous-système  $\mathcal{S}$  ne sera pas unitaire. Formellement, l'évolution de  $\rho^{\mathcal{S}}$  est donnée par

$$\rho^{\mathcal{S}} \rightarrow \mathcal{N}(\rho^{\mathcal{S}}) = \text{Tr}_{\mathcal{E}} [U (\rho^{\mathcal{S}} \otimes |\xi^{\mathcal{E}}\rangle\langle\xi^{\mathcal{E}}|) U^\dagger] \quad (2.27)$$

qui *ne peut pas*, en général, s'écrire sous la forme  $V\rho^{\mathcal{S}}V^\dagger$  où  $V$  est unitaire.

**Théorème 2.5.** *Cette équation peut être mise sous la forme*

$$\mathcal{N}(\rho^{\mathcal{S}}) = \sum_k N_k \rho^{\mathcal{S}} N_k^\dagger \quad (2.28)$$

où les

$$N_k = \langle k^{\mathcal{E}} | U | \xi^{\mathcal{E}} \rangle \quad (2.29)$$

sont des opérateurs linéaires sur  $\mathcal{H}^{\mathcal{S}}$  dits de Kraus qui vérifient

$$\sum_k N_k^\dagger N_k = \mathbf{1}. \quad (2.30)$$

*Démonstration.* La preuve est calculatoire. Décomposons l'opérateur  $U$  sous la forme de produit tensoriel d'opérateurs agissant d'une part sur  $\mathcal{H}^{\mathcal{S}}$  et d'autre part sur  $\mathcal{H}^{\mathcal{E}}$ , ce qui revient à choisir une base  $\{|k^{\mathcal{E}}\rangle\}$  sur l'espace  $\mathcal{H}^{\mathcal{E}}$

$$U = \sum_{kl} V_{kl}^{\mathcal{S}} \otimes w_{kl} |k^{\mathcal{E}}\rangle\langle l^{\mathcal{E}}|. \quad (2.31)$$

Calculons alors

$$\begin{aligned} \mathcal{N}(\rho^{\mathcal{S}}) &= \text{Tr}_{\mathcal{E}} [U (\rho^{\mathcal{S}} \otimes |\xi^{\mathcal{E}}\rangle\langle\xi^{\mathcal{E}}|) U^\dagger] \\ &= \text{Tr}_{\mathcal{E}} \left[ \sum_{kl} V_{kl}^{\mathcal{S}} \otimes w_{kl} |k^{\mathcal{E}}\rangle\langle l^{\mathcal{E}}| (\rho^{\mathcal{S}} \otimes |\xi^{\mathcal{E}}\rangle\langle\xi^{\mathcal{E}}|) \sum_{k'l'} V_{k'l'}^{\mathcal{S}} \otimes w_{k'l'}^* |l'^{\mathcal{E}}\rangle\langle k'^{\mathcal{E}}| \right] \\ &= \sum_{kl} \sum_{k'l'} w_{kl} w_{k'l'}^* \langle l^{\mathcal{E}} | \xi^{\mathcal{E}} \rangle \langle \xi^{\mathcal{E}} | l'^{\mathcal{E}} \rangle (V_{kl}^{\mathcal{S}} \rho^{\mathcal{S}} V_{k'l'}^{\mathcal{S}}) \otimes \text{Tr}_{\mathcal{E}} [|k^{\mathcal{E}}\rangle\langle k'^{\mathcal{E}}|] \\ &= \sum_k \left( \sum_l w_{kl} \langle l^{\mathcal{E}} | \xi^{\mathcal{E}} \rangle V_{kl}^{\mathcal{S}} \right) \rho^{\mathcal{S}} \left( \sum_{l'} V_{k'l'}^{\mathcal{S}} w_{k'l'}^* \langle \xi^{\mathcal{E}} | l'^{\mathcal{E}} \rangle \right). \end{aligned}$$

En définissant les opérateurs  $N_k$  par  $N_k = \langle k^\mathcal{E} | U | \xi^\mathcal{E} \rangle \equiv \sum_l w_{kl} \langle l^\mathcal{E} | \xi^\mathcal{E} \rangle V_{kl}^S$ , nous obtenons la relation (2.29).

Vérifions maintenant la relation de fermeture

$$\begin{aligned}
\sum_k N_k^\dagger N_k &= \sum_k \langle \xi | U^\dagger | k \rangle \langle k | U | \xi \rangle \\
&= \langle \xi | U^\dagger \left( \sum_k | k \rangle \langle k | \right) U | \xi \rangle \\
&= \langle \xi | U^\dagger U | \xi \rangle \\
&= \mathbf{1}. \quad \square
\end{aligned}$$

Une décomposition du type de l'équation 2.28 est appelée une décomposition en somme d'opérateurs. Analysons les propriétés vérifiées par une telle décomposition

1.  $\mathcal{N}$  préserve le caractère hermitien de  $\rho$ .

$$(\mathcal{N}(\rho))^\dagger = \sum_k \left( N_k \rho N_k^\dagger \right)^\dagger = \mathcal{N}(\rho). \quad (2.32)$$

2.  $\mathcal{N}$  préserve la trace de  $\rho$ .

$$\mathrm{Tr} [\mathcal{N}(\rho)] = \mathrm{Tr} \left[ \sum_k N_k^\dagger N_k \rho \right] = \mathrm{Tr} \rho. \quad (2.33)$$

3.  $\mathcal{N}$  préserve la positivité de  $\rho$ .

$$\langle \psi | \mathcal{N}(\rho) | \psi \rangle = \mathrm{Tr} \left[ \sum_k N_k \rho^S N_k^\dagger | \psi \rangle \langle \psi | \right] = \mathrm{Tr} \left[ \sum_k (\langle \psi | N_k) \rho^S \left( N_k^\dagger | \psi \rangle \right) \right] \geq 0. \quad (2.34)$$

Ces trois propriétés sont très intuitives puisqu'elles correspondent aux propriétés d'un superopérateur  $\mathcal{N}$  qui envoie un opérateur densité vers un autre opérateur densité. Toutefois,  $\mathcal{N}$  présente une propriété plus forte que la propriété (3). Il s'agit de la propriété de *positivité complète* : pour toute extension de  $\mathcal{H}^S$  à  $\mathcal{H}^S \otimes \mathcal{H}^R$ , l'opérateur  $\mathcal{N} \otimes \mathbf{1}^R$  est

positif. Physiquement, cette propriété tient compte du fait que le système  $\mathcal{S}$  peut être intriqué avec un système de référence  $\mathcal{R}$  qui n'évolue pas. Ainsi, il ne suffit pas que l'état du système  $\mathcal{S}$  demeure un état quantique valide, il faut aussi que l'état de  $\mathcal{SR}$  reste un état quantique valide. Ceci se traduit par la propriété de positivité complète.

4.  $\mathcal{N}$  préserve complètement la positivité de  $\rho$ .

Nous allons vérifier la propriété sur la décomposition de Schmidt d'un état quelconque  $|\Psi^{SR}\rangle = \sum_i c_i |\phi_i^S \varphi_i^R\rangle$ .

$$\begin{aligned}
\lambda &= \langle \Psi^{SR} | (\mathcal{N}(\rho^S) \otimes |\Gamma^R\rangle\langle\Gamma^R|) | \Psi^{SR} \rangle \\
&= \sum_k \langle \Psi^{SR} | (N_k \rho^S N_k^\dagger \otimes |\Gamma^R\rangle\langle\Gamma^R|) | \Psi^{SR} \rangle \\
&= \sum_{i,j,k} c_i^* c_j \langle \phi_i^S \varphi_i^R | (N_k \rho^S N_k^\dagger \otimes |\Gamma^R\rangle\langle\Gamma^R|) | \phi_j^S \varphi_j^R \rangle \\
&= \sum_{i,k} |c_i|^2 \underbrace{\langle \phi_i^S | (N_k \rho^S N_k^\dagger) | \phi_i^S \rangle}_{\geq 0}
\end{aligned} \tag{2.35}$$

Maintenant que nous avons vu quelles sont les propriétés vérifiées par un superopérateur obtenu en appliquant une évolution unitaire sur le système et son environnement, nous allons évoquer sans le démontrer le résultat réciproque, tiré de [46].

**Théorème 2.6.** *[Représentation de Kraus] Un opérateur linéaire vérifiant les propriétés 1, 2 et 4 possède une décomposition en somme d'opérateurs.*

### 2.2.2.2 Canal à amortissement de phase

En informatique quantique, les superopérateurs sont souvent utilisés pour modéliser la transmission imparfaite d'information quantique. Ils sont alors appelés *canaux quantiques*. Nous allons en présenter un : le *canal à amortissement de phase*. Il nous servira de transition puisque ce canal présente un modèle extrêmement simple qui contient malgré tout les éléments essentiels de la théorie de la décohérence qui fera l'objet du prochain chapitre.

La présentation que nous donnons ici du *canal à amortissement de phase* s'inspire largement de celle donnée dans les notes de cours de John Preskill [62]. Soit un qubit  $\mathcal{S}$  en interaction avec un autre système quantique  $\mathcal{E}$ , son environnement. L'environnement est un système quantique à 3 niveaux<sup>6</sup> et une base orthonormale de son espace de Hilbert  $\mathcal{H}^{\mathcal{E}}$  sera notée  $\{|0^{\mathcal{E}}\rangle, |1^{\mathcal{E}}\rangle, |2^{\mathcal{E}}\rangle\}$ . Initialement, le système  $\mathcal{S}$  est dans un état quelconque  $|\psi\rangle = a|0^{\mathcal{S}}\rangle + b|1^{\mathcal{S}}\rangle$  tandis que l'environnement est dans l'état  $|0^{\mathcal{E}}\rangle$ . Dans le cas où  $\mathcal{S}$  est dans l'état de base  $|0^{\mathcal{S}}\rangle$ , il perturbe l'environnement avec probabilité  $p$ . La perturbation fait passer l'environnement de l'état  $|0^{\mathcal{E}}\rangle$  dans l'état  $|1^{\mathcal{E}}\rangle$ . De façon similaire, dans le cas où  $\mathcal{S}$  est dans l'état excité  $|1^{\mathcal{S}}\rangle$ , il fait passer l'environnement dans l'état  $|2^{\mathcal{E}}\rangle$  avec probabilité  $p$ . Une représentation unitaire de ce canal est donc la suivante :

$$\begin{aligned} |0^{\mathcal{S}}\rangle|0^{\mathcal{E}}\rangle &\mapsto \sqrt{1-p}|0^{\mathcal{S}}\rangle|0^{\mathcal{E}}\rangle + \sqrt{p}|0^{\mathcal{S}}\rangle|1^{\mathcal{E}}\rangle \\ |1^{\mathcal{S}}\rangle|0^{\mathcal{E}}\rangle &\mapsto \sqrt{1-p}|1^{\mathcal{S}}\rangle|0^{\mathcal{E}}\rangle + \sqrt{p}|1^{\mathcal{S}}\rangle|2^{\mathcal{E}}\rangle. \end{aligned} \quad (2.36)$$

Notons que la base de calcul  $\{|0^{\mathcal{S}}\rangle, |1^{\mathcal{S}}\rangle\}$  joue un rôle privilégié dans cette évolution. En effet, si  $\mathcal{S}$  est initialement dans l'état  $|0^{\mathcal{S}}\rangle$  ou l'état  $|1^{\mathcal{S}}\rangle$ , il demeure dans cet état. Il en sera autrement pour une superposition de ces deux états. En effet, l'évolution d'un état quelconque  $|\psi^{\mathcal{S}}\rangle = a|0^{\mathcal{S}}\rangle + b|1^{\mathcal{S}}\rangle$  sera

$$|\psi^{\mathcal{S}}\rangle|0^{\mathcal{E}}\rangle \mapsto \sqrt{1-p}|\psi^{\mathcal{S}}\rangle|0^{\mathcal{E}}\rangle + \sqrt{p}(a|0^{\mathcal{S}}\rangle|1^{\mathcal{E}}\rangle + b|1^{\mathcal{S}}\rangle|2^{\mathcal{E}}\rangle). \quad (2.37)$$

Une trace partielle sur l'environnement va fournir l'état

$$\begin{aligned} \mathcal{N}(\rho^{\mathcal{S}}) &= \text{Tr}_{\mathcal{E}} [U|\psi^{\mathcal{S}}\rangle|0^{\mathcal{E}}\rangle\langle\psi^{\mathcal{S}}|\langle 0^{\mathcal{E}}|U^\dagger] \\ &= (1-p)|\psi^{\mathcal{S}}\rangle\langle\psi^{\mathcal{S}}| + p(|a|^2|0^{\mathcal{S}}\rangle\langle 0^{\mathcal{S}}| + |b|^2|1^{\mathcal{S}}\rangle\langle 1^{\mathcal{S}}|). \end{aligned} \quad (2.38)$$

Notons l'importance de l'orthogonalité de  $|1^{\mathcal{E}}\rangle$  et de  $|2^{\mathcal{E}}\rangle$ . En effet, leur or-

---

<sup>6</sup>Dans le jargon de l'informatique quantique, il s'agit donc d'un *qutrit*.

thogonalité, dont nous avons montré qu'elle était équivalente à leur distinguabilité parfaite, détruit les termes croisés  $|0^S\rangle\langle 1^S|$  et  $|1^S\rangle\langle 0^S|$ . Un calcul utilisant la relation (2.29) permet d'évaluer les opérateurs de Kraus, qui sont aussi visibles sur la relation (2.38). Leurs expressions sont :

$$N_0 = \sqrt{1-p}\mathbf{1}, \quad N_1 = \sqrt{p}|0\rangle\langle 0|, \quad N_2 = \sqrt{p}|1\rangle\langle 1|. \quad (2.39)$$

Ainsi, l'état final du système  $\mathcal{S}$  est un mélange statistique où

- avec probabilité  $1-p$  l'état quantique initial  $|\psi^S\rangle$  n'est pas affecté (ce qui est indiqué par le fait que l'opérateur de Kraus  $N_0$  soit proportionnel à l'identité)
- avec probabilité  $p$ , l'état initial est transformé en un mélange statistique  $\{|0^S\rangle, |a|^2\rangle, |1^S\rangle, |b|^2\rangle\}$ .

Ce canal quantique admet une autre décomposition n'utilisant que deux opérateurs de Kraus qui sont

$$M_0 = \sqrt{1-\tilde{p}}\mathbf{1} \quad \text{et} \quad M_1 = \sqrt{\tilde{p}}\sigma_z$$

où  $\tilde{p} = \frac{p}{2}$ . Le canal s'écrit alors

$$\rho \mapsto \tilde{p}\sigma_z\rho\sigma_z + (1-\tilde{p})\rho$$

ce qui veut dire qu'avec probabilité  $\tilde{p}$ , le qubit subit une erreur de phase alors qu'avec probabilité  $1-\tilde{p}$ , il n'est pas affecté.

Comparons l'état  $\mathcal{N}(\rho^S)$  avec l'état quantique initial  $|\psi^S\rangle = a|0^S\rangle + b|1^S\rangle$ . Pour ce faire, le plus simple est de comparer leurs opérateurs densité dans leur représentation matricielle dans la base de calcul :

$$\rho^S = |\psi^S\rangle\langle\psi^S| = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix} \quad \text{vs.} \quad \mathcal{N}(\rho^S) = \begin{pmatrix} |a|^2 & (1-p)ab^* \\ (1-p)(a^*b) & |b|^2 \end{pmatrix}.$$

Les termes diagonaux sont identiques alors que les termes hors-diagonale ont

été réduits par un facteur  $1 - p$ . Or, ces termes hors-diagonale, désignés par le terme « *cohérences* » dans [25] caractérisent la cohérence de phase entre les états  $|0^S\rangle$  et  $|1^S\rangle$ . Le canal a donc affaibli la cohérence de phase.

- Avec probabilité  $1 - p$ , il agit comme un canal parfait et l'état est transmis sans modification tandis qu'
- avec probabilité  $p$ , le canal détruit la cohérence de phase en laissant une trace dans l'environnement de l'état du système  $\mathcal{S}$ . En effet, un observateur ayant accès à l'environnement pourrait déterminer l'état du qubit  $\mathcal{S}$  en mesurant si l'environnement est dans l'état  $|1^\mathcal{E}\rangle$  ou  $|2^\mathcal{E}\rangle$ .

Notons par contre que le canal n'a aucun effet sur un qubit initialement dans l'état  $|0^S\rangle$  ou  $|1^S\rangle$ . L'environnement a donc privilégié une base de l'espace de Hilbert, ici la base de calcul.

L'évolution du qubit sous l'effet du canal à amortissement de phase se visualise dans la boule de Bloch. En effet, en écrivant  $\rho^S = \frac{1}{2}(\mathbf{1} + \hat{\mathbf{p}} \cdot \boldsymbol{\sigma})$  où  $\hat{\mathbf{p}} \cdot \boldsymbol{\sigma} = \sum_{i=1}^3 p_i \sigma_i$ , l'action du canal s'écrit

$$\begin{aligned}
\mathcal{N}(\rho^S) &= (1 - \tilde{p})\rho^S + \tilde{p}\sigma_3\rho^S\sigma_3 \\
&= \frac{1}{2}\mathbf{1} + \frac{1}{2}\left(1 - \frac{p}{2}\right)\sum_{i=1}^3 p_i\sigma_i + \frac{p}{4}\sum_{i=1}^3 p_i\sigma_3\sigma_i\sigma_3 \\
&= \frac{1}{2}\mathbf{1} + \frac{1}{2}\left(1 - \frac{p}{2}\right)\sum_{i=1}^3 p_i\sigma_i - \frac{p}{4}\sum_{i=1}^2 p_i\sigma_i + \frac{p}{4}p_3\sigma_3 \\
&= \frac{1}{2}\left(\mathbf{1} + \begin{pmatrix} (1-p)p_1 \\ (1-p)p_2 \\ p_3 \end{pmatrix} \cdot \boldsymbol{\sigma}\right). \tag{2.40}
\end{aligned}$$

Ainsi, en terme de vecteur polarisation qui repère l'état dans la boule de Bloch, l'action du canal est

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \mapsto \begin{pmatrix} (1-p)p_1 \\ (1-p)p_2 \\ p_3 \end{pmatrix}. \tag{2.41}$$

Géométriquement, la sphère est envoyée sur un ellipsoïde de révolution autour de l'axe  $z$ . En particulier, nous retrouvons que les états  $|0^S\rangle$  et  $|1^S\rangle$  correspondant aux pôles Nord et Sud ne sont pas affectés. Après plusieurs applications du canal, les points de la sphère sont projetés sur l'axe  $z$ , restreignant ainsi la boule de Bloch au segment de droite entre les deux pôles. Sous l'action du canal à amortissement de phase, trois régions distinctes

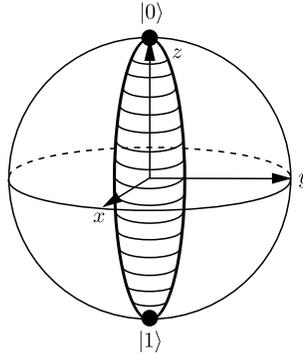


Figure 2.2 – Action du canal à amortissement de phase

apparaissent dans la boule de Bloch.

1. Les pôles correspondent aux états  $|0^S\rangle$  et  $|1^S\rangle$  qui ne sont pas perturbés par le canal et sont appelés *états pointeurs*
2. L'axe  $z$  correspond au mélange statistique d'états pointeurs.
3. Le reste de la boule de Bloch est inaccessible après quelques applications du canal à amortissement de phase.

Le canal à amortissement de phase est un modèle jouet pour plusieurs phénomènes entraînant la *décohérence* d'un qubit. Cette notion de décohérence fera l'objet du prochain chapitre et du reste de ce mémoire.

## Évolution des systèmes ouverts et décohérence

Ce chapitre a permis d'introduire des outils essentiels au traitement mathématique des *systèmes quantiques ouverts*. Nous avons montré que l'état d'un système quantique est généralement décrit non pas par un vecteur de l'espace de Hilbert, mais plutôt par un opérateur densité. De façon similaire, une mesure ne se limite pas à un ensemble de projecteurs, mais est généralement donnée par un ensemble d'opérateurs positifs (POVM). Finalement, bien que l'équation de Schrödinger implique une évolution unitaire du système global, l'évolution d'un sous-système ouvert est le plus souvent donnée par un superopérateur qui transforme l'opérateur densité du sous-système en un autre opérateur densité.

Dans le prochain chapitre, nous allons introduire la théorie de la décohérence. Elle repose sur le constat qu'un système quantique n'est habituellement pas fermé mais en interaction avec une multitude de degrés de liberté qui constituent son environnement. Comme nous l'avons montré dans ce chapitre, de tels systèmes ouverts peuvent avoir une évolution non-unitaire alors que le système global tenant compte de l'environnement présente une évolution unitaire. Cette évolution fait apparaître des règles de supersélection, tel le caractère privilégié accordé à la base de calcul par le canal à amortissement de phase. Ce phénomène va distinguer des états robustes qualifiés de quasi-classiques des autres états quantiques beaucoup plus fragiles. Ainsi, la décohérence entraîne une fragilité extrême des corrélations quantiques essentielles au calcul quantique.

# Chapitre 3

## Théorie de la décohérence

*The “paradox” is only a conflict between reality  
and your feeling of what reality “ought to be”.*

–Richard Feynman, cité par M. Schlosshauer [66]

La mécanique quantique et en particulier le principe de superposition sont difficiles à réconcilier avec notre expérience sensible. Alors que l’espace des états possibles est extrêmement vaste, les objets macroscopiques semblent restreints à un sous-ensemble limité d’états et présentent certaines grandeurs physiques bien définies : position, vitesse. . . Ce décalage pose la question de l’émergence d’un monde classique à partir d’un monde quantique.

Dans ce chapitre, nous introduirons les bases de la théorie de la décohérence. Elle met l’accent sur le rôle joué par l’environnement d’un système quantique, c’est-à-dire tous les degrés de liberté susceptibles de se coupler avec ce système. Nous montrerons que cette interaction crée de l’intrication, ce qui entraînera l’apparition d’états privilégiés qui correspondent aux états classiques. Pour un observateur n’ayant pas accès à l’intégralité de l’environnement, un système initialement dans un état de superposition perdra alors sa cohérence pour aboutir dans un état de mélange statistique. Ainsi, la théorie de la décohérence, tout en se maintenant strictement dans le cadre de la mécanique quantique, propose des mécanismes afin de réconcilier la mécanique quantique à notre expérience sensible.

## 3.1 Transition quantique-classique

Le principe de superposition affirme que *si un système physique peut être dans chacun des deux états  $|\psi\rangle$  et  $|\phi\rangle$  alors toute combinaison linéaire (normalisée)  $\alpha|\psi\rangle + \beta|\phi\rangle$  est un état possible du système*. Ce principe a été vérifié expérimentalement au niveau microscopique. Toutefois, l'application de ce principe au monde macroscopique semble entraîner des conséquences en contradiction avec notre expérience sensible. En particulier, les états macroscopiques dont nous avons l'habitude sont des exceptions par rapport à tous les états possibles dans l'espace de Hilbert. Comment réconcilier l'étendue de l'espace de Hilbert avec l'observation empirique d'un très petit nombre d'états macroscopiques "classiques" définis par un nombre restreint de grandeurs bien déterminées (position, vitesse...)?

### 3.1.1 Limite quantique-classique

Historiquement, ce problème se pose dès les premiers temps de la mécanique quantique. Bohr proposait de tracer une limite entre les "objets quantiques" (atomes, électrons...) et les "objets classiques" (appareils de mesure, observateurs...) et de suspendre le principe de superposition pour les "objets classiques". Cette proposition se heurte toutefois à la question suivante : où placer la limite, est-elle fixe, comment est-elle définie ?

Fondamentalement, tout objet est formé de constituants aux propriétés quantiques. De plus, des expériences effectuées sur des objets de plus en plus "grands" ont confirmé l'existence d'états en superposition via l'observation de phénomènes d'interférence. Citons en particulier les expériences d'interférométrie sur des molécules de plus en plus grosses (fullerènes  $C_{60}$  [4], molécules  $C_{70}$  [39], fluofullerènes  $C_{60}F_{48}$ , molécules organiques  $C_{44}H_{30}N_4$  [40]) et les expériences sur des systèmes opto-mécaniques [73]. Il paraît difficile de croire qu'une telle limite existe. La proposition de Bohr d'introduire une limite entre les mondes microscopique et macroscopique ne paraît donc pas satisfaisante.

De plus, si les lois de la mécanique quantique, autres que le principe de superposition, continuent de s'appliquer au niveau macroscopique, il est possible de faire remonter la "bizarrerie quantique" depuis le niveau microscopique grâce à l'intrication. Donnons un exemple, qui correspond schématiquement à une expérience menée au NIST en 1996 [52] : soit un ion dans une cavité dont on considère deux degrés de liberté, son état interne et sa position. Son état interne est un degré de liberté microscopique. L'ion peut être dans son état fondamental  $|0\rangle$  ou son état excité  $|1\rangle$  ou encore toute combinaison linéaire de ces deux états, par exemple  $|\pm\rangle = \frac{1}{\sqrt{2}}|0\rangle \pm \frac{1}{\sqrt{2}}|1\rangle$ . Dans la vision de Bohr, un tel état de superposition *microscopique* est tout à fait valable. Par contre, la position de l'ion est un degré de liberté macroscopique et à ce niveau, le principe de superposition n'est pas applicable (toujours selon Bohr). Pour simplifier, supposons que l'ion soit dans une cavité et puisse être dans la moitié gauche  $|G\rangle$  ou la moitié droite  $|D\rangle$  de la cavité. Ces deux positions sont séparées de 90 nm, une grande longueur à l'échelle atomique. Soit alors une transformation unitaire  $U$  qui a l'effet suivant

$$\begin{aligned} |0\rangle|G\rangle &\mapsto |0\rangle|G\rangle & |1\rangle|G\rangle &\mapsto |1\rangle|D\rangle \\ |0\rangle|D\rangle &\mapsto |0\rangle|D\rangle & |1\rangle|D\rangle &\mapsto |1\rangle|G\rangle. \end{aligned} \quad (3.1)$$

Cette transformation est tout à fait légitime dans la vision de Bohr. Supposons maintenant que nous préparions l'état  $|+\rangle|G\rangle$ , ce qui est permis puisque le principe de superposition est valide au niveau microscopique, avant d'appliquer  $U$

$$|\Psi\rangle = U(|+\rangle|G\rangle) = \frac{1}{\sqrt{2}}|0\rangle|G\rangle + \frac{1}{\sqrt{2}}|1\rangle|D\rangle. \quad (3.2)$$

Cet état va mettre en évidence une contradiction dans la vision de Bohr, tel que souligné par Schrödinger dès 1935 [67]. En effet, l'état se réécrit

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|+\rangle \left( \frac{1}{\sqrt{2}}|G\rangle + \frac{1}{\sqrt{2}}|D\rangle \right) + \frac{1}{\sqrt{2}}|-\rangle \left( \frac{1}{\sqrt{2}}|G\rangle - \frac{1}{\sqrt{2}}|D\rangle \right). \quad (3.3)$$

Il suffit alors de mesurer l'état interne dans la base  $\{|+\rangle, |-\rangle\}$  pour faire apparaître la position dans un état non-classique  $\frac{1}{\sqrt{2}}|G\rangle \pm \frac{1}{\sqrt{2}}|D\rangle$ . Cet exemple montre que grâce à une transformation créant de l'intrication, il est possible de faire remonter le principe de superposition du monde microscopique au monde macroscopique. Il s'agit d'une réalisation expérimentale de l'expérience du chat de Schrödinger où le caractère vivant ou mort du chat est représenté par la position de l'ion. Schrödinger affirme en effet que l'intrication permet qu'« une indétermination provenant au départ du domaine atomique est ensuite transformée en indétermination macroscopique ».<sup>1</sup> La vérification expérimentale de ce phénomène montre que, en raison de l'intrication, nous devrions rencontrer des objets macroscopiques dans des états de superposition. La signature d'un tel état en superposition est l'interférence quantique. Un problème particulier se pose alors : comment expliquer que nous n'observons pas d'interférence pour des objets macroscopiques ? Autrement dit, pourquoi certains états quantiques sont-ils privilégiés aux dépens des autres ?

### 3.1.2 Problème de la mesure

La transition quantique-classique est souvent discutée dans le cadre du problème de la mesure quantique. Il s'agit d'un formalisme qui tente de rendre compte de la mesure d'un système quantique par un appareil de mesure sans faire intervenir le postulat de réduction du paquet d'onde.

#### 3.1.2.1 Mesure quantique

Nous allons maintenant présenter le schéma de mesure idéale, introduit par von Neumann en 1932 [74]. Soit donc un système  $\mathcal{S}$  associé à l'espace de Hilbert  $\mathcal{H}^{\mathcal{S}}$  dont une base orthonormée est  $\{|s_n\rangle\}$ . De même, soit un appareil de mesure  $\mathcal{A}$  associé à l'espace de Hilbert  $\mathcal{H}^{\mathcal{A}}$  dont une base orthonormée

---

<sup>1</sup>Traduction libre de l'auteur à partir de la traduction de l'allemand à l'anglais réalisée par John D. Trimmer [71] à partir de l'article original de Schrodinger [68].

est  $\{|a_n\rangle\}$ . Des états orthonormés étant parfaitement distinguables, les états  $|a_n\rangle$  correspondent à des états macroscopiques bien identifiables de l'appareil de mesure. Supposons que l'appareil mesure l'observable  $O = \sum_n \lambda_n |s_n\rangle\langle s_n|$  du système. On aimerait que chaque  $|a_n\rangle$  corresponde à un et un seul état  $|s_n\rangle$  afin qu'il soit possible d'affirmer que le système  $\mathcal{S}$  est dans l'état  $|s_n\rangle$  si et seulement si l'appareil est dans l'état  $|a_n\rangle$ . Les états  $|a_n\rangle$  sont alors appelés *états indicateurs*.

Initialement, l'appareil de mesure est dans un état  $|\text{prêt}\rangle$  qui correspond à l'état de l'appareil quand il est prêt à effectuer une mesure. Au contraire, le système  $\mathcal{S}$  est dans un état pur quelconque  $|\psi\rangle = \sum_n c_n |s_n\rangle$  qui va être mesuré. L'interaction entre ces deux systèmes correspond à une transformation unitaire  $U$  qui associe  $|s_n\rangle|\text{prêt}\rangle$  (où  $|\text{prêt}\rangle$  est l'état de l'appareil prêt à mesurer) à  $|s_n\rangle|a_n\rangle$ , ce qui correspond au fait que l'appareil mesure le système  $\mathcal{S}$  dans la base  $\{|s_n\rangle\}$ . Par linéarité, nous avons donc

$$|\psi\rangle|\text{prêt}\rangle \mapsto \sum_n c_n |s_n\rangle|a_n\rangle. \quad (3.4)$$

Une telle décomposition, où les familles  $\{|s_n\rangle\}$  et  $\{|a_n\rangle\}$  sont orthonormales, sera dorénavant appelée une décomposition biorthogonale. Une telle évolution est appelée *pseudo-mesure* (ou *prémesure*). Bien que l'on aimerait l'interpréter comme une mesure, deux problèmes surgissent.

1. Une décomposition biorthogonale n'est pas unique. Il est possible qu'il existe deux décompositions biorthogonales pour un état donné  $|\Psi^{\mathcal{S}\mathcal{A}}\rangle = \sum c_n |s_n\rangle|a_n\rangle = \sum c'_n |s'_n\rangle|a'_n\rangle$  faisant en sorte qu'il serait impossible de distinguer la pseudo-mesure par l'appareil  $\mathcal{A}$  et la pseudo-mesure par l'appareil  $\mathcal{A}'$ . Il s'agit du problème de la base privilégiée.
2. Pourquoi avons-nous l'impression de ne percevoir l'appareil que dans un seul état  $|a_n\rangle$  plutôt que dans un état de superposition des  $|a_n\rangle$ ? Autrement dit, pourquoi avons-nous l'impression que le résultat d'une mesure est unique?

### 3.1.2.2 Base privilégiée et unicité du résultat

**Base privilégiée** L'importance du problème de la base privilégiée a été soulignée par Żurek en 1981 [77] qui a de plus distingué ce problème de celui de l'unicité du résultat. En effet, avant de se poser la question de l'unicité du résultat, il faut pouvoir savoir quels sont les résultats possibles. Toutefois, ce problème est moins reconnu, peut-être parce son importance n'a été réalisée qu'au moment où la théorie de la décohérence fournissait déjà une solution viable.

Le problème de la base privilégiée est étroitement lié à la décomposition de Schmidt.

**Théorème 3.1.** *[Décomposition de Schmidt] Tout état pur  $|\Psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$  d'un système biparti admet une décomposition biorthogonale*

$$|\Psi^{AB}\rangle = \sum_i \sqrt{p_i} |i^A\rangle |i'^B\rangle \quad (3.5)$$

où les familles  $\{|i^A\rangle\}$  et  $\{|i'^B\rangle\}$  sont orthonormales et les  $p_i \in \mathbb{R}^{+*}$  vérifient  $\sum_k p_k = 1$ .

*Démonstration.* Soit  $\rho^A = \text{Tr}_B |\Psi^{AB}\rangle \langle \Psi^{AB}|$ . L'opérateur  $\rho^A$  étant hermitien, il existe une base  $\{|i^A\rangle\}$  tel que

$$\rho^A = \sum_i p_i |i^A\rangle \langle i^A|. \quad (3.6)$$

Soit alors une base orthogonale quelconque de  $\mathcal{H}^B$ , notée  $\{|k^B\rangle\}$ . L'état  $|\Psi^{AB}\rangle$  se décompose sur la base  $\{|i^A\rangle \otimes |k^B\rangle\}$

$$|\Psi^{AB}\rangle = \sum_{ik} c_{ik} |i^A\rangle |k^B\rangle = \sum_i |i^A\rangle |\tilde{i}'^B\rangle$$

où nous avons défini une nouvelle base  $\{|\tilde{i}'^B\rangle\}$  par  $|\tilde{i}'^B\rangle = \sum_k c_{ik} |k^B\rangle$ . Cal-

culons alors  $\rho^A$  par trace partielle

$$\rho^A = \text{Tr}_B |\Psi^{AB}\rangle\langle\Psi^{AB}| = \text{Tr}_B \sum_{ij} |i^A\rangle\langle i^A| \langle j^B| \langle j^B| = \sum_{ij} \langle j^B| \langle j^B| |i^A\rangle\langle i^A|. \quad (3.7)$$

Or,  $\rho^A$  est diagonal dans la base  $\{|i^A\rangle\}$  donc  $\langle j^B| \langle j^B| = p_i \delta_{ij}$ , autrement dit la base  $\{|i^B\rangle\}$  est orthogonale. Il suffit alors de normaliser la base par  $|i^B\rangle = \sqrt{p_i} |\tilde{i}^B\rangle$  pour obtenir la décomposition désirée.  $\square$

Ce théorème garantit donc l'existence d'une décomposition biorthogonale pour tout état pur biparti. Ainsi, tout état pur biparti peut être interprété comme le résultat d'une pseudo-mesure. Toutefois, le problème intervient quand il faut identifier l'observable qui a été mesurée par l'appareil : en effet, la décomposition biorthogonale n'est pas unique.

**Proposition 3.2.** *Un état pur  $|\Psi\rangle \in \mathcal{H}^A \otimes \mathcal{H}^B$  admet une décomposition de Schmidt (3.5) unique si et seulement si  $\rho^A = \text{Tr}_B |\Psi\rangle\langle\Psi|$  n'a pas de valeurs propres non-nulles dégénérées. Autrement dit, la décomposition de Schmidt est unique si et seulement si tous les  $p_k$  sont distincts.*

*Démonstration.*  $\boxed{\Leftarrow}$  La décomposition spectrale de  $\rho^B = \text{Tr}_A |\Psi^{AB}\rangle\langle\Psi^{AB}|$  est  $\rho^B = \sum p_i |i^B\rangle\langle i^B|$ . Les opérateurs  $\rho^A$  et  $\rho^B$  ont donc les mêmes valeurs propres non-nulles. S'il n'y a pas dégénérescence, il suffit de diagonaliser  $\rho^A$  et  $\rho^B$  et de jumeler les vecteurs propres associés à la même valeur propre pour obtenir la décomposition de Schmidt.

$\boxed{\Rightarrow}$  S'il y a dégénérescence,  $\rho^A$  et  $\rho^B$  présentent des sous-espaces propres de même dimension associés à une même valeur propre. Sur de tels sous-espaces de  $\mathcal{H}^A$  et de  $\mathcal{H}^B$ , toute base orthonormale convient pour la décomposition de Schmidt.  $\square$

Notons que s'il existe deux valeurs  $p_{k_1}$  et  $p_{k_2}$  non-nulles alors l'état pur  $|\Psi\rangle$  est forcément intriqué. Ainsi, pour un état pur biparti intriqué, la décomposition biorthogonale peut être ambiguë. Donnons un exemple, tiré de l'ouvrage de M. Schlosshauer [66]. Supposons que l'on veuille mesurer la

composante  $z$  du spin d'un électron  $\mathcal{S}$  et que l'on dispose d'un appareil dont l'état  $|0^{\mathcal{A}}\rangle$  est un état indicateur pour l'état  $|0^{\mathcal{S}}\rangle$  (spin vers le haut dans la direction  $z$ ) tandis que l'état  $|1^{\mathcal{A}}\rangle$  est un état indicateur pour l'état  $|1^{\mathcal{S}}\rangle$  (spin vers le bas dans la direction  $z$ ).

Supposons qu'initialement l'état de l'électron soit  $\frac{1}{\sqrt{2}}|0^{\mathcal{S}}\rangle + \frac{1}{\sqrt{2}}|1^{\mathcal{S}}\rangle$ . Par linéarité, après pseudo-mesure, l'électron et l'appareil de mesure sont dans l'état

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|0^{\mathcal{S}}0^{\mathcal{A}}\rangle + \frac{1}{\sqrt{2}}|1^{\mathcal{S}}1^{\mathcal{A}}\rangle. \quad (3.8)$$

Il s'agit bien d'une décomposition biorthogonale. Or, il est possible de réécrire cet état en faisant apparaître les états  $|\pm^{\mathcal{S}}\rangle = \frac{1}{\sqrt{2}}|0^{\mathcal{S}}\rangle \pm \frac{1}{\sqrt{2}}|1^{\mathcal{S}}\rangle$  qui sont les états propres de l'opérateur  $\sigma^x$  et correspondent donc à des spins alignés suivant la direction  $x$ . L'état  $|\Phi^+\rangle$  se réécrit

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|+^{\mathcal{S}}+^{\mathcal{A}}\rangle + \frac{1}{\sqrt{2}}|-^{\mathcal{S}}-^{\mathcal{A}}\rangle \quad (3.9)$$

qui est aussi une décomposition biorthogonale. Par contre, cette décomposition correspondrait à la pseudo-mesure de la composante du spin suivant  $x$ . Ainsi, l'appareil de mesure semble avoir mesuré à la fois l'observable  $\sigma^z$  et l'observable  $\sigma^x$ . Or, ces deux observables ne commutent pas et une telle observation violerait donc les règles de la mécanique quantique. L'ambiguïté de la décomposition orthogonale empêche donc d'interpréter la pseudo-mesure comme une mesure. Autrement dit, le mécanisme de von Neumann ne permet pas de privilégier une base par rapport à une autre.

Le problème de la base privilégiée va au-delà du contexte de la mesure quantique. En effet, l'expérience sensible indique que les objets ont souvent tendance à être dans des états de position plutôt que dans des superpositions de tels états. Il paraît donc important de mieux comprendre pourquoi la position joue un rôle privilégié.

Nous verrons dans la suite que la théorie de la décohérence fournit un mécanisme explicatif qui repose sur le fait que le système global, composé

du système  $\mathcal{S}$  et l'appareil de mesure  $\mathcal{A}$ , ne constitue pas un système fermé mais plutôt un système ouvert. L'introduction d'un troisième système, l'environnement, va modifier profondément la situation.

**Unicité du résultat** Notre expérience sensible montre que la mesure d'une quantité physique fournit un résultat unique. À cette observation pratique correspond le postulat de "réduction du paquet d'onde". Il peut paraître étonnant que toute évolution quantique obéit à l'équation de Schrödinger *sauf* l'évolution via mesure qui nécessite un postulat particulier. De nombreux efforts ont été consacrés à mieux comprendre ce postulat et à déterminer s'il est vraiment nécessaire. Le schéma de mesure de von Neumann semble être une tentative raisonnable afin d'expliquer la mesure via l'interaction entre un système et un appareil de mesure. Toutefois,

1. pourquoi avons-nous l'impression que l'appareil de mesure se trouve dans un état  $|a_{n_0}\rangle$  et non pas d'un état de superposition ?
2. quel mécanisme sélectionne un état  $|a_{n_0}\rangle$  plutôt qu'un autre ?

Ces questions laissent la porte ouverte à un multitude d'interprétations. Nous utiliserons le terme "interprétation" afin de désigner un schéma explicatif qui accorde une signification à la mécanique quantique, mais qui n'induit pas de différences mesurables. Autrement dit, privilégier une interprétation par rapport à une autre est un choix métaphysique.

De multiples interprétations ont été proposées afin de répondre au problème de l'unicité du résultat. Citons, en vrac, l'interprétation de Copenhague, l'interprétation multi-monde, les histoires consistantes, la mécanique bohémienne, l'interprétation avec intervention de la conscience et les interprétations avec mécanisme d'effondrement. Citons aussi une attitude possible, en vogue dans la communauté de l'informatique quantique. Elle consiste à devenir adepte de l'Église de l'espace de Hilbert étendu. Ses commandements sont les suivants (cf. la présentation de Matt Leifer disponible sur son blog <http://mattleifer.info/research/talk-slides/>) :

1. L'Univers tout entier est décrit par un état *pur* qui intrique tous les sous-systèmes de l'Univers.
2. Toute évolution quantique est unitaire. En particulier, il n'y a pas de réduction du vecteur d'onde.

Cette attitude est très proche des idées de H. Everett [32] et peut mener à une interprétation type multi-monde. Nous ne nous attarderons pas plus sur le problème de l'unicité, qui constitue le cœur du problème de la mesure. À l'heure actuelle, il ne s'agit pas d'un problème physique, mais bien d'un problème métaphysique puisque les différentes interprétations ne donnent pas lieu à des tests expérimentaux. Notons toutefois que cela pourrait bien changer, à l'image de la non-localité qui n'est devenue un problème physique qu'avec le travail de John Bell et les inégalités type CHSH.

Nous verrons dans la suite de ce mémoire que la théorie de la décohérence ne fournit pas de mécanisme explicatif au problème de l'unicité.

### 3.1.3 Intrication et importance de l'environnement

Notons que l'intrication joue un rôle crucial dans ce que nous venons de présenter. En effet, l'intrication permet de faire remonter la bizarrerie quantique au niveau macroscopique (expérience type chat de Schrödinger). De plus, l'intrication est essentielle au phénomène de pseudo-mesure puisque les états distinguables de l'appareil de mesure sont en correspondance avec les états du système mesuré grâce à l'intrication. Est-il alors étonnant que la théorie de la décohérence propose des mécanismes explicatifs à différents problèmes évoqués plus haut en remarquant qu'un système quantique n'est pas habituellement isolé, mais plutôt en interaction avec un environnement avec lequel il va s'intriquer ?

Donnons pour cela un exemple, inspiré de l'expérience de pensée décrite dans le cours "Cohérence quantique et dissipation" [27] de Jean Dalibard à l'École Normale Supérieure, rue d'Ulm à Paris, et de la mise en évidence expérimentale décrite dans [21].

Il s'agit d'une expérience, du type de celle des « fentes de Young », réalisée avec un atome dont on considère deux degrés de liberté : son état interne, qui peut être soit excité  $|e\rangle$  ou fondamental  $|f\rangle$ , et sa position  $x$  sur l'écran d'observation, correspondant à l'observable  $X$ . L'atome peut se désexciter en émettant un photon lors de son passage dans la cavité électromagnétique située après la fente  $a$  (à droite de la fente dans la figure 3.1). L'état de la cavité sans photon est  $|0\rangle$  et son état après la désexcitation de l'atome est  $|1\rangle$ . Ces deux états sont parfaitement distinguables donc  $\langle 0|1\rangle = 0$ . De plus, on suppose que la cavité détecte toujours le passage de l'atome.

Initialement, l'atome est émis par la source dans l'état excité  $|e\rangle$  ; la cavité ne contient aucun photon et est donc dans l'état  $|0\rangle$ . Dans l'expérience classique des fentes de Young, c.-à-d. en absence de cavité, l'état après passage dans les fentes serait

$$\left( \frac{1}{\sqrt{2}}|\psi_a\rangle + \frac{1}{\sqrt{2}}|\psi_b\rangle \right) \otimes |0\rangle|e\rangle \quad (3.10)$$

où  $|\psi_a\rangle$  représente l'état d'un atome passé par la fente  $a$  et  $|\psi_b\rangle$  celui d'un atome passé par la fente  $b$ . La probabilité de mesurer l'atome à une position  $x$  serait alors

$$\mathcal{P}(x) = \frac{1}{2}|\psi_a(x)|^2 + \frac{1}{2}|\psi_b(x)|^2 + \text{Re}(\psi_a^*\psi_b) \quad (3.11)$$

en adoptant la notation traditionnelle  $\psi_a(x) = \text{Tr}[X|\psi_a\rangle\langle\psi_a|]$ . En particulier, le terme d'interférence  $\text{Re}(\psi_a^*\psi_b)$  apparaît.

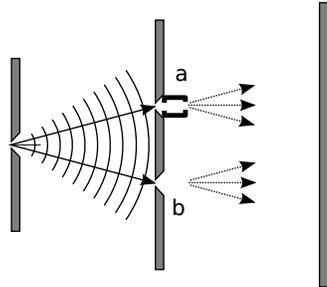


Figure 3.1 – Expérience des fentes de Young avec détecteur

La présence de la cavité modifie l'expérience habituelle. En effet, après passage dans les fentes, l'état sera plutôt

$$|\Psi\rangle = \frac{1}{\sqrt{2}}|\psi_a\rangle|1\rangle|f\rangle + \frac{1}{\sqrt{2}}|\psi_b\rangle|0\rangle|e\rangle. \quad (3.12)$$

La position  $x$  de l'atome sur l'écran est alors mesurée par un détecteur *qui n'est pas sensible à l'état interne de l'atome*. Ainsi, l'observable mesurée est  $X \otimes \mathbf{1}_{\text{cavité}} \otimes \mathbf{1}_{\text{état}}$ . La probabilité de mesurer l'atome à une position  $x$  est

$$\begin{aligned} \mathcal{P}(x) &= \text{Tr} [X \otimes \mathbf{1}_{\text{cavité}} \otimes \mathbf{1}_{\text{état}} |\Psi\rangle\langle\Psi|] \\ &= \frac{1}{2} \text{Tr} [X |\psi_a\rangle\langle\psi_a|] + \frac{1}{2} \text{Tr} [X |\psi_b\rangle\langle\psi_b|] \\ &\quad + \frac{1}{2} \text{Tr} [X |\psi_a\rangle\langle\psi_b|] \langle 0|1\rangle \langle e|g\rangle + \frac{1}{2} \text{Tr} [X |\psi_b\rangle\langle\psi_a|] \langle 1|0\rangle \langle g|e\rangle \\ &= \frac{1}{2} |\psi_a(x)|^2 + \frac{1}{2} |\psi_b(x)|^2. \end{aligned} \quad (3.13)$$

Le terme d'interférence a donc disparu en raison de la présence de la cavité. Plus précisément, le degré de liberté qui nous intéresse, la position de l'atome, s'est intriqué avec deux autres degrés de liberté, qui constituent son environnement. L'un d'entre eux est un degré de liberté interne à l'atome : son état d'énergie tandis que l'autre est un degré de liberté externe, l'état de la cavité. Puisque l'information qui nous intéresse ne porte que sur la position de l'atome, l'influence de ces deux degrés de liberté est « effacée » par l'opération de trace partielle. Or, l'orthogonalité des états de l'environnement permettrait de déterminer la fente par laquelle l'atome est passé. Ainsi, le couplage avec l'environnement transforme la superposition, dont l'interférence manifestait la cohérence, en mélange statistique sans cohérence.

Cet exemple simple présente l'idée de base de la théorie de la décohérence : le système quantique qui nous intéresse n'est habituellement pas fermé mais en interaction avec un environnement. La prise en compte de cet environnement et son couplage avec le système va permettre de faire apparaître une base privilégiée et de transformer une superposition d'états de cette base en mélange statistique.

## 3.2 Modèles de décohérence

Avant d'introduire les avancées théoriques de la décohérence, nous allons présenter plusieurs modèles d'interaction entre un système quantique et son environnement qui mènent à une décohérence du système quantique. En particulier, nous introduirons un modèle qui nous servira d'exemple-type pour la suite : le modèle introduit par Żurek dans son article de 1982 [78].

### 3.2.1 Modèle de Żurek

#### 3.2.1.1 Description du modèle

Dans le modèle de Żurek (voir figure 3.2), deux systèmes interviennent : le système quantique  $\mathcal{S}$  et son environnement  $\mathcal{E}$ . Le système  $\mathcal{S}$  est un système quantique à deux états : physiquement, il peut être vu comme une particule de spin- $\frac{1}{2}$  et il sera traité mathématiquement comme un qubit. Son espace de Hilbert associé est  $\mathcal{H}^{\mathcal{S}}$ . L'environnement  $\mathcal{E}$  est constitué de  $n$  spins- $\frac{1}{2}$  et son espace de Hilbert associé est  $\mathcal{H}^{\mathcal{E}}$  de dimension  $N = 2^n$ .

L'interaction entre  $\mathcal{S}$  et son environnement a pour hamiltonien

$$H_{\mathcal{S}\mathcal{E}} = \sum_{k=1}^n g_k \sigma_{\mathcal{S}}^z \sigma_k^z \quad (3.14)$$

où

- $\sigma_{\mathcal{S}}^z$  est l'opérateur  $z$  de Pauli agissant dans  $\mathcal{H}^{\mathcal{S}}$
- $\sigma_k^z \equiv \mathbf{1}_1 \otimes \dots \otimes \mathbf{1}_{k-1} \otimes \sigma_k^z \otimes \mathbf{1}_{k+1} \dots \otimes \mathbf{1}_n$  est l'opérateur  $z$  de Pauli agissant sur le sous-espace lié au  $k$ ième spin de l'environnement dans  $\mathcal{H}^{\mathcal{E}}$
- $\{g_k\}_{k \in [1;n]}$  sont des constantes de couplage réelles.

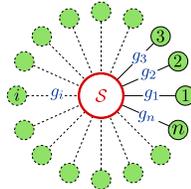


Figure 3.2 – Modèle de Żurek

Autrement dit, chaque spin de l'environnement interagit avec le spin central via une interaction faisant intervenir la composante  $z$  de son spin. La force du couplage entre le  $k$ ième spin de l'environnement et le spin central est caractérisée par  $g_k \in \mathbb{R}$ . Les spins qui forment l'environnement n'interagissent pas. L'environnement ne présente donc pas d'évolution propre. Cette remarque est au cœur d'une des contributions originales de ce mémoire, qui sera présentée dans la section 5.3. De plus, le système  $\mathcal{S}$  n'a pas d'évolution propre bien que le modèle présenté en section 3.2.1.5 introduira une évolution non-triviale.

Il est souvent utile d'exploiter la structure de produit tensoriel de cet hamiltonien. En effet, celui-ci peut s'écrire

$$H_{\mathcal{SE}} = \sigma_{\mathcal{S}}^z \otimes H_{int} \quad \text{où} \quad H_{int} = \sum_k g_k \sigma_k^z. \quad (3.15)$$

Dans toute la suite, nous nous placerons dans la base des états propres de  $\sigma^z$  en notant  $|0\rangle$  et  $|1\rangle$  les états propres de  $\sigma_{\mathcal{S}}^z$  et  $|0_k\rangle$  et  $|1_k\rangle$  les états propres de  $\sigma_k^z$ . Cette base sera appelée base de calcul par analogie avec l'informatique quantique. L'état  $|0\rangle \otimes |x\rangle$  avec  $x \in \{0, 1\}^n$  représente donc un état de  $\mathcal{H}^{\mathcal{S}} \otimes \mathcal{H}^{\mathcal{E}}$  pour lequel  $\mathcal{S}$  est dans l'état  $|0\rangle$  et le  $k$ ième spin de l'environnement est dans l'état du  $k$ ième bit  $x_k$  de la chaîne de bit  $x$ . Cette base joue un rôle particulier car l'hamiltonien d'interaction y est diagonal.

**Proposition 3.3.** *L'hamiltonien d'interaction (3.14) a pour vecteur propre les états  $|0\rangle|x\rangle$  et  $|1\rangle|x\rangle$  où  $x \in \{0, 1\}^n$  représente les  $n$  spins de  $\mathcal{E}$  dans un état propre de  $\bigotimes_{k=1}^n \sigma_k^z$ . Les valeurs propres associées  $E_{0x}$  et  $E_{1x}$  sont*

$$E_{0x} = -E_{1x} = \omega_x = \sum_k (-1)^{x_k} g_k. \quad (3.16)$$

Cette propriété va nous permettre de calculer facilement l'évolution d'un état dans le temps en l'écrivant dans la base de calcul.

## 3.2.1.2 Évolution dans le temps

Initialement, le système  $\mathcal{S}$  est dans un état pur quelconque

$$|\psi(t=0)\rangle = a|0\rangle + b|1\rangle. \quad (3.17)$$

L'environnement est dans un état correspondant à un produit tensoriel d'état pur de chacun des spins

$$|\varepsilon(t=0)\rangle = \bigotimes_{k=1}^n (\alpha_k|0_k\rangle + \beta_k|1_k\rangle). \quad (3.18)$$

Nous verrons que le choix de cet état peut jouer un grand rôle dans l'évolution. L'état global initial  $|\Psi_{\mathcal{SE}}(t=0)\rangle = |\psi(t=0)\rangle \otimes |\varepsilon(t=0)\rangle$  va évoluer sous l'action de l'hamiltonien d'interaction. En raison de la structure de produit tensoriel de l'hamiltonien, son évolution à  $t > 0$  sera donnée par

$$|\Psi_{\mathcal{SE}}(t)\rangle = a|0\rangle \otimes |\varepsilon_0(t)\rangle + b|1\rangle \otimes |\varepsilon_1(t)\rangle \quad (3.19)$$

où les états  $|\varepsilon_0(t)\rangle$  et  $|\varepsilon_1(t)\rangle$  vérifient les équations de Schrödinger

$$\begin{cases} i \frac{d}{dt} |\varepsilon_0(t)\rangle = H_{int} |\varepsilon_0(t)\rangle \\ i \frac{d}{dt} |\varepsilon_1(t)\rangle = -H_{int} |\varepsilon_1(t)\rangle \end{cases} \quad (3.20)$$

avec les conditions initiales  $|\varepsilon_0(t=0)\rangle = |\varepsilon_1(t=0)\rangle = |\varepsilon(t=0)\rangle$ .

La résolution de ces équations fournit le résultat suivant.

**Proposition 3.4.** *L'évolution des états  $|\varepsilon_0(t)\rangle$  et  $|\varepsilon_1(t)\rangle$  est*

$$|\varepsilon_0(t)\rangle = |\varepsilon_1(-t)\rangle = \bigotimes_{k=1}^N \alpha_k e^{-ig_k t} |0\rangle_k + \beta_k e^{ig_k t} |1\rangle_k = e^{i\phi} \bigotimes_{k=1}^N (\alpha_k |0\rangle_k + \beta_k e^{2ig_k t} |1\rangle_k). \quad (3.21)$$

Remarquons que le système  $\mathcal{S}$  sera le plus souvent intriqué avec son environnement, ce qui va induire un déphasage entre les états  $|0\rangle$  et  $|1\rangle$ .

### 3.2.1.3 Opérateur densité réduit de $\mathcal{S}$

Dans cette section, nous allons décrire l'évolution du système  $\mathcal{S}$  du point de vue d'un observateur qui n'a pas accès à l'environnement. Comme nous l'avons montré en 2.1.2, l'état du système  $\mathcal{S}$  sera alors décrit par un opérateur densité  $\rho(t)$  défini par

$$\rho(t) = \text{Tr}_{\mathcal{E}} |\Psi_{\mathcal{SE}}\rangle \langle \Psi_{\mathcal{SE}}|. \quad (3.22)$$

Un calcul simple montre que

$$\rho(t) = |a|^2 |0\rangle \langle 0| + |b|^2 |1\rangle \langle 1| + ab^* r(t)^* |0\rangle \langle 1| + a^* b r(t) |1\rangle \langle 0| \quad (3.23)$$

où le *facteur de cohérence*

$$r(t) = \langle \varepsilon_0(t) | \varepsilon_1(t) \rangle \quad (3.24)$$

mesure la distinguabilité entre les états  $|\varepsilon_0(t)\rangle$  et  $|\varepsilon_1(t)\rangle$ .

Dans la base de calcul, l'évolution du système  $\mathcal{S}$  est donc

$$\rho(t=0) = \begin{pmatrix} |a|^2 & a^*b \\ ab^* & |b|^2 \end{pmatrix} \rightarrow \rho(t) = \begin{pmatrix} |a|^2 & a^*b \times r(t) \\ ab^* \times r(t)^* & |b|^2 \end{pmatrix} \quad (3.25)$$

Bien que les composantes  $|0\rangle \langle 0|$  et  $|1\rangle \langle 1|$  ne soient pas affectées, les termes hors-diagonale sont réduits par un facteur  $r(t)$ . Essayons de mieux comprendre l'impact de ce facteur en considérant les différentes valeurs qu'il peut prendre. Si  $r(t) = e^{i\theta}$ , l'opérateur densité correspond à l'état pur  $a|0\rangle + be^{i\theta}|1\rangle$  : la cohérence du qubit a été préservée et il n'a subi qu'une évolution unitaire. Au contraire, si  $r(t) = 0$ , la superposition initiale  $a|0\rangle + b|1\rangle$  est devenue un mélange statistique  $|a|^2|0\rangle \langle 0| + |b|^2|1\rangle \langle 1|$  qui a perdu toute cohérence de phase. Plus généralement, la pureté de  $\rho$ , définie par  $\text{Tr}\rho^2$  s'exprime simplement en fonction de  $r(t)$

$$\text{Tr}\rho^2 = 1 - 2|a|^2|b|^2(1 - |r(t)|^2). \quad (3.26)$$

Nous sommes donc logiquement amenés à nous intéresser à l'évolution dans le temps du facteur  $r(t)$ .

**Proposition 3.5.** *L'évolution du facteur de cohérence est donnée par*

$$r(t) = \sum_{x \in \{0,1\}^n} p_x e^{2i\omega_x t} \quad (3.27)$$

où  $p_x \equiv |\langle x | \varepsilon(t=0) \rangle|^2 = \prod_k (|\alpha_k|^2 \langle x_k | 0 \rangle + |\beta_k|^2 \langle x_k | 1 \rangle)$  est la probabilité de mesurer l'état initial de l'environnement dans l'état propre  $|x\rangle$ .

La fonction  $t \mapsto r(t)$  est donc une somme d'exponentielles. Toutefois, il ne s'agit pas en général d'une fonction périodique, puisque rien ne garantit que les rapports  $\frac{\omega_x}{\omega_y}$  soient rationnels. Une telle fonction est appelée *presque périodique*, une notion introduite par le mathématicien Harald Bohr, le frère de Niels <sup>2</sup>. Un des résultats importants sur les fonctions presque périodiques est qu'elles admettent une valeur moyenne définie par

$$\overline{f(t)} \equiv \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T f(t) dt. \quad (3.28)$$

Or, la valeur moyenne de  $t \mapsto r(t)$  n'est pas simple à calculer. Puisque la pureté est plutôt fonction de  $t \mapsto |r(t)|^2$  et pour des raisons pratiques, nous allons plutôt nous intéresser à la valeur moyenne de la fonction presque périodique  $t \mapsto |r(t)|^2$ . Un calcul simple montre que

$$|r(t)|^2 = \sum_{x \in \{0,1\}^n} p_x^2 + \sum_{x \neq y} p_x p_y \cos 2(\omega_x - \omega_y)t. \quad (3.29)$$

**Proposition 3.6.** *La valeur moyenne de  $t \mapsto |r(t)|^2$  est*

$$\overline{|r(t)|^2} = \sum_{x \in \{0,1\}^n} p_x^2. \quad (3.30)$$

---

<sup>2</sup>Harald Bohr fut aussi joueur de football pour l'équipe du Danemark et remporta la médaille d'argent aux Jeux Olympiques de 1908.

Comment cette grandeur varie-t-elle avec la taille de l'environnement ? La taille de l'environnement sera caractérisée par le nombre  $n$  de spins qu'il contient. En admettant que les probabilités  $p_x$  soient toutes du même ordre de grandeur, c'est-à-dire que l'amplitude de chacun des états propres de l'hamiltonien d'interaction  $H_{int}$  est du même ordre dans l'état initial de l'environnement  $|\varepsilon(t=0)\rangle$ , la valeur moyenne de  $t \mapsto |r(t)|^2$  est

$$\overline{|r(t)|^2} = 2^{-n} \quad (3.31)$$

qui décroît donc *exponentiellement* avec la taille de l'environnement.

*Remarque 3.7.* Dans le cas particulier où  $\mathcal{E}$  est initialement préparé dans un état propre de l'hamiltonien d'interaction  $H_{int}$ , la cohérence est maintenue. . . Nous reviendrons en grand détail sur ce phénomène dans le chapitre 5.

L'évolution de  $\rho(t)$  peut être représentée dans la boule de Bloch. Les coordonnées cartésiennes du vecteur polarisation  $\mathbf{p}$  défini en sont

$$\begin{cases} x(t) = 2\text{Re}(ab^*r(t)) \\ y(t) = 2\text{Im}(ab^*r(t)) \\ z(t) = |a|^2 - |b|^2. \end{cases} \quad (3.32)$$

Ainsi, en raison des coefficients diagonaux constants, le point représentant  $\rho(t)$  dans la boule de Bloch évolue dans le plan  $z = |a|^2 - |b|^2$ . Cette intersection est un disque de rayon  $2|a||b|$ . En normalisant les coordonnées par les termes constants  $|a|$  et  $|b|$  et en effectuant une rotation du repère afin que le point initial soit de coordonnées  $(1, 0)$ , on obtient une évolution donnée par

$$\begin{cases} \tilde{x}(t) = \text{Re}(r(t)) \\ \tilde{y}(t) = \text{Im}(r(t)) \end{cases} \quad (3.33)$$

qui n'est autre qu'une courbe paramétrique dans le disque unité du plan complexe (voir figure 3.3).

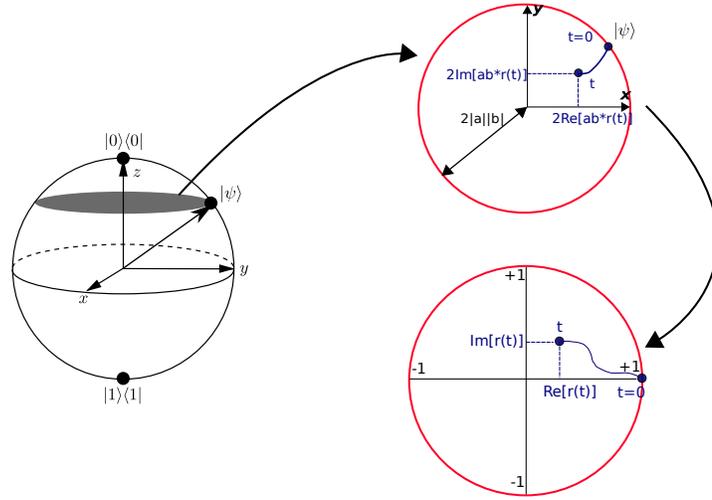


Figure 3.3 – Évolution d'un état dans la boule de Bloch

L'évolution de  $r(t)$  peut être simulée numériquement (voir figure 3.4). Elle présente plusieurs propriétés intéressantes, particulièrement à temps court d'une part et à temps longs d'autre part.

Initialement, le point  $r(0)$  est sur le cercle. S'ensuit alors une phase de décroissance. J.M. Cuchietti, J.P. Paz et W.H. Żurek ont montré [26] que la décroissance initiale était le plus souvent gaussienne, c.-à-d. que pour  $t$  petit par rapport à  $\frac{1}{\max_k g_k}$ , l'évolution est de type

$$r(t) = e^{i\theta t} e^{-s_n^2 t^2 / 2} \quad (3.34)$$

où  $s_n$  est l'écart-type des variables aléatoires  $x_k$  qui valent  $+g_k$  avec probabilité  $|\alpha_k|^2$  et  $-g_k$  avec probabilité  $|\beta_k|^2$ , sous réserve que cet écart-type soit défini. Sinon, la décroissance initiale peut être exponentielle

$$r(t) = e^{-a|t|}. \quad (3.35)$$

À temps longs, la fonction  $t \mapsto |r(t)|$  est presque périodique. Elle admet donc des  $\varepsilon$ -presque périodes  $T$ , aussi appelée période de Poincaré, telles que

$$\sup_{t \in \mathbb{R}} ||r(t + T_\varepsilon)| - |r(t)|| \leq \varepsilon. \quad (3.36)$$

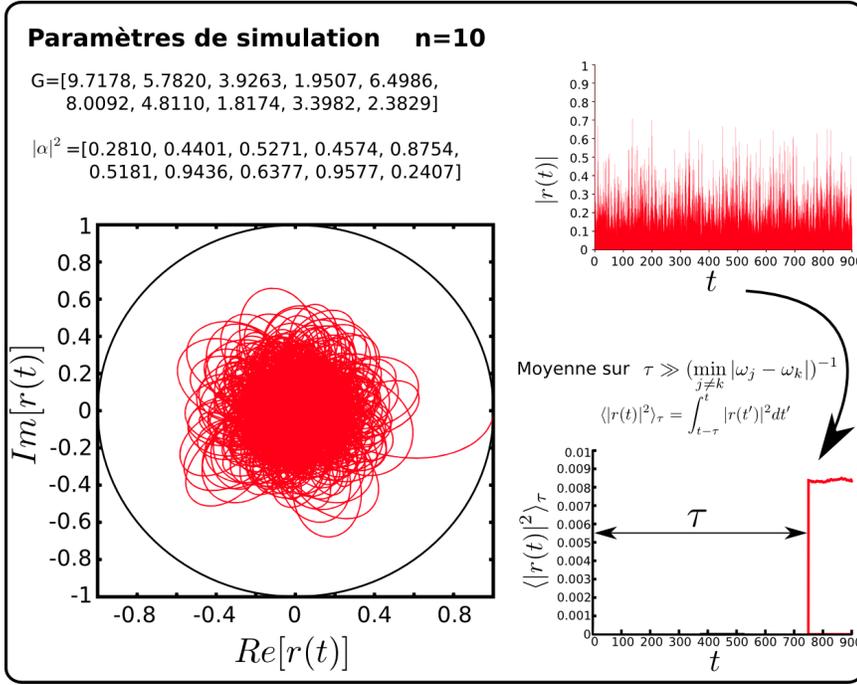


Figure 3.4 – Simulation numérique de l'évolution du facteur de cohérence

En particulier, la cohérence initiale caractérisée par  $|r(t=0)| = 1$  est retrouvée, à  $\varepsilon$  près, après un temps  $T_\varepsilon$ . Ce retour de la cohérence est considéré comme un artefact du modèle. En effet, quand la taille de l'environnement augmente, les presque périodes  $T_\varepsilon$  varient avec  $n!$ . Ainsi, pour des environnements de taille réaliste, les presque périodes pour  $\varepsilon$  petit sont plus longues que l'âge de l'Univers.

L'interaction entre l'environnement et le spin a donc pour effet de sélectionner une base privilégiée. Il s'agit ici de la base  $\{|0\rangle, |1\rangle\}$  puisque si l'état initial du spin  $\mathcal{S}$  est  $|0\rangle$  ou  $|1\rangle$ , l'interaction avec l'environnement n'aura aucun effet. Si l'état initial est une superposition  $a|0\rangle + b|1\rangle$ , l'interaction va réduire la cohérence. Pour un environnement de grande taille et pour la plupart des états initiaux de l'environnement, la superposition initiale est ainsi transformée en un mélange statistique dont l'état est très proche de

$$\rho_{\text{decoherence}} = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|. \quad (3.37)$$

### 3.2.1.4 Caractéristiques générales

Le modèle de Żurek présente les caractéristiques générales d'un modèle de décohérence, qui distingue plusieurs ensembles d'opérateurs densité qui sont ici facilement identifiables dans la boule de Bloch.

L'interaction système-environnement privilégie une base particulière. Il s'agit ici des états purs  $|0\rangle$  et  $|1\rangle$ . Ceux-ci sont sélectionnés par la structure de l'hamiltonien  $H_{SE} = \sigma_S^z \otimes H_{int}$  : l'hamiltonien est un produit tensoriel et les états  $|0\rangle$  et  $|1\rangle$  sont les états propres de  $\sigma_S^z$ . Ce modèle est toutefois très simple puisque ces états ne sont pas du tout affectés par l'interaction. Plus généralement, les modèles de décohérence exhibent des états purs qui sont peu affectés par la décohérence. Ces états sont qualifiés d'états indicateurs en référence au problème de la mesure quantique ou encore d'états quasi-classiques puisqu'ils correspondent habituellement aux états sélectionnés au niveau macroscopique.

La décohérence va aussi transformer une superposition d'états indicateurs en un opérateur densité *presque* diagonal dans cette base. Les états mixtes de la forme  $|a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|$  sont situés sur la droite  $z$  (voir figure 3.5) et correspondent à des distributions de probabilité classiques : le système est dans l'état quasi-classique  $|0\rangle$  avec probabilité  $|a|^2$  ou dans l'état quasi-classique  $|1\rangle$  avec probabilité  $|b|^2$ . Plus généralement, les modèles de décohérence vont isoler une région correspondant aux probabilités classiques.

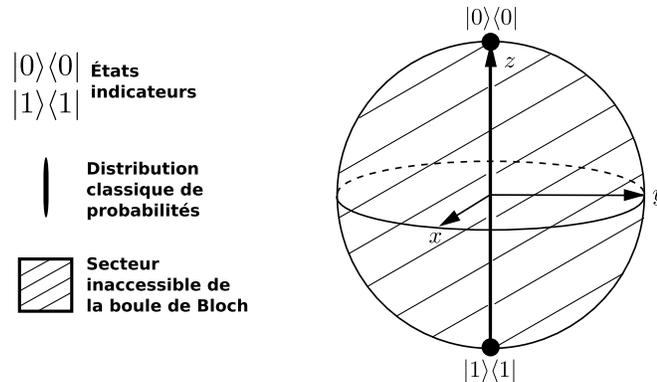


Figure 3.5 – Représentation simplifiée des domaines

Finalement, tout le reste de l'espace de Hilbert est interdit par la décohérence. Il s'agit de tous les états non-classiques théoriquement atteignables selon la mécanique quantique. Or, l'accès à ces états est primordial en informatique quantique. Il faudra donc mettre en place des stratégies pour lutter contre la décohérence, ce qui sera l'objet du chapitre 5.

### 3.2.1.5 Évolution propre du système

Le modèle de Żurek a été étendu par F.M. Cucchietti, J.P. Paz et W.H. Żurek en 2005 [26] en ajoutant une dynamique propre au système à l'hamiltonien (3.14)

$$H = \Delta \sigma_{\mathcal{S}}^x \otimes \mathbf{1}_{\mathcal{E}} + \frac{1}{2} \sigma_{\mathcal{S}}^z \otimes \sum_{k=1}^n g_k \sigma_k^z. \quad (3.38)$$

Cet ajout permet de faire varier l'importance relative de l'évolution propre par rapport à l'évolution liée à l'interaction avec l'environnement.

Dans la limite où l'évolution propre domine, c.-à-d.  $\Delta \gg s_n$  où  $s_n$  est l'écart-type des niveaux d'énergies, et à temps long, c.-à-d.  $t \gg s_n$  et  $t \gg \Delta^{-1}$ , les composantes du vecteur polarisation  $\mathbf{p}$  sont données par

$$\begin{cases} p_x(t) \simeq \gamma \left( \frac{\Delta}{\sqrt{2s_n}} \right) p_x(0) \\ p_y(t) \simeq \sqrt{\frac{\Delta}{2s_n^2 t}} [p_y(0) \cos(2\Delta t + \frac{\pi}{4}) - p_z(0) \sin(2\Delta t + \frac{\pi}{4})] \\ p_z(t) \simeq p_z(0) \left( 1 - \gamma \left( \frac{\Delta}{\sqrt{2s_n}} \right) \right) + \sqrt{\frac{\Delta}{2s_n^2 t}} [p_z(0) \cos(2\Delta t + \frac{\pi}{4}) + p_y(0) \sin(2\Delta t + \frac{\pi}{4})] \end{cases} \quad (3.39)$$

où  $\gamma(x) = \sqrt{\pi} x e^{x^2} (1 - \text{Erf}(x))$  dont l'expansion asymptotique à l'infini vaut  $\gamma(x) \stackrel{x \rightarrow \infty}{\sim} 1 - \frac{1}{2x^2} + o(\frac{1}{x^3})$ . À partir d'une superposition d'états propres de  $\sigma^x$

$$|\psi\rangle = a \left( \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \right) + b \left( \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \right) = a|+\rangle + b|-\rangle \quad (3.40)$$

l'état est transformé en un mélange statistique

$$\rho = (1 - \frac{s_n^2}{\Delta^2}) (|a|^2 |+\rangle\langle +| + |b|^2 |-\rangle\langle -|) + \frac{s_n^2}{\Delta^2} \text{Re}(a^* b) (|+\rangle\langle -| + |-\rangle\langle +|). \quad (3.41)$$

Les états propres de  $\sigma^x$ , c.-à-d. les états propres de l'hamiltonien du système, sont donc les états indicateurs. Cette conclusion tirée ici d'un exemple peut être rendue très générale : dans la limite où la dynamique propre du système l'emporte sur l'interaction entre le système et l'environnement, les états privilégiés sont les états d'énergie [59]. *Cela justifie en partie l'attention particulière portée aux états d'énergie en mécanique quantique.* Il est important de noter que ce cas limite où l'interaction est faible devant la dynamique du système n'est pas équivalente au cas où l'interaction est complètement négligée puisque l'état quantique donné par (3.41) n'est pas un état pur. En effet, les amplitudes des termes hors-diagonale  $|+\rangle\langle-|$  et  $|-\rangle\langle+|$  ont été réduites. En particulier, sa pureté vaut  $\text{Tr}\rho^2 = (1 - 2\frac{s_n^2}{\Delta^2})(1 - 2|a|^2|b|^2) + o(\frac{s_n^3}{\Delta^3})$ .

### 3.2.2 Autres modèles

De nombreux autres modèles de décohérence existent. Toutefois, leur résolution emprunte habituellement une méthode différente de celle de notre exemple. En effet, dans le modèle de Żurek, l'hamiltonien était assez simple pour permettre de calculer l'évolution du système total puis effectuer une trace partielle afin d'obtenir l'opérateur densité réduit du système. Une autre voie (cf. figure 3.6) consiste à d'abord effectuer une trace partielle pour obtenir une équation sur l'évolution du système puis de ne calculer que l'évolution du système. Ces modèles seront évoqués dans l'annexe D.

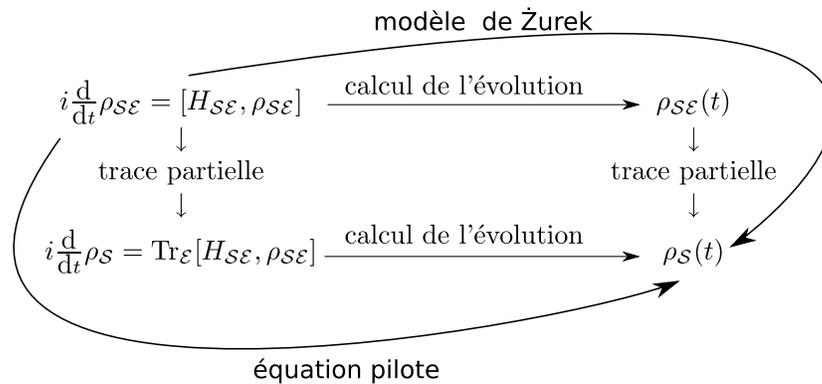


Figure 3.6 – Alternative pour résoudre un modèle

### 3.3 Rôles de l'environnement

Le rôle de l'environnement est essentiel pour la théorie de la décohérence. Dans cette section, nous mentionnerons les différents rôles joués par l'environnement. Tout d'abord, il permet de privilégier une base dans l'espace de Hilbert : ce phénomène de supersélection est nommé *einselection* pour *environment-induced superselection*. De plus, il détruit la cohérence d'une superposition d'états de cette base privilégiée, transformant le plus souvent une superposition cohérente en mélange statistique : il s'agit ici du phénomène de décohérence proprement dit. Ces deux rôles, intimement liés, font de l'environnement un censeur qui restreint les états quantiques accessibles. En ce sens, l'environnement joue un rôle négatif. Il est toutefois possible de percevoir l'environnement comme un agent qui multiplie les copies de l'information classique et les rend disponibles aux observateurs : il s'agit du paradigme de l'environnement en tant que témoin [55].

#### 3.3.1 Supersélection induite par l'environnement

Comme nous l'avons vu dans le modèle de Żurek, l'interaction entre le système et l'environnement permet l'émergence d'une base particulière de l'espace de Hilbert. Les états du système *ouvert* ne sont pas traités sur un pied d'égalité, contrairement à ce que laisserait croire l'application naïve du principe de superposition.

##### 3.3.1.1 Mesure étendue de von Neumann

Dans le modèle de mesure quantique de von Neumann, le système  $\mathcal{S}$  interagit avec un appareil de mesure  $\mathcal{A}$  afin de s'intriquer et d'aboutir dans un état de pseudo-mesure. Or, un tel état présente des difficultés d'interprétation en raison de la possibilité de réécrire une décomposition biorthogonale dans une autre base. Ainsi, il n'est pas possible d'assigner une observable à l'état après pseudo-mesure.

L'introduction d'un environnement  $\mathcal{E}$  qui interagit avec le système conjoint  $\mathcal{SA}$  va changer radicalement la situation puisque l'interaction avec l'environnement va privilégier une observable entre  $\mathcal{S}$  et  $\mathcal{A}$ . De plus, un théorème affirme l'unicité d'une décomposition triorthogonale

**Théorème 3.8.** *Si un état pur  $|\psi^{S\mathcal{A}\mathcal{E}}\rangle \in \mathcal{H}^S \otimes \mathcal{H}^A \otimes \mathcal{H}^{\mathcal{E}}$  s'écrit*

$$|\psi^{S\mathcal{A}\mathcal{E}}\rangle = \sum_i c_i |s_i\rangle |a_i\rangle |e_i\rangle \quad (3.42)$$

où les familles  $\{|s_i\rangle\} \subset \mathcal{H}^S, \{|a_i\rangle\} \subset \mathcal{H}^A$  sont libres et les  $|e_i\rangle \in \mathcal{H}^{\mathcal{E}}$  sont non-colinéaires, alors cette décomposition est unique [20, 24, 31].

Ce théorème n'affirme pas l'existence générale d'une telle décomposition mais permet de montrer que l'interaction avec un troisième système permet de lever l'ambiguïté dans la décomposition biorthogonale. Par contre, ce théorème ne fournit aucun moyen de déterminer la base privilégiée.

Nous allons toutefois présenter certaines limites où il est possible de savoir quelle est cette base privilégiée. Pour simplifier, nous traiterons le système  $\mathcal{SA}$  comme un seul système quantique que nous nommerons  $\mathcal{S}$ .<sup>3</sup> L'hamiltonien total sera de la forme

$$H = H_{S\mathcal{E}} + H_S \otimes \mathbf{1}_{\mathcal{E}} + \mathbf{1}_S \otimes H_{\mathcal{E}}. \quad (3.43)$$

### 3.3.1.2 Limite de la mesure quantique

La limite de la mesure quantique s'intéresse au cas où l'interaction entre le système et l'environnement, représentée par  $H_{S\mathcal{E}}$ , domine les dynamiques propres. Les états indicateurs sont alors des états  $|s_i\rangle \in \mathcal{H}^S$  tels que pour tout état initial de l'environnement  $|e_0\rangle$ , l'évolution subséquente n'intrique pas  $|s_i\rangle$  avec l'environnement, c.-à-d.

$$\forall |e_0\rangle |s_i\rangle |e_0\rangle \mapsto e^{-iH_{S\mathcal{E}}} (|s_i\rangle |e_0\rangle) = |s_i\rangle |e_i(t)\rangle. \quad (3.44)$$

---

<sup>3</sup>Ce choix revient à écrire un état  $\sum_i |s_i\rangle |a_i\rangle |e_i\rangle$  sous la forme  $\sum_i |s_i\rangle |e_i\rangle$ .

Dans le cas particulier où l'hamiltonien est un produit tensoriel

$$H = H_{S\mathcal{E}} = S \otimes E, \quad (3.45)$$

ce qui souvent le cas, il suffit de choisir les états propres de l'opérateur hermitien  $S$  comme états indicateurs [77]. En effet, pour de tels états

$$e^{-iS \otimes E} |s_i\rangle |e_0\rangle = |s_i\rangle e^{-i\lambda_i t} e^{-iEt} |e_0\rangle = |s_i\rangle |e_i(t)\rangle \quad (3.46)$$

où il est clair que le système ne s'intrique pas avec l'environnement. Autrement dit, l'observable privilégiée est

$$O = \sum_i o_i |s_i\rangle \langle s_i| \quad (3.47)$$

qui commute avec l'hamiltonien d'interaction

$$[O \otimes \mathbf{1}_{\mathcal{E}}, H_{S\mathcal{E}}] = 0. \quad (3.48)$$

Ce cas amène un élément de réponse au fait que la position des objets semble jouer un rôle privilégié par rapport aux autres observables. En effet, plusieurs hamiltoniens d'interaction sont de la forme  $X \otimes E$  où  $X$  est l'observable liée à la position. Dans ce cas, les états indicateurs seront les états propres de  $X$ , c.-à-d. les états de position définie.

Plus généralement, l'hamiltonien d'interaction peut toujours se décomposer comme une somme de produits tensoriels d'opérateurs hermitiens

$$H_{S\mathcal{E}} = \sum_k S_k \otimes E_k. \quad (3.49)$$

Dans ce cas, le choix d'une base indicatrice est plus compliqué puisque les bases propres des opérateurs  $S_k$  ne coïncident pas. Des critères plus élaborés ont été proposés afin de déterminer la base indicatrice [29].

### 3.3.1.3 Limite quantique de la décohérence

La limite de la mesure quantique s'intéresse au cas où la dynamique propre du système, représentée par  $H_S$ , domine. Nous l'avons déjà évoqué en section 3.2.1.5. Ce cas, fréquent pour les systèmes microscopiques qui interagissent faiblement avec d'autres degrés de liberté, a été étudié en détail par J.P. Paz et W.H. Żurek [59]. Les états indicateurs sont alors les états propres de l'hamiltonien d'interaction propre  $\mathcal{S}$ . Cela permet d'expliquer le rôle privilégié des états d'énergie pour les systèmes microscopiques.

### 3.3.1.4 Cas intermédiaires

Dans le cas général, les états indicateurs résultent de la compétition entre l'hamiltonien propre  $H_S$  et l'hamiltonien d'interaction  $H_{S\mathcal{E}}$ . Dans ce cas, il faut avoir recours à des critères plus sophistiqués. L'un d'entre eux, introduit par Żurek, est le crible de prévisibilité [79, 81] : pour chaque état initial pur  $|\psi\rangle$  du système, la perte d'information résultant de l'évolution subséquente est mesurée sur l'opérateur densité réduit  $\rho(t)$  en calculant l'entropie de von Neumann (2.11)  $S(\rho) = -\text{Tr}[\rho \log \rho]$  (ou une autre mesure, par exemple la pureté  $\text{Tr}\rho^2$ ). Les états indicateurs sont ceux qui minimisent  $S(\rho)$  après une durée  $\tau$  et pour lesquels ce minimum est robuste devant une variation raisonnable de  $\tau$ .

Ce critère permet de déterminer les états pointeurs du mouvement brownien quantique (dont le modèle est défini en section D.1.1). Le calcul de la variation de pureté  $\xi(\rho) = \text{Tr}\rho^2$  sur une période  $T = \frac{2\pi}{\Omega}$  de l'oscillateur harmonique de la particule donne

$$\xi(\rho(T)) = -2D \left( \Delta x^2 + \frac{\Delta p^2}{M^2\Omega^2} \right) \quad (3.50)$$

où  $\Delta x$  et  $\Delta p$  sont les dispersions en position et en impulsion de l'état initial. Or, la relation d'incertitude de Heisenberg impose  $\Delta x \Delta p \geq \frac{1}{2}$ . La perte de

pureté est alors minimisée pour

$$\Delta x \Delta p = \frac{1}{2} \quad \text{et} \quad \Delta x^2 = \frac{1}{2M\Omega} \quad (3.51)$$

c'est-à-dire pour un état cohérent d'incertitude minimale. Ainsi, ces états sont des états qui se rapprochent le plus d'états classiques dans l'espace des phases  $(x, p)$ . Ils représentent un compromis entre l'interaction avec l'environnement qui privilégie les états de position définie et l'interaction propre du système qui privilégie les états d'impulsion définie.

### 3.3.2 Décohérence induite par l'environnement

Comme nous l'avons montré, la décohérence privilégie certains états, les états indicateurs  $\{|s_i\rangle\}$ , qui ne s'intriquent que peu, voire pas, avec l'environnement. Un phénomène complémentaire accompagne cette supersélection : il s'agit de l'atténuation des termes de cohérence liés à ces états indicateurs. Une superposition cohérente d'états pointeurs

$$|\psi\rangle = \sum_i c_i |s_i\rangle \quad (3.52)$$

correspond à un opérateur densité

$$|\psi\rangle\langle\psi| = \sum_i |c_i|^2 |s_i\rangle\langle s_i| + \sum_{i \neq j} c_i c_j^* |s_i\rangle\langle s_j| \quad (3.53)$$

qui contient des termes  $|s_i\rangle\langle s_j|$  appelés *cohérences*. Ceux-ci se manifestent par des phénomènes d'interférence, par exemple l'interférogramme caractéristique de l'expérience des fentes de Young. Or, en raison de l'interaction avec l'environnement, l'état  $|\psi\rangle$  va s'intriquer avec  $\mathcal{E}$

$$|\Psi^{\mathcal{SE}}\rangle = \sum_i c_i |s_i\rangle |e_i\rangle. \quad (3.54)$$

Plus les états  $|e_i\rangle$  et  $|e_j\rangle$ , associés aux termes de cohérence  $|s_i\rangle\langle s_j|$ , sont

distinguable, plus l'information contenue dans l'environnement est corrélée avec l'état du système. Du point de vue de l'observateur qui possède  $\mathcal{S}$ , les degrés de liberté de l'environnement étant le plus souvent à toute fin pratique inobservables, il va décrire l'état quantique du système  $\mathcal{S}$  par un opérateur densité réduit

$$\rho_{\mathcal{S}} = \text{Tr}_{\mathcal{E}} |\Psi^{S\mathcal{E}}\rangle \langle \Psi^{S\mathcal{E}}| = \sum_i |c_i|^2 |s_i\rangle \langle s_i| + \sum_{i \neq j} c_i c_j |s_i\rangle \langle s_j| \langle e_i | e_j \rangle \quad (3.55)$$

où les termes de cohérence sont donc réduits par un facteur  $\langle e_i | e_j \rangle$ . Or, ces produits scalaires, pour la plupart des modèles physiques, décroissent de façon exponentielle  $\langle e_i | e_j \rangle = e^{-t/\tau}$  ou gaussienne  $\langle e_i | e_j \rangle = e^{-t^2/\tau^2}$  sur des échelles de temps très courtes. Ainsi, encore une fois à toute fin pratique, pour une durée grande devant le temps caractéristique de décohérence  $\tau$ , l'état quantique du système devient

$$\rho_{\text{déc}} = \sum_i |c_i|^2 |s_i\rangle \langle s_i|. \quad (3.56)$$

Pour fixer les idées, donnons l'exemple d'une particule soumise au mouvement brownien quantique (décrit en D.1.1) qui est initialement préparée dans un état de superposition

$$|\psi\rangle = \frac{1}{\sqrt{2}} | -a \rangle - \frac{1}{\sqrt{2}} | +a \rangle \quad (3.57)$$

où  $|\pm a\rangle$  correspondent à des paquets d'onde gaussiens centrés en  $x = \pm a$ , de la forme  $\phi(x \mp a) = e^{-(x \mp a)^2/(2\sigma^2)}$ . Pour qu'il s'agisse bien d'un état "chat de Schrödinger", on impose  $a \gg \sigma$ . La distribution en impulsion d'un tel état est

$$\begin{aligned} \mathcal{P}(p) &= \left| \text{TF} \left[ \frac{1}{\sqrt{2}} \phi(x - a) - \frac{1}{\sqrt{2}} \phi(x + a) \right] \right|^2 \\ &= \frac{1}{2} \left| \tilde{\phi}(p) e^{-ipa} - \tilde{\phi}(p) e^{+ipa} \right|^2 \\ &= 2 \sin^2 pa |\tilde{\phi}(p)|^2 \end{aligned} \quad (3.58)$$

où  $\tilde{\phi}(p)$  est la transformée de Fourier de  $\phi(x)$ . Ainsi, la distribution en impulsion est une enveloppe gaussienne qui contient une modulation de fréquence spatiale  $a$ . Cette oscillation est responsable des phénomènes d'interférence et constitue une signature de la cohérence de l'état.

Aux temps courts, l'évolution de la particule dans le mouvement brownien est dominée par l'échange d'impulsion avec les molécules de l'environnement et il est possible de montrer que

$$\frac{\partial}{\partial t} \langle x | \rho_S | x' \rangle = -D(x - x')^2 \langle x | \rho_S | x' \rangle \quad (3.59)$$

où  $D \in \mathbb{R}$  caractérise la dispersion en impulsion. Nous en déduisons que

$$\langle x | \rho_S(t) | x' \rangle = e^{-D(x-x')^2 t} \langle x | \rho_S(t=0) | x' \rangle. \quad (3.60)$$

La décroissance est donc exponentielle par rapport au carré de la séparation spatiale  $(x - x')^2$ .

Le temps caractéristique de cohérence  $\tau_{\text{coh}}$  pour réduire les termes de cohérence de type  $|x = +a\rangle \langle x = -a|$  est donc

$$\tau_{\text{coh}} = \frac{1}{Da^2} \quad (3.61)$$

qui peut être réécrit en terme du coefficient de friction  $\gamma = \frac{D}{Mk_B T}$  dont l'inverse caractérise le temps de relaxation du système et de la longueur d'onde thermique de la particule  $\lambda_T = (2\pi Mk_B T)^{-1/2}$  pour obtenir

$$\tau_{\text{coh}} = \gamma^{-1} \left( \frac{\lambda_T}{a} \right)^2 \quad (3.62)$$

un résultat obtenu par J.P. Paz, S. Habib et W.H. Żurek en 1993 [58]. Une application numérique montre que pour une séparation macroscopique  $a$  de 1 cm, une masse macroscopique  $M$  de 1 g, la longueur d'onde thermique vaut  $\lambda_T = 1,3 \times 10^{-20}$  cm, soit  $\tau_{\text{coh}} \sim 10^{-40} \gamma^{-1}$ . Ainsi, le temps de décohérence est plus petit de 40 ordres de magnitude devant le temps de relaxation !

### 3.3.3 Environnement en tant que témoin

Jusqu'ici l'environnement a joué un rôle de censeur en restreignant l'accès à l'espace de Hilbert. Essentiellement, il constitue un ensemble de degrés de liberté intriqué avec le système qui est inaccessible à toute fin pratique à un observateur. Ainsi, l'environnement est presque une décharge qui sert à vidanger l'information.

Or, un observateur acquiert habituellement de l'information sur le système non pas en interagissant directement avec lui, mais plutôt en interceptant des fragments de l'environnement qui joue alors le rôle d'un témoin. Par exemple, nous déterminons la position des objets en interceptant des photons qui ont interagi avec l'objet. De plus l'information obtenue via l'interrogation de l'environnement semble *classique* : elle peut être acquise sans perturber l'état du système et elle est redondante permettant à plusieurs observateurs de s'accorder sur l'état du système.

L'environnement joue donc non seulement le rôle de diffuseur d'information, mais de plus il sélectionne une partie de l'information à propos du système qu'il va stocker de façon redondante et encoder de façon robuste. Ce rôle particulier de l'environnement et le changement de paradigme qu'il entraîne a été mis en évidence par H. Ollivier, D. Poulin et W.H. Żurek [55]. La sélection de l'information qui sera stockée de façon robuste et donc accessible aux observateurs a été qualifiée de *darwinisme quantique*, un thème repris et étudié en particulier par R. Blume-Kohout et W.H. Żurek [14, 80] et appuyé expérimentalement [19].

Ce changement de paradigme a permis de mettre en évidence plusieurs caractéristiques importantes sur l'information stockée par l'environnement. En particulier, l'observable sur le système qui laisse le plus de traces dans l'environnement coïncide avec l'observable correspondant aux états indicateurs. Ce résultat permet de faire le lien entre les deux paradigmes. De plus, une mesure a été proposée afin de quantifier la classicalité des corrélations entre deux systèmes physiques : la discordance quantique [56].

## **Théorie de la décohérence et transition quantique-classique**

La théorie de la décohérence propose des mécanismes pour l'émergence d'un monde classique à partir d'un monde quantique. Elle repose essentiellement sur le constat qu'un système quantique n'est habituellement pas fermé mais en interaction avec un grand nombre de degrés de liberté qui constitue son environnement. L'interaction système-environnement va mener à de l'intrication qui privilégie certains états du système, les états indicateurs. Or, à toute fin pratique, les degrés de liberté de l'environnement sont inaccessibles à un observateur qui décrit alors l'état du système comme un opérateur densité réduit. Cet opérateur sera souvent diagonal dans la base des états indicateurs après un temps de décohérence, habituellement très court devant les autres temps caractéristiques du système et de l'interaction. Ce phénomène entraîne une forte atténuation, voire la disparition, de corrélations quantiques qui sont essentielles au calcul quantique ou plus généralement au traitement de l'information quantique.

Dans le prochain chapitre, nous nous intéressons à une tâche bien précise : la transmission et l'emploi d'un gyroscope quantique. L'étude de ce scénario, qui constitue un des deux apports personnels principaux de ce mémoire, nous permettra de mettre en application tous les outils introduits dans le chapitre 2 et de montrer que le gyroscope décohère de façon conforme aux résultats généraux énoncés dans ce chapitre 3.

# Chapitre 4

## Décohérence d'un gyroscope quantique

Dans ce chapitre, nous nous intéresserons à la transmission d'un gyroscope quantique. Plus spécifiquement, nous étudierons son évolution après qu'il ait été utilisé pour mesurer le moment cinétique de plusieurs particules. L'étude de cette situation permettra d'utiliser et de mettre à profit les notions de superopérateurs et de mesure généralisée introduites dans le chapitre 2. Bien que basé sur des travaux antérieurs, une grande partie du travail présenté ici est *original*. Un soin particulier sera porté à distinguer le travail propre à cette maîtrise des résultats tirés de la littérature.

### 4.1 Motivation

Le partage d'un gyroscope quantique entre Alice et Bob leur permet de partager la connaissance d'une direction particulière dans l'espace. Ainsi, un gyroscope quantique est un cas particulier du formalisme des *références quantiques* étudié par S. Bartlett, T. Rudolph et R. Spekkens [8]. Notre travail se rattache plus précisément à la théorie des ressources quantiques développée par G. Gour et R. Spekkens [37]. Dans ce formalisme, la préparation d'états quantiques est restreinte par une *règle de supersélection*

habituellement associée à un groupe de symétrie. Par exemple, l'absence de référence dans l'espace est associée au groupe  $SU(2)$ . Dans de telles théories, certains états quantiques peuvent être préparés tandis que d'autres sont interdits par la règle de supersélection. Ces états interdits permettent souvent de réaliser des tâches qui seraient autrement impossibles et sont alors qualifiés de *ressource*. Dans le cas  $SU(2)$ , un état quantique constitue une ressource s'il permet à Alice et Bob de se mettre d'accord sur une direction privilégiée dans l'espace. Nous n'entrerons pas dans les détails de cette théorie très élégante mathématiquement. Il nous paraissait toutefois important de mentionner ce formalisme général dont découle le travail présenté ici.

Une autre motivation, plus pragmatique, pour la nécessité d'un gyroscope quantique est liée aux tâches de traitement de l'information. Ainsi, les protocoles de communication quantiques demandent souvent à Alice et Bob de mesurer dans des bases particulières, par exemple dans le protocole de distribution quantique de clé BB84 [12]. Or, il faut qu'ils soient capables de se mettre d'accord sur ces bases. Ce problème est aussi crucial pour les objets manipulant de l'informatique quantique et est déjà présent dans des dispositifs expérimentaux [65, 76]. En effet, souvent pour des raisons de miniaturisation, les systèmes physiques qui serviront de référence seront de taille microscopique. Ils seront alors sujets à des fluctuations et des effets de décohérence similaires à ceux que nous évoquerons dans la suite.

## 4.2 Gyroscope quantique

L'utilisation et plus particulièrement la longévité d'un gyroscope quantique a d'abord été étudiée dans [9]. Notre travail reprendra plus spécifiquement l'approche de D. Poulin et J. Yard [61] et toute la suite de cette section 4.2 reprend leur modèle.

L'objectif est de mesurer le moment angulaire de particules de spin  $\frac{1}{2}$  suivant une certaine direction indiquée par une référence au comportement quantique : un gyroscope quantique.

### 4.2.1 Systèmes en présence

Physiquement, le gyroscope est un objet quantique qui présente un grand moment angulaire dans une direction privilégiée. Mathématiquement, le gyroscope quantique sera décrit comme une particule de spin- $\ell$  et son état sera donné par un opérateur densité noté  $\rho$  de dimension  $d = 2\ell + 1$ . Dans toute la suite,  $d$  représentera la *taille* du gyroscope et nous nous intéresserons au régime  $\ell \gg 1$ . Une base habituelle pour un spin- $\ell$  est  $\{|\ell, m\rangle\}_{m \in [-\ell; +\ell]}$ .

Bien que l'objectif même du modèle suppose qu'il n'existe *a priori* aucune direction privilégiée, il est essentiel d'introduire un référentiel  $(x, y, z)$  afin de pouvoir décrire mathématiquement les phénomènes. En particulier, au moment angulaire du gyroscope est associé l'observable  $\mathbf{L} = (L_x, L_y, L_z)$  qui vérifie les relations habituelles de commutation

$$[L_i, L_j] = i\varepsilon^{ijk} L_k. \quad (4.1)$$

Idéalement,  $\rho$  correspond à un état cohérent de  $SU(2)$ , c'est-à-dire un état dont le moment angulaire pointe maximale dans une direction de coordonnées polaires  $(\theta, \phi)$

$$e^{-i\phi L_z} e^{-i\theta L_y} |\ell, \ell\rangle. \quad (4.2)$$

Le gyroscope servira à mesurer le moment angulaire de particules de spin  $\frac{1}{2}$  qui seront toutes dans le même état décrit par un opérateur densité  $\xi$ .

Au moment angulaire d'une particule de spin  $\frac{1}{2}$  est associé l'observable  $\mathbf{S} = (S_x, S_y, S_z)$  où les  $S_i$  sont proportionnels aux matrices de Pauli  $S_i = \frac{1}{2}\sigma_i$  et obéissent donc à la relation

$$S_i S_j = \frac{1}{4} \delta_{ij} + \frac{i}{2} \varepsilon^{ijk} S_k. \quad (4.3)$$

### 4.2.2 Mesure induite sur la particule

Afin de mesurer le moment angulaire des particules de spin  $\frac{1}{2}$ , la seule mesure non triviale<sup>1</sup> qui soit invariante par rotation est la mesure conjointe du moment angulaire total. Elle correspond à l'observable  $\mathbf{J}^2$

$$\mathbf{J}^2 = (\mathbf{L} + \mathbf{S})^2. \quad (4.4)$$

La mesure de  $\mathbf{J}^2$  aura pour effet de projeter le système total  $\{\mathcal{R} + \mathcal{S}\}$  sur un espace propre de  $\mathbf{J}^2$  associé à la valeur propre  $j(j+1)$  où  $j = \ell \pm \frac{1}{2}$ . Les projecteurs correspondants sont

$$\Pi_{\pm} = \frac{1}{2} \left( \mathbf{1}_{\mathcal{R}\mathcal{S}} \pm \frac{4\mathbf{L} \cdot \mathbf{S} + \mathbf{1}_{\mathcal{R}\mathcal{S}}}{d} \right). \quad (4.5)$$

Caractérisons maintenant la mesure du point de vue de la particule  $\mathcal{S}$  en utilisant la notion de POVM introduite au chapitre 2 en section 2.2.1.2. Les éléments de POVM  $\Lambda_{\pm}$  sont donnés par l'équation (2.21)

$$\Lambda_{\pm} = \text{Tr}_{\mathcal{R}} [\Pi_{\pm} (\rho \otimes \mathbf{1}_{\mathcal{S}})] = \frac{1}{2} \left( \mathbf{1}_{\mathcal{S}} \pm \frac{4\langle \mathbf{L} \rangle \cdot \mathbf{S} + \mathbf{1}_{\mathcal{S}}}{d} \right) \quad (4.6)$$

où  $\langle \mathbf{L} \rangle$  est l'espérance du moment angulaire de la référence, défini par  $\langle \mathbf{L} \rangle_i = \text{Tr}_{\mathcal{R}} [L_i \rho]$ . En définissant le vecteur  $\mathbf{n}_{\rho}$  par

$$\mathbf{n}_{\rho} = \frac{2}{d} \langle \mathbf{L} \rangle, \quad (4.7)$$

les éléments de POVM se réécrivent

$$\Lambda_{+} = \frac{\ell+1}{d} \mathbf{1}_{\mathcal{S}} + \mathbf{n}_{\rho} \cdot \mathbf{S} \quad \Lambda_{-} = \frac{\ell}{d} \mathbf{1}_{\mathcal{S}} - \mathbf{n}_{\rho} \cdot \mathbf{S}. \quad (4.8)$$

Dans la limite quasi-classique  $\ell \rightarrow \infty$ , on retrouve

$$P_{\hat{\mathbf{n}}_{\rho}}^{\pm} = \frac{1}{2} \mathbf{1}_{\mathcal{S}} \pm \hat{\mathbf{n}}_{\rho} \cdot \mathbf{S} \quad (4.9)$$

---

<sup>1</sup>En effet, les opérateurs  $\mathbf{L}^2 = \ell(\ell+1)\mathbf{1}_{\mathcal{R}} \otimes \mathbf{1}_{\mathcal{S}}$  et  $\mathbf{S}^2 = \mathbf{1}_{\mathcal{R}} \otimes \frac{3}{2}\mathbf{1}_{\mathcal{S}}$  agissent trivialement.

qui sont les opérateurs associés à la décomposition spectrale de l'observable  $\hat{\mathbf{n}}_\rho \cdot \mathbf{S}$  où

$$\hat{\mathbf{n}}_\rho = \frac{\langle \mathbf{L} \rangle}{\|\langle \mathbf{L} \rangle\|} \quad (4.10)$$

est un vecteur unitaire indiquant la direction selon laquelle le spin  $\frac{1}{2}$  est mesuré.

Ainsi, les éléments de POVM  $\{\Lambda_\pm\}$  sont des approximations imparfaites des projecteurs  $P_{\hat{\mathbf{n}}_\rho}^\pm$  pour  $\ell$  fini. Autrement dit, pour une taille du gyroscope quantique finie, la mesure conjointe du gyroscope et de la particule de spin  $\frac{1}{2}$  se traduit par une mesure bruitée du moment angulaire suivant le vecteur  $\mathbf{n}_\rho = \frac{2}{d}\langle \mathbf{L} \rangle$ . Le bruitage est d'autant plus important que la norme  $\|\mathbf{n}_\rho\|$  est petite devant 1. Dans le cas extrême où  $\mathbf{n}_\rho$  est nul, la mesure répond + ou – de façon presque équiprobable. Ainsi, *la norme  $\|\mathbf{n}_\rho\|$  détermine la qualité de la mesure.*

Nous avons donc montré que la mesure conjointe induit une mesure généralisée sur la particule. La qualité de cette mesure dépend de l'état de la référence via  $\mathbf{n}_\rho = \frac{2}{d}\text{Tr}_{\mathcal{R}}[\mathbf{L}\rho]$ . Il est donc essentiel de caractériser l'état de la référence. Or, l'état de la référence va évoluer après chaque mesure d'une particule de spin  $\frac{1}{2}$ . Cette rétroaction quantique va entraîner une dégradation de la référence.

### 4.3 Évolution du gyroscope

Dans cette section, nous allons tout d'abord introduire le canal quantique décrivant l'évolution de la référence, tel que calculé dans l'article de D. Poulin et J. Yard [61]. Dans un second temps, nous allons démontrer que leur modèle est équivalent à un autre modèle où les particules de spin  $\frac{1}{2}$  interagissent une après l'autre avec le gyroscope via une interaction de Heisenberg  $\mathbf{L} \cdot \mathbf{S}$ . Les techniques utilisées pour démontrer ce résultat *original* pourraient être utilisées pour décrire des interactions avec spins d'ordre supérieur à  $\frac{1}{2}$ .

### 4.3.1 Canal quantique

Dans le modèle introduit précédemment, après la mesure conjointe de la référence et de la particule de spin  $\frac{1}{2}$ , l'état global est

$$\Pi_+ (\rho \otimes \xi) \Pi_+ + \Pi_- (\rho \otimes \xi) \Pi_- \quad (4.11)$$

en supposant que le résultat de la mesure n'est pas conservé<sup>2</sup>. L'état global est alors intriqué et lors de la prochaine utilisation de la référence, son état sera décrit par

$$\mathcal{E}_\xi(\rho) = \text{Tr}_S [\Pi_+ (\rho \otimes \xi) \Pi_+ + \Pi_- (\rho \otimes \xi) \Pi_-] \quad (4.12)$$

puisque la particule de spin  $\frac{1}{2}$  sera inaccessible. L'évolution de l'état de la référence est donc donnée par un canal quantique  $\mathcal{E}$ . Ce superopérateur peut être réécrit

$$\mathcal{E}_\xi(\rho) = \left( \frac{1}{2} + \frac{1}{2d^2} \right) \rho + \frac{8}{d^2} \text{Tr}_S [(\mathbf{L} \cdot \mathbf{S}) (\rho \otimes \xi) (\mathbf{L} \cdot \mathbf{S})] + \frac{2}{d^2} (\rho (\mathbf{L} \cdot \langle \mathbf{S} \rangle) + (\mathbf{L} \cdot \langle \mathbf{S} \rangle) \rho) \quad (4.13)$$

où  $\langle \mathbf{S} \rangle = \text{Tr}_S [\mathbf{S}\xi]$  est l'espérance du moment angulaire de la particule.

### 4.3.2 Interaction de Heisenberg

Considérons un modèle où la mesure conjointe est remplacée par une interaction entre la particule de spin  $\frac{1}{2}$  et la référence. À  $t = 0$ , une particule de spin  $\frac{1}{2}$ , dans un état décrit par l'opérateur densité  $\xi$ , commence à interagir avec la référence via une interaction de Heisenberg

$$H_{\mathcal{R}S} = \mathbf{L} \cdot \mathbf{S}. \quad (4.14)$$

---

<sup>2</sup>Nous nous plaçons dans le cadre d'un schéma de mesure non-adaptatif.

À  $t = \tau^-$ , l'interaction se termine et la particule de spin  $\frac{1}{2}$  est rejetée. Ceci définit un nouveau superopérateur  $\mathcal{E}'$  qui s'écrit formellement

$$\mathcal{E}'(\rho) = \text{Tr}_S [e^{-iH_{\mathcal{R}S}\tau}(\rho \otimes \xi)e^{+iH_{\mathcal{R}S}\tau}]. \quad (4.15)$$

Nous allons montrer que ce superopérateur est presque équivalent au superopérateur (4.13) pour un temps d'interaction bien choisi.

### 4.3.3 Équivalence des modèles

Afin de calculer une formule explicite pour  $\mathcal{E}'$ , nous devons d'abord calculer l'opérateur d'évolution

$$U(\tau) = e^{-i\mathcal{H}_{\mathcal{R}S}\tau} = \sum_{k=0}^{+\infty} \frac{(-i)^k \tau^k}{k!} (\mathbf{L} \cdot \mathbf{S})^k. \quad (4.16)$$

Cet opérateur d'évolution peut être exprimé analytiquement.

**Lemme 4.1.**  $(\mathbf{L} \cdot \mathbf{S})^k$  est une combinaison linéaire de  $\mathbf{1}$  et de  $\mathbf{L} \cdot \mathbf{S}$ .

$$\forall k \in \mathbb{N} \quad (\mathbf{L} \cdot \mathbf{S})^k = a_k \mathbf{1} + b_k (\mathbf{L} \cdot \mathbf{S}). \quad (4.17)$$

*Démonstration.* Par récurrence

Initialisation : trivialement, la propriété est vérifiée pour  $k = 0, 1$  avec

$$\begin{cases} a_0 = 1 & b_0 = 0 \\ a_1 = 0 & b_1 = 1. \end{cases}$$

Le cas  $k = 2$  est essentiel pour appliquer l'hypothèse de récurrence. Un calcul simple montre que

$$(\mathbf{L} \cdot \mathbf{S})^2 = \frac{\ell(\ell+1)}{4} \mathbf{1} - \frac{1}{2} \mathbf{L} \cdot \mathbf{S}.$$

Hérédité : soit  $k \in \mathbb{N} \setminus \{0, 1\}$  et supposons que  $(\mathbf{L} \cdot \mathbf{S})^k = a_k \mathbf{1} + b_k (\mathbf{L} \cdot \mathbf{S})$ .

$$\begin{aligned}
(\mathbf{L} \cdot \mathbf{S})^{k+1} &= a_k \mathbf{L} \cdot \mathbf{S} + b_k (\mathbf{L} \cdot \mathbf{S})^2 \quad \text{selon l'hypothèse de récurrence} \\
&= a_k \mathbf{L} \cdot \mathbf{S} + b_k \left( \frac{\ell(\ell+1)}{4} \mathbf{1} - \frac{1}{2} \mathbf{L} \cdot \mathbf{S} \right) \quad \text{selon le cas } k = 2 \\
&= \frac{\ell(\ell+1)}{4} b_k \mathbf{1} + \left( a_k - \frac{b_k}{2} \right) \mathbf{L} \cdot \mathbf{S}
\end{aligned}$$

□

Ceci définit donc deux suites  $(a_k)_{k \in \mathbb{N}}$  et  $(b_k)_{k \in \mathbb{N}}$  via une relation de récurrence

$$\begin{cases} a_{k+1} = \frac{\ell(\ell+1)}{4} b_k \\ b_{k+1} = a_k - \frac{b_k}{2} \end{cases} \quad \text{dont les valeurs initiales sont } a_0 = 1 \quad b_0 = 0.$$

**Lemme 4.2.** *Les termes génériques des deux suites sont pour tout  $k \in \mathbb{N}$*

$$\begin{cases} a_k = \frac{\ell+1}{d} \left( \frac{\ell}{2} \right)^k + (-1)^k \frac{\ell}{d} \left( \frac{\ell+1}{2} \right)^k \\ b_k = \frac{2}{d} \left( \frac{\ell}{2} \right)^k - (-1)^k \frac{2}{d} \left( \frac{\ell+1}{2} \right)^k \end{cases} \quad (4.18)$$

*Démonstration.* La relation de récurrence permet d'écrire la relation de récurrence linéaire  $b_{k+2} = -\frac{b_{k+1}}{2} + \frac{\ell(\ell+1)}{4} b_k$ .

Son équation caractéristique est  $r^2 + \frac{r}{2} - \frac{\ell(\ell+1)}{4} = 0$  dont les solutions sont  $r_+ = \frac{\ell}{2}$  et  $r_- = -\frac{\ell+1}{2}$ . Ainsi, l'expression générale de  $b_k$  est

$$b_k = \lambda \left( \frac{\ell}{2} \right)^k + \mu (-1)^k \left( \frac{\ell+1}{2} \right)^k \quad \text{avec} \quad \begin{cases} \lambda + \mu = b_0 = 0 \\ \frac{\ell}{2} \lambda - \frac{\ell+1}{2} \mu = a_0 - \frac{b_0}{2} = 1 \end{cases}.$$

La solution de ce système est  $\lambda = -\mu = \frac{2}{d}$ . □

Il est alors possible d'exprimer l'opérateur d'évolution

$$U(\tau) = \sum_{k=0}^{+\infty} \frac{(-i)^k \tau^k}{k!} (\mathbf{L} \cdot \mathbf{S})^k = \underbrace{\sum_{k=0}^{+\infty} \frac{(-i)^k \tau^k}{k!} a_k}_{a(\tau)} \mathbf{1} + \underbrace{\sum_{k=0}^{+\infty} \frac{(-i)^k \tau^k}{k!} b_k}_{b(\tau)} (\mathbf{L} \cdot \mathbf{S}) \quad (4.19)$$

ce qui permet ensuite d'exprimer l'évolution unitaire du système total.

**Lemme 4.3.** *L'opérateur d'évolution  $U(\tau) = e^{-iH_{RS}\tau}$  vaut  $a(\tau)\mathbf{1} + b(\tau)\mathbf{L} \cdot \mathbf{S}$*

$$\text{où } \begin{cases} a(\tau) = \frac{\ell+1}{d} e^{-i\tau\frac{\ell}{2}} + \frac{\ell}{d} e^{i\tau\frac{\ell+1}{2}} \\ b(\tau) = \frac{2}{d} \left( e^{-i\tau\frac{\ell}{2}} - e^{i\tau\frac{\ell+1}{2}} \right) \end{cases} \quad \text{et l'évolution unitaire de } \rho_{RS} \text{ est}$$

$$\begin{aligned} \rho_{RS}(t+\tau) &= a(\tau)a(-\tau)\rho_{RS} + b(\tau)b(-\tau)\mathbf{L} \cdot \mathbf{S}\rho_{RS}\mathbf{L} \cdot \mathbf{S} \\ &\quad + a(\tau)b(-\tau)\rho_{RS}\mathbf{L} \cdot \mathbf{S} + a(-\tau)b(\tau)\mathbf{L} \cdot \mathbf{S}\rho_{RS} \end{aligned} \quad (4.20)$$

Une fois l'opérateur densité du système total obtenu, il suffit d'effectuer une trace partielle sur la particule pour obtenir l'expression du superopérateur.

**Proposition 4.4.** *Le superopérateur  $\mathcal{E}'$  s'exprime sous la forme*

$$\begin{aligned} \mathcal{E}'(\rho) &= \left( \cos^2 \frac{\tau d}{4} + \frac{\sin^2 \frac{\tau d}{4}}{d^2} \right) \rho + \frac{4}{d^2} \sin^2 \frac{\tau d}{4} \{\rho, \mathbf{L} \cdot \langle \mathbf{S} \rangle\} \\ &\quad + \frac{16}{d^2} \sin^2 \frac{\tau d}{4} \text{Tr}_S \mathbf{L} \cdot \mathbf{S} (\rho \otimes \xi) \mathbf{L} \cdot \mathbf{S} + \frac{2}{d^2} i \sin \frac{\tau d}{2} [\rho, \mathbf{L} \cdot \langle \mathbf{S} \rangle] \end{aligned} \quad (4.21)$$

Pour  $\tau = \frac{\pi}{d}$ , l'expression se réduit à

$$\begin{aligned} \mathcal{E}'(\rho) &= \left( \frac{1}{2} + \frac{1}{2d^2} \right) \rho + \frac{2}{d^2} \{\rho, \mathbf{L} \cdot \langle \mathbf{S} \rangle\} \\ &\quad + \frac{8}{d^2} \text{Tr}_S [\mathbf{L} \cdot \mathbf{S} (\rho \otimes \xi) \mathbf{L} \cdot \mathbf{S}] + \frac{2}{d^2} i [\rho, \mathbf{L} \cdot \langle \mathbf{S} \rangle] \end{aligned} \quad (4.22)$$

Ainsi, le superopérateur décrivant l'évolution de la référence après interaction de Heisenberg est le même superopérateur que celui décrivant l'évolution après une mesure conjointe, si ce n'est le terme  $-\frac{2i}{d^2} [\mathbf{L} \cdot \langle \mathbf{S} \rangle, \rho]$  qui correspond à une rotation d'un angle  $-\frac{2}{d} \|\langle \mathbf{S} \rangle\|$  autour de l'axe  $\langle \mathbf{S} \rangle$ . Si on néglige cette précession autour de l'axe de polarisation privilégié des particules de spin  $\frac{1}{2}$ , *les deux superopérateurs sont identiques*. Ce résultat suggère que, au moins dans ce cas particulier, une mesure induit la même rétroaction quantique qu'une interaction entre l'appareil de mesure et le système mesuré.

## 4.4 Régime quasi-classique

Dans la section qui suit, nous allons nous intéresser au modèle avec mesure dans le régime quasi-classique pour lequel le moment cinétique de la référence est grand devant le moment cinétique de la particule de spin  $\frac{1}{2}$ . Autrement dit, nous nous intéressons au cas où la taille de la référence vérifie  $\ell \gg 1$ . Nous allons rappeler le résultat de D. Poulin et J. Yard qui met en évidence le rôle particulier joué par les états cohérents de la référence avant de retrouver ce résultat par une approche plus systématique qui permet de prolonger leur analyse. Ces états correspondent aux états quasi-classiques. Finalement, nous montrerons qu'une superposition de tels états quasi-classiques décohèrent conformément à la théorie de la décohérence.

### 4.4.1 Choix des axes

Afin de pousser plus loin l'analyse, nous allons choisir un système d'axes de référence, en accord avec le choix fait dans [61].

- L'axe  $z$  correspond à la polarisation des particules de spin  $\frac{1}{2}$ , de telle façon que leur état s'écrive

$$\xi = \frac{1}{2}\mathbf{1} + 2\langle S_z \rangle S_z. \quad (4.23)$$

- L'axe  $x$  est choisi de telle façon qu'initialement, l'espérance du moment cinétique de la référence  $\langle \mathbf{L} \rangle$  soit dans le plan  $xz$ .
- Finalement, l'axe  $y$  est choisi de façon à compléter le trièdre direct.

Plutôt que de travailler avec les opérateurs  $L_x, L_y, L_z$ , il est commode d'effectuer une rotation d'un angle  $\theta$  autour de l'axe  $y$  et d'utiliser les opérateurs

$$\begin{cases} L_x^\theta = \cos \theta L_x - \sin \theta L_z \\ L_z^\theta = \sin \theta L_x + \cos \theta L_z. \end{cases} \quad (4.24)$$

L'angle  $\theta(t)$  sera choisi de telle façon que

$$\langle L_x^{\theta(t)}(t) \rangle = 0, \quad (4.25)$$

c.-à-d. que le moment cinétique est nul en moyenne sur l'axe  $x^{\theta(t)}$ , et que

$$\langle L_z^{\theta(t)}(t) \rangle = lr(t) \quad (4.26)$$

où  $r(t) \in [0, 1]$ , c'est-à-dire que l'axe  $z^{\theta(t)}$  est l'axe de polarisation privilégié du gyroscope et sa polarisation est quantifiée par  $r(t)$ . Toutes ces définitions sont représentées sur la figure 4.1.

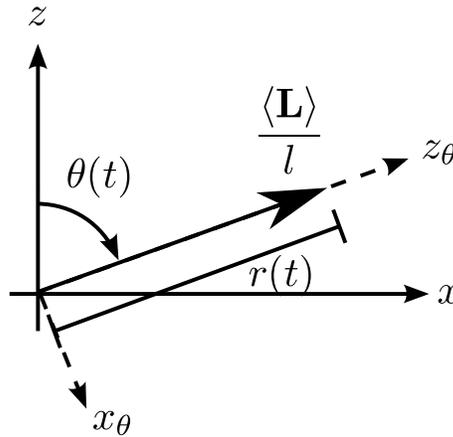


Figure 4.1 – Choix des axes

## 4.4.2 Évolution quasi-classique

### 4.4.2.1 État cohérent

D. Poulin et J. Yard ont mis en évidence le rôle particulier des états cohérents. Il s'agit d'états dont le moment cinétique est maximal dans une direction donnée. Avec notre choix d'axes, ces états sont de la forme

$$|\theta\rangle = e^{-iL_y\theta}|\ell, \ell\rangle \quad (4.27)$$

et ont donc une polarisation maximale, c.-à-d.  $r(t) = 1$ .

Afin de montrer que les états cohérents jouent un rôle privilégié, D. Poulin et J. Yard ont tout d'abord écrit le superopérateur  $\mathcal{E}_\xi$  sous la forme d'une décomposition de Kraus  $\mathcal{E}_\xi(\rho) = \sum_i E_i \rho E_i^\dagger$  où les opérateurs de Kraus sont

$$\begin{aligned} \frac{1}{\sqrt{2d}} \sqrt{d^2 + 1 - 4\langle S_z \rangle^2} \mathbf{1} & \quad \frac{\sqrt{2}}{d} \left( L_z^\theta + 2i\langle S_z \rangle \sin \theta L_y + \langle S_z \rangle \cos \theta \right) \\ \frac{\sqrt{2}}{d} i \sqrt{1 - 4\langle S_z \rangle^2} L_y & \quad \frac{\sqrt{2}}{d} \left( L_x^\theta + 2i\langle S_z \rangle \cos \theta L_y - \langle S_z \rangle \sin \theta \right). \end{aligned} \quad (4.28)$$

Un développement en puissance de  $\frac{1}{\ell}$  leur permet alors de montrer que, à l'ordre dominant en  $\frac{1}{\ell}$ , le superopérateur se réduit<sup>3</sup> à

$$\mathcal{E}_\xi(\rho) \sim \rho + i \frac{r\langle S_z \rangle}{\ell} \sin \theta [L_y, \rho]. \quad (4.29)$$

Le second terme n'est rien d'autre qu'une rotation d'angle  $\frac{r\langle S_z \rangle}{\ell} \sin \theta$  autour de l'axe  $y$ . L'angle  $\theta(t)$  vérifie alors l'équation

$$\frac{d\theta}{dt} = -r(t) \frac{\langle S_z \rangle}{\ell} \sin \theta + O\left(\frac{1}{\ell^2}\right). \quad (4.30)$$

De plus, une analyse numérique montre que pour un état initial cohérent,  $r(t=0) = 1$ , la polarisation reste très proche de 1 pour toute l'évolution. Or, l'équation différentielle  $\frac{d}{dt}\theta = -\frac{\langle S_z \rangle}{\ell} \sin \theta$  a pour solution

$$\tan \frac{\theta(t)}{2} = e^{-\frac{\langle S_z \rangle}{\ell} t} \tan \frac{\theta(t=0)}{2}. \quad (4.31)$$

Physiquement, ce résultat indique que le gyroscope initialement préparé dans un état cohérent va s'aligner progressivement avec la direction de polarisation des particules de spin  $\frac{1}{2}$ . Cette relaxation a pour temps caractéristique

$$\tau_{\text{relaxation}} = \frac{\ell}{\langle S_z \rangle}. \quad (4.32)$$

---

<sup>3</sup>Cette expression n'est qu'approchée. En particulier, elle n'est pas positive.

## 4.4.2.2 Équations du mouvement

L'article de D. Poulin et J. Yard ne fournit pas d'équation différentielle sur la polarisation  $r(t)$ . Nous allons présenter une méthode plus systématique afin d'obtenir un couple d'équations différentielles sur  $\theta(t)$  et  $r(t)$  dans la limite  $\ell \gg 1$ .

Pour ce faire, il suffit d'exprimer les valeurs moyennes  $\langle L_x^{\theta(t)}(t+1) \rangle$  et  $\langle L_z^{\theta(t)}(t+1) \rangle$  à l'instant<sup>4</sup>  $t+1$  en fonction de  $\langle (L_x^\theta)^2 \rangle$ ,  $\langle (L_z^\theta)^2 \rangle$  et  $\langle L_x^\theta L_z^\theta \rangle$  à l'instant  $t$ . Plus précisément, en utilisant la décomposition de Kraus 4.28, nous calculons  $\langle L_x^{\theta(t)}(t+1) \rangle = \text{Tr} \left[ L_x^{\theta(t)} \mathcal{E}_\xi(\rho) \right]$  et  $\langle L_z^{\theta(t)}(t+1) \rangle = \text{Tr} \left[ L_z^{\theta(t)} \mathcal{E}_\xi(\rho) \right]$ .

**Proposition 4.5.** *L'évolution des valeurs moyennes est donnée par*

$$\begin{aligned} \langle L_x^{\theta(t)}(t+1) \rangle &= -\frac{4\langle S_z \rangle}{d^2} \left[ \sin \theta(t) \left( \ell(\ell+1) - \langle (L_x^{\theta(t)})^2 \rangle \right) + \cos \theta(t) \langle L_x^{\theta(t)} L_z^{\theta(t)} \rangle \right] \\ \langle L_z^{\theta(t)}(t+1) \rangle &= \frac{4\langle S_z \rangle}{d^2} \left[ \cos \theta(t) \left( \ell(\ell+1) - \langle (L_z^{\theta(t)})^2 \rangle \right) + \sin \theta(t) \langle L_x^{\theta(t)} L_z^{\theta(t)} \rangle \right] \\ &\quad + \ell \left( 1 - \frac{2}{d^2} \right) r(t). \end{aligned} \tag{4.33}$$

*Démonstration.* Le résultat découle d'un calcul long et pénible, sans difficultés particulières. Il suffit de calculer chaque terme en utilisant à outrance la cyclicité de la trace et les relations de commutation  $[L_i, L_j] = i\varepsilon^{ijk} L_k$ . Par ailleurs, ces formules ont été vérifiées numériquement.  $\square$

Ces expressions, exactes pour toute valeur de  $\ell$ , peuvent maintenant être développées en puissance de  $\frac{1}{\ell}$  pour fournir les équations de mouvement sur  $r(t)$  et  $\theta(t)$ . Il suffit d'écrire

$$\begin{cases} \theta(t) \stackrel{\ell \gg 1}{\approx} \frac{\langle L_x^{\theta(t)}(t+1) \rangle}{\langle L_z^{\theta(t)}(t+1) \rangle} \\ \ell r^2(t+1) = \left( \langle L_x^{\theta(t)}(t+1) \rangle \right)^2 + \left( \langle L_z^{\theta(t)}(t+1) \rangle \right)^2 \end{cases} \tag{4.34}$$

<sup>4</sup>Attention, la valeur moyenne  $\langle L_x^{\theta(t)}(t+1) \rangle$  à l'instant  $t+1$  est prise pour  $\theta(t)$  à l'instant  $t$ . En effet,  $\langle L_x^{\theta(t+1)}(t+1) \rangle$  est nul par définition de  $\theta$  et n'aurait donc aucun intérêt.

et de développer ces expressions en puissances de  $1/\ell$ .

**Théorème 4.6.** *Les équations du mouvement quasi-classiques sont*

$$\begin{cases} \frac{dr}{dt} = \lambda \frac{1-r^2}{r} \cos \theta(t) + O\left(\frac{1}{\ell^2}\right) \\ \frac{d\theta}{dt} = -\lambda r(t) \sin \theta(t) + O\left(\frac{1}{\ell^2}\right) \end{cases} \quad (4.35)$$

où  $\lambda = \frac{\langle S_z \rangle}{\hbar}$  fixe l'échelle de temps de la relaxation.

Ces équations mettent en évidence le rôle essentiel joué par le facteur  $\lambda$  qui n'est autre que le ratio entre les moments cinétiques moyens de la particule et de la référence. Il s'agit donc du rapport des propriétés quasi-classiques des deux objets en présence et il paraît donc logique que ce soit leur rapport qui dicte la vitesse de la relaxation.

Par rapport à l'approche de D. Poulin et J. Yard, notre approche permet non seulement de retrouver l'équation quasi-classique sur  $\frac{d\theta}{dt}$ , mais aussi d'en obtenir une sur  $\frac{dr}{dt}$  qui justifie l'approximation  $r(t) \sim 1$  si  $r(t=0) = 1$ .

### 4.4.3 Superposition d'états cohérents

Les équations de mouvement quasi-classiques confirment le statut privilégié des états cohérents, qui vérifient  $r(t=0) = 1$ . Un état cohérent demeure cohérent durant toute l'évolution et relaxe afin de s'aligner avec la polarisation des spin  $\frac{1}{2}$ .

Nous allons maintenant nous intéresser à une référence initialement préparée dans une superposition d'états cohérents de la forme

$$|\psi\rangle = a|\alpha\rangle + b|\beta\rangle \quad (4.36)$$

où  $|\alpha\rangle = e^{-i\alpha L_y}|\ell, \ell\rangle$  et  $|\beta\rangle = e^{-i\beta L_y}|\ell, \ell\rangle$ . Nous connaissons déjà l'évolution quasi-classique des termes  $|\alpha\rangle\langle\alpha|$  et  $|\beta\rangle\langle\beta|$ . Par contre, il est intéressant d'évaluer l'évolution des termes de cohérence  $|\alpha\rangle\langle\beta|$  et  $|\beta\rangle\langle\alpha|$ . Un calcul

sans difficulté particulière montre que

$$\begin{aligned} \langle \alpha | \mathcal{E}(|\alpha\rangle\langle\beta|) | \beta \rangle &= \cos^2 \frac{\alpha - \beta}{2} \\ &\quad - \frac{1}{d} \cos(\alpha - \beta) + \frac{2\ell \langle S_z \rangle}{d^2} (\cos \alpha + \cos \beta) \\ &\quad + \frac{1}{d^2} \left( \cos^2 \frac{\alpha - \beta}{2} - 2\langle S_z \rangle^2 \right). \end{aligned} \quad (4.37)$$

Ainsi, les termes de cohérence décroissent d'autant plus vite qu'ils correspondent à des états cohérents classiquement éloignés, c.-à-d. d'autant plus vite que  $|\alpha - \beta|$  est grand (cf. figure 4.2).

$$\langle \alpha | \mathcal{E}(|\alpha\rangle\langle 0|) | 0 \rangle$$

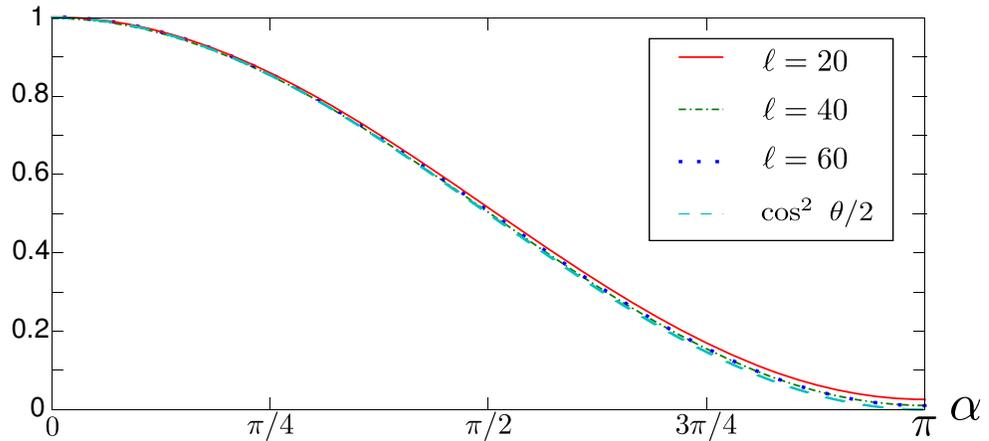
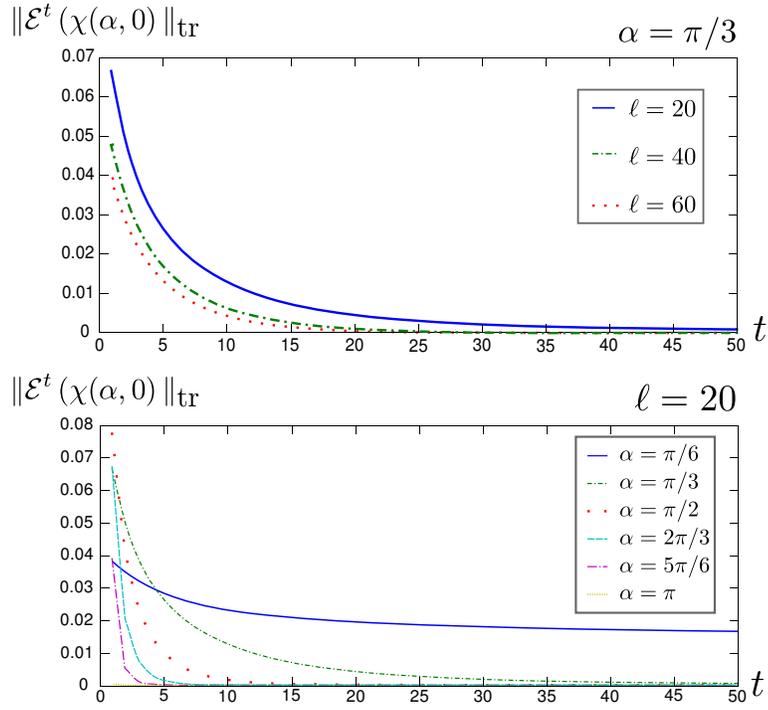


Figure 4.2 – Évolution numérique de  $\langle \alpha | \mathcal{E}(|\alpha\rangle\langle \beta = 0|) | \beta = 0 \rangle$

La superposition  $|\psi\rangle$  évolue selon

$$\begin{aligned} \mathcal{E}(|\psi\rangle\langle\psi|) &\stackrel{\ell \gg 1}{\approx} |a|^2 |\alpha + d\alpha\rangle\langle\alpha + d\alpha| + |b|^2 |\beta + d\beta\rangle\langle\beta + d\beta| \\ &\quad + ab^* \left( \cos^2 \frac{\alpha - \beta}{2} |\alpha\rangle\langle\beta| + \chi \right) + a^*b \left( \cos^2 \frac{\alpha - \beta}{2} |\alpha\rangle\langle\beta| + \chi^\dagger \right) \end{aligned} \quad (4.38)$$

où  $d\alpha = -\lambda \sin \alpha$  et  $\chi = \mathcal{E}(|\alpha\rangle\langle\beta|) - (\langle \alpha | \mathcal{E}(|\alpha\rangle\langle\beta|) | \beta \rangle) |\alpha\rangle\langle\beta|$  est un “résidu” quantique, essentiellement lié à la préservation de la trace par  $\mathcal{E}$ . Des analyses numériques montrent que l’opérateur  $\chi$  ne joue pas de rôle dans l’évolution. En effet, la norme dite de trace, définie par  $\|A\|_{\text{tr}} = \text{Tr} \sqrt{A^\dagger A}$ , de  $\mathcal{E}^t(\chi(\alpha, 0))$  devient négligeable pour  $t$  petit (cf. figure 4.3). Autrement dit, quelques applications du canal quantique suffisent à faire disparaître l’opérateur  $\chi$ .

Figure 4.3 – Simulation numérique de l'évolution de l'opérateur  $\chi$ 

À toute fin pratique, dans un temps exponentiellement rapide en  $|\theta - \phi|$ , la superposition  $|\psi\rangle = a|\theta\rangle + b|\phi\rangle$  est transformée en mélange statistique

$$|a|^2|\alpha(t)\rangle\langle\alpha(t)| + |b|^2|\beta(t)\rangle\langle\beta(t)|. \quad (4.39)$$

Cet exemple illustre donc bien le phénomène de décohérence et souligne l'efficacité et la rapidité avec lesquelles ce phénomène agit. Par ailleurs, le mélange statistique va dans un second temps se relaxer jusqu'à atteindre

$$|\ell, \ell\rangle\langle\ell, \ell|$$

après un temps proportionnel à  $\lambda = \frac{\langle S_z \rangle}{\ell}$ . La relaxation agit donc sur une échelle de temps beaucoup plus grande que la décohérence. Cette distinction entre décohérence (très) rapide et relaxation lente est typique.

# Chapitre 5

## Lutte contre la décohérence

Dans ce chapitre, nous montrerons rapidement l'impact catastrophique de la décohérence sur le calcul quantique avant de nous intéresser aux différentes stratégies disponibles afin de lutter contre ce phénomène. L'une d'entre elles est d'utiliser des codes correcteurs d'erreur. Cette voie est l'objet de recherche intensive à l'heure actuelle et semble incontournable pour la mise au point d'un ordinateur quantique de taille raisonnable. Il ne s'agit toutefois pas de la seule option. D'autres approches, souvent qualifiées de passives, protègent le système quantique soit en exploitant des symétries des processus physiques menant à la décohérence (sous-espaces protégés de la décohérence) ou encore en agissant ponctuellement sur la dynamique de l'environnement (contrôle quantique). Finalement, nous proposons une nouvelle approche qui consiste à *préparer l'état initial de l'environnement*. Nous présentons des résultats analytiques qui encadrent les résultats qui peuvent être obtenus par une telle technique.

### 5.1 Décohérence et calcul quantique

#### 5.1.1 Décohérence et interférométrie

La puissance du calcul quantique repose sur l'exploitation de corrélations quantiques. Afin d'avoir accès à ces corrélations, il est essentiel de pouvoir

préparer des états en superposition.

Fondamentalement, la plupart des algorithmes quantiques répondent à un gabarit qui fait apparaître deux grandes étapes, comme nous l'avons montré dans le chapitre 1. La première consiste à exploiter le parallélisme quantique (voir section 1.3.1.2) tandis que la seconde consiste à faire interférer les différentes branches de calcul entre elles (voir section 1.3.1.3). Le parallélisme permet à partir d'une superposition d'entrées classiques d'obtenir

$$\sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle |0\rangle \mapsto \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle |f(x)\rangle.$$

L'étape d'interférométrie permet de réduire cette superposition à un seul terme

$$\sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle |f(x)\rangle \mapsto |x_0\rangle |f(x_0)\rangle$$

Ainsi, un ordinateur quantique peut être perçu comme un gigantesque interféromètre. Or, la décohérence a justement pour effet de détruire la cohérence des différentes branches de calcul. Très grossièrement, une décohérence complète juste après l'étape de parallélisme aura pour effet de transformer la superposition des entrées/sorties classiques en mélange statistiques des entrées/sorties classiques

$$\sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle |f(x)\rangle \xrightarrow{\text{décohérence}} \rho = \sum_{x \in \{0,1\}^n} \frac{1}{2^n} |x\rangle \langle x| \otimes |f(x)\rangle \langle f(x)|.$$

L'étape d'interférométrie est d'autant plus inefficace que la cohérence de la superposition a été atténuée.

Dans la prochaine section, nous allons nous attarder à un modèle plus réaliste de décohérence et à son impact sur l'algorithme de Grover présenté en section 1.3.2. Notre approche reprendra les grandes lignes de l'article de Hiroo Azuma [6].

## 5.1.2 Algorithme de Grover avec décohérence

### 5.1.2.1 Modèle d'erreur

Nous allons analyser l'algorithme de Grover, introduit en 1.3.2, en supposant pour simplifier que l'état  $|w\rangle$  que nous cherchons à identifier est  $|0\rangle^{\otimes n}$  qui sera noté  $|0\rangle$ . Rappelons que l'algorithme de Grover consiste à appliquer  $M$  fois une itération de Grover définie par

$$U_D U_f = (\mathbb{H}^{\otimes n} P \mathbb{H}^{\otimes n}) U_f.$$

Rappelons que  $P = 2|0\rangle\langle 0| - \mathbf{1}$  et que  $\mathbb{H}$  est la porte de Hadamard. De plus, sous l'hypothèse que  $|w\rangle = |0\rangle$ , nous pouvons écrire que  $U_f = -P$ .

Le modèle d'erreur que nous utiliserons s'appuie sur le canal à amortissement de phase, déjà introduit en section 2.2.2.2. Rappelons qu'il consiste à appliquer l'opérateur  $\sigma_z$  avec probabilité  $p$  et à ne rien appliquer avec probabilité  $(1 - p)$

$$\rho \mapsto p\sigma_z\rho\sigma_z + (1 - p)\rho.$$

Ce superopérateur est appliqué à chaque qubit de façon indépendante avant chaque application de l'opérateur  $P$ , dit d'inversion de phase, de l'algorithme. Puisque le canal à amortissement de phase contient les éléments fondamentaux de la théorie de la décohérence, ce modèle d'erreur est raisonnable et souvent utilisé.<sup>1</sup>

### 5.1.2.2 Impact sur l'algorithme de Grover

L'analyse de l'algorithme de Grover en présence de décohérence présenté dans l'article [6] est mené dans la limite où le nombre  $n$  de qubits est grand. Elle permet de déterminer le nombre minimal  $M_{\text{seuil}}$  d'itérations de Grover qui permette de déterminer  $|w\rangle$  avec probabilité au moins  $p_{\text{seuil}}$ . En absence de décohérence, c.-à-d. pour  $p = 0$ , le nombre minimal d'itérations de Grover

---

<sup>1</sup>Un autre modèle d'erreur est d'appliquer le canal dépolarisant  $\rho \mapsto \frac{p}{2}\mathbf{1} + (1 - p)\rho$ .

est donné par

$$M_{\text{seuil}} = \frac{1}{2\sqrt{2^n}} \arcsin \sqrt{p_{\text{seuil}}}$$

ce qui permet de retrouver la valeur de  $M_{\text{seuil}} = \frac{\pi}{4\sqrt{2^n}}$  lorsque  $p_{\text{seuil}}$  est proche de 1. L'introduction de décohérence va avoir deux effets.

1.  $M_{\text{seuil}}$  sera maintenant une fonction croissante de  $p$  :  $M_{\text{seuil}}(p)$ . Ainsi, plus la décohérence est importante, plus le nombre d'itérations de Grover sera grande afin d'obtenir une réponse garantie avec la même probabilité. Si  $p$  est inconnu, il n'est pas possible de déterminer  $M_{\text{seuil}}(p)$ .
2. Au-delà d'une valeur critique de  $p$ , notée  $p_{\text{cr}}(p_{\text{seuil}})$ , il n'est plus possible d'obtenir la bonne réponse avec probabilité  $p_{\text{seuil}}$  (transition de phase). Ainsi, si la décohérence est trop importante, l'algorithme de Grover ne sert plus à rien. Par exemple, pour la valeur  $p_{\text{seuil}} = \frac{1}{2}$ , la valeur critique de  $p$  est  $p_{\text{cr}} \simeq 0,00589$ .

## 5.2 Différentes stratégies possibles

Comme nous venons de l'illustrer, la décohérence est un problème majeur, sinon l'obstacle essentiel à la mise au point d'un ordinateur quantique de grande taille. Notons que vouloir éviter à tout prix la décohérence risquerait de mener à des dispositifs sans intérêt pour le calcul quantique. En effet, le substrat physique des qubits répond à deux exigences contradictoires. D'un côté, afin de bénéficier de la puissance du calcul quantique, il est nécessaire d'utiliser des portes à deux qubits, telle la porte CNOT, afin de créer de l'intrication. Les systèmes physiques qui encodent les qubits doivent donc permettre à ceux-ci d'interagir entre eux. Or, d'un autre côté, ces mêmes systèmes ne doivent pas s'intriquer avec leur environnement pour éviter la décohérence. Ainsi, d'un point de vue pratique, le choix du support physique des qubits résulte d'un compromis délicat entre la facilité pour les qubits d'interagir entre eux tout en les protégeant de l'interaction avec leur environnement.

### 5.2.1 Correction d'erreur

La perspective de construire un jour un ordinateur quantique a longtemps été assombrie par l'apparente impossibilité d'utiliser des techniques de correction d'erreur pour un ordinateur quantique. Or, Shor et Steane ont indépendamment montré en 1995 qu'il n'en était rien en exhibant chacun un code correcteur d'erreur quantique. La correction d'erreur quantique est aujourd'hui un secteur de recherche très actif.

Toutefois, afin de pouvoir utiliser la correction d'erreur, il faut être capable d'effectuer certaines tâches élémentaires, par exemple les opérations nécessaires à l'encodage et au décodage, sans introduire de nouvelles erreurs. En particulier, il faut à tout prix éviter de propager les erreurs. Pour ce faire, il faut mettre en œuvre les portes quantiques de façon robuste (*fault tolerant* en anglais). Sans entrer dans les détails du calcul robuste, notons que cet effort débouche sur un résultat essentiel : le théorème-seuil, dont la première version a été démontrée par D. Arahonov et M. Ben-Or en 1996 [1]. Il montre que si la correction d'erreur est mise en œuvre de façon robuste et que le taux d'erreur par porte quantique élémentaire est inférieure à un certain seuil, il est possible de réaliser des calculs quantiques de taille arbitraire.

### 5.2.2 Prévention de la décohérence

La correction d'erreur quantique est souvent qualifiée de *stratégie active* contre la décohérence. En effet, il ne s'agit pas de réduire le niveau de décohérence, mais plutôt, étant donné un modèle d'erreur, de lutter contre elle. D'autres stratégies existent pour essayer de limiter la décohérence et sont alors qualifiées de stratégie passive. Nous mentionnerons ici deux grandes familles : les espaces protégés de la décohérence et le contrôle quantique.

#### 5.2.2.1 Espace protégé de la décohérence

L'idée au cœur de cette technique est de stocker ou encore de calculer dans des sous-espaces de l'espace de Hilbert dont tous les vecteurs sont af-

fectés de la même façon par la décohérence. Par exemple, pour un système en interaction avec son environnement, l'hamiltonien d'interaction peut toujours s'écrire

$$H_{S\mathcal{E}} = \sum_{\alpha} S_{\alpha} \otimes E_{\alpha}.$$

S'il existe un sous-espace dégénéré commun à tous les  $S_{\alpha}$ , autrement dit, s'il existe au moins deux états  $|s_k\rangle \in \mathcal{H}^S$  qui vérifient

$$S_{\alpha}|s_k\rangle = \lambda^{(\alpha)}|s_k\rangle \text{ pour tout } \alpha \text{ et tout } k,$$

il est possible d'encoder un qubit dans le sous-espace  $\text{Vect}\{|s_k\rangle\}$ . En effet, quel que soit l'état initial de l'environnement, l'interaction aura pour effet de ne pas intriquer le système et l'environnement :

$$\begin{aligned} e^{-iH_{S\mathcal{E}}t}|\psi\rangle|E_0\rangle &= e^{-iH_{S\mathcal{E}}t} \left( \sum_k c_k |s_k\rangle \right) |E_0\rangle \\ &= \sum_k c_k e^{-i \sum_{\alpha} \lambda^{(\alpha)} \mathbf{1} \otimes E_{\alpha} t} (|s_k\rangle |E_0\rangle) \\ &= \left( \sum_k c_k |s_k\rangle \right) e^{-i \sum_{\alpha} \lambda^{(\alpha)} \mathbf{1} \otimes E_{\alpha} t} |E_0\rangle \\ &= |\psi\rangle \underbrace{e^{-i \sum_{\alpha} \lambda^{(\alpha)} \mathbf{1} \otimes E_{\alpha} t} |E_0\rangle}_{|E(t)\rangle}. \end{aligned}$$

Ainsi, l'état  $|\psi\rangle$  du qubit n'est pas affecté puisque tout le sous-espace "décohère" de la même façon.

L'exemple introduit ici est très simplifié. La théorie des espaces protégés de la décohérence est beaucoup plus générale et, en particulier, peut tenir compte de la dynamique propre du système. Pour un aperçu plus complet, l'article de D.A. Lidar, I.L. Chuang et K.B. Whaley [48] constitue un excellent point de départ.

### 5.2.2.2 Contrôle quantique

Une autre approche afin de limiter la décohérence consiste à agir directement sur l'environnement. Or, par sa nature même, l'environnement ne peut être que partiellement contrôlé : sinon, il suffirait de détruire l'intrication entre l'environnement et le système pour éviter toute décohérence !

Une première stratégie, proche de l'idée des sous-espaces protégés de la décohérence, est appelée "Ingénierie de l'environnement". Elle consiste à modifier la dynamique de l'interaction entre le système et l'environnement afin de faire apparaître ou d'accentuer les symétries [28], souvent de façon à faire apparaître des sous-espaces protégés.

Une autre approche consiste à agir sur le système via un hamiltonien dépendant du temps, par exemple en contrôlant le système par des impulsions laser. Lorsque réalisé de façon efficace, ces perturbations permettent de compenser l'action de l'environnement et de préserver la cohérence du système. Une telle méthode est surtout efficace si le contrôle du système est possible sur une échelle de temps petite devant celle de la décohérence. Or, comme nous l'avons vu, la décohérence agit habituellement extrêmement rapidement. La mise en œuvre d'un tel « contrôle quantique » [72] constitue un formidable problème expérimental.

## 5.3 Préparation de l'environnement

Dans cette section 5.3, nous allons présenter le travail original qui constitue l'apport majeur de ce mémoire à la recherche sur la décohérence. Un article résumant cet apport a été accepté pour publication dans le journal *Physical Review A* [47]. Une version en ligne est disponible à l'adresse <http://arxiv.org/abs/0908.0958>. L'idée de base de cette contribution est de creuser l'idée, à prime abord farfelue, de préparer l'environnement afin de supprimer ou à tout le moins minimiser la décohérence du système lors de l'évolution subséquente.

### 5.3.1 Motivation

La théorie de la décohérence repose essentiellement sur l'interaction entre un système quantique et l'ensemble des degrés de liberté qui interagissent avec lui et qui constituent son environnement. L'intrication induite par l'interaction aura pour effet que l'état du système ne sera plus décrit par un état pur, mais plutôt par un opérateur densité. En plus de l'interaction, la décohérence introduite est fonction de l'état initial  $|\xi\rangle_{\mathcal{E}}$  de l'environnement puisque l'état du système au temps  $t$  est donné par

$$\rho_{\mathcal{S}}(t) = \text{Tr}_{\mathcal{E}} [U(t) (|\psi\rangle\langle\psi|_{\mathcal{S}} \otimes |\xi\rangle\langle\xi|_{\mathcal{E}}) U(t)^{\dagger}].$$

Or, l'interaction système/environnement n'est souvent qu'un produit tensoriel. Par exemple, dans le modèle de Żurek, l'interaction est de la forme

$$H_{\mathcal{S}\mathcal{E}} = \sigma_z \otimes \tilde{H}$$

où  $\sigma_z$  agit sur le qubit  $\mathcal{S}$  et  $\tilde{H}$  agit sur l'environnement. Si l'environnement est préparé dans un état propre  $|\Lambda\rangle$  de  $\tilde{H}$  (associé à la valeur propre  $\lambda \in \mathbb{R}$ ), le système va évoluer de façon unitaire puisque

$$e^{-iH_{\mathcal{S}\mathcal{E}}t}|\psi\rangle|\Lambda\rangle = e^{-i\sigma_z t}|\psi\rangle e^{-i\lambda t}|\Lambda\rangle = (U(t)|\psi\rangle)|\Lambda\rangle.$$

Ainsi, le système évolue en évitant la décohérence. Or, ces états initiaux particuliers de l'environnement sont habituellement négligés, soit en affirmant qu'ils ne risquent pas d'apparaître dans des cas réalistes [66] ou encore en supposant que l'évolution propre de l'environnement va interdire l'existence de tels états [60]. Dans le cadre de cette maîtrise, nous nous sommes donc intéressés à une classe de modèles où le système interagit avec un environnement présentant une dynamique propre. Notre travail a permis d'obtenir un critère mathématique permettant de déterminer s'il existe des états initiaux de l'environnement qui entraînent une évolution unitaire du système.

### 5.3.2 Modèles étudiés

Nous nous intéressons à un modèle où l'hamiltonien total s'écrit

$$H = S \otimes \tilde{H} + \mathbf{1}_S \otimes H_{\mathcal{E}}.$$

L'opérateur hermitien  $S$  agit sur l'espace de Hilbert du système qui est supposé de dimension 2. Autrement dit, notre système quantique est un qubit. Les opérateurs hermitiens  $\tilde{H}$  et  $H_{\mathcal{E}}$  agissent sur l'espace de Hilbert de l'environnement sur lequel il n'est fait a priori aucune hypothèse. Sans perte de généralité, il est possible de supposer que  $S = \sigma_z$  puisqu'il suffit d'écrire  $S$  dans sa base propre et de choisir le zéro d'énergie pour le ramener à  $\sigma_z$ . L'état initial de  $\mathcal{S}$  sera un état pur quelconque  $|\psi(0)\rangle = a|0\rangle + b|1\rangle$  où  $|0\rangle$  et  $|1\rangle$  sont les états propres de  $\sigma_z$  associés à 1 et  $-1$ . L'état initial du système global est alors

$$|\Psi(0)\rangle = |\psi(0)\rangle \otimes |I\rangle$$

où  $|I\rangle$  est l'état initial de l'environnement.

À un temps  $t$  quelconque, l'état global s'écrit

$$|\Psi(t)\rangle = a|0\rangle \otimes |\varepsilon_0(t)\rangle + b|1\rangle \otimes |\varepsilon_1(t)\rangle$$

où les états  $|\varepsilon_0(t)\rangle$  et  $|\varepsilon_1(t)\rangle$  vérifient les équations de Schrödinger

$$i \frac{d}{dt} |\varepsilon_k(t)\rangle = H_k |\varepsilon_k(t)\rangle \quad k = 0, 1 \quad (5.1)$$

avec les conditions initiales  $|\varepsilon_0(t=0)\rangle = |\varepsilon_1(t=0)\rangle = |I\rangle$  et où nous avons défini  $H_0 \equiv H_{\mathcal{E}} + \tilde{H}$  et  $H_1 \equiv H_{\mathcal{E}} - \tilde{H}$ .

Comme pour le modèle de Żurek original, la décohérence sera caractérisée par le facteur de cohérence

$$r(t) = \langle \varepsilon_0(t) | \varepsilon_1(t) \rangle.$$

### 5.3.3 États initiaux de l'environnement permettant une évolution unitaire du système

Nous allons maintenant nous intéresser aux états initiaux de l'environnement qui permettent au système d'évoluer de façon unitaire, autrement dit tel que

$$|r(t)| = |\langle \varepsilon_0(t) | \varepsilon_1(t) \rangle| = 1 \quad \text{pour tout } t. \quad (5.2)$$

#### 5.3.3.1 Condition d'existence

Tout d'abord, remarquons que puisque  $|\varepsilon_0(t)\rangle$  et  $|\varepsilon_1(t)\rangle$  sont normalisés, la condition (5.2) équivaut à l'existence d'une fonction infiniment continue et dérivable  $t \mapsto \theta(t)$  telle que

$$|\varepsilon_0(t)\rangle = e^{i\theta(t)} |\varepsilon_1(t)\rangle \quad \text{pour tout } t \quad (5.3)$$

selon le cas d'égalité de l'inégalité de Cauchy-Schwarz. Cette remarque préliminaire nous permet de démontrer le lemme suivant

**Lemme 5.1.** *L'existence d'un état  $|I\rangle$  qui permet de vérifier la condition (5.2) implique que*

$$\forall k \in \mathbb{N} \quad H_{\mathcal{E}}^k |\varepsilon(0)\rangle \in \text{Ker}(\tilde{H} - \lambda \mathbf{1}) \cap \text{Ker}([\tilde{H}, H_{\mathcal{E}}]).$$

*Autrement dit, toutes les puissances  $H_{\mathcal{E}}^k$  maintiennent  $|I\rangle$  dans un espace propre de  $\tilde{H}$  et dans le noyau du commutateur de  $\tilde{H}$  et  $H_{\mathcal{E}}$ .*

*Démonstration.* Selon la relation (5.3), nous avons

$$\frac{d}{dt} |\varepsilon_0(t)\rangle = i\dot{\theta} |\varepsilon_0(t)\rangle + e^{i\theta(t)} \frac{d}{dt} |\varepsilon_1(t)\rangle.$$

En substituant dans l'équation de Schrodinger (5.1), nous obtenons

$$\begin{aligned} -i \left( \tilde{H} + H_{\mathcal{E}} \right) |\varepsilon_0(t)\rangle &= i\dot{\theta}|\varepsilon_0(t)\rangle - i \left( -\tilde{H} + H_{\mathcal{E}} \right) |\varepsilon_0(t)\rangle \\ \dot{\theta}|\varepsilon_0(t)\rangle &= -2\tilde{H}|\varepsilon_0(t)\rangle. \end{aligned}$$

Le vecteur  $|\varepsilon_0(t)\rangle$  est donc un état propre de  $\tilde{H}$  lié à la valeur propre  $\lambda$  et  $\theta(t) = -2\lambda t$ . Son expression s'écrit pour tout  $t$

$$|\varepsilon_0(t)\rangle = e^{-i\lambda t} e^{-iH_{\mathcal{E}}t} |I\rangle.$$

Puisque  $|\varepsilon_0(t)\rangle = e^{-i\lambda t} \sum_{k=0}^{+\infty} \frac{(-it)^k}{k!} H_{\mathcal{E}}^k |I\rangle$  est un état propre de  $\tilde{H}$  pour tout temps  $t$ , nous en déduisons que chaque terme est un état propre de  $\tilde{H}$

$$\forall k \in \mathbb{N} \quad H_{\mathcal{E}}^k |I\rangle \in \text{Ker}(\tilde{H} - \lambda \mathbf{1}).$$

Ceci implique que  $\forall k \in \mathbb{N} \quad \tilde{H} H_{\mathcal{E}}^k |I\rangle = \lambda H_{\mathcal{E}}^k |I\rangle = H_{\mathcal{E}}^k \tilde{H} |I\rangle$ . D'où,

$$\forall k \in \mathbb{N} \quad H_{\mathcal{E}}^k |I\rangle \in \text{Ker}([\tilde{H}, H_{\mathcal{E}}]). \quad \square$$

Ce lemme va permettre de singulariser un sous-espace de l'espace de Hilbert de l'environnement. Ce sous-espace contient l'état initial  $|I\rangle$ .

**Lemme 5.2.** *L'existence d'un état  $|I\rangle$  qui permet de vérifier la condition (5.2) implique que  $|I\rangle$  est une combinaison linéaire de vecteurs propres de  $H_{\mathcal{E}}$  qui sont chacun des états propres dégénérés de  $\tilde{H}$  associés à la même valeur propre.*

*Démonstration.* Soit  $E = \text{Vect}\{H_{\mathcal{E}}^n |I\rangle \mid n \in \mathbb{N}\}$ . Autrement dit,  $E$  est le sous-espace vectoriel qui contient toutes les combinaisons linéaires des puissances de  $H_{\mathcal{E}}$  appliquées sur  $|I\rangle$ .  $E$  est un sous-espace vectoriel de l'intersection  $\text{Ker}(\tilde{H} - \lambda \mathbf{1}) \cap \text{Ker}([\tilde{H}, H_{\mathcal{E}}])$  selon le lemme précédent. De plus,  $E$  contient au moins  $|I\rangle$  et est donc de dimension  $k \geq 1$ .

$E$  est stable sous l'action de  $\tilde{H}$  puisqu'il est un sous-espace d'un espace propre de  $\tilde{H}$ . Il est aussi stable sous l'action de  $H_{\mathcal{E}}$  par définition. Ceci

permet d'assurer que les restrictions de  $\tilde{H}$  et  $H_{\mathcal{E}}$  sur  $E$  sont bien définies. Or, selon le lemme précédent, ces restrictions commutent. Il existe donc une base propre commune à  $\tilde{H}$  et  $H_{\mathcal{E}}$  sur le sous-espace vectoriel  $E$  et  $|I\rangle$  est une combinaison linéaire de ces états propres.  $\square$

Le lemme 5.2 affirme donc que l'existence d'un état  $|I\rangle$  qui permet de vérifier la condition (5.2) n'est possible que s'il existe un état propre commun à  $\tilde{H}$  et à  $H_{\mathcal{E}}$ . Réciproquement, si un tel état propre  $|\Lambda\rangle$  associé à  $\lambda$  pour  $\tilde{H}$  et  $\mu$  pour  $H_{\mathcal{E}}$  existe, alors il suffit de préparer cet état pour vérifier (5.2) puisque dans ce cas

$$\begin{aligned} |\varepsilon_0\rangle &= e^{-i(\tilde{H}+H_{\mathcal{E}})t}|\Lambda\rangle = e^{-i(\lambda+\mu)t}|\Lambda\rangle \\ |\varepsilon_1\rangle &= e^{-i(-\tilde{H}+H_{\mathcal{E}})t}|\Lambda\rangle = e^{-i(-\lambda+\mu)t}|\Lambda\rangle \end{aligned}$$

et

$$r(t) = e^{2i\lambda t}.$$

Pour résumer, nous avons donc démontré le théorème suivant.

**Théorème 5.3.** *L'existence d'un état initial  $|I\rangle$  qui permet de vérifier la condition (5.2) est équivalente à l'existence d'un vecteur propre commun de  $\tilde{H}$  et  $H_{\mathcal{E}}$ .*

Toutefois, bien que l'existence d'un état initial adéquat soit équivalente à l'existence d'un état propre commun, l'état initial adéquat n'est pas nécessairement un état propre commun. En effet, toute combinaison linéaire d'états propres de  $\tilde{H}$  et  $H_{\mathcal{E}}$  associés à la même valeur propre dégénérée  $\lambda$  de  $\tilde{H}$  convient.

### 5.3.3.2 Rareté

Nous venons de montrer que l'existence d'états initiaux de l'environnement qui permettent au système d'évoluer de façon unitaire n'est possible que si les hamiltoniens d'interaction  $\tilde{H}$  et d'évolution propre  $H_{\mathcal{E}}$  partagent

un vecteur propre. Nous allons montrer, en dimension finie, que les couples d'hamiltoniens  $(\tilde{H}, H_\varepsilon)$  qui présentent cette propriété particulière sont très rares grâce à des arguments topologiques. En dimension finie, nous assimilerons les hamiltoniens  $\tilde{H}$  et  $H_\varepsilon$  à des matrices hermitiennes de dimension  $N$ .

**Lemme 5.4.** *Les paires de matrices hermitiennes qui n'ont pas de vecteurs propres en commun sont denses dans l'espace des paires de matrices hermitiennes.*

*Démonstration.* Nous allons prouver que tout couple  $(G, H)$  de matrices hermitiennes est la limite d'une suite de paires de matrices hermitiennes  $(G_\varepsilon, H_\varepsilon)$  sans vecteur propre commun.

Trivialement, si  $G$  et  $H$  ne partagent pas de vecteur propre commun, il suffit de choisir  $G_\varepsilon = G$  et  $H_\varepsilon = H$  pour tout  $\varepsilon$ .

Sinon, il va falloir construire la suite  $(G_\varepsilon, H_\varepsilon)$ . Tout d'abord, levons la dégénérescence éventuelle de  $G$ . La matrice  $G$  étant hermitienne, il existe une base orthonormale  $\{|n\rangle \mid n \in [1; N]\}$  dans laquelle  $G$  est diagonale et peut présenter des dégénérescences. Ces dégénérescences peuvent être levées en ajoutant une matrice de perturbation  $V_\varepsilon = \sum_{n=1}^N n\varepsilon|n\rangle\langle n|$ . Pour  $\varepsilon$  petit devant la plus petite des différences des valeurs propres de  $G^2$ , la matrice  $G + V_\varepsilon$  n'a plus de dégénérescence. Toutefois,  $H$  et  $G_\varepsilon$  partagent toujours des états propres puisque les états propres de  $G$  sont aussi ceux de  $G_\varepsilon$ . Supposons que ces vecteurs propres communs correspondent aux  $k \leq N$  premiers vecteurs  $|n\rangle$  associées aux valeurs propres  $\mu_n$ . Afin d'éviter que ces vecteurs demeurent des vecteurs propres de  $H$ , nous allons utiliser une autre matrice de perturbation définie  $W_\varepsilon = \varepsilon \sum_{n=1}^{k-1} |n\rangle\langle n+1| + |n+1\rangle\langle n|$  pour obtenir  $H_\varepsilon = H + W_\varepsilon$ . Nous avons alors  $H_\varepsilon|n\rangle = \mu_i|n\rangle + W_\varepsilon|n\rangle = \mu_i|n\rangle + \varepsilon|n+1\rangle + \varepsilon|n-1\rangle$ . Ainsi,  $|n\rangle$  n'est pas un vecteur propre de  $H_\varepsilon$  alors qu'il est un vecteur propre de  $G_\varepsilon$  (qui ne présente pas de dégénérescence pour  $\varepsilon$  petit). Nous en concluons que pour  $\varepsilon$  petit  $H_\varepsilon$  and  $G_\varepsilon$  ne partagent pas de

---

<sup>2</sup>La condition  $\varepsilon < \min \Delta\lambda/N^2$  suffit.

vecteur propre commun bien que la suite  $(G_\varepsilon, H_\varepsilon)$  converge vers  $(G, H)$ .  $\square$

Autrement dit, il existe toujours une perturbation infinitésimale sur l'hamiltonien d'interaction  $\tilde{H}$  et l'hamiltonien d'évolution propre  $H_\varepsilon$  qui va empêcher le système quantique d'évoluer unitairement.

**Lemme 5.5.** *Les couples de matrices hermitiennes qui ne partagent pas un vecteur propre sont un ensemble ouvert.*

*Démonstration.* Soit  $(G_\varepsilon, H_\varepsilon)$  une suite *convergente* de paires de matrices hermitiennes possédant un vecteur propre en commun. Elle converge vers une paire de matrices hermitiennes  $(G, H)$ . Pour montrer que l'espace des paires de matrices hermitiennes qui partagent un vecteur propre est fermé, il faut et il suffit de montrer que  $G$  et  $H$  possède un vecteur propre commun. Ce résultat est appelé *caractérisation séquentielle* de la fermeture.

Pour  $\varepsilon$  petit, les opérateurs  $\Delta_G(\varepsilon) \equiv G_\varepsilon - G$  et  $\Delta_H(\varepsilon) \equiv H_\varepsilon - H$  sont des perturbations, autrement dit  $\Delta_G(\varepsilon)$  est très petit devant  $G$  et de même pour  $H$ . Dans ce cas, la théorie des perturbations [44] montre qu'il existe une famille orthonormée de vecteurs propres  $\{|\phi_k(\varepsilon)\rangle\}$  de  $G_\varepsilon$  et  $\{|\varphi_k(\varepsilon)\rangle\}$  de  $H_\varepsilon$  qui peuvent être développés en série entière de  $\varepsilon$

$$|\phi_k(\varepsilon)\rangle = |\phi_k\rangle + \varepsilon|\phi_k^{(1)}\rangle + \varepsilon^2|\phi_k^{(2)}\rangle + \dots = \sum_{n=0}^{\infty} \varepsilon^n |\phi_k^{(n)}\rangle$$

où  $\forall \varepsilon > 0$   $|\phi_k(\varepsilon)\rangle$  est un vecteur propre de  $G_\varepsilon$  (et de même pour  $H_\varepsilon$ ) et  $|\phi_k\rangle$  est un vecteur propre de  $G$  (de même pour  $H$ ). Puisque pour tout  $\varepsilon > 0$ , les matrices  $G_\varepsilon$  et  $H_\varepsilon$  partagent un vecteur propre commun, il existe  $k_0$  et  $k'_0$  tel que

$$|\phi_{k_0}(\varepsilon)\rangle - |\varphi_{k'_0}(\varepsilon)\rangle = \sum_{n=0}^{\infty} \varepsilon^n \left( |\phi_{k_0}^{(n)}\rangle - |\varphi_{k'_0}^{(n)}\rangle \right) = 0.$$

Pour que cette égalité soit vraie pour tout  $\varepsilon > 0$ , chacun des termes de la

somme doit s'annuler. En particulier,

$$|\phi_{k_0}^{(n)}\rangle = |\varphi_{k'_0}^{(n)}\rangle$$

autrement dit, les matrices  $G$  et  $H$  partagent un vecteur propre.  $\square$

La combinaison des deux lemmes démontrés jusqu'à présent aboutit au théorème suivant.

**Théorème 5.6.** *Les couples de matrices hermitiennes qui partagent un vecteur propre commun constituent un ensemble fermé d'intérieur vide. En particulier, cet ensemble n'est dense nulle part.*

Autrement dit, les couples de matrices hermitiennes avec un vecteur propre en commun sont très peu courants. Toutefois, ce théorème ne permet pas d'affirmer que cet ensemble est de mesure zéro.<sup>3</sup> Néanmoins, le résultat mathématique obtenu indique que les hamiltoniens d'interaction et d'évolution propre partagent rarement une structure permettant l'existence d'un état initial de l'environnement permettant une évolution sans décohérence du système. De plus, même si les hamiltoniens partagent cette structure délicate, la plupart des perturbations la détruiront.

Nos résultats peuvent-ils être étendus à un environnement de dimension infinie? Au moins un problème surgit. La théorie des perturbations ne s'applique pas si le spectre des opérateurs non perturbés est continu. Un tel cas de figure empêcherait notre démonstration de s'appliquer.

### 5.3.4 Perturbation due à la dynamique de l'environnement

Dans cette section, nous allons nous intéresser au régime dans lequel l'hamiltonien total est dominé par l'hamiltonien d'interaction  $H_{S\mathcal{E}} = S \otimes E$  et l'évolution propre de l'environnement  $H_{\mathcal{E}}$  n'est qu'une perturbation.

---

<sup>3</sup>Par exemple, l'ensemble de Smith–Volterra–Cantor est dense nulle part mais de mesure strictement positive.

Puisque  $H_{S\mathcal{E}}$  domine, nous allons préparer l'environnement dans un état propre de  $E$  et chercher à quantifier l'erreur introduite par l'évolution propre de l'environnement.

Nous allons répondre à cette question dans un modèle particulier, qui n'est autre que le modèle de Żurek, auquel nous ajoutons un terme d'évolution propre de la forme

$$H_{\mathcal{E}} = \lambda \sum_{x,y \in \{0,1\}^n} |x\rangle\langle y|$$

où  $\lambda$  est un paramètre de perturbation. Notons que cet hamiltonien est proportionnel au projecteur sur  $|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$  puisque

$$H_{\mathcal{E}} = \lambda N |\Phi\rangle\langle\Phi|.$$

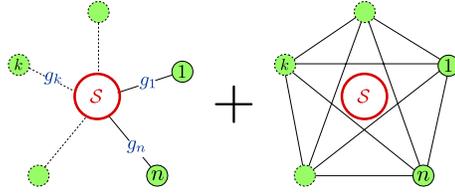


Figure 5.1 – Modèle de décohérence avec environnement dynamique ( $n = 5$ )

Les hamiltoniens  $H_{\mathcal{E}}$  et  $\tilde{H} = \sum_k g_k \sigma_z^k$  (dont on supposera que le choix des coefficients  $g_k$  ne fait pas apparaître de dégénérescence) n'ont pas de vecteurs propres en commun puisque les vecteurs propres de  $\tilde{H}$  sont les  $|x\rangle$  avec  $x \in \{0, 1\}$  qui ne sont pas des vecteurs propres de  $H_{\mathcal{E}}$ .

Supposons que l'environnement soit préparé dans l'état

$$|0\rangle = \bigotimes_{k=1}^n |0\rangle_k \quad (5.4)$$

qui est un état propre de  $\tilde{H}$  associé à la valeur propre  $\omega_0$ .

Calculons le facteur de décohérence pour cet état initial de l'environ-

nement. Un calcul standard en théorie des perturbations jusqu'au second ordre, valable pour  $\lambda \ll \min_{x,y \in \{0,1\}^n} |\omega_x - \omega_y|$ , montre que

$$|r(t)|^2 = 1 - 16\lambda^2 \sum_{x \neq 0} \frac{\sin^4\left(\frac{\omega_x - \omega_0}{2} t\right)}{(\omega_0 - \omega_x)^2}.$$

La valeur moyenne de cette quantité vaut

$$\overline{|r(t)|^2} = 1 - 6\lambda^2 \sum_{x \neq 0} \frac{1}{(\omega_0 - \omega_x)^2}.$$

Ainsi, la moyenne de  $|r(t)|^2$  est réduite par un facteur proportionnel à  $\sum_{x \neq 0} \frac{1}{(\omega_0 - \omega_x)^2}$  qui caractérise à quel point les niveaux d'énergie (non-perturbés) sont proches autour du niveau d'énergie (non-perturbé)  $\omega_0$  de l'état initial.

### 5.3.5 Préparation imparfaite de l'environnement

Replaçons nous maintenant dans le modèle original de Żurek pour lequel il existe des états initiaux de l'environnement permettant une évolution sans décohérence du système. Toutefois, supposer la capacité de pouvoir préparer parfaitement l'environnement est irréaliste et nous allons donc quantifier l'impact d'une préparation imparfaite de l'environnement dans le modèle de Żurek. Supposons que nous voulions préparer l'état 5.4. Ceci revient à préparer chaque qubit de l'environnement dans l'état  $\alpha|0\rangle_k + \beta|1\rangle_k$ , avec  $\alpha_k = 1$  et  $\beta_k = 0$ . Notre capacité limitée de préparation se traduit par l'assurance que  $|\beta_k|^2 \leq \varepsilon \ll 1$ . Autrement dit, chaque qubit est préparé avec une petite erreur. Dans ce cas, une borne inférieure sur la valeur moyenne de  $|r(t)|^2$  est

$$\overline{|r(t)|^2} \geq ((1 - \varepsilon)^2 + \varepsilon^2)^n \xrightarrow{\varepsilon \ll 1} 1 - 2n\varepsilon$$

qui est atteinte pour  $|\beta_k|^2 = \varepsilon$  pour tout  $k$ . En conclusion, pour des erreurs faibles et indépendantes sur chacun des  $n$  spins de l'environnement, la perte de pureté moyenne du système est proportionnelle au nombre de particules

dans l'environnement. Cet exemple particulier illustre bien que, même si un état initial de l'environnement permet une évolution unitaire du système, l'erreur introduite par une préparation imparfaite grandit linéairement avec la taille de l'environnement.

### 5.3.6 Contrôle imparfait de l'environnement

Jusqu'ici, nous nous sommes intéressés à l'existence d'états initiaux de l'environnement qui permettent d'éliminer toute décohérence. Nous avons obtenu un critère analytique qui permet de déterminer l'existence de tels états à partir de la structure des hamiltoniens d'interaction et d'évolution propre. Posons-nous maintenant une question plus générale : étant donné des hamiltoniens d'interaction et d'évolution propre qui ne partagent pas de vecteur propre commun, quel est le choix optimal d'état initial d'environnement afin de *minimiser* autant que possible la décohérence ?

Afin de répondre à cette question, il faut tout d'abord définir une notion d'optimalité. Deux options paraissent naturelles. L'une d'elle consiste à minimiser la décohérence en moyenne. Elle permettra toutefois que le système subisse ponctuellement de fortes baisses de cohérence. L'autre option est de demander à minimiser la décohérence en pire cas, c.-à-d. d'exiger que le plus haut niveau de décohérence atteint durant l'évolution soit le plus faible possible. Cette notion d'optimalité rejettera toutefois un état qui entraîne une évolution dans laquelle la cohérence subit une importante baisse de cohérence de façon ponctuelle bien que la cohérence soit très bonne en moyenne. Dans la suite, nous utiliserons la notion d'optimalité en pire cas, simplement parce qu'elle semble plus maniable mathématiquement.

Nous allons répondre à la question du choix optimal du vecteur initial de l'environnement sur un exemple. Il s'agit d'un exemple particulièrement simple, voire le plus simple, d'une situation où aucun vecteur propre commun

n'existe. Considérons un hamiltonien de la forme

$$H = \varepsilon_1 \sigma_z \otimes \sigma_x + \varepsilon_3 \mathbf{1}_S \otimes \sigma_z$$

où  $\varepsilon_1$  et  $\varepsilon_3$  caractérisent l'importance relative de l'hamiltonien d'interaction  $\tilde{H} = \varepsilon_1 \sigma_x$  et d'évolution propre  $H_E = \varepsilon_3 \sigma_z$ . Dans ce modèle, il est possible de définir  $|\varepsilon_0(t)\rangle$  et  $|\varepsilon_1(t)\rangle$  qui obéissent aux équations de Schrodinger (5.1). Il est possible de réécrire

$$\begin{cases} |\varepsilon_0(t)\rangle = e^{-i\epsilon t \hat{m}_0 \cdot \sigma} \text{ où } \hat{m}_0 = (\varepsilon_1/\varepsilon, 0, \varepsilon_3/\varepsilon) \\ |\varepsilon_1(t)\rangle = e^{-i\epsilon t \hat{m}_1 \cdot \sigma} \text{ où } \hat{m}_1 = (-\varepsilon_1/\varepsilon, 0, \varepsilon_3/\varepsilon) \end{cases}$$

avec  $\varepsilon^2 = \varepsilon_1^2 + \varepsilon_3^2$  afin que les vecteurs  $\hat{m}_{0,1}$  soient unitaires. Il est alors possible de réécrire ces vecteurs sous la forme

$$\hat{m}_0 = (\sin \alpha, 0, \cos \alpha) \quad \hat{m}_1 = (-\sin \alpha, 0, \cos \alpha)$$

où  $0 < \alpha < \pi/2$ . Ceci va permettre de réécrire le problème du choix de l'état initial  $|I\rangle$  de l'environnement en un problème où un spin 1/2 interagit avec deux champs magnétiques de même intensité dont la direction est donnée par  $\hat{m}_0$  et  $\hat{m}_1$ . Le spin 1/2, initialement dans une direction  $\mathbf{I}$  va alors précesser autour de  $\hat{m}_0$ , ce qui définit  $\mathbf{I}_0(t)$ , ou autour de  $\hat{m}_1$ , ce qui définit  $\mathbf{I}_1(t)$ . Ces deux vecteurs obéissent à

$$\begin{cases} \frac{d}{dt} \mathbf{I}_0(t) = \hat{m}_0 \times \mathbf{I}_0(t) \\ \frac{d}{dt} \mathbf{I}_1(t) = \hat{m}_1 \times \mathbf{I}_1(t) \end{cases} .$$

La norme du facteur de cohérence  $|r(t)| = |\langle \varepsilon_0(t) | \varepsilon_1(t) \rangle| = \cos \gamma(t)/2$  où  $\gamma(t)$  est l'angle entre  $\mathbf{I}_0(t)$  et  $\mathbf{I}_1(t)$ . Ainsi, nous voulons déterminer le choix de  $\mathbf{I}$  tel que l'angle maximal entre  $\mathbf{I}_0(t)$  et  $\mathbf{I}_1(t)$  au cours d'une période est minimisé. Une idée qui paraît raisonnable est de préparer un état propre de  $H_0$  ou  $H_1$ , c'est-à-dire de choisir  $\mathbf{I} = \hat{m}_0$  ou  $\mathbf{I} = \hat{m}_1$ . Dans ce cas, l'angle

maximal est le minimum entre  $4\alpha$  et  $2\pi - 4\alpha$ , atteint après une demi-période de précession. Toutefois, ce choix n'est pas optimal pour toute valeur de  $\alpha$ .

Trouver l'angle maximal entre  $\mathbf{I}_0(t)$  et  $\mathbf{I}_1(t)$  pour un  $\mathbf{I}$  arbitraire est une tâche non-triviale analytiquement. Nous avons donc numériquement balayé toute la sphère pour différentes valeurs de  $\alpha$  afin de déterminer la valeur minimale de la décohérence en pire cas, que nous noterons  $|r_{\min}|$ . Les résultats numériques sont représentés sur la figure (5.2).

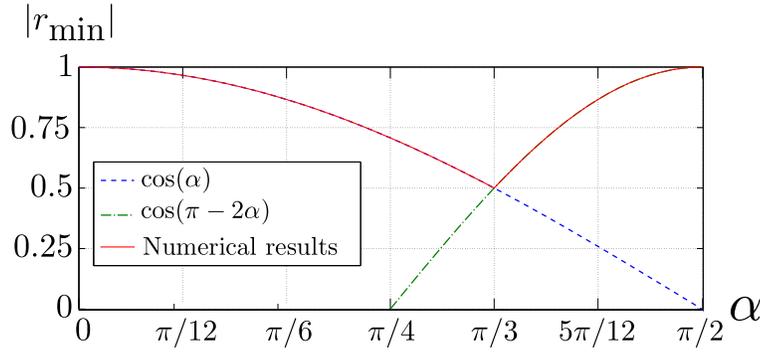


Figure 5.2 – Résultats numériques

Pour  $\alpha \geq \pi/3$ , le choix intuitif est optimal. Un état initial optimal est  $\mathbf{I} = \hat{m}_0$  ou  $\mathbf{I} = \hat{m}_1$ . L'angle maximal est alors  $\gamma_{\max} = 2\pi - 4\alpha$  qui fournit

$$|r_{\min}| = \cos(\pi - 2\alpha).$$

Toutefois, pour  $\alpha \leq \pi/3$ , le choix intuitif n'est pas optimal. L'état initial optimal est  $\mathbf{I} = \hat{y}$  qui correspond à l'état  $\frac{1}{\sqrt{2}}|0\rangle + i\frac{1}{\sqrt{2}}|1\rangle$ . L'angle maximal est alors  $\gamma_{\max} = 2\alpha$  atteint après un quart de période de précession et fournit

$$|r_{\min}| = \cos \alpha.$$

Ainsi, pour  $\alpha \leq \pi/3$ , l'état initial optimal n'est pas vecteur propre d'aucun des hamiltoniens en présence ( $H_0, H_1, H_{\mathcal{E}}, \tilde{H}$ ). Nous allons maintenant tenter de comprendre pourquoi dans le cas  $\alpha \leq \pi/3$ , le choix de l'état initial optimal est non-trivial alors qu'il semble intuitif dans le cas  $\alpha \geq \pi/3$ .

Dans le régime  $\alpha \geq \pi/3$ , l'interaction entre le système et l'environnement

domine et l'évolution propre de l'environnement n'est qu'une perturbation. En particulier, le système et l'environnement jouent des rôles presque symétriques. Réduire la décohérence revient alors à minimiser l'intrication qui se crée entre le système et son environnement. Les états initiaux optimaux de l'environnement sont alors les états indicateurs de l'environnement, ce qui est conforme à la théorie de la décohérence. Au contraire, dans le régime  $\alpha \leq \pi/3$ , l'hamiltonien d'évolution propre domine l'hamiltonien  $\tilde{H}$ . Toutefois, l'évolution du système quantique se fait exclusivement via l'interaction entre le système et l'environnement. Ainsi, du point de vue de l'évolution du système, l'hamiltonien  $\tilde{H}$  ne peut pas être considéré comme une perturbation de  $H_{\mathcal{E}}$ , et ce aussi petit soit-il. Dans ce cas, l'évolution de l'environnement est dominée par sa dynamique propre, mais l'impact sur le système quantique est transmis via l'hamiltonien d'interaction  $\tilde{H}$ . Trouver un critère analytique caractérisant un état initial de l'environnement qui minimise la décohérence du système lors de son évolution est une tâche difficile puisque ce critère doit tenir compte du compromis délicat entre les hamiltoniens d'évolution propre et d'interaction qui agissent sur l'environnement.

## Préparation de l'environnement : conclusion

Dans la section 5.3, nous avons proposé une méthode originale afin de protéger un système quantique de la décohérence. Il s'agit de préparer l'état de l'environnement initialement afin de forcer l'évolution subséquente du système à maintenir la cohérence du système. Notre analyse, dans la section 5.3.3.1, a permis de déterminer sous quelles conditions de tels états existent dans une classe de modèle où le système interagit avec un environnement dynamique. Cette classe est vaste, mais n'est pas la plus générale puisque le système n'a pas de dynamique propre et l'hamiltonien d'interaction est un produit tensoriel (plutôt qu'une somme de produits tensoriels). Les couples d'hamiltoniens permettant l'existence de ces états particuliers forment toutefois un sous-ensemble très réduit des couples d'hamiltoniens, au moins en

dimension finie (section 5.3.3.2). Toutefois, de tels états initiaux existent systématiquement si l'environnement est statique, mais une faible dynamique de l'environnement entraîne une perte de cohérence liée à la densité des niveaux d'énergie proches du niveau d'énergie initialement préparé (section 5.3.4). De plus, même dans le cas où un état de l'environnement convient, la préparation imparfaite de cet état, qui paraît inévitable en pratique, entraîne dans le modèle de Żurek une perte de pureté proportionnelle au nombre de particules dans l'environnement (section 5.3.5). Finalement, nous nous sommes attardés au cas général dans lequel il n'existe pas d'état permettant d'éviter complètement la décohérence n'existe pas. Nous avons étudié un exemple afin de déterminer l'état optimal à préparer sur l'environnement afin de minimiser la décohérence du système (section 5.3.6). Cette étude a permis de mettre en évidence la non-trivialité de cette tâche, en particulier dans le régime où la dynamique propre de l'environnement domine. En effet, dans ce cas, la dynamique de l'environnement est dominée par son évolution propre, mais l'impact de cette évolution sur le système se fait grâce à l'interaction entre le système et l'environnement, aussi faible soit-elle. L'état optimal est donc déterminé par cet équilibre délicat. La mise en place d'outils afin de caractériser un état optimal reste donc un défi ouvert.

# Chapitre 6

## Conclusion

Ce mémoire comporte trois chapitres qui mettent en place les notions et les outils nécessaires à la compréhension du travail original présenté dans les deux derniers chapitres. L'intérêt de protéger un système quantique de la décohérence est motivé par le domaine de l'informatique quantique, brièvement introduit au chapitre 1. La décohérence, qui repose sur l'interaction entre un système et son environnement, s'appuie fortement sur la notion de système quantique *ouvert*. Le traitement mathématique d'un tel système requiert des outils spécifiques, introduits au chapitre 2. Munis de ces outils, nous avons présenté les caractéristiques générales de la décohérence au chapitre 3. Rappelons que les deux avancées fondamentales de cette théorie, qui reste dans le cadre du formalisme traditionnel de la mécanique quantique sont l'émergence d'états privilégiés et la destruction de la cohérence d'une superposition de ces états.

Le travail novateur de ce mémoire s'articule autour de deux grands thèmes. Le premier est l'étude d'un gyroscope quantique au chapitre 4. Notre étude a permis de mettre en évidence que cet objet subit une décohérence via des mécanismes conformes aux résultats généraux de la théorie de la décohérence. Plus précisément, nous avons obtenu un résultat d'équivalence entre un modèle de mesure et un modèle d'interaction, suggérant qu'une mesure est une forme particulière d'interaction. De plus, nous avons montré qu'une par-

ticule de grand spin servant à mesurer le moment angulaire d'électrons perd sa cohérence en un temps très court par rapport au temps caractéristique de relaxation. Le second apport original de ce mémoire est l'introduction d'une approche originale afin de lutter contre la décohérence dans le chapitre 5. Celle-ci consiste à *préparer l'environnement* afin de réduire la perte de cohérence du système lors de l'évolution subséquente. Notre étude nous a permis d'obtenir une caractérisation formelle de l'existence d'états initiaux de l'environnement permettant une suppression complète de la décohérence du système dans une gamme générale de modèles où le système interagit avec un environnement dynamique. Toutefois, nous avons prouvé des résultats topologiques qui suggèrent que les conditions d'existence de tels états sont rarement respectées. Ce constat nous amené à tenter de caractériser les états optimaux afin de minimiser la décohérence lorsqu'il n'est pas possible de l'éviter. Sans parvenir à cette caractérisation, nous avons mis en évidence les raisons pour lesquelles elle constitue un défi de taille.

## BIBLIOGRAPHIE

- [1] D. Aharonov et M. Ben-Or : Fault-tolerant quantum computation with constant error. *In Proceedings of the 29th Annual ACM Symposium on Theory of Computation (STOC)*, 1997.
- [2] P. Anderson : More is different. *Science*, 177(4047): 393–396, 1972.
- [3] W. Appel : *Mathématiques pour la physique et les physiciens*. H&K, 3<sup>e</sup> édn, 2005.
- [4] M. Arndt, O. Nairz, J. Vos-Andreae, C. Keller, G. van der Zouw et A. Zeilinger : Wave-particle duality of C<sub>60</sub> molecules. *Nature*, 401(6754): 680–682, oct. 1999.
- [5] A. Aspect, J. Dalibard et G. Roger : Experimental test of Bell’s inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25): 1804–1807, 1982.
- [6] H. Azuma : Decoherence in Grover’s quantum algorithm : Perturbative approach. *Phys. Rev. A*, 65(4): 042311, Apr 2002.
- [7] M. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. Itano, J. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri et D. J. Wineland : Deterministic quantum teleportation of atomic qubits. *Nature*, 429(6993): 737–739, 2004.
- [8] S. D. Bartlett, T. Rudolph et R. W. Spekkens : Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.*, 79(2): 555, 2007.
- [9] S. D. Bartlett, T. Rudolph, R. W. Spekkens et P. S. Turner : Degradation of a quantum reference frame. *New J. Phys.*, 8(4): 58, 2006.
- [10] J. S. Bell : On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, 38(3): 447–452, 1966.

- [11] G. Benenti, G. Casati et G. Strini : *Principles of Quantum Computation and Information*. World Scientific, Singapour, 2004.
- [12] C. Bennett et G. Brassard : Quantum cryptography : Public key distribution and coin tossing. *In Proceedings of International Conference on Computers, Systems and Signal Processing*, vol. 175, 1984.
- [13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres et W. K. Wootters : Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13): 1895–1899, 1993.
- [14] R. Blume-Kohout et W. H. Zurek : Quantum darwinism : Entanglement, branches, and the emergent classicality of redundantly stored quantum information. *Phys. Rev. A*, 73(6): 062310, 2006.
- [15] D. Boschi, S. Branca, F. De Martini, L. Hardy et S. Popescu : Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 80(6): 1121–1125, Feb 1998.
- [16] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter et A. Zeilinger : Experimental quantum teleportation. *Nature*, 390(6660): 575–579, 1997.
- [17] G. Brassard : Quantum information processing for computer scientists. (manuscrit).
- [18] G. Brassard : Is information the key? *Nature Physics*, 1(1): 2–4, 2005.
- [19] R. Brunner, R. Akis, D. K. Ferry, F. Kuchar et R. Meisels : Coupling-induced bipartite pointer states in arrays of electron billiards : Quantum darwinism in action? *Phys. Rev. Lett.*, 101(2): 024102, 2008.
- [20] J. Bub : *Interpreting the quantum world*. Cambridge University Press, 1999.

- [21] E. Buks, R. Schuster, M. Heiblum, D. Mahalu et V. Umansky : Dephasing in electron interference by a "which-path" detector. *Nature*, 391(6670): 871–874, 1998.
- [22] A. O. Caldeira et A. J. Leggett : Path integral approach to quantum brownian motion. *Physica A : Statistical and Theoretical Physics*, 121(3): 587 – 616, 1983.
- [23] J. F. Clauser, M. A. Horne, A. Shimony et R. A. Holt : Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15): 880–884, Oct 1969.
- [24] R. Clifton : *The triorthogonal uniqueness theorem and its irrelevance to modal interpretation of quantum mechanics*, p. 45–60. Atlantica Séguier Frontières, 1994.
- [25] C. Cohen-Tannoudji, B. Diu et F. Laloë : *Mécanique Quantique*. Hermann, 1977.
- [26] F. M. Cucchietti, J. P. Paz et W. H. Zurek : Decoherence from spin environments. *Phys. Rev. A*, 72(5): 052113, Nov 2005.
- [27] J. Dalibard : Cohérence quantique et dissipation. Notes de cours, 2006.
- [28] D. A. R. Dalvit, J. Dziarmaga et W. H. Żurek : Decoherence in bose-einstein condensates : Towards bigger and better schrödinger cats. *Phys. Rev. A*, 62(1): 013607, Jun 2000.
- [29] D. A. R. Dalvit, J. Dziarmaga et W. H. Żurek : Predictability sieve, pointer states, and the classicality of quantum trajectories. *Phys. Rev. A*, 72(6): 062101, Dec 2005.
- [30] A. Einstein, B. Podolsky et N. Rosen : Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10): 777–780, May 1935.

- [31] A. Elby et J. Bub : Triorthogonal uniqueness theorem and its relevance to the interpretation of quantum mechanics. *Phys. Rev. A*, 49(5): 4213–4216, May 1994.
- [32] H. Everett : "relative state" formulation of quantum mechanics. *Rev. Mod. Phys.*, 29(3): 454–462, Jul 1957.
- [33] E. Farhi et S. Gutmann : Analog analogue of a digital quantum computation. *Phys. Rev. A*, 57(4): 2403–2406, Apr 1998.
- [34] E. Farhi et S. Gutmann : Quantum computation and decision trees. *Phys. Rev. A*, 58(2): 915–928, Aug 1998.
- [35] I. Gelfand et M. Neumark : *On the imbedding of normed rings into the ring of operators in Hilbert space*. American Mathematical Society, 1994.
- [36] V. Gorini, A. Kossakowski et E. C. G. Sudarshan : Completely positive dynamical semigroups of n-level systems. *Journal of Mathematical Physics*, 17(5): 821–825, 1976.
- [37] G. Gour et R. W. Spekkens : The resource theory of quantum reference frames : manipulations and monotones. *New J. Phys.*, 10(3): 033023 (63pp), 2008.
- [38] L. K. Grover : Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2): 325–328, Jul 1997.
- [39] L. Hackermüller, K. Hornberger, B. Brezger, A. Zeilinger et M. Arndt : Decoherence of matter waves by thermal emission of radiation. *Nature*, 427(6976): 711–714, 2004.
- [40] L. Hackermüller, S. Uttenthaler, K. Hornberger, E. Reiger, B. Brezger, A. Zeilinger et M. Arndt : Wave nature of biomolecules and fluorofullerenes. *Phys. Rev. Lett.*, 91(9): 090408, Aug 2003.

- [41] K. Hornberger : *Entanglement and Decoherence*, vol. 768 de *Lecture Notes in Physics*, p. 221–276. Springer Berlin / Heidelberg, 2009.
- [42] B. L. Hu, J. P. Paz et Y. Zhang : Quantum brownian motion in a general environment : Exact master equation with nonlocal dissipation and colored noise. *Phys. Rev. D*, 45(8): 2843–2861, Apr 1992.
- [43] G. Jaeger : *Quantum information : An overview*. Springer-Verlag, 2007.
- [44] T. Katō : *Perturbation theory for linear operators*. Springer, 1966.
- [45] P. Kaye, R. Laflamme et M. Mosca : *An introduction to quantum computing*. Oxford University Press, USA, 2007.
- [46] K. Kraus : *States, effects, and operations : Fundamental notions of quantum theory*, vol. 190 de *Lecture Notes in Physics*. Springer-Verlag, Berlin, 1983.
- [47] O. Landon-Cardinal et R. MacKenzie : Decoherence suppression via environment preparation. *Phys. Rev. A*, à paraître.
- [48] D. A. Lidar, I. L. Chuang et K. B. Whaley : Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81(12): 2594–2597, Sep 1998.
- [49] G. Lindblad : On the generators of quantum dynamical semigroups. *Communications in Mathematical Physics*, 48(2): 119–130, 1976.
- [50] N. Mermin : *Quantum computer science : An introduction*. Cambridge University Press, 2007.
- [51] C. Mochon : Hamiltonian oracles. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 75(4): 042313, 2007.
- [52] C. Monroe, D. M. Meekhof, B. E. King et D. J. Wineland : A “schrodinger cat” superposition state of an atom. *Science*, 272(5265): 1131–1136, 1996.

- [53] M. Nakahara et T. Ohmi : *Quantum computing : from linear algebra to physical realizations*. CRC Press, 2008.
- [54] M. A. Nielsen et I. L. Chuang : *Quantum Information and Quantum Information*. Cambridge University Press, 2000.
- [55] H. Ollivier, D. Poulin et W. H. Zurek : Environment as a witness : Selective proliferation of information and emergence of objectivity in a quantum universe. *Phys. Rev. A*, 72(4): 042113, Oct 2005.
- [56] H. Ollivier et W. H. Zurek : Quantum discord : A measure of the quantumness of correlations. *Phys. Rev. Lett.*, 88(1): 017901, Dec 2001.
- [57] S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan et C. Monroe : Quantum teleportation between distant matter qubits. *Science*, 323(5913): 486–489, 2009.
- [58] J. P. Paz, S. Habib et W. H. Zurek : Reduction of the wave packet : Preferred observable and decoherence time scale. *Phys. Rev. D*, 47(2): 488–501, Jan 1993.
- [59] J. P. Paz et W. H. Zurek : Quantum limit of decoherence : Environment induced superselection of energy eigenstates. *Phys. Rev. Lett.*, 82(26): 5181–5185, Jun 1999.
- [60] J. P. Paz et W. H. Zurek : *Coherent Matter Waves, Lectures from the 72nd Les Houches Summer School, 1999*, p. 533–614. Springer-Verlag, Berlin, 2001.
- [61] D. Poulin et J. Yard : Dynamics of a quantum reference frame. *New J. Phys.*, 9(5): 156, 2007.
- [62] J. Preskill : Quantum information and computation. Lecture notes for physics 229, California Institute of Technology, 1998.

- [63] M. Riebe, H. Häffner, C. Roos, W. Hänsel, J. Benhelm, G. Lancaster, T. Körber, C. Becher, F. Schmidt-Kaler, D. James et R. Blatt : Deterministic quantum teleportation with atoms. *Nature*, 429(6993): 734–737, 2004.
- [64] J. Roland et N. J. Cerf : Quantum-circuit model of hamiltonian search algorithms. *Phys. Rev. A*, 68(6): 062311, Dec 2003.
- [65] D. Rugar, R. Budakian, H. J. Mamin et B. W. Chui : Single spin detection by magnetic resonance force microscopy. *Nature*, 430(6997): 329–332, juil. 2004.
- [66] M. Schlosshauer : *Decoherence and the Quantum to Classical Transition*. Springer-Verlag Berlin, 2007.
- [67] E. Schrödinger : Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23(49): 823–828, déc. 1935.
- [68] E. Schrodinger : The present situation in quantum mechanics. *Naturwissenschaften*, 23: 807–812, 1935.
- [69] P. Shor : Algorithms for quantum computation : Discrete logarithms and factoring. p. 124–134, Nov 1994.
- [70] P. W. Shor : Why haven't more quantum algorithms been found? *J. ACM*, 50(1): 87–90, 2003.
- [71] J. D. Trimmer : The present situation in quantum mechanics : A translation of schrödinger's "cat paradox" paper. *Proceedings of the American Philosophical Society*, 124(5): 323–338, 1980.
- [72] L. Viola et S. Lloyd : Dynamical suppression of decoherence in two-state quantum systems. *Phys. Rev. A*, 58(4): 2733–2744, Oct 1998.
- [73] D. Vitali, S. Gigan, A. Ferreira, H. R. Böhm, P. Tombesi, A. Guerreiro, V. Vedral, A. Zeilinger et M. Aspelmeyer : Optomechanical entangle-

- ment between a movable mirror and a cavity field. *Phys. Rev. Lett.*, 98(3): 030405, 2007.
- [74] J. von Neumann : *Mathematische Grundlagen der Quantenmechanik*. Springer, 1932.
- [75] W. Wootters et W. Zurek : A single quantum cannot be cloned. *Nature*, 299, 1982.
- [76] J. Wróbel, T. Dietl, A. Łusakowski, G. Grabecki, K. Fronc, R. Hey, K. H. Ploog et H. Shtrikman : Spin filtering in a hybrid ferromagnetic-semiconductor microstructure. *Phys. Rev. Lett.*, 93(24): 246601, Dec 2004.
- [77] W. H. Zurek : Pointer basis of quantum apparatus : Into what mixture does the wave packet collapse? *Phys. Rev. D*, 24(6): 1516–1525, Sep 1981.
- [78] W. H. Zurek : Environment-induced superselection rules. *Phys. Rev. D*, 26(8): 1862–1880, Oct 1982.
- [79] W. H. Zurek : Preferred states, predictability, classicality and the environment-induced decoherence. *Progress of Theoretical Physics*, 89(2): 281–312, 1993.
- [80] W. H. Zurek : Quantum darwinism. *Nature Physics*, 5: 181–188, 2009.
- [81] W. H. Zurek, S. Habib et J. P. Paz : Coherent states via decoherence. *Phys. Rev. Lett.*, 70(9): 1187–1190, Mar 1993.

# Annexe A

## Algorithmes à la physicienne

Jusqu'à présent, nous avons introduit les algorithmes quantiques dans le modèle des circuits quantiques. Nous allons maintenant envisager ces algorithmes d'un autre point de vue, plus intuitif pour un physicien.

### A.1 Oracle hamiltonien

Comme nous l'avons déjà mentionné, la plupart des algorithmes quantiques font intervenir un oracle représenté par un opérateur  $U_f$ . Dans la nouvelle approche que nous sommes en train de décrire, nous allons nous intéresser à une version hamiltonienne de ces oracles (voir [51] pour une discussion exhaustive des oracles hamiltoniens). Ainsi, un oracle sera défini par un hamiltonien  $H_f$ . Afin de réconcilier les deux approches, imposons que pour une durée d'interaction  $\tau$ , l'évolution sous l'action de  $H_f$  durant  $\tau$  corresponde à l'évolution sous l'action de la porte unitaire  $U_f$ , c'est-à-dire

$$e^{-iH_f\tau} = e^{i\varphi}U_f$$

où  $\varphi$  est une phase arbitraire.

À titre d'exemple, nous allons définir une version hamiltonienne de l'oracle de Grover [64], défini par  $U_f|x\rangle = (-1)^{f(x)}|x\rangle$ . Considérons l'ha-

miltonien

$$H_f = \mathbf{1} - |w\rangle\langle w|$$

Son action dans la base de calcul vérifie

$$e^{-iH_f t}|x\rangle = \begin{cases} |x\rangle & x = w \\ e^{-it}|x\rangle & \forall x \neq w. \end{cases}$$

Ainsi, pour une durée d'interaction  $\tau = \pi$ , nous obtenons

$$e^{-iH_f \tau} = -U_f$$

## A.2 Algorithme hamiltonien

Décrivons maintenant la construction et l'exécution d'un algorithme quantique général dans l'approche hamiltonienne.

La construction d'un algorithme commence par la prise en main du problème. Celui-ci est habituellement défini par un oracle hamiltonien  $H_f$ . Cet hamiltonien varie donc en fonction de l'exemplaire du problème. Tout le travail du concepteur de l'algorithme consiste alors à construire un hamiltonien total  $H$  de la forme  $H(t) = a(t)H_f + H_D(t)$ , qui se réduit à  $H = H_f + H_D$  dans le cas où  $H$  ne dépend pas du temps. La difficulté est donc de trouver un hamiltonien pilote  $H_D$  (*driving hamiltonian*) qui ne dépend pas de l'exemplaire et qui va entraîner l'évolution voulue. Le choix de  $H_D$  est intimement lié au choix d'un état initial  $|\psi(t=0)\rangle$ , d'une durée d'évolution  $T$  et d'une mesure  $\mathcal{M}$  (liée à un observable  $M$ ). Ainsi, l'algorithme quantique est défini par le quadruplet  $(H_D, |\psi(0)\rangle, T, \mathcal{M})$ .

L'exécution de l'algorithme quantique se déroulera alors en 3 étapes :

1. la préparation de l'état initial  $|\psi(0)\rangle$  ;
2. l'évolution durant un temps  $T$  sous l'action de  $H$  ; et
3. la mesure de  $M$  sur  $|\psi(T)\rangle$ .

Nous allons maintenant présenter la version hamiltonienne de l'algorithme de Grover, introduite par Fahri et Gutmann [33]. Nous avons déjà présenté la version hamiltonienne de l'oracle. Est-il possible de trouver un hamiltonien qui corresponde à l'inversion par rapport à la moyenne? Considérons l'hamiltonien

$$H_D = \mathbb{H}^{\otimes n} (\mathbf{1} - |0\rangle\langle 0|) \mathbb{H}^{\otimes n} = \mathbf{1} - |s\rangle\langle s|.$$

Il est facile de montrer que pour une durée d'interaction  $\tau = \pi$

$$e^{-iH_D\pi} = U_D.$$

L'état initial de la version hamiltonienne sera  $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$  comme dans la version circuit de l'algorithme de Grover. Laissons cet état initial évoluer sous l'action de

$$H = H_D + H_f$$

L'état résultant peut être calculé dans le sous-espace engendré par  $|w\rangle$  et  $|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$ . Nous obtenons alors

$$\begin{aligned} |\psi(\tau)\rangle &= e^{-i(H_D+H_f)\tau} |s\rangle \\ &= e^{-i\tau} \left( \cos \frac{\tau}{\sqrt{N}} |s\rangle + i \sin \frac{\tau}{\sqrt{N}} |w\rangle \right) \end{aligned}$$

Ainsi, pour  $\tau = \frac{\pi}{2}\sqrt{N}$ , nous obtenons alors

$$|\psi(\frac{\pi}{2}\sqrt{N})\rangle \propto |w\rangle.$$

Il suffit alors de mesurer l'état quantique après une durée  $\frac{\pi}{2}\sqrt{N}$  afin d'obtenir  $w$  avec probabilité 1.



# Annexe B

## Téléportation quantique

L'utilisation de la notion d'opérateur densité réduit trouve une magnifique application dans la compréhension du protocole de téléportation quantique. L'objectif de ce protocole est de permettre à Alice qui possède un qubit dans un état pur  $|\psi\rangle$  inconnu de l'envoyer à Bob sans toutefois transporter le système physique lui-même. Ce protocole a été proposé théoriquement en 1993 [13] avant d'être testé expérimentalement à maintes reprises, d'abord avec des photons [15, 16], puis des atomes [7, 63]. Il fait toujours l'objet de recherche expérimentale [57]. Nous allons rapidement décrire ce protocole en trois étapes afin de nous intéresser à la description du protocole du point de vue de Bob.

### B.1 Partage d'intrication

La première étape consiste à partager de l'intrication entre Alice et Bob. Plus précisément, ils créent une paire EPR dans l'état  $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$  et gardent chacun un qubit de la paire. Alice part alors en exploration spatiale alors que Bob demeure sur la terre. L'intrication qu'ils partagent va se révéler une ressource importante dans la suite du protocole.

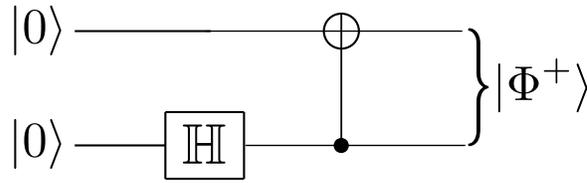


Figure B.1 – Partage d'intrication

## B.2 Mesure de Bell chez Alice

Alice et Bob sont maintenant éloignés l'un de l'autre. Ils ne peuvent alors qu'effectuer des *opérations locales* sur leur qubit respectif et *communiquer de façon classique*, c'est-à-dire avec des bits classiques. Dans le jargon de l'informatique quantique, ils sont limités à des LOCC (*local operations and classical communication*). Au cours de son voyage intersidéral, Alice récupère alors un qubit dans un état  $|\psi\rangle$  inconnu que l'on supposera pur par commodité (bien que ce ne soit pas nécessaire). Elle veut maintenant l'envoyer à Bob, mais ne peut envoyer l'objet physique lui-même. Elle va donc intriquer le qubit inconnu avec sa moitié de paire EPR en appliquant une opération CNOT suivie d'une porte de Hadamard sur le qubit inconnu. Pour les besoins du calcul, on écrit  $|\psi\rangle = a|0\rangle + b|1\rangle$ , bien qu'Alice ne possède aucune information sur  $a$  et  $b$ . Au niveau global, l'opération locale d'Alice aura pour effet de créer l'état

$$\frac{a}{2} (|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \frac{b}{2} (|001\rangle + |010\rangle - |101\rangle - |110\rangle). \quad (\text{B.1})$$

Alice mesure alors les deux qubits qu'elle possède et obtient deux bits classiques. Quatre possibilités équiprobables se présentent :

1. Alice mesure 00 et sait donc que Bob possède maintenant un qubit dans l'état  $a|0\rangle + b|1\rangle = |\psi\rangle$
2. Alice mesure 01 et sait donc que Bob possède maintenant un qubit dans l'état  $b|0\rangle + a|1\rangle = X|\psi\rangle$
3. Alice mesure 10 et sait donc que Bob possède maintenant un qubit dans l'état  $a|0\rangle - b|1\rangle = Z|\psi\rangle$

4. Alice mesure 11 et sait donc que Bob possède maintenant un qubit dans l'état  $-b|0\rangle + a|1\rangle = XZ|\psi\rangle$

Ainsi, après mesure, Alice connaît l'opérateur unitaire que Bob doit appliquer sur son qubit afin d'obtenir un qubit dans l'état  $|\psi\rangle$ . Notons toutefois qu'Alice n'a rien appris sur l'état  $|\psi\rangle$  lui-même.

### B.3 Signal classique et correction

Alice communique le résultat de sa mesure à Bob à l'aide d'un canal de communication classique. Bob reçoit alors deux bits d'information classique. *Ce n'est qu'à la réception de ces deux bits que Bob peut décrire son qubit comme étant le qubit  $|\psi\rangle$  auquel a été appliqué une opération unitaire  $U \in \{1, X, Z, XZ\}$ .* L'information reçue d'Alice permet de plus d'identifier l'opérateur  $U$ . Bob applique alors l'opération unitaire adéquate afin d'obtenir un qubit dans l'état  $|\psi\rangle$ .

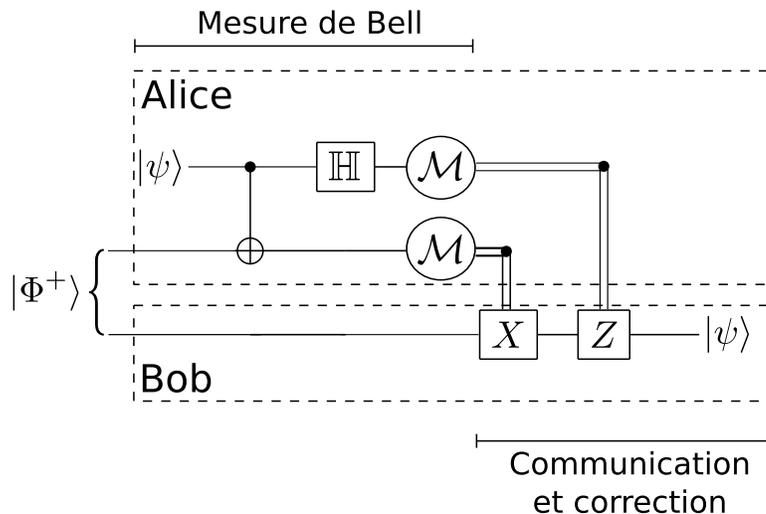


Figure B.2 – Représentation en circuit du protocole de téléportation

Avant de recevoir le message classique d'Alice, les actions d'Alice ne peuvent pas avoir d'influence mesurable par Bob. Assurons-nous que ce soit bien le cas. Initialement, Bob possède une moitié de paire EPR dont

l'opérateur densité est  $\frac{1}{2}\mathbf{1}$ , voir équation (2.8). Toutefois, à l'issue de la phase durant laquelle Alice intrique l'état inconnu avec sa moitié de paire EPR, Bob *semble* obtenir de l'information sur  $|\psi\rangle$ . En fait, il n'en est rien : avant d'avoir reçu le résultat de la mesure d'Alice, la description de l'état de Bob, du point de vue de Bob est un mélange statistique  $\{(|\psi\rangle, \frac{1}{4}), (X|\psi\rangle, \frac{1}{4}), (Z|\psi\rangle, \frac{1}{4}), (XZ|\psi\rangle, \frac{1}{4})\}$ . Or, nous avons montré en (2.14) que l'opérateur densité de ce mélange statistique est  $\rho = \frac{1}{2}\mathbf{1}$  et ce quel que soit l'état  $|\psi\rangle$ . Ainsi, tant que Bob n'a pas reçu d'information classique d'Alice, sa description de son état quantique ne change pas.

# Annexe C

## Mesure généralisée

Nous allons donner ici un exemple de l'utilité d'une mesure généralisée et montrer qu'un POVM permet de faire mieux qu'une mesure projective. Cet exemple est tiré du cours "Introduction à l'informatique quantique" enseigné par Gilles Brassard à l'Université de Montréal. Son approche est reprise dans un livre à paraître [17]. Supposons que Bob reçoive des qubits de la part d'Alice qui lui assure que chacun d'entre eux est soit dans l'état  $|0\rangle$ , soit dans l'état  $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$  et que ces deux possibilités sont équiprobables *a priori*. L'objectif de Bob est de déterminer dans lequel des deux états chacun des qubits se trouvent et ce de façon optimale. Or, que veut dire optimal dans un tel scénario ?

Une option est d'obtenir un résultat probabiliste, c.-à-d. effectuer une mesure qui permette d'induire l'état du qubit avec une certaine probabilité, et maximiser cette probabilité. Une telle mesure est qualifiée de *mesure de Helstrom*. Dans le scénario proposé ici, il peut être démontré que la mesure optimale dans ce sens est une mesure projective qui consiste à mesurer dans la base  $\{\sin \frac{\pi}{8}|0\rangle + \cos \frac{\pi}{8}|1\rangle, \cos \frac{\pi}{8}|0\rangle - \sin \frac{\pi}{8}|1\rangle\}$ . Un raisonnement bayésien montre alors que la probabilité que le qubit soit dans l'état  $|+\rangle$  sachant que le résultat de la mesure est  $\sin \frac{\pi}{8}|0\rangle + \cos \frac{\pi}{8}|1\rangle$  est  $\cos^2 \frac{\pi}{8}$ . Les autres probabilités se déduisent par symétrie.

Supposons maintenant que Bob ne se satisfasse pas d'un résultat proba-

biliste : il veut à tout prix connaître l'état du qubit de façon concluante ! Il est prêt à accepter que parfois le résultat de la mesure ne lui apprenne rien sur l'état du qubit. Toutefois, il insiste pour qu'un résultat significatif lui permette de conclure sur l'état du qubit. Dans ce cas, une stratégie naïve est de mesurer dans la base de calcul : si Bob obtient  $|1\rangle$ , il saura que l'état du qubit n'était pas  $|0\rangle$  et qu'il était donc  $|+\rangle$ . De façon équivalente, Bob pourrait mesurer dans la base  $\{|+\rangle, |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\}$ . Il peut aussi mesurer dans une des deux choisie au hasard chaque fois qu'il reçoit un qubit d'Alice. Cette stratégie sera concluante avec probabilité  $\frac{1}{4}$ .

Bob peut-il faire mieux, c.-à-d. augmenter cette probabilité ? S'il est limité à des mesures projectives, cette stratégie est optimale. Il peut toutefois faire mieux en utilisant un système ancillaire. Il suffit alors d'adjoindre un qubit initialisé dans l'état  $|0\rangle$  au qubit reçu d'Alice pour former  $|?\rangle \otimes |0\rangle$  puis d'appliquer la transformation unitaire

$$U = \begin{pmatrix} a & -b^2/a^2 & b^2/a & 0 \\ b & b/a & -b & 0 \\ 0 & b/a & b/a^2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{où} \quad \begin{cases} a = 2^{-1/4} \\ b = \sqrt{1-a^2} \end{cases} . \quad (\text{C.1})$$

Deux cas de figure se présentent selon l'état du qubit d'Alice

- s'il est dans l'état  $|0\rangle$ ,  $U$  transforme  $|00\rangle$  en  $a|00\rangle + b|01\rangle$ .
- s'il est dans l'état  $|+\rangle$ ,  $U$  transforme  $|+\rangle \otimes |0\rangle$  en  $a|00\rangle + b|10\rangle$ .

Ainsi, si Bob mesure 00, ce qui arrive avec probabilité  $\frac{1}{\sqrt{2}}$ , il n'obtient aucune information. Au contraire, s'il mesure 01 (ou 10), il peut conclure que le qubit d'Alice était dans l'état  $|0\rangle$  (ou  $|+\rangle$ ). La stratégie de Bob est concluante avec probabilité  $1 - \frac{1}{\sqrt{2}} \simeq 29\%$  qui est mieux que la stratégie précédente et peut être démontré optimal.

Dans le formalisme des POVM, la mesure généralisée précédente corres-

pond à un POVM à 3 éléments qui sont

$$E_{01} = \begin{pmatrix} b^2 & -b^2 \\ -b^2 & b^2 \end{pmatrix} = 2b^2|-\rangle\langle-| \quad E_{10} = 2b^2|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 2b^2 \end{pmatrix}$$

$$E_{00} = \begin{pmatrix} a^2 & b^2 \\ b^2 & b^4/a^2 \end{pmatrix} = \mathbf{1} - 2b^2|-\rangle\langle-| - 2b^2|1\rangle\langle 1|.$$

La mesure de l'élément  $E_{01}$  permet de conclure que l'état inconnu est  $|0\rangle$  puisqu'il correspond à un projecteur sur l'état  $|-\rangle$  qui est orthogonal à  $|+\rangle$ . Un raisonnement similaire indique que la mesure de  $E_{10}$  permet de conclure que l'état inconnu est  $|+\rangle$ . Pourquoi alors se contenter de multiplier ces projecteurs par  $2b^2 = 2 - \sqrt{2}$  plutôt que par un autre facteur plus proche de 1 ? Un calcul montre que pour assurer la positivité de  $E_{00} = \mathbf{1} - E_{01} - E_{10}$ , le facteur multiplicatif maximal admissible est  $2 - \sqrt{2}$ .



# Annexe D

## Modèles de décohérence avec équation pilote

Ces deux voies permettent toutes deux de calculer  $\rho_S(t)$  et paraissent donc équivalentes. Pourtant, la voie qui consiste à écrire une équation différentielle sur  $\rho_S$  est plus pratique lorsque vient le temps d'introduire des approximations<sup>1</sup>. Une telle équation sur  $\rho_S$  est appelée *équation pilote*. Les équations pilotes provenant de différents modèles peuvent être regroupées dans plusieurs grandes familles. Nous en mentionnerons rapidement deux : les équations pilotes avec approximations de Born-Markov et les équations de Lindblad.

### D.1 Équation pilote avec approximation de Born-Markov

Les systèmes en jeu sont l'environnement  $\mathcal{E}$  et le système  $\mathcal{S}$ . L'hamiltonien total  $H$  est composé de trois termes

$$H = H_S \otimes \mathbf{1}_E + \mathbf{1}_S \otimes H_E + H_{SE} \tag{D.1}$$

---

<sup>1</sup>Or, n'est-ce pas le travail de tout physicien d'introduire des approximations et de les justifier afin de donner une solution approchée valide dans le cadre des approximations ?

où

- $H_S$  est l'hamiltonien d'évolution propre du système
- $H_E$  est l'hamiltonien d'évolution propre de l'environnement
- $H_{SE}$  est l'hamiltonien d'interaction entre le système et son environnement.

Pour simplifier, nous allons considérer une interaction de la forme  $H_{SE} = S \otimes E$ , mais les résultats obtenus se généralisent à  $H_{SE} = \sum_{\alpha} S_{\alpha} \otimes E_{\alpha}$ .

Ce type d'équation pilote repose sur deux approximations<sup>2</sup>. Nous allons nous contenter d'explicitier ces approximations et d'esquisser le raisonnement qui permet d'obtenir l'équation pilote.

L'approximation de Born repose sur l'hypothèse que le couplage entre l'environnement et le système est faible et l'hypothèse que la taille de l'environnement est grande devant celle du système. L'approximation consiste alors à négliger l'évolution de l'environnement  $\mathcal{E}$  due au couplage avec le système  $\mathcal{S}$  et à négliger les corrélations d'ordre supérieur qui s'établissent entre  $\mathcal{S}$  et  $\mathcal{E}$ . Cette approximation se traduit par la propriété suivante

$$\rho_{SE}(t) \simeq \rho_S \otimes \rho_E^{(\text{stat})} \quad (\text{D.2})$$

où  $\rho_E^{(\text{stat})}$  est l'état stationnaire de l'environnement s'il n'interagissait pas avec le système. Le plus souvent l'environnement sera un bain d'oscillateurs et  $\rho_E^{(\text{stat})}$  correspondra à l'état d'équilibre thermique. De façon plus formelle, l'approximation consiste en un développement limité en puissance de l'opérateur d'interaction.

L'approximation de Markov repose sur l'hypothèse que les effets de mémoire se dissipent dans l'environnement sur une échelle de temps petite de-

---

<sup>2</sup>Bien évidemment, il existe des cas où une approche similaire peut être employée sans avoir recours à des approximations. Un exemple bien connu est celui du mouvement brownien quantique qui peut être résolu exactement [42] bien que le recours aux approximations de Born et de Markov donne une solution approchée très satisfaisante dans la plupart des cas. L'équation pilote pour le mouvement brownien quantique et en particulier sa limite pour un bain à haute température, l'équation de Caldeira-Leggett [22], constitue un des modèles de référence pour l'étude des phénomènes de dissipation.

vant celle de l'interaction entre l'environnement et le système. Formellement, cela revient à supposer le terme de corrélation intra-environnement

$$g(\tau) = \text{Tr} \left[ E(t)E(t - \tau)\rho_{\mathcal{E}}^{(\text{stat})} \right] \quad (\text{D.3})$$

ne prend des valeurs non-nulles que sur une échelle  $\tau_c$  petite devant le temps d'interaction entre  $\mathcal{S}$  et  $\mathcal{E}$ .

L'application de ces deux approximations dans la représentation d'interaction permet d'aboutir [27] à une équation pilote qui s'écrit dans la représentation de Schrödinger

$$\frac{d\rho_{\mathcal{S}}}{dt} = -i[H_{\mathcal{S}}, \rho_{\mathcal{S}}(t)] + U\rho_{\mathcal{S}}(t)S + S\rho_{\mathcal{S}}(t)U^\dagger - SU\rho_{\mathcal{S}}(t) - \rho_{\mathcal{S}}(t)U^\dagger S \quad (\text{D.4})$$

où  $U = \int_0^{+\infty} g(\tau)e^{-iH_{\mathcal{S}}\tau}Se^{iH_{\mathcal{S}}\tau}d\tau$ .

### D.1.1 Mouvement brownien quantique

Une application particulièrement importante de cette approche est l'équation pilote du mouvement brownien quantique qui s'intéresse à une particule de masse  $M$  dans un potentiel harmonique, couplée harmoniquement avec  $N$  molécules légères. L'hamiltonien total est alors

$$\begin{aligned} H &= H_{\mathcal{S}} \otimes \mathbf{1}_{\mathcal{E}} + H_{\mathcal{S}\mathcal{E}} + \mathbf{1}_{\mathcal{S}} \otimes H_{\mathcal{E}} \\ &= \left( \frac{1}{2M}P^2 + \frac{1}{2}M\Omega X^2 \right) \otimes \mathbf{1}_{\mathcal{E}} + \sum_j \frac{1}{2}m_j\omega_j^2(X - x_j)^2 \\ &\quad + \mathbf{1}_{\mathcal{S}} \otimes \sum_j \frac{1}{2m_j}p_j^2. \end{aligned} \quad (\text{D.5})$$

L'application des approximations de Born-Markov fournit l'équation-pilote

$$\frac{d}{dt}\rho_{\mathcal{S}} = -i \left[ \frac{P^2}{2M}, \rho_{\mathcal{S}} \right] - i\frac{\gamma}{2} [X, P\rho_{\mathcal{S}} + \rho_{\mathcal{S}}P] - D[X, [X, \rho_{\mathcal{S}}]] \quad (\text{D.6})$$

où  $D \in \mathbb{R}$  est le coefficient de dispersion en impulsion.

## D.2 Équation de Lindblad

En raison des approximations qui entrent en jeu dans sa dérivation, rien ne garantit qu'une équation pilote avec approximation de Born-Markov ne préserve la positivité de  $\rho_S$ . Les équations pilotes avec approximation de Born-Markov qui préservent la positivité de  $\rho_S$  sont appelés équations de Lindblad [36, 49] et ont la forme suivante

$$\frac{d\rho_S}{dt} = -i[H_S, \rho_S(t)] + \sum_{\alpha, \beta} \gamma_{\alpha\beta} \left( S_\alpha \rho_S(t) S_\beta^\dagger - \frac{1}{2} S_\beta^\dagger S_\alpha \rho_S(t) - \frac{1}{2} \rho_S(t) S_\beta^\dagger S_\alpha \right) \quad (\text{D.7})$$

où les opérateurs  $S_\alpha$  sont les opérateurs apparaissant dans la décomposition  $H_{S\mathcal{E}} = \sum_\alpha S_\alpha \otimes E_\alpha$ . Les coefficients  $\gamma_{\alpha\beta} \in \mathbb{C}$  contiennent toute l'information sur les phénomènes de décohérence et de dissipation. La matrice  $\Gamma = (\gamma_{\alpha\beta})$  est de plus positive et peut donc être diagonalisée afin de fournir

$$\frac{d\rho_S}{dt} = -i[H'_S, \rho_S(t)] + \sum_\mu \eta_\mu \left( L_\mu \rho_S(t) L_\mu^\dagger - \frac{1}{2} L_\mu^\dagger L_\mu \rho_S(t) - \frac{1}{2} \rho_S(t) L_\mu^\dagger L_\mu \right) \quad (\text{D.8})$$

où les opérateurs  $L_\mu$  sont les opérateurs de Lindblad ou opérateurs de sauts quantiques et  $H'_S$  est un opérateur hermitien qui peut être différent de  $H_S$ . En effet, l'équation est invariante sous la transformation [41]

$$\begin{cases} L_\mu \rightarrow L_\mu + c_\mu \\ H'_S \rightarrow H'_S - \frac{i}{2} \sum_\mu \eta_\mu (c_\mu^* L_\mu - c_\mu L_\mu^\dagger) \end{cases} \quad (\text{D.9})$$

donc l'hamiltonien du système peut recevoir une contribution de l'interaction avec l'environnement qui a pour effet de renormaliser son hamiltonien propre et modifier ses niveaux d'énergie. Un tel phénomène est appelé *Lamb shift*.

Une interprétation d'une équation de Linblad est alors possible en terme d'évolution stochastique, qui revient *grosso modo* à dire que le passage de  $\rho_S(t)$  à  $\rho_S(t + dt)$  est

- avec probabilité  $\delta p_\mu = \eta_\mu \delta t \text{Tr} [L_\mu \rho_S(t) L_\mu^\dagger]$ , le système subit un saut quantique et passe dans l'état  $\rho_S(t + dt) \propto \eta_\mu L_\mu \rho_S(t) L_\mu^\dagger$
- avec probabilité  $1 - \sum_\mu \delta p_\mu$ , le système ne subit pas de saut quantique et évolue sous l'action du pseudo-hamiltonien

$$\tilde{H} = H'_S - \frac{i}{2} \sum_\mu \eta_\mu L_\mu^\dagger L_\mu. \quad (\text{D.10})$$

Pour ceux qui seraient intéressés par cette approche, voir [27].

Les équations pilotes ne seront pas beaucoup utilisées dans ce mémoire, sauf à titre d'exemple pour appuyer notre propos. Il paraissait toutefois important de les introduire puisqu'elles constituent l'outil essentiel de description de la décohérence dans des modèles complexes.



# Annexe E

## Correction d'erreur

La perspective de construire un jour un ordinateur quantique a longtemps été assombrie par l'apparente impossibilité d'utiliser des techniques de correction d'erreur pour un ordinateur quantique. En effet, contrairement à la correction d'erreur classique, son équivalent quantique semble vouer à l'échec pour au moins trois raisons.

### E.1 Correction d'erreur classique

Tout d'abord, la correction d'erreur classique repose lourdement sur l'idée de redondance : toute information utile est copiée et stockée en multiples exemplaires. Or, Żurek et Wootters ont montré dès 1982 [75] que le clonage d'information quantique est impossible. Plus précisément, il n'existe pas d'évolution unitaire  $U$  qui prend en entrée un qubit dans un état quantique pur quelconque  $|\psi\rangle$  (et un autre qubit initialisé dans un état  $|0\rangle$ ) et qui retourne deux copies sous la forme  $|\psi\rangle \otimes |\psi\rangle$ . Ainsi, la redondance est une option interdite à la correction d'erreur quantique.

De plus, la correction d'erreur classique utilise des mesures afin de détecter les erreurs. Or, toute mesure sur un système quantique va le perturber. Ainsi, il n'est pas possible de simplement *observer* les erreurs en mesurant le système lui-même. La correction d'erreur quantique doit trouver un moyen

pour détecter les erreurs sans mesurer les systèmes eux-mêmes.

Finalement, pour un bit classique qui ne peut prendre que deux valeurs, la seule erreur possible est de complémenter la valeur du bit, autrement dit d'envoyer 0 sur 1 ou 1 sur 0. Au contraire, pour un *qubit*, un état pur est caractérisé par deux nombres *réels* qui peuvent varier continûment. Ainsi, il ne s'agit plus d'une erreur discrète, mais plutôt d'un ensemble continu d'erreur qu'il semble falloir détecter et corriger.

Toutes ces raisons ont longtemps laissé croire que la correction d'erreur quantique était impossible. Heureusement, Shor a montré en 1995 qu'il n'en était rien en exhibant un code correcteur d'erreur quantique. Présenter ce code correcteur dans son intégralité nous amènerait trop loin. Toutefois, nous allons présenter les idées qui lui permettent de fonctionner.

## E.2 Correction d'erreur quantique

### E.2.1 Numérisation de l'erreur

Comme nous l'avons mentionné, la correction d'erreur quantique semble s'attaquer à un ensemble continu d'erreurs. Il est toutefois possible de montrer que toute opérateur correspondant à une erreur est une combinaison linéaire d'opérateurs élémentaires. Par exemple, tout opérateur sur un qubit est une combinaison linéaire de matrices de Pauli

$$U = c_0 \mathbf{1} + \sum_{i=1}^3 c_i \sigma_i = \sum_{\mu=0}^3 c_\mu \sigma_\mu.$$

Afin de ramener l'ensemble continu d'erreur à un ensemble discret, l'idée est d'intriquer le qubit avec un système auxiliaire de façon à ce que

$$|\psi\rangle|\text{prêt}\rangle \mapsto \sum_{\mu=0}^3 c_\mu (\sigma_\mu |\psi\rangle) |a_\mu\rangle$$

de telle façon que les  $|a_\mu\rangle$  soient orthogonaux. Une mesure des  $|a_\mu\rangle$  aura alors pour effet de projeter la combinaison linéaire sur un terme

$$\sigma_{\mu_0}|\psi\rangle|a_{\mu_0}\rangle.$$

Le résultat de la mesure permet alors d'identifier laquelle des erreurs élémentaires a été appliquée sur le qubit et de corriger cette erreur en appliquant l'opérateur inverse

$$(\sigma_{\mu_0})^{-1}\sigma_{\mu_0}|\psi\rangle = |\psi\rangle.$$

Il est très important de noter qu'à aucun moment nous n'avons appris quoi que ce soit sur l'état  $|\psi\rangle$  du qubit. Ceci permet de ne pas perturber cet état.

### E.2.2 Code à 3 qubits

Nous allons donner ici l'exemple d'un code qui corrige les renversements de bit, c.-à-d. les opérateurs  $\sigma_x$ . La première étape consiste à intriquer le qubit à protéger, initialement dans un état pur  $|\psi\rangle = a|0\rangle + b|1\rangle$ , avec deux qubits auxiliaires de façon à obtenir

$$a|0\rangle_L + b|1\rangle_L$$

où  $|0\rangle_L = |000\rangle$  et  $|1\rangle_L = |111\rangle$ . Cette étape, dite d'encodage, permet de délocaliser l'information d'un qubit sur trois qubits. Notons que cet état semble contenir de la redondance, bien qu'aucune information quantique n'est en fait été copiée.

Supposons maintenant qu'un opérateur  $\sigma_x^i$  soit appliqué sur le qubit  $i$ . Bien évidemment, nous ne savons pas lequel des qubits a été perturbé. Il faut alors procéder à l'étape de décodage, qui consiste essentiellement à mesurer

deux observables<sup>1</sup>

$$\sigma_z^1 \otimes \sigma_z^2 \otimes \mathbf{1}^3 \quad \text{et} \quad \mathbf{1}^1 \otimes \sigma_z^2 \otimes \sigma_z^3.$$

La valeur de ces deux observables, appelés syndromes, va permettre de corriger l'erreur introduite. En effet, l'application d'un opérateur  $\sigma_x^i$  sur le sous-espace  $\{|0\rangle_L, |1\rangle_L\}$  va envoyer l'état quantique vers un autre sous-espace orthogonal. Autrement dit, les 4 sous-espaces  $\{|0\rangle_L, |1\rangle_L\}$ ,  $\{\sigma_x^1|0\rangle_L, \sigma_x^1|1\rangle_L\}$ ,  $\{\sigma_x^1|0\rangle_L, \sigma_x^1|1\rangle_L\}$  et  $\{\sigma_x^1|0\rangle_L, \sigma_x^1|1\rangle_L\}$  sont tous orthogonaux. La mesure des syndromes va permettre de savoir sur lequel des sous-espaces l'état quantique à été envoyé, puis de corriger l'erreur introduite. Ainsi, après correction, nous retrouverons notre qubit dans l'état initial  $|\psi\rangle = a|0\rangle + b|1\rangle$  bien que nous n'ayons acquis aucune information sur  $a$  et  $b$ .

### E.2.3 Calcul robuste et théorème-seuil

La mise en évidence de code correcteur d'erreur a été une percée fondamentale vers la mise au point d'un ordinateur quantique. Toutefois, pour utiliser la correction d'erreur, il faut être capable d'effectuer certaines tâches élémentaires, par exemple les opérations nécessaires à l'encodage et au décodage, sans introduire de nouvelles erreurs. En particulier, il faut à tout prix éviter de propager les erreurs. Pour ce faire, il faut mettre en œuvre les portes quantiques de façon robuste (*fault tolerant* en anglais). Sans entrer dans les détails du calcul robuste, notons que cet effort débouche sur un résultat essentiel : le (ou plutôt les) théorème-seuil, dont la première version a été démontrée par D. Arachonov et M. Ben-Or en 1996 [1]. Il montre que si la correction d'erreur est mise en œuvre de façon robuste et que le taux d'erreur par porte quantique élémentaire est inférieure à un certain seuil, il est possible de réaliser des calculs quantiques de taille arbitraire.

---

<sup>1</sup>Attention, ces observables ne doivent pas être mesurées en mesurant  $\sigma_z^1$ , puis  $\sigma_z^2$  et enfin  $\sigma_z^3$ , ce qui reviendrait à mesurer chacun des trois qubits et à détruire l'information quantique. Il faut se contenter de mesurer ces deux observables, sans chercher à en apprendre plus.