Université de Montréal

Classicalité du calcul quantique

Par

David Poulin

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

Décembre 2001

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé

Classicalité du calcul quantique

présenté par

David Poulin

a été évalué par un jury composé des personnes suivantes :

Richard MacKenzie
président-rapporteur

Gilles Brassard
directeur de recherche

Raymond Laflamme
membre du jury

Sommaire

Plusieurs indices nous portent à croire que la théorie quantique de la matière offre un potentiel de calcul supérieur à la théorie classique. En raison de la fragilité de l'information quantique, toutes tentatives d'implantation expérimentale de calculateur quantique utile ont rencontré des obstacles technologiques jusqu'à ce jour insurmontables. Pour cette raison, l'utilisation de calculateurs quantiques doit être réservée aux tâches «classiquement impraticables».

Dans ce mémoire, nous étudions la possibilité de substituer certaines parties d'une procédure quantique par une dynamique classique. Lorsqu'une telle substitution est possible, cela signifie que le processus original n'est pas fondamentalement quantique, donc qu'il y a «gaspillage» de ressources quantiques. La légitimité d'une substitution nous est dictée par des règles de consistance ; lorsque les conditions de consistance sont satisfaites, la substitution peut se faire en toute quiétude.

Au premier chapitre, nous présentons les concepts généraux de la théorie quantique et, plus spécifiquement, de l'informatique quantique. Au second chapitre, nous décrivons, sans entrer dans le détail de son interprétation, le formalisme des histoires consistantes qui nous servira à définir les règles de consistance mentionnées ci-haut. Le troisième chapitre fusionne le calcul quantique et la théorie des histoires consistantes. On y montre comment certaines modifications du formalisme permettent d'utiliser les histoires consistantes afin d'étudier la classicalité d'un calcul quantique. Finalement, le chapitre quatre analyse les conséquences d'une telle étude de classicalité. En particulier, on y montre comment une étude de classicalité pourrait permettre d'augmenter la résistance au bruit des calculateurs quantiques. De plus, nous tirons certaines conclusions sur la classicalité du calcul avec états mixtes, sujet grandement débattu au cours des dernières années.

Pour un résumé plus complet, voir [73].

Mots clés : Calcul quantique, domaine classique, histoires consistantes, transition quantique-classique, résonance magnétique nucléaire, interprétation de la mécanique quantique, décohérence.

Abstract

For a wide variety of reasons, it is believed that quantum theory offers a greater computational power that its classical analog. Nevertheless, every experimental attempt to implement a "useful" quantum computer has failed up to now, for both theoretical and practical reasons. Therefore, quantum computing devices should be restricted to those problems that are classically intractable.

In this thesis, we investigate the possibility of substituting part of a quantum algorithm by classical dynamics. If such a substitution is possible, it would indicate that the original quantum process wasn't fundamentally quantum, at least not from a computational point of view. This would imply a waste of precious quantum resources. How and when these substitutions can take place is dictated by consistency rules, borrowed from the consistent histories formalism.

In chapter one, we introduce the basic concepts of quantum computing. We then describe the consistent histories formalism, without paying any attention to their interpretation. The third chapter brings these two ideas together : Consistent histories in quantum information processing. Finally, chapter four analyses the consequences that can be drawn from a classicality analysis. Interesting results are increase of noise robustness and new insights on the quantumness of mixed-state quantum computing.

For a more detailed summary, see [73].

Key words : Quantum information processing, classical domain, consistent histories, quantum classical transition, nuclear magnetic resonance, interpretation of quantum mechanics, decoherence.

Table des matières

Table des figures

Avant-propos

L'univers qui nous entoure est gouverné par deux équations :

$$\mathsf{G} = 8\pi\mathsf{T} \qquad \text{et} \qquad i\hbar\frac{\partial}{\partial t}|\psi\rangle = \hat{H}|\psi\rangle.$$

L'équation de gauche est l'équation de champ d'Einstein. Elle est utilisée pour décrire les objets *macroscopiques* telles les galaxies, les planètes et les boules de billard. En gros, elle formalise le principe de conservation (ou plutôt de transformation) de la quadri-impulsion. Lorsque la vitesse relative des objets décrits est faible devant celle de la lumière, que les énergies en jeu sont négligeables devant leur énergie au repos ($E = mc^2$) et que la densité de matière est suffisamment faible, l'équation d'Einstein peut être approximée avec très grande précision par l'équation du mouvement de Newton :

$$m\frac{d^2}{dt^2}\boldsymbol{r} = \boldsymbol{F},$$

équation qui régit le comportement des objets de notre vie quotidienne, dits *classiques.*

L'équation de droite est celle de Schrödinger[1]. Elle s'applique au monde *microscopique*, tels les électrons, les atomes et les petites molécules. Elle donne naissance à la théorie *quantique* de la matière. Le théorème d'Erenfest nous indique que sous certaines conditions, il est possible de retrouver les lois de la mécanique de Newton à partir de limites de l'équation de Schrödinger. Néanmoins, ces conditions sont beaucoup moins naturelles que celles permettant de dériver la mécanique classique à partir de l'équation d'Einstein. D'ailleurs, l'absence de phénomènes quantiques à l'échelle macroscopique demeure partiellement mystérieuse.

La thèse de Church-Turing décrète que tout ce qui est calculable peut être calculé à l'aide d'une *machine de Turing universelle.* Dans sa description, une telle machine est implicitement macroscopique, elle se comporte selon l'équation

[1]En fait, l'équation de Schrödinger est une approximation non relativiste des équations des champs quantiques telle que l'équation de Klein-Gordon, de Dirac *etc.* À des fins d'introduction, nous nous contentons d'une telle approximation.

de champ d'Einstein. La thèse dite forte de Church-Turing ajoute à cela que le temps nécessaire à une machine de Turing à effectuer le calcul est, à un facteur polynomial en la taille de l'entrée près[2], le même que pour tout autre système physique. En d'autres termes, tous les systèmes physiques pouvant manipuler de l'information de façon universelle doivent mettre un temps polynomialement équivalent à accomplir une tâche calculatoire.

C'est cette dernière affirmation qui est remise en question lorsque les systèmes physiques manipulant l'information obéissent à l'équation de droite plutôt qu'à celle de gauche. En effet, plusieurs indications nous portent à croire que les systèmes quantiques peuvent effectuer certaines tâches calculatoires en un temps *exponentiellement* plus court que celui requis par tout système classique.

Ce qui suit est une tentative déguisée d'exploration des avantages calculatoires fondamentaux du monde quantique vis-à-vis le monde classique. Tentative, puisque les idées présentées ne sont pas suffisamment développées pour aller au bout de la question ; déguisée en raison de certaines conséquences plutôt « pratiques » tirées de cette étude. En effet, bien que les multiples motifs évoqués lors de l'introduction du formalisme et de son analyse soient tout autre, le lecteur devrait garder à l'esprit que LA motivation fondamentale de ce mémoire est de répondre à la noble question : *Quel est l'ingrédient qui permet à la mécanique quantique de surpasser la mécanique classique en puissance de calcul, le cas échéant ?*

En raison de ce thème qui sort de l'ordinaire, ce mémoire présente surtout des idées : on n'y trouve pas de réponse définitive aux principales questions soulevées, mais plutôt des pistes et des indices. En conséquence, plusieurs portes restent ouvertes, plusieurs avenues inexplorées, laissant beaucoup de latitude à la réflexion pour le lecteur. En particulier, la plupart des sections des chapitres 3 et 4 pourraient individuellement alimenter une thèse si elles étaient décortiquées à fond.

[2]En informatique théorique, l'efficacité d'un algorithme est mesurée par une fonction reliant le temps d'exécution à la taille de l'entrée du calcul, c'est-à-dire le nombre de chiffres nécessaires à sa représentation. (Taille(N)$\propto \log N$.)

Remerciements

Ce mémoire est l'aboutissement des deux années que j'ai passées au Laboratoire d'informatique théorique et quantique (LITQ). Au cours de ces années, j'ai eu l'occasion de partager mes idées avec plusieurs personnes que je souhaite ici remercier.

Merci d'abord à Gilles Brassard qui m'a donné la liberté d'étudier un sujet aussi farfelu qu'était celui de la classicalité du calcul quantique. C'est en grande partie en raison de ses nombreux encouragements que j'ai mené ce projet à terme. C'est également grâce à Gilles que j'ai eu l'occasion de rencontrer un si grand nombre de gens intéressants en si peu de temps. Outre son appuie financier qui m'a permis de voyager librement, mon simple attachement à son groupe de recherche a été, à maintes reprises, un laissez-passer vers des discussions qui m'ont beaucoup appris. C'est un grand privilège d'avoir passé ces deux années sous sa direction.

Merci également à Alexandre Blais, José Manuel Fernandez, Raymond Laflamme et Wojciech Żurek avec qui j'ai partagé d'enrichissantes et agréables conversations (ou avec qui j'ai eu un plaisir fou à m'obstiner). Merci également aux membres du LITQ qui ont su accueillir les idées d'un physicien égaré.

Je remercie également le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), la fondation Marc Bourgie, BCE Emergis inc. et Louise et Bernard Lamarre pour leur soutien financier.

Finalement, merci à mes amis et ma famille qui me permettent d'apprécier pleinement chaque instant. En particulier, merci à Isabelle d'être ce qu'elle est et de m'aimer pour ce que je suis.

I should like to write "Door meten tot weten" [through measuring to knowing] as a motto above every physics laboratory [3]... une prophétie ?

—HEIKE KAMERLINGH ONNES

[3]Lieden, 1882. Cité dans *Dictionary of Scientific Biography*, vol. VII, Scribner, 1976.

1 — Préliminaires

Le présent chapitre établit les principaux concepts qui seront rencontrés tout au long de ce mémoire. Deux objectifs sont visés : initier le physicien aux notions de base de l'informatique quantique et reformuler certaines idées sur des bases physiques pour l'informaticien déjà initié au calcul quantique. Il est évidemment hors de question de faire un tour d'horizon des accomplissements du domaine de l'information quantique : même un manuel de 650 pages ne peut qu'effleurer chaque sujet [66]. En particulier, nous passerons sous le silence la plupart des notions de la théorie de l'information quantique. Pire encore, aucun prototype physique ne sera décrit, si ce n'est que pour motiver certains aspects de la classicalité.

Plusieurs raisons motivent ces négligences. L'existence de bonnes introductions en français tant pour physiciens [16] que pour informaticiens [88, 78, 15] saurait à elle seule expliquer cette omission. Pourtant, c'est le contenu même de ce mémoire qui forme l'argument principal. La classicalité du calcul quantique est la fusion de deux domaines qui, *a priori*, ne possèdent rien en commun : l'informatique quantique et les histoires consistantes. Il nous sera donc nécessaire d'introduire ces deux champs et c'est pourquoi nous nous en tenons au strict nécessaire.

Finalement, ce qui suit n'est pas présenté de façon chronologique ni même académique. Ainsi, certains concepts sont rencontrés avant même d'être formellement définis, mais le lecteur initié à la mécanique quantique ne devrait pas s'en trouver encombré. Un seul critère motive la structure de ce chapitre de préliminaires : rendre sa lecture agréable. Ceci étant dit, bonne lecture !

1.1. Postulats de la mécanique quantique

Dans ce qui suit, nous énonçons et commentons les postulats de base de la mécanique quantique non relativiste. Cette science étant fondée sur les observa-

tions expérimentales, il semble tout à fait approprié d'introduire ces postulats tels que retrouvés dans tout manuel élémentaire de *physique* quantique. Nous choisissons ici l'ouvrage de Cohen-Tannoudji, Diu et Laloë [24]. Cependant, les répercussions de ces postulats sur les limitations des systèmes quantiques à des fins de manipulation d'information sont de prime abord fort énigmatiques. En raison de l'interdisciplinarité du domaine de l'informatique quantique, certains éclaircissements seront apportés à ce sujet. En particulier, nous verrons que les états purs décrits au premier postulat doivent être généralisés afin de tenir compte de mélanges statistiques (section 1.4).

Énoncé des postulats

1er Postulat : À un instant t_0 fixé, l'état d'un système physique est défini par la donnée d'un ket $|\psi(t_0)\rangle$ appartenant à l'espace des états $\mathcal{H}$. En général, nous choisissons la normalisation $\langle\psi|\psi\rangle = 1$.

2e Postulat : Toute grandeur physique mesurable $\mathcal{O}$ est décrite par un opérateur $\hat{O}$ agissant dans $\mathcal{H}$; cet opérateur est une observable.

3e Postulat : La mesure d'une grandeur physique $\mathcal{O}$ ne peut donner comme résultat qu'une des valeurs propres de l'observable $\hat{O}$ correspondante.

4e Postulat : Lorsqu'on mesure la grandeur physique $\mathcal{O}$ sur un système dans l'état $|\psi\rangle$ normé, la probabilité $Pr(a_n)$ d'obtenir comme résultat la valeur propre a_n de l'observable $\hat{O}$ correspondante est :

$$Pr(a_n) = \sum_{j=1}^{g_n} |\langle\phi_n^j|\psi\rangle|^2 \tag{1.1}$$

où g_n est la dégénérescence de la valeur propre a_n et les $|\phi_n^j\rangle$ sont les vecteurs propres normés de $\hat{O}$ associés à la valeur propre a_n.

5e Postulat : Si la mesure de la grandeur physique $\mathcal{O}$ sur le système dans l'état $|\psi\rangle$ donne le résultat a_n, l'état du système immédiatement après la mesure est la

projection normée,

$$\frac{\hat{P}_n|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_n|\psi\rangle}} \tag{1.2}$$

de $|\psi\rangle$ sur le sous-espace propre associé à a_n, *i.e.* $\hat{P}_n = \sum_{j=1}^{g_n} |\phi_n^j\rangle\langle\phi_n^j|$.

6^e Postulat : L'évolution dans le temps du vecteur d'état $|\psi(t)\rangle$ est régie par l'équation de Schrödinger :

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}(t)|\psi(t)\rangle \tag{1.3}$$

où $\hat{H}(t)$ est l'observable associée à l'énergie totale du système.

État

L'espace des états $\mathcal{H}$ est un espace de Hilbert. Sa dimension peut être finie ou infinie. Ici, nous allons toujours supposer un espace de dimension finie. L'énoncé des postulats 4 et 5 est modifié lorsque l'espace des états est de dimension infinie. Comme nous le verrons à la section 1.4.1, le postulat 1 n'est pas universel ; l'état le plus général d'un système physique est décrit par une matrice de densité. Il s'en suivra une reformulation des postulats 3-6 (*cf.* section 1.4.5).

Observable et projecteur

La notion d'observable introduite au deuxième postulat est fondamentale en physique mais très rarement rencontrée en informatique quantique, particulièrement chez les auteurs issus des domaine de l'informatique ou des mathématiques. Une observable peut être perçue comme une partition de l'espace des états en sous-espaces mutuellement orthogonaux. À chacun de ces sous-espaces est associée une valeur de la grandeur physique décrite par l'observable. Par exemple, l'observable associée à la projection du spin d'un électron selon l'axe z peut être décrite par les sous-espaces $\mathcal{H}_+$ et $\mathcal{H}_-$ générés par les vecteurs $\{|n;\ell,m_\ell;\frac{1}{2}\rangle\}_{,n=0\ldots\infty,\ell=0\ldots\infty,m_\ell=-\ell\ldots\ell}$ et $\{|n;\ell,m_\ell;-\frac{1}{2}\rangle\}_{n=0\ldots\infty,\ell=0\ldots\infty,m_\ell=-\ell\ldots\ell}$ auxquels sont associées les valeurs $\frac{\hbar}{2}$ et $-\frac{\hbar}{2}$

respectivement[1]. Ces deux valeurs sont donc les seuls résultats possibles lors de la mesure du spin de l'électron selon l'axe z en raison du troisième postulat.

La probabilité associée à ces résultats est donnée par le support de la fonction d'onde $|\psi\rangle$ sur chacun des sous-espaces. Soit les deux fonctions d'onde $|\psi\rangle$ et $|\phi\rangle = e^{i\alpha}|\psi\rangle$; leur support sur tout sous espace étant le même, elles ne pourront en aucun cas êtres distinguées. Il s'en suit que les fonctions d'onde ne différant que par une phase globale représentent le même état physique.

Les probabilités ne reflètent pas l'ignorance de l'expérimentateur mais sont de nature fondamentale : la mécanique quantique n'est pas une science déterministe[2]. À la suite de cette mesure, seules les composantes de $|\psi\rangle$ appartenant au sous-espace ressortant de la mesure persistent ; en général une renormalisation de la fonction d'onde s'impose. Cette partie de la mesure se nomme la *réduction du paquet d'onde.*

La mesure décrite plus haut est légèrement idéalisée. Bien que toute mesure susceptible d'informer l'observateur perturbe le système, il existe des mesures à la suite desquelles le système n'est carrément plus accessible. Par exemple, pour mesurer la polarisation d'un photon, on le fait d'abord passer par une lentille polarisée puis on tente de le détecter. Si détection il y a, cela signifie que le résultat de la mesure est une polarisation parallèle à l'axe de la lentille. Dans ce cas, le photon est absorbé par le détecteur. L'absence de photon au détecteur signifie une polarisation perpendiculaire à l'axe de la lentille. Cette fois, c'est la lentille qui absorbe le photon. Dans les deux cas, le système n'est plus accessible à la suite de la mesure.

En informatique quantique, ce ne sont pas tant les valeurs associées aux sous-espaces qui importent mais leur *distinguabilité.* Ceci reflète le caractère fongible de l'information. C'est pourquoi nous choisissons généralement de décrire une mesure par l'ensemble de projecteurs associés à l'observable, tel que décrit au cinquième

[1] n est le nombre quantique radial alors que ℓ et m_ℓ sont les nombres orbitaux (moment cinétique). Se référer à la théorie quantique des forces centrales pour plus de détails.

[2] L'évolution de la fonction d'onde est déterministe, c'est le résultat de la mesure qui ne l'est pas. Nous voulons ici éviter les questions d'interprétation de la théorie, bien que fascinantes, puisqu'elles ne sont pas directement liées au sujet à l'étude.

postulat. Souvent, les mesures utilisées ne sont pas de réels observables physiques mais sont en bijection avec une ou plusieurs véritables observables. Par exemple, nous choisirons parfois d'associer la valeur 0 à $\mathcal{H}_+$ et la valeur 1 à $\mathcal{H}_-$. Ainsi, nous établissons une bijection entre des grandeurs physiques et des nombres abstraits : $\frac{\hbar}{2} \leftrightarrow 0, \quad -\frac{\hbar}{2} \leftrightarrow 1$.

Il est également possible que l'observable artificiel soit en fait associé à de multiples observables physiques. Par exemple, un système composé de deux particules à spins $\frac{1}{2}$ peut être utilisé pour encoder les nombres de 0 à 3. L'observable associant ces nombres à des sous-espaces mutuellement orthogonaux correspond en fait à deux observables physiques. Le tableau suivant illustre deux choix d'encodage.

Nombre	Encodage 1	Encodage 2
0	$\lvert s_{z1} = \frac{\hbar}{2}, s_{z2} = \frac{\hbar}{2}\rangle$	$\lvert J = 0, m = 0\rangle$
1	$\lvert s_{z1} = \frac{\hbar}{2}, s_{z2} = -\frac{\hbar}{2}\rangle$	$\lvert J = \hbar, m = -\hbar\rangle$
2	$\lvert s_{z1} = -\frac{\hbar}{2}, s_{z2} = \frac{\hbar}{2}\rangle$	$\lvert J = \hbar, m = 0\rangle$
3	$\lvert s_{z1} = -\frac{\hbar}{2}, s_{z2} = -\frac{\hbar}{2}\rangle$	$\lvert J = \hbar, m = \hbar\rangle$

L'encodage 1 a recours aux observables de spin selon l'axe z de la particule 1 et de la particule 2 séparément, s_{z1} et s_{z2}. Le second encodage se réfère à l'observable de spin total $J = |\boldsymbol{J}| = |\boldsymbol{S}_1 + \boldsymbol{S}_2|$ et à la projection du spin total selon l'axe z, soit m. Dans ces deux exemples, on compte deux observables physiques pour un observable abstrait désignant le nombre encodé $\hat{n} = \sum_{n=0}^{3} n|n\rangle\langle n|$.

Une mesure sera dite *complète* si elle sépare l'espace de Hilbert en sous-espaces de dimension 1. En général, une telle mesure est associée à un ensemble complet d'observables qui commutent (ECOC). Complet puisque la spécification de la valeur de chaque observable physique de l'ensemble ne laisse qu'un seul état comme candidat. Il est primordial que les observables de cet ensemble commutent pour être physiquement compatibles. Par exemple, la spécification de la valeur de $|\boldsymbol{J}|$ et de s_{z1} ne sont pas compatibles puisque $|J = 0, m = 0\rangle = \frac{1}{\sqrt{2}}(|s_{z1} = \frac{1}{2}, s_{z2} = -\frac{1}{2}\rangle + |s_{z1} = -\frac{1}{2}, s_{z2} = \frac{1}{2}\rangle)$ donc s_{z1} n'a pas de valeur bien définie lorsque $|\boldsymbol{J}| = 0$.

Unitarité

Le sixième postulat impose des contraintes sur le type d'évolution que peut suivre le système. Puisque $\hat{H}$ est l'observable représentant l'énergie totale du système et que celle-ci est nécessairement réelle (comme toute observable physique), il s'en suit que l'opérateur $\hat{H}$ est Hermitien, c'est-à-dire $\hat{H}^\dagger = \hat{H}$. La solution formelle de l'équation (1.3) est

$$|\psi(t)\rangle = \exp\left\{-\frac{i}{\hbar}\int_{t'=0}^{t} \mathcal{T}\hat{H}(t')\right\}|\psi(0)\rangle \equiv U(t,0)|\psi(0)\rangle \tag{1.4}$$

où nous avons défini l'opérateur d'évolution U.[3] De l'hermiticité de $\hat{H}$, nous déduisons que $UU^\dagger = U^\dagger U = \mathbb{1}$; l'évolution est unitaire. En informatique quantique, l'unitarité de l'évolution se traduit par une conservation de l'information. Puisque toute matrice unitaire possède un inverse, il n'est possible que d'implanter des fonction injectives directement sur un système quantique.

Le problème majeur de la théorie quantique actuelle repose en une contradiction entre le cinquième et le sixième postulat : la projection de la fonction d'onde sur un sous-espace n'est pas unitaire. Ce problème sera étudié à la section 1.5.

1.2. Modèle de calcul & notation

Calcul classique

Les calculateurs classiques modernes consistent en l'application d'un ensemble de portes universelles sur un certain nombre de bits (*binary digits*). En général, ces portes sont le *non-et* dont la table de vérité est :

A	B	Non-Et(A,B)
0	0	1
0	1	1
1	0	1
1	1	0

[3] L'opérateur $\mathcal{T}$ est celui de mise en ordre temporelle, voir [77] pour plus de détails.

et la *copie* qui crée une copie supplémentaire de son bit d'entrée. Cet ensemble est universel puisque toute transformation $f : \{0,1\}^n \to \{0,1\}^m$ peut être réalisée par une série d'applications de ces portes.

Le qubit

L'unité logique quantique fondamentale est le qubit (pour *quantum binary digit*). On l'associe à un système quantique à deux niveaux que l'on note généralement $|0\rangle$ et $|1\rangle$. De tels systèmes sont en fait des idéalisations : dans la nature, nous devons ignorer certains degrés de liberté afin d'obtenir un système à deux niveaux *effectifs*. Des exemples simples de tels systèmes sont le spin d'une particule de spin $\frac{1}{2}$ (*e.g.* électron), la polarisation d'un photon et les niveaux d'énergie de certains atomes. Dans le premier cas, nous devons ignorer les degrés de liberté radiaux et orbitaux n, ℓ et m_ℓ de la particule afin d'obtenir un système à deux niveaux. Dans le cas du photon, c'est la dépendance en nombre d'onde qui est ignorée pour laisser place uniquement au deux degrés de liberté de polarisation. Finalement, deux niveaux d'excitation particuliers de certains atomes peuvent se comporter comme un système à deux niveaux effectifs. Dans ce dernier cas, ce ne sont pas des degrés de liberté qui sont mis de côté mais des sous-espaces. En effet, les trois exemples précédents se résument ainsi : $\mathcal{H}_{électron} = \mathcal{H}_{spin} \otimes \mathcal{H}_{orb.}$, $\mathcal{H}_{photon} = \mathcal{H}_{pol.} \otimes \mathcal{H}_k$, $\mathcal{H}_{atome} = \mathcal{H}_{1,2} \oplus \mathcal{H}_{3,4,\ldots}$.

L'état général d'un qubit est $\alpha|0\rangle + \beta|1\rangle$ où α et β sont complexes avec comme seule restriction $|\alpha|^2 + |\beta|^2 = 1$. Nous pouvons décrire l'état d'un système de n qubits par

$$|\psi\rangle = \sum_{(j_1,\ldots,j_n)\in\{0,1\}^n} c_{j_1\ldots j_n} |j_1\rangle \otimes \ldots \otimes |j_n\rangle \tag{1.5}$$

$$= \sum_{j=0}^{\Omega-1} c_j |j\rangle \tag{1.6}$$

où $\Omega = 2^n$ est la dimension de l'espace des états et j est le nombre représenté par l'extension binaire $j_1 \ldots j_n$; *i.e.* $j = \sum_{k=1}^{n} j_k 2^{n-k}$. La condition de normalisation décrite au premier postulat se traduit par $\sum_j |c_j|^2 = 1$. Les kets $|j\rangle$ forment

une base pour l'espace des états de n qubits, c'est-à-dire que tout vecteur dans $\mathcal{H}_\Omega = \mathcal{H}_2^{\otimes n}$ peut s'exprimer comme une combinaison linéaire de ces derniers.

Modèle de calcul

Il existe plusieurs modèles de calcul quantique offrant la même performance. Ils sont tous dérivés des six postulats énoncés à la section précédente. D'abord Deutsch [27] puis, plus formellement, Bernstein et Varizani [14] ont proposé un modèle semblable à celui de Turing mais adapté au monde quantique. Plus récemment, un modèle basé sur le théorème adiabatique proposé par Farhi, Goldstone, Gutmann et Sipser [36] offre une puissance équivalente à la machine de Turing quantique pour certaines classes de problème ; leur universalité demeure une question ouverte. Encore plus surprenant sont les modèles qui n'ont pas recours aux propriétés dynamiques de la mécanique quantique tel l'ordinateur quantique basé sur la téléportation de Gottesman et Chuang [45] ou peut-être encore plus général celui basé sur les réseaux enchevêtrés de Raussendorf et Briegel [75].

Sans doute le plus répandu est le modèle du circuit, initialement proposé par Deutsch [28]. Chaque qubit y est représenté par un fil. L'évolution temporelle se fait de la gauche vers la droite. Tout comme dans le cas classique, les opérations élémentaires sont limitées à un petit nombre de qubits. Elles sont représentées par des portes. Le sixième postulat impose que l'effet de ces portes puisse être associé à une matrice unitaire de dimension $2^l \times 2^l$ où l est le nombre de qubits affectés par la porte en question. La réalisation physique d'une porte consiste en l'application d'un hamiltonien $\hat{H}(t)$ pendant un temps T de sorte que $\exp\left[\frac{i}{\hbar}\int_0^T \mathcal{T}\hat{H}(t)dt\right] = U$ où U est la matrice unitaire représentée par la porte. L'état initial du système est spécifié à la gauche du circuit, tel qu'illustré à la figure suivante.

La porte H (en caractère différent que le H de Hamiltonien) agissant sur un seul qubit représente la transformation de Walsh-Hadamard définie par

$$\mathsf{H} : \begin{cases} |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases} \quad \text{ou encore} \quad \mathsf{H} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \tag{1.7}$$

La seconde porte qui agit sur deux qubits est un *ou-exclusif*, aussi appelé *non-contrôlé*. Son action sur la base de calcul est d'inverser la valeur du qubit cible

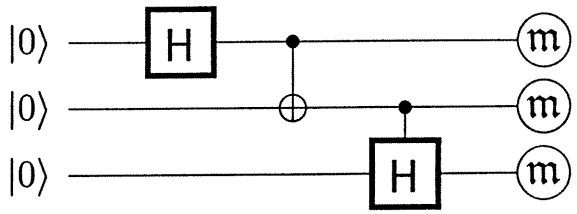

FIG. 1.1 – Exemple d'un circuit quantique.

(celui noté par $\oplus$) si et seulement si le qubit de contrôle (celui noté par $\bullet$) prend la valeur 1. Connaissant l'action d'une porte dans une base nous permet de la déduire pour toute base, par linéarité. Ainsi, on montre facilement que la matrice représentant le contrôle-non dans la base de calcul est

$$\text{c-non} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{1.8}$$

Finalement, la troisième porte est une transformation de Walsh-Hadamard contrôlée. Son action dans la base de calcul est l'application de H au qubit du bas si et seulement si le qubit de contrôle est dans l'état $|1\rangle$. La généralisation à une porte U contrôlée est immédiate. Nous pouvons ainsi suivre à la trace l'état du système à chaque étape du calcul quantique :

$$|000\rangle \xrightarrow{\text{H}} \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle) \tag{1.9}$$

$$\xrightarrow{c-\text{non}} \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) \tag{1.10}$$

$$\xrightarrow{c-\text{H}} \frac{1}{\sqrt{2}}\left(|000\rangle + \frac{1}{\sqrt{2}}[|110\rangle + |111\rangle]\right). \tag{1.11}$$

Si la matrice unitaire représentée par une porte à deux qubits ne peut s'écrire sous une forme factorisée $U = U_1 \otimes U_2$ où les matrices U_1 et U_2 agissent sur les qubits 1 et 2 respectivement, alors cette porte requiert une interaction entre les qubits. Physiquement, cette interaction peut se faire à l'aide d'un médiateur quantique tel un troisième qubit ou un système de plus grande dimension, mais que ce soit de façon directe ou indirecte, une interaction doit avoir lieu.

Tout comme pour le cas classique, il existe un ensemble universel de portes quantiques. Par exemple, le non-contrôlé et l'ensemble des portes agissant sur un seul qubit (le groupe $SU(2)$) forment un ensemble universel. En fait, pratiquement toute interaction à deux qubits assistée de l'ensemble des portes à un qubit forment un ensemble universel. Par universel, nous entendons que toute transformation *unitaire* peut être obtenue par l'application de ces portes. (Étrangement, si nous exigeons de la part d'un calculateur classique universel d'être thermodynamiquement réversible, une porte à trois bits est nécessaire. Pour un calculateur quantique, les portes à deux qubits sont suffisantes puisqu'elles constituent un ensemble universel et sont unitaires, c'est-à-dire qu'elles résultent d'une force conservative [6].)

Initialisation

L'état de l'ordinateur quantique à la fin du calcul dépend de son état initial. Dans l'exemple précèdent, nous avons supposé que cet état était $|000\rangle$. La préparation de l'état initial ne se fait pas sans difficulté. En théorie, il suffit de mesurer chaque qubit dans sa base de calcul puis, si le résultat obtenu ne coïncide pas avec l'état désiré, lui appliquer la porte *non* qui transforme $|0\rangle$ en $|1\rangle$ et vice versa (pour les physiciens, cette porte correspond à la matrice de Pauli σ_x). En raison du cinquième postulat, cette procédure devrait résulter en l'état convoité. En pratique, ce n'est pourtant pas toujours si simple comme nous le verrons à la section 1.4.5 et 4.4.2.

Unitarité

La contrainte d'unitarité se traduit par plusieurs restrictions sur le type de manipulation d'information réalisable. Par exemple, le nombre de qubits à l'entrée du circuit doit être le même que celui à sa sortie, ce qui n'était pas nécessaire classiquement. De plus, l'unitarité et la linéarité de l'évolution impliquent qu'il est impossible de cloner l'information quantique [93, 30]. Le circuit quantique de la figure 1.2 qui prend en entrée un état inconnu $|\psi\rangle$ et un qubit dans un état initial standard, disons $|0\rangle$, et produit deux copies de $|\psi\rangle$ est physiquement

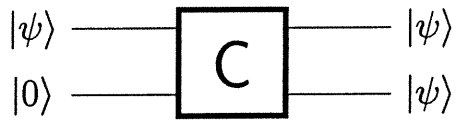

FIG. 1.2 – Circuit clonant l'information quantique.

irréalisable : une conséquence de la linéarité de la mécanique quantique. Si l'état à cloner est connu, le clonage devient possible. Les répercussions de ce résultat sont nombreuses et de grande importance. Par exemple, la possibilité de cloner offrirais une attaque aux protocoles de cryptographie quantique. De plus, s'il était possible de cloner, une quantité infinie d'information pourrait être transmise dans un seul qubit. La transmission du qubit dans l'état $\alpha|0\rangle + \beta|1\rangle$, suivie de multiples clonages serait suffisante pour transmettre la valeur de α et de β, soit une quantité infinie d'information.

Bien que la contrainte d'unitarité semble fort imposante, ses répercussions sur les capacités calculatoires des systèmes quantiques ne sont pas si encombrantes. L'unitarité implique que le calcul doit être réversible mais Bennett a montré que tout calcul peut être effectué réversiblement sans coût important en la taille ou en temps d'exécution [6]. Cette découverte était motivée par le coût thermodynamique associé aux opérations logiquement irréversibles dans l'étude du démon de Maxwell.

Mesure

Le dernier ingrédient du modèle de calcul sont les mesures finales. Toute l'information utile du calcul nous est fournie par ces dernières. Il est à noter que cette information est classique. Sans perte de généralité, on peut supposer que la mesure se fait dans la base de calcul $|0\rangle$ *vs* $|1\rangle$ pour chaque qubit puisque tout autre choix peut être rapporté à ce dernier par une transformation unitaire. La probabilité associée à chaque résultat est donnée par le quatrième postulat. Dans notre exemple de la figure 1.1, les résultats possibles sont 000, 110 et 111 avec probabilité $\frac{1}{2}$, $\frac{1}{4}$ et $\frac{1}{4}$ respectivement comme nous l'indique (éq.1.11).

Pour être tout à fait général, nous pouvons ajouter des qubits ancillaires au

modèle. Ces derniers servent de « mémoire tampon » au calcul. Il est primordial qu'ils soient tous retournés à un état standard à la fin du calcul, sans quoi l'interférence n'aurait pas lieu. Les qubits ancillaires peuvent également servir à généraliser les mesures. Une interaction entre le système $\mathcal{S}$ et les qubits ancillaires $\mathcal{A}$ suivie d'une mesure du système $\mathcal{S} \otimes \mathcal{A}$ se traduit sur $\mathcal{S}$ par une mesure dite POVM (*positive operator value measurement*) (voir [66] pour plus de détails).

1.3. Algorithme de Simon & autres exploits

Nous sommes déjà en mesure de donner un exemple d'algorithme quantique non trivial. Nous choisissons l'algorithme de Simon [85] pour plusieurs raisons. D'abord, pour sa simplicité mais également puisqu'il constitue le premier exemple historique où le monde quantique offre un gain exponentiel dans un contexte réaliste. Réaliste, puisque nous nous contentons de la part du calculateur classique d'une réponse ayant une probabilité constante de succès.

Algorithme de Simon

Soit la fonction $f : \{0,1\}^n \to \{0,1\}^{n-1}$ telle que $\exists x \in \{0,1\}^n$ de sorte que $f(x) = f(y)$ si et seulement si $x = y$ ou $x \oplus y = s$, c'est-à-dire $s_j = (x_j + y_j)\mathsf{mod}2 \quad \forall j = 0, \ldots, n-1$. Le but est de déterminer s. La fonction f nous est donnée sous forme de boîte noire illustrée à la figure 1.3. Dans ce circuit, chaque fil représente plusieurs bits ou qubits ; n pour le fil du haut et $n-1$ pour celui du bas. Une copie de l'entrée x est conservée afin de rendre le calcul réversible, sans quoi son implantation quantique serait impossible.

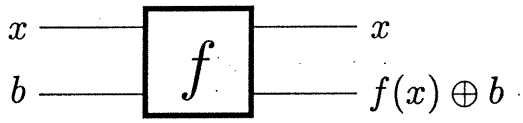

FIG. 1.3 – Boîte noire implantant la fonction f de façon réversible.

Si la fonction f est choisie au hasard parmi toutes les fonctions obéissant à cette condition, alors aucun algorithme classique ne peut déterminer s avec

une probabilité meilleure qu'exponentiellement petite sans avoir recours à la boîte noire un nombre exponentiel de fois [85]. En d'autres termes, un temps exponentiel (en n) est requis afin d'obtenir s avec une probabilité $\geq \epsilon$ pour un ϵ fixe et non nul.

Le circuit quantique illustré à la figure 1.4 permet de trouver s après un nombre espéré d'appels à la boîte noire linéaire en n. La porte $\mathsf{H}^{\otimes n}$ est l'application d'une

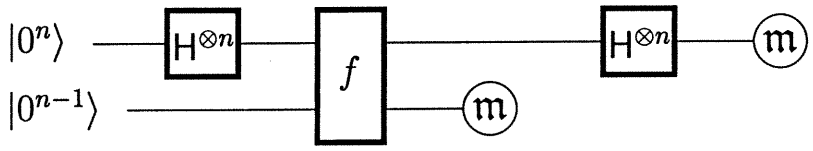

FIG. 1.4 – Circuit réalisant l'algorithme de Simon.

transformation de Walsh-Hadamard sur chacun des n qubits séparément. Cela constitue un exercice élémentaire de montrer que son effet sur la base de calcul est

$$\mathsf{H}^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \tag{1.12}$$

où le produit interne $x \cdot y$ est le nombre de positions k pour lesquelles $x_k = y_k = 1$, modulo 2.

Initialement, l'état de l'ordinateur est $|0^n\rangle|0^{n-1}\rangle$. À la suite de la première tour de Walsh-Hadamard, le registre du haut est dans une superposition uniforme de tous les entiers de 0 à $2^n - 1$. Puis, la porte f décrite à la figure 1.3 transforme cet état en $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$. La mesure du registre inférieur est celle associée à l'observable

$$\sum_{x=0}^{2^n-1} |x\rangle\langle x| \otimes \sum_{y=0}^{2^{n-1}-1} y|y\rangle\langle y|, \tag{1.13}$$

c'est-à-dire qu'elle donne un résultat différent pour chaque état de la base de calcul du registre inférieur sans distinguer les 2^n états du registre supérieur. Étant donné la symétrie de l'état de l'ordinateur, tous les résultats possibles de cette mesure

ont la même probabilité. Nous obtenons donc un nombre y choisi uniformément dans $\{0, 1, \ldots, 2^{n-1} - 1\}$. Par le cinquième postulat, l'état de l'ordinateur à la suite de cette mesure sera $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_1\rangle)|y\rangle$ où $f(x_0) = f(x_1) = y$.

À ce stade, le registre du haut est en superposition de deux nombres x_0 et x_1 tels que $x_0 \oplus x_1 = s$, le nombre recherché. Malheureusement, une mesure de ce registre ne nous en donne qu'un des deux aléatoirement, ce qui est absolument inutile. Ici, la possibilité de cloner serait fort utile puisqu'il s'agirait de créer plusieurs copies du registre du haut puis de les mesurer. Chaque mesure nous donnerait x_0 ou x_1 aléatoirement, donc, avec k clones en plus de l'original, nous obtiendrions s avec probabilité $1 - \left(\frac{1}{2}\right)^k$. Puisqu'il est impossible de cloner, nous devons trouver une solution plus astucieuse nous permettant d'acquérir de l'information sur s à l'aide de cette superposition.

La dernière transformation à l'effet suivant sur le registre supérieur :

$$\mathsf{H}^{\otimes n}\frac{|x_0\rangle + |x_1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^{n+1}}}\sum_{z=0}^{2^n-1}\left[(-1)^{x_0\cdot z} + (-1)^{x_1\cdot z}\right]|z\rangle. \tag{1.14}$$

La mesure finale donnera donc le résultat z avec probabilité

$$\begin{aligned} Pr(z) &= \left|\frac{1}{\sqrt{2^{n+1}}}\left[(-1)^{x_0\cdot z} + (-1)^{x_1\cdot z}\right]\right|^2 \\ &= \begin{cases} \frac{1}{2^{n-1}} & \text{si } x_0 \cdot z = x_1 \cdot z \\ 0 & \text{sinon} \end{cases}. \end{aligned} \tag{1.15}$$

Un peu d'algèbre élémentaire nous permet de constater que la probabilité d'obtenir un z donné est non nulle si et seulement si $(x_0 \oplus x_1)\cdot z = s \cdot z = 0$. Ainsi, l'obtention d'un z fournit une contrainte linéaire sur s de sorte qu'il suffit d'obtenir n chaînes z linéairement indépendantes parmi les 2^{n-1} candidats afin de connaître s. En moyenne, un temps linéaire en n suffit.

Calcul à oracle quantique

En raison de la présence de la boîte noire, le problème de Simon ne constitue pas une preuve de la puissance de calcul supérieure du monde quantique. Si la fonction f n'était pas cachée dans une boîte noire, il serait possible qu'une

stratégie classique exploitant certaines caractéristiques de f puisse déterminer s en un temps plus raisonnable. Il existe plusieurs exemples de tels calculs dits *à oracle*. Le Problème de Deutsch [27] fournissait le tout premier exemple où un seul appel à la boîte noire suffit quantiquement alors que deux appels sont nécessaires classiquement.[4] Il fut ensuite perfectionné par Deutsch et Jozsa [29] de sorte que deux appels soient encore suffisants mais qu'un nombre exponentiel soit requis classiquement. Ce gain est plus qu'exponentiel, il est non borné. Cependant, on demande aux calculateurs de fournir une réponse avec probabilité 1 ce qui n'est pas réaliste en raison des erreurs inévitables des ordinateurs quantiques (*cf.* section 1.5.6). Si on se contente d'une probabilité constante, le calculateur classique s'en tire très bien avec une probabilité $1 - \left(\frac{1}{2}\right)^k$ après k appels. Bernstein et Vazirani [13] ont fourni un premier exemple de calcul à oracle où une probabilité constante de succès est demandée et ont réussi à obtenir un gain super polynomial : $n^{c(\log n)}$ *vs* $poly(n)$ où c est une constante.

Toujours dans les problèmes à oracle, l'algorithme d'abord proposé par Grover [49] offre un gain moins intéressant mais demeure attrayant en raison de sa grande utilité. Il consiste à chercher un élément x_0 dans une base de donnée non ordonnée. Son implantation se fait à l'aide de la boîte noire $h : \{0,1\}^n \otimes \{0,1\} \mapsto \{0,1\}^n \otimes \{0,1\}$:

$$h(x,b) = \begin{cases} (x, b \oplus 1) & \text{si } x = x_0 \\ (x,b) & \text{sinon} \end{cases} . \tag{1.16}$$

Classiquement, il faut en moyenne $2^n/2$ appels à l'oracle pour trouver x_0 alors qu'on y parvient avec $O(\sqrt{2^n})$ quantiquement [17].

Factorisation

L'algorithme de Shor [83] permet de factoriser les grands nombres en facteurs premiers en un temps polynomial en la taille n du nombre à factoriser, c'est-à-

[4] En fait, l'algorithme de Deutsch est probabiliste. Sa probabilité de succès étant 1/2, il faut en moyenne deux appels à la boîte noire. De plus, transformer un circuit arbitraire en circuit réversible nécessite généralement le double de calculs. L'astuce du "*phase kick back*" permet d'accomplir l'algorithme de Deutsch de même que celui de Deutsch et Jozsa en un seul appel.

dire le nombre de bits nécessaires à sa représentation. Classiquement, le meilleur algorithme connu réussit à accomplir cette tâche en temps $O(\exp[cn^{1/3}\log^{2/3} n])$ où c est une constante. Cet algorithme n'utilise *pas* d'oracle. Néanmoins, il ne constitue pas une preuve de l'avantage du monde quantique puisque nous ne savons pas s'il existe un algorithme classique efficace (polynomial) pour factoriser. Il se peut que l'avantage apparent du calculateur quantique provienne de notre manque d'imagination lorsque vient le temps de concevoir des algorithmes classiques !

L'algorithme de factorisation fait partie d'une classe de problèmes appelée sous-groupe Abélien caché. Les algorithmes de Deutsch, Deutsch-Jozsa, Simon et Shor font tous partie de cette classe de problème, comme l'a réalisé Jozsa [53]. La généralisation de cette classe de problèmes à des groupes non Abéliens est une question d'actualité.

Simulation de systèmes physiques quantiques

La toute première proposition d'application de calculateurs quantiques était à des fins de simulations de systèmes à N corps quantiques [5, 37], puis étudié dans [86, 91, 1]. Il semble en effet que ce problème soit classiquement difficile puisque nos meilleurs algorithmes requièrent des ressources exponentielles. Nous savons aujourd'hui comment construire ces simulations quantiques efficaces pour une variété de systèmes physiques.

Il est toutefois important de noter que ces simulations nous donnent moins d'informations que les simulations classiques. En effet, les simulations classiques sont inefficaces en raison de manipulations d'un nombre exponentiel de nombres complexes. Cependant, ces simulations décrivent *classiquement* l'état du système quantique, contrairement aux simulateurs quantiques dans lesquels cette information est cachée sous forme quantique dans l'état de l'ordinateur. Ainsi, une simulation classique nous permet d'extraire toute l'information désirée sur le système quantique alors que nous sommes restreints à une seule mesure pour les simulations quantiques. Il reste donc à savoir s'il est possible d'extraire des quantités physiquement pertinentes de ces simulations.

Cette remarque se s'applique également à la classicalité du calcul quantique.

Récemment, Jozsa et Linden [54] ont étudié la possibilité de simuler classiquement certains algorithmes quantiques. Leur conditions de classicalité impose à la fonction d'onde de l'ordinateur quantique d'être factorisable en blocs de taille polynomiale à toutes étapes du calcul. Cette condition est nécessaire si nous tenons à connaître entièrement la fonction d'onde, ce qui est beaucoup plus que ce qu'offre l'ordinateur quantique : le résultat d'une seule mesure. En gros, si nous exigeons de connaître une quantité exponentielle d'information, alors il fut des ressources exponentielles, l'argument tout bête de Feynman !

Communication quantique

Outre certains problèmes à oracle qui bénéficient, de façon démontrable, d'un gain exponentiel lorsque implantés quantiquement, certains problèmes de communication sont accomplis plus efficacement à l'aide d'information quantique : il existe même certains problèmes qui sont accomplis à l'aide de la mécanique quantique alors qu'il est strictement impossible de les accomplir classiquement. C'est le cas de la cryptographie quantique. Supposons que deux individus physiquement séparés, disons Alice et Bob, désirent échanger un message secret M encodé en bits de sorte qu'il soit impossible à un troisième individu, Ève, de connaître le contenu de ce message. Classiquement, cette tâche est réalisable uniquement si Alice et Bob partagent initialement une chaîne de bits secrète X, la clée, de taille supérieure ou égale à celle du message. Le protocole est ensuite très simple : Alice calcule $Y = M \oplus X$ et envoie Y à Bob. Si Ève intercepte Y, elle n'acquiert aucune information sur M puisqu'elle ignore X. Sur réception de Y, Bob peut facilement retrouver $M = Y \oplus X$. Évidemment, ce protocole est très coûteux et peu pratique puisqu'il requière de la part des deux individus un moyen de communication sécuritaire préalable leur permettant d'échanger la clée, par exemple de se rencontrer en personne.

Sans la possession d'une telle clé, la probabilité qu'Ève puisse acquérir une certaine information sur le message est non nulle. Le décryptage du message peut impliquer de grosses tâches calculatoires, telle la factorisation de grands nombres. La plupart des protocoles d'encryption modernes qui assurent la protection de

transactions électroniques sont d'ailleurs basés sur la factorisation ; cela malgré que nous ne possédions pas de preuve de la difficulté de factoriser et malgré l'éventuelle menace de l'ordinateur quantique. Si Ève possède une très grande capacité calculatoire ou si elle dispose de beaucoup de temps, elle pourra décrypter le message.

Fort heureusement, la théorie de l'information quantique offre la solution de la cryptographie inconditionnellement sécuritaire [8]. Si Alice et Bob partagent initialement une clé de petite taille, ils pourront en générer une plus grande tout aussi secrète sans avoir à se réunir. Ainsi, ils n'ont qu'à se rencontrer une seule fois à la suite de quoi ils pourront échanger un nombre infini de messages. Ce qui assure la sécurité de ce protocole est une version généralisée du théorème interdisant le clonage. Bennett, Brassard et Mermin ont démontré que toute opération sur un système quantique qui, avec une probabilité non nulle, peut révéler de l'information sur son état va le perturber avec une probabilité non nulle, sauf si l'état du système appartient à un ensemble d'états orthogonaux (état classique) [10]. Ainsi, dès qu'Ève tente d'acquérir de l'information sur la clé secrète, son intervention sera détectée par Alice et Bob qui agiront en conséquence.

Les autres exploits en communication font intervenir la notion de complexité de la communication. Supposons qu'Alice possède la chaîne de bits $x \in \{0,1\}^n$ alors que Bob possède $y \in \{0,1\}^n$. Leur but est de calculer la fonction $f(x,y)$ en échangeant le moins d'information possible. Évidemment, n bits de communication est suffisant pour toute fonction f, mais il est parfois possible de faire mieux. Maintenant, si nous permettons à Alice et Bob d'échanger des qubits plutôt que des bits, peuvent-ils économiser de la communication ? À première vue, la réponse semble être *non* puisqu'il est impossible de transmettre plus d'un bit d'information par qubit transmis selon le théorème de Holevo[5] [51]. Pourtant, certaines fonctions f permettent une réduction de communication. Pour un compte rendu des exploits en complexité de communication quantique, voir [19].

[5]Si Alice et Bob partagent initialement des particules enchevêtrées, ce qui n'est pas le cas ici, il est possible de transmettre deux bits par qubit. Nous reviendrons sur la notion d'enchevêtrement à la section 1.4

1.4. Enchevêtrement & mélange statistique

La notion d'*enchevêtrement* ou intrication est au coeur de la théorie de l'information quantique. Considérons l'état des deux qubits supérieurs de la figure 1.1 à la suite de l'application des deux premières portes : $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (*cf.* (éq. 1.9)). La fonction d'onde décrit l'état global des deux particules, il n'existe pas de vecteur d'état décrivant l'un ou l'autre des qubits pris séparément. En d'autres termes, cette fonction d'onde ne peut s'écrire sous la forme $|\phi_1\rangle \otimes |\phi_2\rangle$. Nous dirons d'un tel état qu'il est enchevêtré.

Matrice de densité

Afin de décrire l'état *d'une* des particules d'une paire enchevêtrée, nous devons introduire le formalisme des matrices de densité. Supposons que nous ne possédions que de l'information partielle sur l'état d'un système de sorte qu'il puisse être dans l'état $|\psi_1\rangle$ avec probabilité p_1, dans l'état $|\psi_2\rangle$ avec probabilité p_2, *etc.*, que l'on note $\{(|\psi_j\rangle, p_j)\}$. La matrice de densité décrivant ce mélange statistique est

$$\rho = \sum_{j=1} p_j |\psi_j\rangle\langle\psi_j|, \quad \text{avec} \quad \sum_{j=1} p_j = 1. \tag{1.17}$$

Cette matrice est positive c'est-à-dire $\langle\phi|\rho|\phi\rangle \geq 0 \quad \forall\phi$, et de trace 1. Ici, les probabilités p_j ne sont pas de nature fondamentale comme celles apparaissant au quatrième postulat, elle proviennent d'un manque d'information. Nonobstant cette ignorance, il est possible d'attribuer ces probabilités à une cause fondamentale, c'est le cas lorsque le système décrit par la matrice de densité est enchevêtré avec un second système auquel l'observateur n'a pas accès.

Soit, par exemple, les deux qubits de l'exemple précédent. Leur état global est $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ou, sous forme de matrice de densité :

$$\rho_{12} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{1.18}$$

L'état du premier qubit est obtenu en appliquant une trace partielle sur l'espace du second qubit : $\rho_1 = Tr_2\{\rho_{12}\}$. Dans ce cas, nous obtenons

$$\rho_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.19}$$

Plusieurs « recettes » peuvent mener à la même matrice de densité. Celle de (éq. 1.19) a été obtenue en ignorant la présence du second qubit enchevêtré, mais décrit également les mélanges $\{(|0\rangle,\ \frac{1}{2}), (|1\rangle,\ \frac{1}{2})\}$ et $\{(|0\rangle,\ \frac{1}{3}), (\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle,\ \frac{1}{3}), (\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle,\ \frac{1}{3})\}$ pour n'en nommer que deux. Peu importe la recette utilisée afin d'obtenir le mélange, les systèmes décrits par la même matrice de densité sont *physiquement indistinguables.* Autrement dit, la matrice de densité renferme toute l'information physiquement accessible du système ; cela explique donc pourquoi les fonctions d'onde ne différant que par une phase globale représentent le même état physique, *cf.* section 1.1. Une matrice de densité sera dite pure si elle représente une fonction d'onde : $\rho = |\psi\rangle\langle\psi|$, c'est-à-dire lorsqu'elle est de rang 1 ; sinon, elle est *mélangée* ou mixte.

Classiquement, c'est l'entropie de Gibbs-Shannon qui mesure le degré de manque d'information sur l'état du système qui est décrit par une distribution de probabilité $\{Pr_j\}$: $H[Pr] = -\sum_j Pr_j \log Pr_j$ [26, 76, 82].[6] En mécanique quantique, c'est l'entropie de von Neumann qui joue ce rôle [90]

$$S(\rho) = -Tr\{\rho \log \rho\} = H[\lambda_j] \tag{1.20}$$

où les λ_j sont les valeurs propres de ρ. L'interprétation de formules entropiques à la von Neumann telles l'entropie mutuelle, l'entropie conjointe et les différentes entropies conditionnelles forme un champ d'activité très actif connu sous le nom de théorie de l'information quantique. Cette théorie diffère de la théorie classique élaborée par Shannon en raison de l'existence de l'enchevêtrement et d'états non orthogonaux.

[6] Dans tout ce qui suit, le logarithme log est en base 2. Il s'en suit que l'unité de mesure d'information de Gibbs-Shannon est le bit et que celle de von Neumann est le qubit.

Enchevêtrement

Les particules enchevêtrées affichent des corrélations qui n'ont aucun équivalent classique. Supposons par exemple que le premier qubit de la paire $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ se trouve chez Alice alors que Bob est en possession du second. Bob mesure son qubit selon une base choisie arbitrairement, $\{|\mu_0\rangle, |\mu_1\rangle\}$, $\langle\mu_j|\mu_k\rangle = \delta_{jk}$ et obtient le résultat $|\mu_j\rangle$. Selon le cinquième postulat, le qubit d'Alice se retrouve instantanément dans l'état $|\mu_{j\oplus 1}\rangle$. Cet étrange comportement de la nature fut d'abord soulevé par Einstein, Podolsky et Rosen [33] qui y soupçonnaient une incomplétude de la théorie quantique. Ce n'est qu'en 1964 que Bell trouva comment il était possible de décider expérimentalement si ce semblant de paradoxe était dû à la présence de variables cachées manquant à la théorie de l'époque ou s'il illustrait un comportement sans équivalent classique [4]. En fait, ce que Bell montra est que les prédictions de la théorie quantique ne peuvent pas être expliquées par une théorie réaliste locale, le rêve d'Einstein. Les expériences d'Aspect, Grangier et Roger réalisées 17 ans plus tard vinrent démontrer que ce phénomène est bel et bien un nouvel aspect de la théorie quantique [3]. Des résultats pouvant être expliqués à l'aide de théorie réaliste locale auraient invalidés la théorie quantique.

En raison de *l'instantanéité* de la réduction du paquet d'onde, la causalité imposée par la relativité restreinte semble être violée. Cependant, une analyse détaillée des mesures montre que tel n'est pas le cas. Suite à la mesure effectuée par Bob, l'état du système en possession d'Alice est $|\mu_0\rangle$ si Bob a obtenu μ_0, ce qui se produit avec probabilité $\frac{1}{2}$, et $|\mu_1\rangle$ dans le cas contraire, avec probabilité complémentaire. Puisqu'Alice ne connaît pas le résultat obtenu par Bob, le système en sa possession est décrit par la matrice

$$\rho_{\mathcal{A}} = \frac{1}{2}|\mu_0\rangle\langle\mu_0| + \frac{1}{2}|\mu_1\rangle\langle\mu_1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.21}$$

Ce résultat étant indépendant du choix de la base $\{|\mu_0\rangle, |\mu_1\rangle\}$, aucune information n'est transmise de Bob à Alice par l'action de la mesure. De plus, $\rho_{\mathcal{A}}$ correspond à la matrice de densité marginale d'Alice avant la mesure de Bob $Tr_{\mathcal{B}}\{|\Phi^+\rangle\langle\Phi^+|\}$. En fait, aucun protocole local de la part de Bob ne peut affecter la matrice de

densité chez Alice. Cela implique qu'aucune action de la part d'Alice ne lui permet de déterminer la base choisie par Bob ou même de détecter si Bob a mesuré son système. Si Bob communique avec Alice pour lui indiquer le résultat de sa mesure, d'étranges corrélations entre les résultats seront présentes, mais ces dernières ne sont pas proscrites par le principe de causalité.

Seul un hamiltonien comprenant un terme de couplage peut créer de l'enchevêtrement entre deux systèmes $\mathcal{A}$ et $\mathcal{B}$. Comme nous l'avons mentionné à la section 1.2, ce couplage peut être médié par un tierce système quantique. Ainsi, la transmission d'un qubit peut générer de l'enchevêtrement entre le système d'Alice et celui de Bob.

Mesure d'enchevêtrement

Les quatre états

$$\begin{aligned} |\Phi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ |\Psi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \end{aligned} \tag{1.22}$$

forment une base pour les systèmes à deux qubits. Ce sont tous des états maximalement enchevêtrés à deux qubits. On y réfère souvent sous *états de Bell* ou paires de particules EPR (pour Einstein, Podolsky et Rosen). La mesure d'enchevêtrement pour un état pur partagé entre deux individus Alice et Bob est l'entropie de von Neumann de la matrice de densité marginale [7] :

$$E(|\psi\rangle) = S(\rho_{\mathcal{A}} \log \rho_{\mathcal{A}}) = S(\rho_{\mathcal{B}} \log \rho_{\mathcal{B}}) \quad \text{où} \quad \begin{cases} \rho_{\mathcal{A}} = Tr_{\mathcal{B}}\{|\psi\rangle\langle\psi|\} \\ \rho_{\mathcal{B}} = Tr_{\mathcal{A}}\{|\psi\rangle\langle\psi|\} \end{cases}. \tag{1.23}$$

Elle correspond au nombre de paires EPR que doivent partager Alice et Bob s'ils veulent construire l'état $|\psi\rangle$ á l'aide de transformations locales et communication classique (OLCC), de façon asymptotique, ou à l'inverse au nombre de paires EPR qu'ils peuvent produire par OLCC s'ils partagent $|\psi\rangle$. En d'autres termes,

$$E(|\psi\rangle) = \lim_{n\to\infty} \max_{m} \left\{ \frac{n}{m} : |\Phi^+\rangle^{\otimes n} \rightsquigarrow |\psi\rangle^{\otimes m} \right\} \tag{1.24}$$

$$= \lim_{m\to\infty} \max_{n} \left\{ \frac{n}{m} : |\psi^{\otimes m}\rangle \rightsquigarrow |\Phi^+\rangle^{\otimes n} \right\} \tag{1.25}$$

où $\rightsquigarrow$ désigne que la transformation requiert uniquement des opérations locales chez Alice et Bob et de la communication classique. L'expression de (éq.1.24) porte le nom d'enchevêtrement *de formation* E_f alors que celle de (éq.1.25) est dite *de distillation* E_d. Ces mesures coïncident lorsque l'état du système global $\mathcal{A}B$ est pur. Lorsque l'état global est mixte, il arrive que $E_f > E_d$ ce qui implique que le processus de formation est irréversible [89]. La mesure d'enchevêtrement pour les états purs partagés entre de multiples individus n'a à ce jour pas de définition universelle. Le problème est l'existence de classes d'enchevêtrement qui ne peuvent pas être transformées les unes dans les autres localement, ce qui entraîne une confusion pour l'unité fondamentale d'enchevêtrement. Par exemple, si Alice, Bob et Charlie partagent deux triplets $\frac{1}{\sqrt{2}}(|0_A0_B0_C\rangle + |1_A1_B1_C\rangle)$, ils ne peuvent pas obtenir les trois paires EPR $\frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$, $\frac{1}{\sqrt{2}}(|0_A0_C\rangle + |1_A1_C\rangle)$ et $\frac{1}{\sqrt{2}}(|0_B0_C\rangle + |1_B1_C\rangle)$.

Téléportation quantique

Nous allons maintenant démontrer que les états de Bell sont les états maximalement enchevêtrés à deux qubits tel que mentionné ci-haut. D'abord, ils possèdent tous la même quantité d'enchevêtrement puisqu'ils peuvent êtres transformés les uns dans les autres par l'application chez Alice d'une des matrices de Pauli :

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1.26)$$

De plus, soit la fonction d'onde de deux qubits $|\psi\rangle$ et la transformation U telle que $U|00\rangle = |\psi\rangle$. Si Alice et Bob partagent initialement une paire $|\Phi^+\rangle$, ils peuvent la transformer en une paire $|\psi\rangle$ à l'aide du circuit 1.5 qui ne requiert pas d'interaction entre les systèmes d'Alice et de Bob, uniquement des OLCC, donc $E(|\Phi^+\rangle) \geq E(|\psi\rangle)\ \ \forall\psi$. En effet, les qubits 1, 2 et 3 sont dans le laboratoire d'Alice alors que le 4 est en la possession de Bob ; il n'interagit pas avec les qubits d'Alice.

Les mesures d'Alice sont effectuées dans la base de calcul. Les résultats a et b sont transmis à Bob (communication classique) qui applique une des quatre matrices de Pauli en conséquence : $(0,0) \mapsto 0$, $(0,1) \mapsto z$, $(1,0) \mapsto x$ et $(1,1) \mapsto y$.

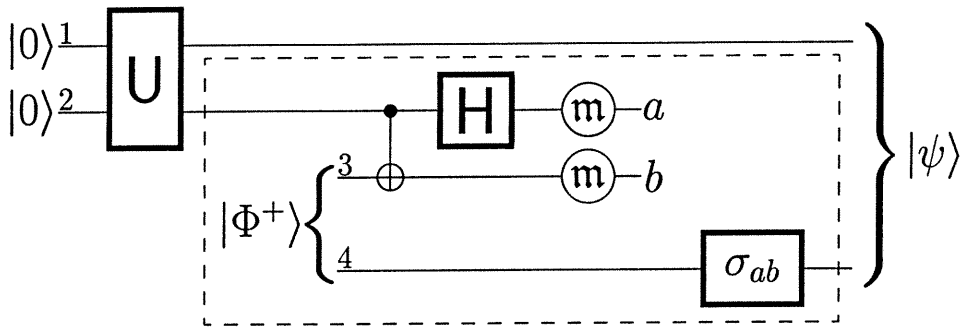

FIG. 1.5 – Téléportation quantique.

La partie du circuit dans la boîte pointillée représente la téléportation quantique [9]. Peu importe ce qui se trouve à l'entrée de cette boîte au fil 2 se retrouvera à sa sortie au fil 4, malgré que ces deux qubits ne soient jamais entrés en interaction outre que par communication classique. Il est à noter que c'est *l'état* du qubit qui est téléporté, pas le système physique. D'ailleurs, le support physique est sans importance, il est par exemple possible de téléporter l'état d'un photon sur celui d'un électron. La description de l'état d'un qubit requiert deux nombres réels. Pourtant, le circuit de la figure 1.5 transmet cet état à l'aide de deux bits et d'une paire EPR uniquement et cela malgré le fait qu'une paire EPR ne peut servir à transmettre de l'information classique !

La téléportation quantique n'est que la pointe de l'iceberg en ce qui concerne les applications de l'enchevêtrement. Ici, nous n'osons même pas entamer une liste puisque des mots sans explication sont inutiles. L'article de revue de Bennett et Shor [12] est sans doute un bon point de départ pour explorer ce monde étrange.

Cette section traite à la fois de l'enchevêtrement et de mélanges statistiques puisque ce sont deux concepts très intriqués ! D'abord, l'état marginal d'une paire enchevêtrée est mixte. De plus, la mesure d'enchevêtrement pour les états purs est la même que celle du degré d'incertitude d'un mélange. La mesure d'enchevêtrement des états mixtes forme un champ de recherche en soi : il n'existe pas d'analogue de (éq.1.24) et (éq.1.25) lorsque l'état partagé est mixte. Finalement, *l'Église de l'espace de Hilbert élargi* prêche que tout mélange statistique

provient d'enchevêtrement entre le système à l'étude et un autre système auquel nous n'avons pas accès ! Opératoirement, cet énoncé est valable puisqu'aucune expérience ne peut nous permettre de distinguer ce mélange d'une pure ignorance. Fondamentalement, c'est à chacun de choisir son interprétation...

Adaptation des postulats

Afin de compléter cette section, nous devons expliquer ce qu'il advient des postulats de la mécanique quantique lorsque l'état du système est mixte. Toute matrice de densité peut s'écrire sous forme diagonale

$$\rho = \sum_{j=1}^{r} \lambda_j |\psi_j\rangle\langle\psi_j|, \quad \sum_{j=1}^{r} \lambda_j = 1 \quad \langle\psi_j|\psi_k\rangle = \delta_{jk} \tag{1.27}$$

où r est le rang de ρ et $0 \leq \lambda_j \leq 1$. Les quatrième, cinquième et sixième postulats prennent simplement leur valeur moyenne sur le mélange statistique $\{(|\psi_j\rangle,\ \lambda_j)\}$; il suffit de remplacer les expressions :

$$Pr(a_n) = \sum_{j=1}^{g_n} |\langle\phi_n^j|\psi\rangle|^2 \quad \text{par} \quad Pr(a_n) = \sum_{k=1}^{r} \lambda_k \sum_{j=1}^{g_n} |\langle\phi_n^j|\psi_k\rangle|^2$$
$$= \sum_{j=1}^{g_n} \langle\phi_n^j|\rho|\phi_n^j\rangle \tag{1.28}$$

pour le quatrième postulat ;

$$\frac{\hat{P}_n|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_n|\psi\rangle}} \quad \text{par} \quad \frac{\hat{P}_n\rho\hat{P}_n}{Tr\{\hat{P}_n\rho\}} \tag{1.29}$$

pour le cinquième et finalement

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}(t)|\psi(t)\rangle \quad \text{par} \quad i\hbar\frac{d}{dt}\rho = [\hat{H}, \rho] \tag{1.30}$$

pour l'équation du mouvement qui porte le nom d'équation de Liouville. Cette formulation du quatrième postulat (éq.1.28) nous permet d'introduire une définition opératoire d'état pur : l'état d'un système est pur si et seulement si il existe une mesure dont le résultat est déterministe ; si une telle mesure n'existe pas, l'état est mixte.

En principe, le troisième postulat reste intact, mais certaines situations nécessitent un éclaircissement. Supposons qu'un système quantique soit composé de $N \gg 1$ sous-systèmes de même nature et que seules les observables macroscopiques nous soient accessibles (situation typique en thermodynamique quantique). Ces valeurs nous permettent, aidé du principe d'entropie maximale, d'inférer l'état moyen $\rho = \frac{1}{N}\sum_{j=1}^{N}\rho_j$ des sous-systèmes individuels. Ainsi, le système est une réalisation de l'ensemble statistique décrit par ρ. Lors de la mesure de l'observable $\mathcal{A}$, nous avons uniquement accès à *la somme macroscopique des résultats des systèmes individuels*; ce résultat est $NTr\{\rho\hat{A}\}$ et l'état du système est pratiquement inchangé, il n'y a pas de réduction du paquet d'onde. Ceci constitue une mesure d'ensemble très fréquente en spectroscopie. Lorsque seules les mesures d'ensemble sont réalisables expérimentalement, la préparation de l'état initial d'un système quantique est problématique puisque le simple protocole présenté à la section 1.2.4 requiert des mesures projectives. Nous reviendrons sur ce problème à la section 4.4.

1.5. Mesure & décohérence

Mesure de von Neumann

La mesure est l'ingrédient clé de ce travail. C'est grâce à la celle-ci que nous pourrons rendre partiellement classiques certains algorithmes quantiques. Apprendre les coefficients c_j d'une fonction d'onde $|\psi\rangle = \sum_{j=0}^{\Omega-1} c_j|\phi_j\rangle$ dans une base donnée est impossible. Pour s'en convaincre, il suffit de constater qu'une telle mesure nous permettrait de cloner le système quantique. Ainsi, par mesure d'un système quantique, nous entendons le type de mesure décrite aux postulats 3 à 5. Comme nous l'avons déjà mentionné, cette mesure fait intervenir une évolution non unitaire allant à l'encontre du sixième postulat et c'est ce que nous tentons d'élucider dans la présente section.

Soit un appareil de mesure $\mathcal{A}$ et le système quantique subissant la mesure $\mathcal{S}$. Comme l'a démontré von Neumann [90], l'évolution unitaire seule suffit à établir des corrélations entre le système et l'appareil. Le scénario est le suivant. Le système

$\mathcal{S}$ est dans un état arbitraire pur $|\psi\rangle_{\mathcal{S}} = \sum_{j=0}^{\Omega-1} c_j|\phi_j\rangle$ et l'appareil de mesure est préparé dans un état initial standard $|\Psi_0\rangle_{\mathcal{A}} = \sum_{k=0}^{M-1} a_k|A_k\rangle$. Dans ce qui suit, nous allons supposer que $M = \Omega$, mais seule la condition $M \geq \Omega$ est nécessaire. Il existe une transformation unitaire U_{m} dont l'effet sur l'état conjoint du système et de l'appareil est

$$|\psi\rangle_{\mathcal{S}} \otimes |\Psi_0\rangle_{\mathcal{A}} \mapsto \sum_{j=0}^{\Omega-1} c_j|\phi_j\rangle \otimes |A_j\rangle \tag{1.31}$$

pour tout $|\psi\rangle_{\mathcal{S}}$ et un $|\Psi_0\rangle_{\mathcal{A}}$ fixe. À première vue, la mesure semble être terminée puisque l'état de l'appareil de mesure est très fortement corrélée à celui du système. L'observable qui semble être mesurée est évidemment $\sum_j f_j|\phi_j\rangle\langle\phi_j|$, $f_i \neq f_j \ \forall i \neq j$.

Si la mesure était effectivement terminée à ce stade, nous pourrions appliquer la transformation $U_{\mathrm{m}}^{\dagger}$ aux systèmes conjoints et retrouver l'état initial de $\mathcal{S}$ intact. À la suite de cela, nous pourrions recommencer le processus de mesure en choisissant une autre observable et ce, jusqu'à ce que l'état $|\psi\rangle_{\mathcal{S}}$ nous soit connu avec précision arbitraire. Une telle acquisition d'information étant impossible puisqu'elle viole le théorème de Bennett, Brassard et Mermin (*cf.* sec. 1.3.5 et [10]) nous indique que la transformation U_{m} ne règle pas le problème de la mesure.

De plus, en choisissant une autre base pour l'appareil de mesure $|A'_j\rangle = \sum_k \langle A_k|A'_j\rangle|A_k\rangle$, l'observable mesuré par l'application de U_{m} ne semble plus ressortir de façon si explicite :

$$\begin{aligned} \sum_{j=0}^{\Omega-1} c_j|\phi_j\rangle \otimes |A_j\rangle &= \sum_{j=0}^{\Omega-1}\sum_{k=0}^{\Omega-1} c_j\langle A'_k|A_j\rangle|\phi_j\rangle \otimes |A'_k\rangle \\ &= \sum_{k=0}^{\Omega-1} c'_j|\mu_k\rangle \otimes |A'_k\rangle. \end{aligned} \tag{1.32}$$

Ici, les kets $|\mu_k\rangle$ sont normalisés mais pas nécessairement orthogonaux. Dans le cas où les coefficients c_j sont tous égaux, $\langle\mu_j|\mu_k\rangle = \delta_{jk}$. Il semble donc que la réduction du paquet d'onde de $\mathcal{S}$ se fera selon un ensemble d'états différent dépendamment de la base que nous choisissons pour décrire l'appareil de mesure !

Base privilégiée

Puisqu'un montage expérimental mesure toujours la même observable physique, peu importe la description que nous en avons, il doit y avoir une base privilégiée associée à $\mathcal{A}$. En pratique, nous connaissons cette base. Prenons l'exemple d'une mesure binaire où le résultat est affiché par l'aiguille d'un cadran pointant à gauche $|G\rangle$ si le système se trouve dans l'état $|\phi_0\rangle$ et à droite $|D\rangle$ si le système est décrit par $|\phi_1\rangle$. Si la position initiale de l'aiguille est à gauche, alors la transformation unitaire requise pour accomplir le type de corrélations décrites par (éq.1.31) est :

$$U_{\mathrm{m}} = |\phi_0 G\rangle\langle\phi_0 G| + |\phi_1 D\rangle\langle\phi_1 G| + |\phi_0 D\rangle\langle\phi_0 D| + |\phi_1 G\rangle\langle\phi_1 D|. \tag{1.33}$$

Les vecteurs/valeurs propres de cette transformation sont

$$|\phi_0 G\rangle,\ 1\ ;\ |\phi_0 D\rangle,\ 1\ ;\ |\phi_1\rangle\frac{|G\rangle + |D\rangle}{\sqrt{2}},\ 1\ \text{ et }\ |\phi_1\rangle\frac{|G\rangle + |D\rangle}{\sqrt{2}},\ -1 \tag{1.34}$$

En fait, cette transformation est simplement un ou-exclusif dont l'aiguille constitue la cible.

Le hamiltonien général du système $\mathcal{SA}$ s'écrit sous la forme $\hat{H} = \mathbb{1}_{\mathcal{S}} \otimes \hat{H}_{\mathcal{A}} + \hat{H}_{\mathcal{S}} \otimes \mathbb{1}_{\mathcal{A}} + \hat{H}_I$ (où $\mathbb{1}$ est l'identité) : l'énergie totale est la somme de l'énergie de l'appareil, celle du système et l'énergie d'interaction. Supposons que seul le hamiltonien d'interaction $\hat{H}_I$ est non nul. L'interaction

$$\hat{H}_I = g|\phi_1\rangle\langle\phi_1| \otimes \left(\frac{|G\rangle - |D\rangle}{\sqrt{2}}\right)\left(\frac{\langle G| - \langle D|}{\sqrt{2}}\right), \tag{1.35}$$

où g est un paramètre de couplage, peut réaliser la transformation U_{m} si $\exp\{i\hat{H}_I t/\hbar\}$ $= U_{\mathrm{m}} \ \Rightarrow\ e^{\frac{igt}{\hbar}} = -1$. Par exemple, cette condition est observée lorsque $t = t_0 = \frac{\pi\hbar}{g}$.

Si le système $\mathcal{S}$ se trouvait initialement dans l'état $\frac{|\phi_0\rangle+|\phi_1\rangle}{\sqrt{2}}$, alors l'action de l'interaction après un temps t_0 se traduira par l'état $\frac{|\phi_0 G\rangle+|\phi_1 D\rangle}{\sqrt{2}}$ qui peut également s'écrire

$$\frac{\frac{1}{2}(|\phi_0\rangle + |\phi_1\rangle)(|G\rangle + |D\rangle) + (|\phi_0\rangle - |\phi_1\rangle)(|G\rangle - |D\rangle)}{\sqrt{2}}, \tag{1.36}$$

d'où l'ambiguïté de ce qui a été mesuré. Cependant, nous savons que ce qui a *réellement* été mesuré est l'observable $f_0|\phi_0\rangle\langle\phi_0| + f_1|\phi_1\rangle\langle\phi_1|$ puisque jamais nous n'observons l'aiguille d'un cadran en superposition d'un état à gauche et d'un état à droite. Ainsi, la question «Qu'est-ce qui est mesuré ?» se transpose en «Pourquoi n'observe-t-on pas de superpositions *étranges* des objets macroscopiques ?».

Décohérence

La décohérence offre une réponse opératoire à cette question. Cette explication principalement due à Żurek [95, 96] repose sur la notion fondamentale de sous-système quantique. Le postulat de la mesure, donc la mécanique quantique conventionnelle, ne s'applique qu'à des sous-systèmes quantiques. En effet, tous les systèmes que nous observons font en fait partie d'un système plus vaste, l'environnement $\mathcal{E}$. C'est en excluant de notre description les nombreux degrés de liberté de l'environnement que l'évolution non unitaire apparaît.

L'évolution unitaire $U(t)$ du système $\mathcal{S} \otimes \mathcal{E}$ se traduit, pour un observateur n'ayant pas accès à $\mathcal{E}$, par :

$$\rho_{\mathcal{S}}(0) \mapsto Tr_{\mathcal{E}}\{U(t)\rho_{\mathcal{S}}(0) \otimes \rho_{\mathcal{E}}(0)U^{\dagger}(t)\} \tag{1.37}$$

qui est unitaire si et seulement si l'évolution $U(t)$ n'engendre aucune corrélation, classique ou quantique, entre $\mathcal{S}$ et $\mathcal{E}$, c'est-à-dire si et seulement si

$$U(t)\rho_{\mathcal{S}}(0) \otimes \rho_{\mathcal{E}}(0)U^{\dagger}(t) = \rho_{\mathcal{S}}(t) \otimes \rho_{\mathcal{E}}(t). \tag{1.38}$$

Cela se produit uniquement lorsque le hamiltonien est séparable $\hat{H} = \hat{H}_{\mathcal{S}} \otimes \mathbb{1}_{\mathcal{E}} + \mathbb{1}_{\mathcal{S}} \otimes \hat{H}_{\mathcal{E}}$. Mathématiquement, l'évolution générale (éq.1.37) peut être modélisée par un super-opérateur (voir [81] pour plus de détails).

Sous certaines hypothèses réalistes, l'effet de ce couplage sera de transformer l'état du système en $\rho(t \to \infty) = \sum_j p_j|\phi_j\rangle\langle\phi_j|$ où $p_j = \langle\phi_j|\rho(t=0)|\phi_j\rangle$. Les termes hors diagonaux $|\phi_j\rangle\langle\phi_k|$ sont présents initialement mais leur amplitude décroît exponentiellement avec le temps : $\rho_{jk}(t) \approx \rho_{jk}(0)e^{-\lambda t}$. Le temps de cohérence $1/\lambda$ dépend du couplage et de la taille de l'environnement.

La base $\{|\phi_j\rangle\}$ est entièrement déterminée par le hamiltonien $\hat{H}$ des systèmes. À fort couplage, lorsque $\hat{H}_S \ll \hat{H}_I$, les $|\phi_j\rangle$ seront les vecteurs propres de l'observable couplée par l'interaction $Tr_\mathcal{E}\{\hat{H}_I\}$ [96]. Dans le cas contraire, $\hat{H}_I \ll \hat{H}_S$, ce sont les vecteurs propres de l'énergie du système H_S qui formeront la base privilégiée [72]. C'est d'ailleurs cette hypothèse qui est utilisée en thermodynamique quantique lorsque les matrices de densité s'écrivent $Z^{-1}\exp\{-\beta\hat{H}_S\}$. Pour des couplages intermédiaires, il n'existe pas de règle universelle, la base privilégiée doit être déterminée au cas par cas.

En résumé, l'effet d'une interaction entre l'environnement et un sous-système est la sélection d'une base privilégiée $\{|\phi_j\rangle\}$, entièrement déterminée par le type de couplage $\hat{H}_I$ et l'énergie interne $\hat{H}_S$ du sous-système. Sous cette interaction, toute superposition cohérente des vecteurs de la base privilégiée se transforme en un mélange statistique de ces derniers, la probabilité de chaque état étant donnée par le module carré de son amplitude dans la superposition initiale.

Bien que nous ne pouvons pas le formuler sous forme de loi universelle, la base privilégiée coïncide habituellement avec la base classique pour les objets macroscopiques. Par base «classique», nous entendons base des états que nous observons dans la vie courante. En particulier, ces bases ne font pas intervenir de superposition de *position* des objets. Cela s'explique par le fait que les équations des champs sont des équations *locales*.

Tout cela explique donc pourquoi nous n'observons jamais de superposition quantique d'objets macroscopiques. Ces derniers subissent d'innombrables perturbations dues à des interactions avec leur environnement.[7] Cet environnement est composé en partie de rayons cosmiques, de molécules de l'air ambiant, de photons de la lumière du laboratoire, etc. Par exemple, des calculs simples montrent que la lumière solaire reçue sur terre à elle seule suffit à transformer l'état pur d'un grain de poussière de 10^{-5} cm en un mélange statistique en l'espace de 10^{-7} secondes [52] !

[7] Ou d'un autre point de vue, peut-être plus intéressant, ces systèmes perturbent leur environnement, donc divulguent de l'information sur leur état [67].

Mesure & décohérence

Pour en revenir au problème de la mesure, il suffit de considérer que l'appareil de mesure $\mathcal{A}$ étant macroscopique peut difficilement être isolé, donc subit de la décohérence. Dans ce cas, l'évolution du sous système $\mathcal{S} \otimes \mathcal{A}$ est

$$\begin{aligned} |\psi\rangle_{\mathcal{S}} \otimes |\Psi_0\rangle_{\mathcal{A}} &\mapsto \sum_{j=0}^{n-1} c_j |\phi_j\rangle \otimes |A_j\rangle \\ &\mapsto \sum_{j=0}^{n-1} |c_j|^2 |\phi_j\rangle\langle\phi_j| \otimes |A_j\rangle\langle A_j|, \end{aligned} \tag{1.39}$$

la première ligne étant simplement (éq.1.31) et la seconde, une conséquence de la présence d'un environnement inaccessible. Cette évolution pourrait, en principe, être renversée, mais cela requérerait le contrôle parfait de chaque particule de l'environnement, rendant la décohérence *pratiquement irréversible.* Tout de même, d'un point de vue fondamental, ce problème donne naissance au paradoxe de l'ami de Wigner [92]. Ce paradoxe apparaît lorsqu'on considère l'observateur comme un système quantique. Lorsque l'état du système, de l'appareil de mesure, de l'observateur et de l'environnement sont tenues en compte, l'évolution demeure unitaire donc il n'y a pas de réduction du paquet d'onde.

La résolution fondamentale du problème de la mesure nécessite l'introduction de nouveaux concepts. Les univers parallèles d'Everett [35] forment sans doute l'interprétation sortant gagnante du rasoir d'Occam. Malgré qu'elle soit très peu acceptée et cela en raison du nom rappelant la science-fiction qu'on lui a accordé, cette théorie est fort utile pour développer une intuition des phénomènes rencontrés en information quantique.

Mesure en informatique quantique

L'informatique quantique est à la fois une application de la théorie quantique et un banc d'essai servant à faire ressortir certains aspects nouveaux de la théorie. Du point de vue application, une réponse opératoire au problème de la mesure est entièrement satisfaisante. Le modèle de calcul découlant des six postulats énoncés

au début de ce chapitre colle bien à la réalité. Du point de vue fondamental, la question reste ouverte.

L'explication offerte par la décohérence repose en partie sur *l'impossibilité technologique* de contrôler l'environnement ; ce concept étant tout à fait subjectif, il n'est pas essentiel. Ainsi, le simple établissement de corrélations décrites à (éq.1.31) reproduit l'effet de la mesure, bien qu'aucune irréversibilité, ni même pratique, n'est introduite. Par exemple, l'application d'une porte non contrôlée entre le qubit 1 (contrôle) et 2 (cible) reproduit l'effet d'une mesure du premier qubit si le second qubit n'intervient plus dans son évolution subséquente. Dans cet exemple, le second qubit joue à la fois le rôle de l'appareil de mesure $\mathcal{A}$ puisqu'il est corrélé au système et le rôle de l'environnement $\mathcal{E}$ puisque nous ne tentons pas de le contrôler. Cette procédure est connue sous le nom de *pseudomesure*. Une mesure subséquente du second qubit, en toute fin pratique, ne fait que dévoiler l'état du premier qubit au moment de la pseudomesure. L'instant auquel la réduction du paquet d'onde s'est réellement produite (si réduction il y a) n'est pas pertinente.

Décohérence et calcul quantique

L'effet de l'environnement est de transformer une superposition cohérente des états privilégiés en un mélange statistique de ces derniers. Cela règle le problème de l'absence de phénomènes quantiques à l'échelle macroscopique mais engendre bien des problèmes au niveau de la manipulation de l'information quantique. En effet, le calcul quantique requiert, en général, des superpositions cohérentes. Par exemple, supposons que la base de calcul coïncide avec la base privilégiée et que nous implantons l'algorithme de Simon. Si, avant l'application de la porte f (*cf.* figure 1.4), la superposition $\sqrt{2^{-n}}\sum_j |j\rangle$ est remplacée par le mélange $2^{-n}\sum_j |j\rangle\langle j|$, alors on montre facilement que les résultats des mesures seront un nombre choisi uniformément dans l'ensemble $\{0,\ldots,2^n-1\}$ pour le registre du haut et l'ensemble $\{0,\ldots 2^{n-1}-1\}$ pour celui du bas. Évidemment, ces nombres ne nous sont d'aucune utilité.

Afin de contrer cet effet néfaste de la décohérence, plusieurs techniques ont été mises au point. Les sous-systèmes libres de décohérence utilisent un encodage de

l'information de sorte que l'effet net de l'interaction avec l'environnement n'affecte pas l'information encodée bien que le système soit physiquement perturbé [94]. Il existe également des méthodes actives de corrections d'erreur [84, 87, 44, 57]. Dans ce cas, les perturbations dues à l'environnement sont détectées par des mesures qui n'affectent pas l'information encodée sur le système. À la suite de ces mesures, des corrections peuvent être appliquées si nécessaire. Ces techniques permettent de réduire le taux de décohérence mais n'éliminent pas complètement les effets de l'environnement. Divers auteurs [2, 56, 61, 74] ont évalué une borne sur le taux de décohérence en deça de laquelle le calcul quantique devient praticable.

2 — Histoires consistantes

Dans ce chapitre, nous introduisons le formalisme des histoires consistantes (HC). Initialement proposées par Griffiths [46] comme interprétation de la mécanique quantique, les HC furent par la suite développées davantage et réinterprétées par Omnès [69, 70] puis adaptées à la cosmologie quantique par Gell-Mann et Hartle [39]. Il n'existe pas d'accord commun entre les auteurs tant sur la formulation des conditions de consistances, l'interprétation du formalisme ni même sur la terminologie. Certains auteurs utilisent d'ailleurs histoire décohérente comme synonyme d'HC alors que d'autres y voient une distinction [43, 41].

Nous ne tenterons pas ici de régler ces désaccords puisque nous utilisons les histoires comme un moyen et non comme une fin en soi. Ainsi, l'interprétation rattachée aux HC n'est pas discutée, nous référons aux ouvrages cités ci-haut. Au risque d'empirer la situation, nous empruntons les concepts des divers auteurs et les modelons au langage de l'informatique quantique, bien sûr en nous assurant que le tout soit cohérent. [1]

2.1. Exemple non consistant

Un électron est préparé de sorte que son spin soit orienté dans la direction x, c'est-à-dire $|\uparrow\rangle_x = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$ où la base de référence standard est z. Cet électron traverse un appareil de Stern-Gerlach (S-G 1) dont le gradient de la composante z du champ est orienté selon l'axe z, $\partial B_z/\partial z < 0$. L'effet de ce champ sera de

[1] Selon certains auteurs, la condition de consistance doit uniquement être exigée pour les couples d'histoires (α, β) dont la somme constitue une histoire. Nous passerons sous le silence toutes ces subtilités du formalisme et en présenterons naïvement qu'une version simplifiée. Le lecteur initié aux HC sera probablement en désaccord avec l'attribution des qualificatifs fort, moyen et faible utilisés ici.

coupler le spin de la particule avec sa position. En effet, la composante $|\uparrow\rangle$ du spin se voit couplée avec la trajectoire du haut alors que la composante $|\downarrow\rangle$ se couple avec la trajectoire du bas (voir figure 2.1). L'électron traverse ensuite un

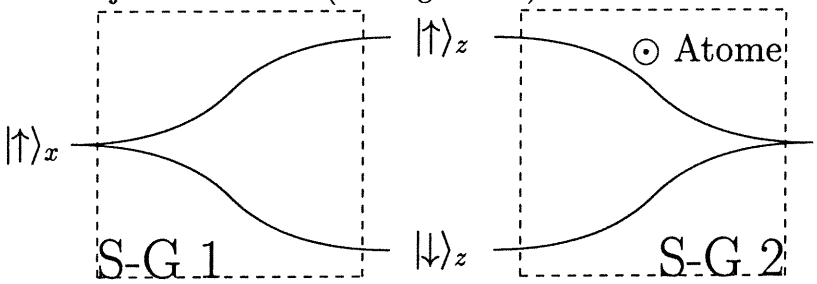

FIG. 2.1 – Représentation schématique du montage expérimental.

second appareil de Stern-Gerlach (S-G 2) dont le gradient de champ est l'opposé du premier, son effet sera donc d'inverser la première transformation. Ainsi, l'état de l'électron à la sortie des deux appareils est le même qu'à son entrée, soit $|\uparrow\rangle_x$. Une mesure subséquente de la projection du spin selon l'axe x donne $\hbar/2$ à coup sûr.

Maintenant, un atome bistable dans le premier niveau excité $|n=1\rangle$ est placé près du parcours supérieur. L'interaction de ce dernier avec l'électron est décrit par l'hamiltonien

$$H_I = g\nu(\boldsymbol{r} - \boldsymbol{r}_A)\sigma_z^{\text{électron}} \otimes (|n=1\rangle\langle n=0| + |n=0\rangle\langle n=1|) \tag{2.1}$$

où g est une constante de couplage, $\boldsymbol{r}_A$ est la position de l'atome et ν est une fonction valant 1 autour de $\mathbf{0}$ et qui devient rapidement nulle lorsqu'on s'en éloigne. En ajustant adéquatement la position de l'atome, de sorte que le temps d'interaction soit $t_0 = \frac{\pi\hbar}{4g}$ (ou plus précisément une action totale de $\frac{\pi\hbar}{4}$), l'état final du système (à la sortie du second appareil de Stern-Gerlach) sera

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow, n=0\rangle + |\downarrow, n=1\rangle). \tag{2.2}$$

Cette fois-ci, la mesure de la projection du spin selon l'axe x est non déterministe :

$$Pr(\hbar/2) = |\langle\psi|\uparrow_x, n=0\rangle|^2 + |\langle\psi|\uparrow_x, n=1\rangle|^2 = \frac{1}{2} \tag{2.3}$$

$$Pr(-\hbar/2) = |\langle\psi|\downarrow_x, n=0\rangle|^2 + |\langle\psi|\downarrow_x, n=1\rangle|^2 = \frac{1}{2}, \tag{2.4}$$

résultat qui diffère des prédictions en l'absence de l'atome.

Cette différence est causée par la possibilité qu'offre l'atome de déterminer lequel des deux trajets a été emprunté par l'électron. Cette connaissance nous permet d'inférer la probabilité finale selon la règle de somme

$$\begin{aligned} Pr(\hbar/2) &= Pr(\hbar/2|\uparrow_z)Pr(\uparrow_z) + Pr(\hbar/2|\downarrow_z)Pr(\downarrow_z) && (2.5) \\ &= \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{2}. && (2.6) \end{aligned}$$

Classiquement, cette prédiction serait valable indépendamment de la présence ou de l'absence de l'atome, c'est-à-dire indépendamment de l'existence d'un événement intermédiaire à la mesure finale.

C'est l'interférence entre les deux trajectoires qui est responsable du désaccord entre le résultat classique et le résultat quantique. À la suite de son passage dans le premier appareil de Stern-Gerlach, l'électron est en superposition cohérente des deux trajectoires ; *il n'existe pas de probabilité qu'il soit dans l'une ou l'autre des trajectoires, sauf si nous tentons de le déterminer à l'aide d'une mesure.* C'est exactement ici qu'entre en jeu l'atome. L'interaction entre cette dernière et l'électron reproduit l'effet d'un ou-exclusif. Comme mentionné à la section 1.5.5, cela est suffisant pour mimer l'effet d'une mesure puisqu'à la suite de cette interaction, l'atome n'influence plus l'évolution de l'électron.[2] En oubliant la présence de l'atome, l'état de l'électron après l'interaction est une mixture $\rho = \frac{1}{2}(|\uparrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow|)$, alors qu'en absence de l'atome, son état est pur $|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$. Puisque ces états diffèrent, il est tout à fait naturel que les statistiques qu'on puisse en tirer ne soient pas les mêmes.

L'exemple précédent nous montre que la possibilité de calculer des probabilités pour une mesure éventuelle n'implique pas l'existence de ces probabilités. En effet, les déductions logiques qu'on en tire, telle l'inférence statistique, sont erronées si l'existence de ces probabilités est tenue pour acquise. Le formalisme que nous présentons dans ce chapitre nous permet de décider dans quelles situations les règles de la théorie des probabilités classiques s'appliquent, c'est-à-dire quand

[2] Techniquement, ce type de mesure est connu sous « pseudomesure » ou plus approprié « mesure non destructive ».

peut-on assigner une probabilité à un événement.

2.2. Domaine classique

Au risque de se répéter, l'absence de phénomènes quantiques à l'échelle macroscopique est fondamentalement incomprise. Ce monde est dit classique, il se comporte selon les équations du mouvement d'Einstein, ou de Newton dans le cas non relativiste. Qu'est-ce qui caractérise ce domaine classique ? Voila la question qui est au centre du fondement de la théorie quantique. Le domaine classique se reconnaît simplement, mais ne possède pas de définition formelle. [3]

Les principales caractéristiques du domaine classique sont l'absence d'interférence et de superpositions d'états classiques et le déterminisme de son évolution. La première caractéristique est formalisée à l'aide des HC, sujet de la prochaine section. Effectivement, l'absence d'interférence mène à la validité des résultats de la théorie des probabilités. Ainsi, les règles de consistance traduisent non pas l'absence totale d'interférence mais l'absence d'interférence physiquement détectable. De plus, les HC permettent d'expliquer, dans certaines situations, le déterminisme du domaine classique [50]. Nous n'aborderons malheureusement pas cet aspect des HC ici.

La seconde caractéristique est plus difficilement formalisable puisqu'elle est en quelque sorte une autoréférence : *le domaine classique est l'ensemble des états classiques*! Le fameux chat de Schrödinger constitue un exemple d'une telle superposition. Tous conviendront que jamais dans la nature un chat n'est en superposition d'être mort et vivant : tout chat est soit mort, soit vivant. Pourtant, Schrödinger a décrit un montage expérimental qui, en principe, devrait mener à un tel état.

[3] Robert Laughlin, prix Nobel de Physique 1998, faisait face à la même situation lorsque venait le temps de décrire ce qu'est le bruit dans des mesures expérimentales. « *Noise is a lot like pornography : I can't tell you exactly what it is but I know it when I see it* ». Conférence donnée à l'Université de Sherbrooke, octobre 1999.

Règles de supersélection

Les règles de sélection de la mécanique quantique interdisent certaines transitions. Ces règles sont dérivées de principes fondamentaux telles des symétries de la nature. Par exemple, il est impossible qu'un système isolé de charge totale q sous l'effet des forces de la nature ait, à un temps subséquent, une charge $q' \neq q$. Cette conservation de la charge découle de la forme des interactions fondamentales de la nature, en particulier de l'invariance de jauge de la force électromagnétique. Pourtant, cette transition est mathématiquement possible puisqu'elle peut découler d'une évolution unitaire ; c'est la nature qui s'y oppose.

Les règles de supersélection sont une généralisation statique des règles de sélections dynamiques. Elles proscrivent l'existence même de certains états. Par exemple, un système physique ne peut se trouver en une superposition de charge totale.[4] Cette règle est obtenue en combinant la conservation de la charge à une condition initiale de l'univers très particulière. De telles règles ne peuvent être dérivées de principes fondamentaux, elles ne peuvent qu'être postulées.

Il est tentant de postuler des règles de supersélection interdisant la superposition d'états classiques. Plusieurs obstacles nuisent à l'énoncé de ce postulat. Premièrement, il n'existe pas de règle de sélection dynamique associée à cette supersélection comme le montre l'exemple du chat de Schrödinger. Deuxièmement, la formulation du postulat exige une définition précise d'*état classique*, ce qui est un peu le but de tout cet exercice ! Ainsi, le mieux que l'on puisse faire est de formuler des règles de supersélection induites par l'environnement [96] en espérant qu'elles englobent tout le domaine classique. Ces règles reposent donc sur une impossibilité de contrôler l'environnement : la dynamique marginale du sous-système en interaction avec un environnement ne peut mener à une superposition *d'états classiques* (la base privilégiée *cf.* section 1.5). Néanmoins, cette supersélection n'est pas fondamentale et ne repose pas sur une seule hypothèse tel l'état initial de l'univers. De plus, lorsque des précautions formidables sont prises afin d'isoler le

[4] La théorie BCS de la supraconductivité conventionnelle fait intervenir des superpositions de charge, mais ce ne sont pas des charges totales : les électrons de valence sont en contact avec une mer de Fermi.

système de l'environnement, certaines superpositions macroscopiques quantiques sont observées (voir par exemple [65]).

2.3. Formalisme

Cadre logique

L'idée de base de la théorie des HC est de fixer un cadre logique cohérent au système à l'étude. À l'intérieur de ce cadre, toute déduction logique portant sur les événements possibles est valable. Ainsi, un cadre logique est un ensemble d'événements logiquement compatibles. Un événement est la spécification d'un sous-espace et d'un temps : «le système physique est dans le sous-espace $\mathcal{W}$ au temps t» constitue un événement. En général, on caractérise le sous-espace à l'aide du projecteur qui lui est associé.

Le montage expérimental de la figure 2.1 fournit un contre-exemple de cadre logique cohérent. En notant t_0 le temps où l'électron se trouve entre les deux appareils de S-G et t_1 le temps après lequel il a franchi le second, les événements associant une valeur au spin de l'électron selon l'axe z au temps t_0 et à son spin selon x au temps t_1 sont logiquement incompatibles.

Par contre, ce que nous observons dans le monde classique, c'est-à-dire les sous-espaces ressortant des règles de supersélection induites par l'environnement, fait toujours partie d'un cadre logique consistant. Ceci est du au fait que l'environnement détruit continuellement la cohérence entre les états classiques. Les systèmes se retrouvent ainsi dans des mélanges statistiques d'états classiques, donc aucune interférence n'est présente dans ce cadre logique. Par exemple, lorsque l'atome (environnement) est introduit entre les deux appareils de S-G, les déductions logiques mènent à des conclusions valides. Les inférences logiques faisant référence aux événements qui sortent d'un cadre sont vouées à l'échec.

Tout système, qu'il soit classique ou quantique, possède une infinité de cadres logiques cohérent. Toute déduction logique doit être faite à l'intérieur d'un seul cadre logique consistant fixe. Les conclusions tirées de cadres cohérent différents peuvent être en désaccord.

Histoire

Une histoire est une suite d'événements, c'est-à-dire un ensemble de projecteurs ordonnés dans le temps. En voici la définition formelle.

Un ensemble exhaustif de projecteurs exclusifs (EEPE) est un ensemble de projecteurs $\hat{\sigma} = \{\hat{P}_\alpha\}_{\alpha=1,\dots,m}$ qui satisfait aux deux conditions

$$\sum_{\alpha=1}^{m} \hat{P}_\alpha = \mathbb{1} \quad \text{et} \quad \hat{P}_\alpha \hat{P}_\beta = \delta_{\alpha\beta} \hat{P}_\alpha. \tag{2.7}$$

Cet ensemble est exhaustif puisque l'union des sous-espaces est l'espace complet et exclusif puisque l'intersection entre les sous-espaces est nul.

Une telle décomposition de l'identité est effectuée à n temps différents $t_1 < t_2 < \dots < t_n$, définissant ainsi n EEPE indépendants : $\sigma^{(j)}(t_j) = \{P_{\alpha_j}^{(j)}(t_j)\}_{\alpha_j=1,\dots m_j}$. Les projecteurs sont maintenant dans la représentation de Heisenberg $P(t) = U^\dagger(t,0)\hat{P}U(t,0)$, d'où la perte de leur chapeau ! Puisqu'on ne risque aucune confusion, la dépendance explicite en temps sera dorénavant omise puisqu'elle est redondante : $P_\alpha^{(j)} = P_\alpha^{(j)}(t_j)$.

Une histoire est construite en choisissant un indice de projecteur α_j dans chaque EEPE $\sigma^{(j)}$. À cette histoire est associé un opérateur $C_\alpha = P_{\alpha_1}^{(1)} P_{\alpha_2}^{(2)} \dots P_{\alpha_n}^{(n)}$ où α est un vecteur d'indices de n dimensions $\alpha = (\alpha_1, \dots, \alpha_n)$.

Une famille exhaustive d'histoires disjointes (FEHD) est obtenue en choisissant un indice α_j dans chaque EEPE $\sigma^{(j)}$, de toutes les façons possibles. Elle est donc la famille des histoires engendrées par les

$$N = \prod_{j=1}^{n} m_j \tag{2.8}$$

vecteurs d'indices de n dimension. Elle est exhaustive puisque les N opérateurs d'histoire C_α somment à l'identité. Les histoires sont disjointes puisqu'elles diffèrent toutes en au moins un temps.

Nous choisissons d'inclure un état initial du système ρ dans la famille d'histoire, malgré le fait que les matrices de densité représentant des états mixtes ne soient pas des projecteurs. Toutes les histoires de la famille débutent dans cet état. En conséquence, nous notons une famille d'histoires par $\mathcal{S} = \{\rho, \sigma^{(1)}, \dots, \sigma^{(n)}\}$.

Fonction de cohérence

Connaissant l'état initial du système ρ, la probabilité associée à une histoire α, *i.e.* la probabilité que le système soit dans le spectre de $P^{(1)}_{\alpha_1}$ au temps t_1, dans le spectre de $P^{(2)}_{\alpha_2}$ au temps t_2, *etc.* est donnée par

$$\begin{aligned} Pr(\alpha) &= Pr(\alpha_1, \alpha_2, \ldots, \alpha_n) && (2.9)\\ &= Tr\{P^{(n)}_{\alpha_n} \ldots P^{(2)}_{\alpha_2} P^{(1)}_{\alpha_1} \rho P^{(1)}_{\alpha_1} P^{(2)}_{\alpha_2} \ldots P^{(n)}_{\alpha_n}\} && (2.10)\\ &= Tr\{C^{\dagger}_{\alpha} \rho C_{\alpha}\} && (2.11) \end{aligned}$$

que nous pouvons simplement dériver des postulats 4, 5 et 6.

Cette dernière expression correspond à un terme diagonal de la fonction de cohérence $D : \mathcal{S} \times \mathcal{S} \mapsto \mathbb{C}$ qui est définie par

$$D(\alpha;\beta) = Tr\{C^{\dagger}_{\alpha} \rho C_{\beta}\} \tag{2.12}$$

qui forme une matrice hermitienne N par N, *cf.* (éq. 2.8). On se convainc facilement que les termes diagonaux de cette fonction correspondent à des probabilités. L'interprétation des termes hors diagonaux demande un peu plus de réflexion.

Intégrales de Feynman

Voici, pour les initiés aux intégrales de Feynman, une autre façon de décrire la fonction de cohérence qui est due à Gell-Mann et Hartle [39] et qui risque d'éveiller une plus forte intuition. Pour les non-initiés, nous référons l'ouvrage original de Feynman et Hibbs [38]. Afin d'alléger la notation, supposons que le système soit restreint à se mouvoir dans une seule dimension, que nous supposerons continue. Dans cet espace, les projecteurs $\hat{P}_j$ peuvent êtres représentés par des intervalles Δ_j d'une variable canonique q choisie adéquatement. Il s'en suit que la fonction de cohérence $D(\alpha;\beta)$ des histoires $\alpha = (\Delta_1, \Delta_2, \ldots \Delta_n)$ et $\beta = (\Delta'_1, \Delta'_2, \ldots \Delta'_n)$ est donnée par

$$D(\alpha;\beta) = \int_{\alpha} \delta q(t) \int_{\beta} \delta q'(t)\ \delta(q(t_f) - q'(t_f)) \exp i\left\{I[q(t)] - I[q'(t)]\right\} \rho(q'_0, q_0) \tag{2.13}$$

où l'on ne doit pas confondre l'intégrant δq de la distribution de Dirac $\delta(q)$. L'intégrale fonctionnelle doit être effectuée selon la prescription suivante (*cf.* figure 2.2) : on intègre sur tous les chemins $q(t)$ et $q'(t)$ qui débutent en q_0 et q'_0 respectivement, passent par les intervalles Δ_i et Δ'_i respectivement et aboutissent en un point commun q_f. L'intégrale est complétée en intégrant sur q_0, q'_0 et q_f. La fonctionnelle I est l'action. Cette représentation de la fonction de cohérence fait plus clairement ressortir l'interprétation de la fonction de cohérence : elle quantifie l'interférence entre les différentes histoires.

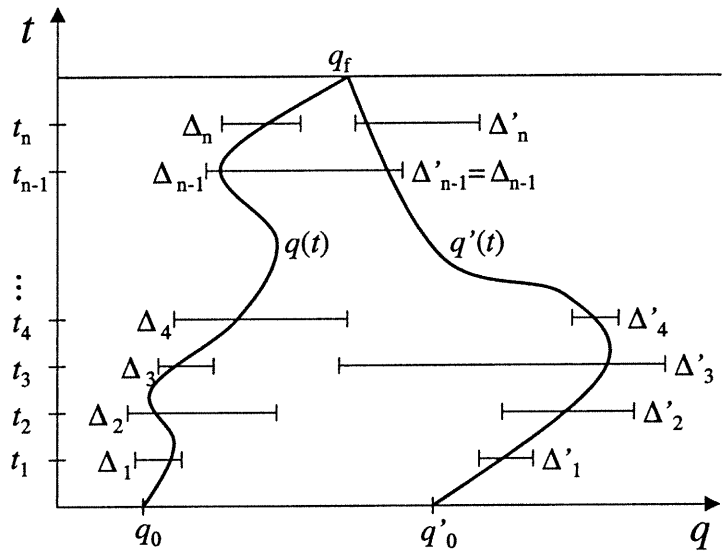

FIG. 2.2 – Intégrales de Feynman pour la fonction de cohérence.

2.4. Conditions de consistance

Le cadre logique constitué des n ensembles de projecteurs $\sigma^{(j)}$ est consistant, c'est-à-dire qu'il permet d'utiliser les règles d'inférence logiques en toute quiétude, s'il obéit à la condition nécessaire et suffisante suivante :

$$Re\{D(\alpha;\beta)\} = Pr(\alpha)\delta_{\alpha\beta} \quad \forall \alpha, \beta \in \mathcal{S} \tag{2.14}$$

où Re est la partie réelle.

Cette condition est connue sous le nom de condition de consistance faible. Elle reflète une insensibilité mutuelle des mesures. Les statistiques de la mesure $\sigma^{(j)}$ au temps t_j sont les mêmes peu importe si la mesure $\sigma^{(k)}$ au temps t_k est réalisée ou non. En d'autres termes, $Pr(\alpha_j) = \sum_{\alpha_k} Pr(\alpha_k, \alpha_j) = \sum_{\alpha_k} Pr(\alpha_j|\alpha_k)Pr(\alpha_k)$: les probabilités associées aux événements du cadre logique sont réelles. C'est en fait cette dernière égalité qui définit un cadre logique cohérent.

Observables commutantes

Les ouvrages généraux traitant sur la théorie quantique enseignent que seules les observables $\mathcal{O}_j$ commutantes peuvent êtres mesurées simultanément sans quoi les statistiques des résultats seront faussées. Si les mesures ne sont pas effectuées simultanément mais toujours sur un même système, alors ce sont les observables de la représentation de Heisenberg $\mathcal{O}_j(t_j)$ qui doivent commuter, où t_j est le temps auquel la mesure de $\mathcal{O}_j$ est effectuée. Afin de s'en convaincre, il suffit d'étudier l'évolution des particules dans un sélecteur de vitesse.[5] Le montage expérimental est fort simple : un faisceau de particules chargées se propage en direction x. On plonge ce faisceau dans un champ magnétique orienté selon l'axe y. La force résultant sur la particule j est $\boldsymbol{F}_j = q\boldsymbol{v}_j \times \boldsymbol{B}$ où nous avons supposé que la charge est la même pour chaque particule. L'effet de cette force sera une rotation de la direction de propagation de chaque particule autour de l'axe y. L'angle de rotation θ_j est proportionnel à la vitesse de la particule $|\boldsymbol{v}_j|$. Ainsi, la mesure de la position des particules en x à la suite de leur interaction avec le champ magnétique nous informe de leur vitesse selon x avant cette interaction. Puisqu'une mesure de position est incompatible avec une mesure de vitesse en raison de la relation d'incertitude de Heisenberg, nous en venons à la conclusion que les mesures de l'observable X avant et après l'interaction avec le champ magnétique sont logiquement incompatibles.

Soit $\sigma^{(j)}$, l'ensemble des projecteurs associés à l'observable $\mathcal{O}_j(t_j)$ (*cf.* cinquième postulat). Afin d'alléger la notation, supposons que nous ne désirions me-

[5] Nous nous contentons ici d'un traitement semi classique, le traitement quantique étant moins intuitif.

surer que deux observables $\mathcal{O}_0$ et $\mathcal{O}_1$. La fonction de cohérence associée à ces observables est

$$\begin{aligned} D(\alpha,\beta) &= Tr\{P^{(1)}_{\alpha_1}P^{(0)}_{\alpha_0}\rho P^{(0)}_{\beta_0}P^{(1)}_{\beta_1}\} && (2.15)\\ &= Tr\{\rho P^{(0)}_{\beta_0}P^{(1)}_{\beta_1}P^{(1)}_{\alpha_1}P^{(0)}_{\alpha_0}\} && (2.16)\\ &= \delta_{\alpha_0\beta_0}\delta_{\alpha_1\beta_1}Tr\{\rho P^{(0)}_{\alpha_0}P^{(1)}_{\alpha_1}\} \\ &+ \delta_{\alpha_1\beta_1}Tr\{\rho[P^{(0)}_{\beta_0},P^{(1)}_{\alpha_1}]P^{(0)}_{\alpha_0}\} && (2.17)\end{aligned}$$

donc les histoires construites à partir des valeurs de ces observables sont automatiquement consistantes, peu importe l'état initial, si $[P^{(0)}_{\beta_0},P^{(1)}_{\alpha_1}]=0 \ \ \forall(\alpha_1,\beta_0)$ c'est-à-dire si $[\mathcal{O}_0(t_0),\mathcal{O}_1(t_1)]=0$, comme il se doit. L'égalité (éq.2.16) provient simplement de la cyclicité de la trace alors que (éq.2.17) est due à l'orthogonalité des sous-espaces propres d'un opérateur hermitien.

La condition faible (éq.2.14) est donc automatiquement satisfaite lorsque les observables commutent. En fait, la mesure d'observables commutantes correspond à un raffinement de la partition de l'espace des états. Une première mesure apporte une partition de l'espace des états en sous-espaces mutuellement orthogonaux. Une seconde mesure «compatible» avec la première va simplement diviser davantage chacun des sous-espaces et ainsi de suite. Ce processus mène à la formation d'un ECOC que nous avons décrit à la section 1.1.3, c'est-à-dire une observable effective qui partitionne entièrement l'espace des états.

La commutation des observables nous assure que la condition de consistance sera satisfaite ; l'inverse n'est généralement pas vrai.

Théorème 1. *La règle de consistance faible implique la commutation des observables si nous exigeons qu'elle soit satisfaite pour tous les états initiaux possibles.*

Preuve. Nous allons montrer que si $ReD(\alpha;\beta)=0 \ \forall\, \alpha\neq\beta$ et tout choix d'état initial possible, alors les projecteurs utilisés afin de construire les familles commutent. Il est général de supposer que les histoires sont constituées de deux événements en sommant sur toutes les possibilités des événements intermédiaires. De cette façon, nous pouvons démontrer que toute paire de projecteurs commutent.

Soit $\mathcal{A}$ et $\mathcal{B}$, deux observables auxquelles sont associées les projecteurs $\{Q_j\}$

et $\{P_j\}$ respectivement que l'on représente comme suit :

$$Q_j = \sum_{i \in A_j} |a_i\rangle\langle a_i| \quad et \quad P_j = \sum_{i \in B_j} |b_i\rangle\langle b_i| \tag{2.18}$$

c.f. quatrième postulat. La condition de consistance faible associée à la mesure de $\mathcal{A}$ suivie de la mesure de $\mathcal{B}$ pour un état initial $|\psi\rangle = \sum_j \alpha_j |a_j\rangle$ s'écrit, après un peu d'algèbre

$$Re\left[\sum_{j \in A_m i \in A_n} \alpha_j^* \langle a_j|P_\ell|a_i\rangle \alpha_i\right] = \delta_{mn} Pr(m,\ell) \tag{2.19}$$

donc pour le cas particulier $\ell = 1$, $m = 1$ et $n = 2$, $X = \sum_{j \in A_1 i \in A_2} \alpha_j^* \langle a_j|P_1|a_i\rangle \alpha_i$ est imaginaire. Puisque cette condition doit être satisfaite pour tout $|\psi\rangle$, choisissons α_1 $(1 \in A_1)$ de sorte que $Y = \sum_{i \in A_2} \alpha_1^* \langle a_1|P_1|a_i\rangle \alpha_i$ soit réel. Construisons un autre état initial $|\psi'\rangle = \sum_j \beta_j |a_j\rangle$ tel que $\beta_1 = i\alpha_1$ et $\beta_j = \alpha_j \; \forall j > 1$. Pour cet état, la condition de consistance pour notre choix particulier de ℓ, m et n est

$$Re\left[\sum_{j \in A_1 i \in A_2} \beta_j^* \langle a_j|P_1|a_i\rangle \alpha_i\right] = Re\,[X - (1+i)Y] = 0, \tag{2.20}$$

ce qui est uniquement possible lorsque $Y = 0$. Cette construction étant valable pour toutes les combinaisons de Q_i et P_j, on en vient à la conclusion que $\langle a_i|P_k|a_j\rangle = \delta_{ij} \;\; \forall \; (i,j,k)$ donc que $[Q_i, P_j] = 0 \; \forall \; (i,j)$. □

Lorsque la condition de consistance est imposée uniquement pour un sous-ensemble d'états initiaux, situation typique en informatique quantique, alors il n'est pas nécessaire que les observables commutent. Ceci est valable même lorsque l'ensemble d'états forme une base. Nous verrons des exemples un peu plus loin (*e.g.* section 4.2.2).

Conditions plus restrictives

La condition (éq.2.14) est suffisante afin d'assurer la validité de la logique classique. Par contre, lorsque les HC sont utilisées dans le but de caractériser le domaine classique, cette condition n'est plus suffisante [39]. Afin de combler cette lacune, des conditions plus restrictives ont vu le jour. Sans vouloir entrer

dans le détail des démarches qui ont mené aux différents résultats, mentionnons quelques autres conditions rencontrées dans la littérature. La condition de consistance moyenne [39] est simplement obtenue en exigeant que les termes hors diagonaux de la fonction de cohérence soient nuls

$$D(\alpha;\beta) = Pr(\alpha)\delta_{\alpha\beta}, \tag{2.21}$$

plutôt que uniquement la partie réelle.

Encore plus restrictive est la condition de consistance forte [42] qui exige que pour chaque opérateur d'histoire C_α, il existe un projecteur R_α dont les effets sur l'état du système soient identiques :

$$\forall C_\alpha \quad \exists R_\alpha \text{ tel que } C_\alpha\rho = R_\alpha\rho \text{ et } R_\alpha^2 = R_\alpha. \tag{2.22}$$

Cette condition est intimement liée à la notion de décohérence de la section 1.5 puisqu'elle implique l'existence d'information sur le passé du système [40], ce qui est assuré par la présence de perturbations infligées à l'environnement par le système. Il est à noter qu'un opérateur d'histoire qui est le produit de n projecteurs n'est, en général, pas un projecteur.

La condition de consistance ordonnée de Kent [55] est d'autant plus restrictive mais, selon notre opinion, n'est pas bien motivée puisqu'elle impose des conditions sur des événements appartenant à différents cadres logiques, ce qui ne possède pas de sens physique selon l'interprétation originale.

Les mesures composées d'observables commutantes obéissent à toutes ces conditions. En fait, la commutation des observables est sans doute la condition de consistance la plus restrictive que l'on puisse imposer.

Conditions initiales

Les conditions de consistance imposent des restrictions *dynamiques* sur les systèmes. Soit $\mathcal{S} = \{\rho, \sigma_1, \ldots, \sigma_n\}$ une famille consistante. On se convainc aisément qu'une transformation unitaire globale $\mathcal{S} \mapsto \mathcal{S}'$, *i.e.* $\rho \mapsto U\rho U^\dagger$ et $P_{\alpha_j}^{(j)} \mapsto U^\dagger P_{\alpha_j}^{(j)} U$, n'affecte pas la fonction de cohérence (éq.2.12). Par exemple, si l'observation de la lune à la position $\boldsymbol{r}_1 = (r, \theta, \phi)$ aujourd'hui sachant qu'elle était hier à la position

$\boldsymbol{r}_0 = (r, \theta, \phi + \pi)$ est consistante, alors son observation aujourd'hui dans l'état $\frac{1}{\sqrt{2}}(|\boldsymbol{r}_0\rangle + |\boldsymbol{r}_1\rangle)$ conditionnellement à ce qu'elle était hier dans l'état $\frac{1}{\sqrt{2}}(|\boldsymbol{r}_0\rangle - |\boldsymbol{r}_1\rangle)$ est également consistante.

Il s'en suit que les conditions de consistance seules ne peuvent pas déterminer le domaine classique. Elles servent plutôt de règles de sélection dynamiques. Contrairement aux règles de conservation découlant de symétries fondamentales de la nature, la règle de sélection de consistance est introduite *ad hoc*. Afin d'obtenir une règle de supersélection qui, possiblement, identifie le domaine classique, il est nécessaire d'ajouter des conditions initiales sur la fonction d'onde de l'univers.

2.5. Trajectoires consistantes

Classiquement, l'histoire d'un système est décrite par une trajectoire dans l'espace des phases, c'est-à-dire dans un diagramme *impulsion vs position*. En mécanique quantique, une telle description n'existe pas puisque les observables $\boldsymbol{P}$ et $\boldsymbol{R}$ sont incompatibles[6]. Les trajectoires consistantes introduites par Griffiths [47] jouent un rôle analogue aux trajectoires classiques.

Grosso modo, une trajectoire est une histoire constituée entièrement de projecteurs de rang 1. En général, nous choisissons de travailler dans la représentation de Schrödinger. Les projecteurs de rang 1 peuvent s'exprimer sous la forme $\hat{P}^{(j)}_{\alpha_j} = |\phi^{(j)}_{\alpha_j}\rangle\langle\phi^{(j)}_{\alpha_j}|$. Ainsi, un ensemble $\hat{\sigma}$ exhaustif de projecteurs exclusifs de rang 1 correspond à un choix de base, chaque vecteur de la base étant associé à un projecteur.

La condition de consistance pour une famille exhaustive de trajectoires disjointes peut se vérifier à l'aide d'un graphe. Les sommets du graphe sont disposés sur une grille rectangulaire comportant n colonnes (n étant le nombre de temps t_j dans la famille d'histoires) et Ω lignes (Ω étant la dimension de l'espace de Hilbert). Ainsi, le sommet (j, α_j) est associé au vecteur de base (ou projecteur) $|\phi^{(j)}_{\alpha_j}\rangle$ (voir figure 2.3). Seuls les sommets de colonnes adjacentes peuvent êtres reliés par

[6] La distribution de Wigner joue un rôle similaire à une distribution classique dans l'espace des phases, mais ne possède pas toutes les caractéristiques d'une distribution de probabilité.

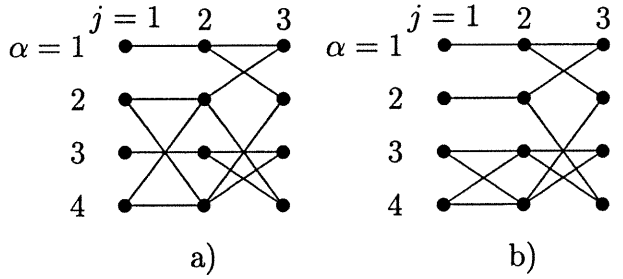

FIG. 2.3 – Exemple de graphes représentant des trajectoires a) consistantes b) non consistantes en raison des deux chemins reliant (1,3) à (3,3). L'axe horizontale représente le temps t_j alors que l'axe verticale représente les différents choix de projecteurs.

une arête. La condition pour que deux sommets soient reliés est

$$G_{\alpha_j \alpha_{j+1}}(t_j, t_{j+1}) \equiv \langle \phi^{(j+1)}_{\alpha_{j+1}} | U(t_{j+1}, t_j) | \phi^{(j)}_{\alpha_j} \rangle \neq 0. \tag{2.23}$$

L'expression de gauche de (éq.2.23) porte le nom de propagateur ou fonction de Green.

Sur le graphe, une trajectoire est donc représentée par un chemin orienté de la gauche vers la droite. La condition de consistance moyenne (éq.2.21) se traduit sur le graphe par : *Il y a au plus une trajectoire reliant deux sommets.* Cela constitue un exercice élémentaire de démontrer l'équivalence des deux formulations lorsque les projecteurs sont de rang 1.

L'exemple a) de la figure 2.3 représente un ensemble de projecteurs consistant puisqu'il y a au plus une trajectoire reliant deux sommets. Cependant, une légère modification de l'opérateur d'évolution $U(t_2, t_1)$ représentée à la figure 2.3 b) rend la famille inconsistante puisque deux trajectoires relient les sommets (1,3) et (3,3) ainsi que (1,4) et (3,3).

L'intérêt d'une analyse de graphe est, à première vue, limité puisqu'elle est restreinte aux familles composées de projecteurs de rang 1. Néanmoins, nous montrerons au prochain chapitre que l'analyse par graphe s'étend au cas où les projecteurs sont de rangs quelconques lorsque l'état initial est pur, situation typique en informatique quantique théorique.

3 — Histoires consistantes en informatique quantique

Ce chapitre établit un parallèle entre les deux chapitres précédents. On y montre comment les histoires consistantes peuvent être utiles à l'analyse d'un algorithme ou d'un protocole quantique. L'intérêt d'une telle analyse sera d'abord fondé sur des motifs fondamentaux, mais le chapitre 4 y apportera également certains motifs plus pratiques.

Certaines modifications du formalisme présenté au chapitre précédent seront également de mise. En particulier, nous verrons comment régler les obstacles mentionnés à la section 2.2, c'est-à-dire comment formuler des règles de supersélection lorsque le système à l'étude sert uniquement de support à l'information quantique. La notion d'HC sera généralisée afin d'incorporer la possibilité de processus de décision par des êtres intelligents au cours de l'évolution du système. Finalement, certains théorèmes généraux sur la structure des histoires consistantes seront établis.

3.1. Motivation

Les quelques exploits de l'informatique quantique décrits à la section 1.3 sont suffisants pour motiver son utilisation dans certaines situations. Malheureusement, la réalisation expérimentale de ces protocoles est extrêmement difficile. Ce commentaire s'applique même à la cryptographie quantique qui, déjà, est réalisée en laboratoire : les dispositifs qui réalisent cette tâche n'offrent pas une sécurité inconditionnelle puisqu'ils diffèrent des propositions théoriques. En fait, la cryptographie quantique inconditionnellement sécuritaire n'est possible, avec les technologies actuelles, qu'à courte distance et à faible débit [20]. En particulier, cette différence est attribuée à la difficulté technique de construire des détecteurs et des sources à photon unique.

Pour ce qui est des calculs quantiques, le plus gros ordinateur quantique construit à ce jour possède sept qubits [59], ce qui est facilement simulable sur l'ordinateur utilisé pour rédiger ce mémoire.

Plusieurs obstacles sont rencontrés lors de la construction de calculateurs quantiques. D'abord, l'impossibilité d'isoler parfaitement un sous-système quantique du reste de l'univers mène au processus de décohérence décrit à la section 1.5. Les précieuses superpositions quantiques sont alors remplaçées par de vulgaires mélanges statistiques ce qui, en général, altère les résultats du processus. En plus du problème de décohérence, le simple fait d'augmenter la taille du calculateur apporte de nombreuses difficultés. En particulier, l'interaction naturelle entre les diverses composantes de l'ordinateur se complexifie à un tel point que leur manipulation cohérente devient, dans de nombreux modèles, irréalisable avec les technologies actuelles.

Utilisation judicieuse

Ces limitations ne sont pas fondamentales puisqu'un nombre de solutions théoriques existent pour chacune d'entre elles. Néanmoins, des efforts considérables devraient êtres déployés afin de s'assurer que l'utilisation que nous faisons de ces calculateurs est essentielle. En particulier, nous devrions nous assurer qu'aucun calculateur classique ne puisse accomplir la même tâche sans nécessiter un temps considérablement plus grand. Idéalement, seulement les problèmes appartenant à des classes de complexité quantique et classique différentes devraient nécessiter l'intervention d'un calculateur quantique.

Toutefois, nous ne connaissons pas de tel problème, sauf en complexité de communication. Le problème de factorisation est soupçonné d'appartenir à différentes classes classique et quantique mais nous n'en possédons aucune preuve. Ainsi, nous devons nous contenter de «classes de complexité effectives», c'est-à-dire de celles qui correspondes aux meilleurs algorithmes connus.

L'utilisation judicieuse de la théorie quantique à des fins calculatoires est intimement liée à la question : *Quel est l'ingrédient qui permet à la mécanique quantique de surpasser la mécanique classique en puissance de calcul, le cas échéant ?*

En effet, si nous savions lesquelles des caractéristiques du monde quantique parmi l'enchevêtrement, la superposition d'états et l'interférence lui acquièrent ces avantages, nous serions en mesure de juger de l'utilité d'un processus quantique.

Simulation classique

La possibilité de simuler efficacement un processus quantique à l'aide d'un calculateur classique est de toute évidence un argument suffisant pour proscrire l'utilisation du système quantique. Tout type de calculateur classique doit être considéré ici. Par exemple, l'utilisation d'ondes électromagnétiques, de pendules, de mouvement angulaire classique ou d'ondes à la surface de l'eau peuvent parfois expliquer certains comportements qui semblent, à prime abord, quantiques. Néanmoins, Feynman a conjecturé que la simulation de systèmes quantiques demande des ressources exponentielles. *Grosso modo*, son argument se rattache à la croissance exponentielle des matrices servant à décrire l'état et l'évolution des systèmes. Toutefois, cette intuition est toujours en quête d'une preuve ; la simulation de certains systèmes quantiques appartient à la liste des problèmes qui diffèrent de *classe de complexité effective* puisque nous savons comment simuler efficacement une certaine classe de systèmes physiques à l'aide de calculateur quantiques, (*cf.* section 1.3.4) alors que nos meilleurs algorithmes classiques sont de complexité exponentielle.

Malgré cette croissance exponentielle des matrices, une simulation classique n'est pas *nécessairement* inaccessible. Aharonov et Ben-Or [2] ont démontré que lorsque le calculateur quantique subit suffisamment de décohérence, la simulation classique devient possible. Cette transition entre un algorithme *connu* efficace et inefficace est caractérisé par le taux de décohérence η. Ce résultat se traduit par la triste constatation que lorsque le taux de décohérence est trop élevé, aucun avantage calculatoire ne peut être tiré du monde quantique.

Systèmes hybrides

La possibilité qu'uniquement une partie d'un processus quantique puisse être simulée ou substituée par du calcul classique est également à considérer. L'algo-

rithme de Simon fournit un bon exemple d'un tel *système hybride* puisque l'ordinateur quantique sert uniquement à trouver des contraintes linéaires qui seront par la suite traitées classiquement. L'algorithme de Shor est également hybride. Nous ne voulons pas entrer dans les détails ici, mais une grande partie de l'algorithme de factorisation repose sur l'analyse classique des données de l'ordinateur quantique. Cleve et Watrous [23] ont réduit la profondeur du calcul quantique de polynomial à logarithmique en introduisant un pré-calcul classique ainsi que d'avantage d'analyses post-calculatoires. Cela indique que l'algorithme original de factorisation tel que proposé par Shor n'est peut-être pas entièrement fondamentalement quantique.

Mesure de classicalité

Ces idées peuvent servir à définir une mesure de *classicalité* d'un algorithme quantique. Par exemple, le coût optimal de simulation classique d'un processus quantique donne une indication de l'importance de ses caractéristiques quantiques. Si aucun coût supplémentaire n'est associé à cette simulation, alors le processus est purement classique, du moins d'un point de vue calculatoire.

De même, l'utilisation d'ordinateur hybride classique quantique peut servir à définir la classicalité d'un algorithme. Par exemple, nous pourrions conclure que seulement une fraction logarithmique de l'algorithme original de Shor est quantique. Cependant, une certaine prudence s'impose puisque plusieurs mesures servent à définir la «grandeur» d'un calcul, la profondeur n'est peut-être pas la mesure idéale dans cette situation.

L'approche que nous proposons va bien au-delà des deux idées mentionnées ci-haut. Elle constitue en une substitution systématique des parties du processus qui ne sont pas fondamentalement quantiques. Cette substitution est réalisée à l'aide de mesures qui «forcent» certaines composantes du système à des états classiques. Où et quand ces mesures peuvent prendre place nous sont dictés par des règles de consistance. Une fois la mesure terminée, l'information acquise est classique et représente exactement l'état du sous-système mesuré en raison du cinquième postulat.

3.2. Conditions de consistance

Comme nous l'avons mentionné à la section 2.2, les règles de consistance ne peuvent, à elles seules, séparer le domaine classique du domaine quantique : une référence à une base privilégiée est également requise. Dans une théorie générale, il est fort difficile de déterminer quelle est cette base privilégiée sans entrer dans un cercle vicieux ! Fort heureusement, lorsque nous nous bornons à des processus quantiques utilisés à des fins de manipulation d'information, une base tout à fait naturelle s'offre à nous : la base de calcul. Cette base coïncide avec les états accessibles aux calculateurs classiques.

Ainsi, il sera possible de substituer de l'information quantique par de l'information classique à l'aide d'une mesure obéissant aux deux conditions suivantes :

C1 : L'ensemble de projecteurs $\hat{\sigma}$ décrivant la mesure fait partie d'une famille consistante.

C2 : La mesure est dans la base de calcul, c'est-à-dire chaque projecteur peut s'écrire sous la forme $\hat{P}_k = \hat{Q}_1 \otimes \ldots \otimes \hat{Q}_n$ et $\hat{Q}_j \in \{|0\rangle\langle 0|, |1\rangle\langle 1|, \mathbb{1}\}$. [1]

Calcul stochastique classique

La condition **C2** élimine toutes les objections soulevées envers les HC dans la littérature puisqu'elle spécifie une base privilégiée donc, avec **C1**, une règle de supersélection. Les deux conditions sont purement mathématiques et ne laissent pas place à interprétation : elles définissent le calcul classique stochastique. Afin de s'en convaincre, supposons qu'un certain calcul quantique, que nous caractérisons par un ensemble de portes $\{U(t_{k-1}, t_k)\} = \{U_k\}$ ordonnées dans le temps et d'un état initial $|\psi_0\rangle$, admette des mesures obéissant aux conditions **C1** et **C2** entre chaque porte. Supposons également que ces mesures soient complètes, c'est-à-dire qu'elles distinguent chacun des états de la base de calcul $|j_k)$ à chaque temps t_k. Ici, nous utilisons la notation $|\cdot)$ afin de souligner que ces états sont classiques.

Ainsi, la condition de consistance faible (éq.2.14) nous assure la validité de

[1] Nous verrons dans ce qui suit que cette condition n'est pas nécessaire.

l'égalité suivante :

$$\langle\psi_0|U_1U_2\ldots U_n|j_n) = \sum_{j_0,j_1,\cdots j_{n-1}} |\langle\psi_0|j_0)|^2 \cdot (\mathcal{T}_1)_{j_0j_1} \cdot \ldots \cdot (\mathcal{T}_n)_{j_{n-1}j_n}. \qquad (3.1)$$

Les matrices $\mathcal{T}_k$ définies par $(j|\mathcal{T}_k|m) = |(j|U_k|m)|^2$ sont des matrices stochastiques. Ainsi, l'interprétation de (éq.3.1) est que l'évolution cohérente quantique $\{U_k\}$ d'une superposition initiale quantique $|\psi_0\rangle$ produit les mêmes statistiques qu'une évolution stochastique classique $\{\mathcal{T}_k\}$ sur un mélange statistique d'états classiques $\{(\ |j_0), |\langle\psi_0|j_0)|^2\ )\}$.

Évidemment, l'exigence qu'une mesure complète dans la base de calcul puisse être entreprise de façon consistante à chaque étape du calcul est fortement restrictive. Cependant, il est possible d'effectuer une mesure partielle, c'est-à-dire de mesurer uniquement un sous-ensemble des qubits, et cela à diverses étapes du calcul. Cette situation décrit donc un calcul hybride classique quantique.

Consistance calculatoire

Ce qui est quantique dans le calcul quantique, c'est la manipulation d'information. En effet, la formulation du problème ainsi que l'extraction d'information utile—la mesure finale—est classique. Ainsi, ce qui importe vraiment lors d'un calcul quantique sont les corrélations entre les réponses obtenues et les questions posées. Pour un circuit quantique donné, la liste des questions possibles est l'ensemble des chaînes de n bits [2], la même que pour l'ensemble des réponses[3].

La condition de consistance faible (éq.2.14) assure bien plus que la conservation de ces corrélations. En fait, elle assure que les corrélations entre toutes les mesures seront respectées ; même les mesures insérées au long du calcul dans l'unique but de substituer l'information quantique. Pourtant, le résultat de ces mesures

[2] Il est possible que l'état initial soit un mélange statistique de ces possibilités. Cela n'affecte pas la présente discussion puisque la consistance d'un mélange d'histoires consistantes est automatique.

[3] Il ne faut pas confondre état final et réponse. L'état final d'un calcul quantique peut être n'importe quel vecteur de l'espace de Hilbert. Cependant, la réponse finale est obtenue en mesurant dans la base de calcul.

intermédiaires ne nous est d'aucun intérêt. Cela nous conduit donc à la formulation d'une condition de consistance moins restrictive ; une condition qui n'assure que l'invariance des corrélations entre les questions et les réponses finales.

Mathématiquement, nous devons sommer la fonction de cohérence (éq.2.12) sur tous les événements intermédiaires de la famille d'histoire $\mathcal{S}$, de sorte que

$$\sum_{\alpha\in\mathcal{S}}\sum_{\beta<\alpha\in\mathcal{S}} Re\left[Tr\left\{P_k^{(n)}C_\alpha^\dagger\rho C_\beta\right\}\right]=0 \quad \forall P_k^{(n)}\in\sigma^{(n)}. \tag{3.2}$$

Le projecteur $P_k^{(n)}$ assure que toutes les histoires aboutissent en un point commun, sans quoi leur contribution à la somme est automatiquement nulle. Nous baptisons cette nouvelle condition, la plus faible introduite jusqu'ici, *condition de consistance calculatoire.*

Le nombre de contraintes imposées par cette condition est m_n—la cardinalité du dernier ensemble de projecteurs $\sigma^{(n)}$—alors que la condition faible en impose $N(N+1)/2$, $N=\prod_{j=1}^{n} m_j$. Cependant, la condition de consistance calculatoire ne permet pas de faire de rétrodiction, c'est-à-dire d'inférer les résultats obtenus aux mesures intermédiaires conditionnellement au résultat final. Cela est du au fait que les mesures intermédiaires ne font plus partie d'un cadre logique consistant.

3.3. Relaxation des conditions

La stricte conservation des corrélations entre les questions posées et les réponses obtenues nous a mené à formuler la condition de consistance calculatoire. Dans cette section, nous montrons comment cette condition ainsi que la condition **C2** peut être relaxée davantage si nous sommes prêts à faire quelques sacrifices.

La ϵ consistance

La direction évidente de ces relaxations est l'exigence d'une conservation *approximative* des corrélations. Ainsi, la substitution d'information quantique par de l'information classique lors d'un processus transforme les corrélations entre questions et réponses de $Pr(\alpha_n|\rho)$ à $Pr'(\alpha_n|\rho)$ de sorte que $\left|Pr(\alpha_n|\rho)-Pr'(\alpha_n|\rho)\right|$ soit borné. La condition de consistance associée à ce type de conservation est

simplement

$$\sum_{\alpha\in\mathcal{S}}\sum_{\beta<\alpha\in\mathcal{S}} Re\left[Tr\left\{P_k^{(n)}C_\alpha^\dagger\rho C_\beta\right\}\right] \leq \epsilon \ \ \forall P_k^{(n)} \in \sigma^{(n)}. \tag{3.3}$$

Évidemment, cette approximation se généralise aux autres types de consistances. Il est possible de fixer un cadre où la logique est approximativement respectée. Nous pouvons ainsi définir la ϵ consistance faible, moyenne et forte tout comme nous l'avons fait pour la consistance calculatoire. Toutefois, lorsque les HC sont utilisées comme interprétation de la mécanique quantique, donc comme pierre angulaire de la science moderne, les équations approximatives sont à éviter !

Bases locales

À l'aide de la ϵ consistance, il nous est possible de relaxer la condition **C2**. La principale caractéristique que nous associons à l'information quantique étant l'enchevêtrement, nous qualifierons de classiques toutes mesures effectuées dans une base locale. Ainsi, la restriction à la base de calcul se voit remplacée par une restriction de localité.

L'information acquise par ces mesures ne peut malheureusement pas être représentée parfaitement sous format classique : la spécification d'une mesure locale demande deux nombres réels, donc une quantité infinie d'information en général. Cette difficulté peut être surmontée en exigeant uniquement une ϵ consistance des mesures. En effet, la spécification d'une mesure avec précision δ requiert de l'ordre de $\log\frac{1}{\delta}$ bits d'information. Afin que (éq.3.3) soit satisfaite, la précision de chaque mesure doit obéir à $\delta \leq \epsilon/\ell^2$ où ℓ est le nombre d'étapes du calcul [14]. Les calculs dits efficaces comportent un nombre polynomial d'étapes en la taille de l'entrée n. Avec ces considérations, nous en venons à la conclusion que le coût de substitution de l'information quantique est de $\log(poly(n))$ où n est la taille de l'entrée.

Si un algorithme quantique admet des mesures locales consistantes à chaque étape de son évolution, alors sa dynamique peut être simulée par des spins classiques avec évolution stochastique. Ces spins classiques sont simplement des vecteurs dans un espace Euclidien à trois dimensions, de norme inférieure ou égale

à 1. La représentation de l'état quantique ρ d'un qubit sur ce système classique est donnée par un vecteur de Bloch $\vec{r}$: $\rho = \frac{1}{2}(\mathbb{1} + \vec{r} \cdot \vec{\sigma})$ où $\vec{\sigma} = \sigma_x \hat{x} + \sigma_y \hat{y} + \sigma_z \hat{z}$ (voir [66] pour plus de détails).

Mesures conjointes

Dans ce qui précède, nous avons permis l'ajout d'une transformation unitaire locale (sur les qubits séparés) afin de rendre la mesure dans la base de calcul consistante. (Ou, de façon équivalente, nous avons admis les extensions consistantes dans des bases locales plutôt qu'uniquement dans la base de calcul.) La généralisation de cette idée est évidente : permettre l'ajout d'une transformation à un plus grand nombre de qubits. Cependant, certaines conditions s'imposent. La spécification d'une transformation unitaire sur n qubits requiert $2^{2n} - 1$ nombres réels, ce qui nécessite une quantité d'information exponentielle si nous exigeons une erreur constante. Il est donc nécessaire de limiter le nombre de qubits qui peuvent être affectés par la transformation unitaire à une taille logarithmique. Cette condition exige la notion d'uniformité[4], ce qui complique largement l'analyse. Pour cette raison, nous laissons tomber cette direction de recherche.

Néanmoins, il est important de garder cette remarque à l'esprit : si un algorithme quantique admet des mesures consistantes conjointes sur un nombre borné logarithmique de qubits, alors il sera possible de simuler classiquement sa dynamique de façon efficace. Lorsque les mesures locales sont consistantes, la dynamique quantique peut être simulée par une évolution stochastique de spins classiques dans un espace à trois dimensions. Lorsque les mesures bornées à un nombre logarithmique de qubits sont consistantes, la dynamique quantique peut être simulée par des spins classiques dans un espaces de dimension polynomial.

Comme nous l'avons mentionné en début de chapitre, Aharonov et Ben-Or ont démontré que lorsque le taux de décohérence est supérieure à une valeur critique, la dynamique du système peut être simulée efficacement classiquement [2]. Cette simulation est possible puisque les effets quantiques sont limités à des sous-

[4]Section 4.5.

systèmes de petite taille en raison de l'absence de cohérence à grande échelle. S'il n'y a pas de cohérence entre les sous-systèmes de petite taille, alors nous pouvons les mesurer séparément de façon consistante. Néanmoins, l'absence de cohérence entre les sous-systèmes n'est pas *nécessaire* à la condition de consistance. Ainsi, l'argument présenté ici est plus général que celui de Aharonov et Ben-Or.

3.4. Retour d'information

Jusqu'ici, nous avons montré comment il est possible de substituer une partie de l'information quantique par de l'information classique sans affecter le résultat du processus, ou du moins que très peu. Cependant, l'information classique ne sert que de *support*. C'est uniquement le support de l'information qui est un système hybride. Afin de généraliser le modèle, nous devons également permettre une *manipulation* d'information classique.

Retour d'information

Mathématiquement, ce sont les histoires consistantes à embranchement qui permettront de formaliser cette liberté [69, 39]. Dans le contexte des histoires à embranchement, l'information acquise lors des mesures intermédiaires est utilisée afin de déterminer les mesures subséquentes. Ainsi, l'ensemble de projecteurs utilisés au temps t_k dépend des résultats des mesures antérieures, nous le notons donc : $\sigma^{(k,\alpha_{k-1},\alpha_{k-2},\cdots,\alpha_1)}$.

Un certain calcul peut être nécessaire afin de déterminer quelle mesure doit être effectuées à la prochaine étape. L'information classique acquise lors des mesures doit être manipulée avant d'être retournée au système. Il est primordial de borner polynomialement le temps alloué à ces manipulations.

L'image qui ressort de ce modèle est un ordinateur hybride classique quantique dont uniquement les tâches *fondamentalement quantiques* sont effectuées sur un système quantique. Entre ces opérations quantiques, une partie de l'information est storée sous forme classique et manipulée alors que ce qui ne peut être mesuré de façon consistante demeure sous forme quantique. L'information classique peut

ensuite être re-transférée sur un système quantique si certaines transformations fondamentalement quantiques doivent y être apportées.

Espace de Hilbert élargi

Le retour d'information ainsi que les autres processus semi-classiques peuvent être modélisés à l'aide d'un système purement quantique. À première vue, cette proposition semble aller à l'encontre du but même de toute cette procédure, mais peut être très utile à des fins d'analyse.

Afin de réaliser cette modélisation, il suffit d'utiliser la notion de pseudomesure décrite à la section 1.5.5. Supposons que le processus semi-classique exige la mesure du qubit 1 selon la base $\{|\psi_0\rangle, |\psi_1\rangle\}$, puis, en fonction de la réponse obtenue 0 ou 1, une mesure du qubit 2 dans la base $\{|\phi_0^0\rangle, |\phi_1^0\rangle\}$ ou $\{|\phi_0^1\rangle, |\phi_1^1\rangle\}$ respectivement. En définissant les trois transformations suivantes :

$$\mathsf{U} \quad : \quad \begin{cases} |0\rangle \mapsto |\psi_0\rangle \\ |1\rangle \mapsto |\psi_1\rangle \end{cases} \tag{3.4}$$

$$\mathsf{V}_0 \quad : \quad \begin{cases} |0\rangle \mapsto |\phi_0^0\rangle \\ |1\rangle \mapsto |\phi_1^0\rangle \end{cases} \tag{3.5}$$

$$\mathsf{V}_1 \quad : \quad \begin{cases} |0\rangle \mapsto |\phi_0^1\rangle \\ |1\rangle \mapsto |\phi_1^1\rangle \end{cases}, \tag{3.6}$$

le circuit quantique de la figure 3.1 simule exactement ce processus semi-classique. Le qubit 3 sert d'abord à storer l'information classique acquise lors de la mesure

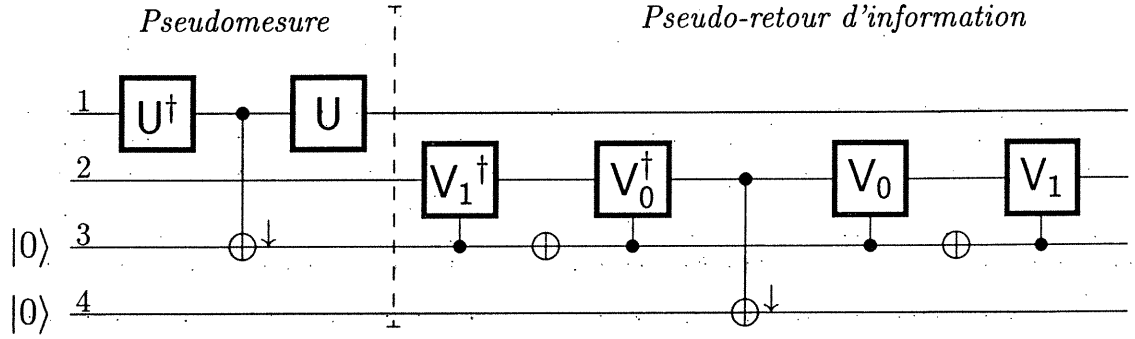

FIG. 3.1 – Espace de Hilbert élargi pour processus semi-classique.

du qubit 1. Par la suite, il sert à décider selon quelle base sera prise la mesure du qubit 2. L'information acquise lors de cette dernière mesure est storée sur le qubit 4.

L'inverse de cette construction est immédiat. Si les qubits 3 et 4 n'interagissent plus avec les qubits 1 et 2, alors leur mesure aux endroits marqués d'une flèche est consistant si nous permettons l'utilisation des histoires à embranchement.

Cryptographie quantique

Lors de l'analyse de sécurité d'un protocole de cryptographie quantique, toutes les attaques possibles doivent être considérées. En particulier, la possibilité qu'un espion mesure une partie du système quantique et agisse ensuite en fonction de l'information acquise est à envisager. Une analyse complète semble ainsi constituer une tâche insurmontable. Fort heureusement, en raison de ce que nous avons décrit ci-haut, toutes ces possibilités peuvent être étudiées à l'aide d'un modèle où l'espion a accès à des qubits ancillaires mais est limité à des opérations unitaires et une mesure finale. Ainsi, nous n'avons pas à considérer toutes les combinaisons possibles de mesures intermédiaires.

Comme nous l'avons mentionné à la section 1.2.3, il est possible de simuler toute transformation unitaire à l'aide d'un ensemble universel de portes élémentaires. Ainsi, à première vue, le retour d'information ne semble apporter aucune nouvelle possibilité intéressante. Voici donc trois bonnes raisons d'utiliser un retour d'information.

Augmenter la classicalité

Premièrement, comme nous venons d'en discuter, le retour d'information peut contribuer à diminuer le nombre d'étapes fondamentalement quantiques d'un calcul. En particulier, certaines mesures qui sont, de façon générale, inconsistantes peuvent devenir consistantes conditionnellement aux résultats de mesures antécédentes. Le circuit suivant illustre une telle situation. Les mesures $\hat{\mathrm{m}}$ et m y sont effectuées dans la base de calcul. La seule mesure $\tilde{\mathrm{m}}$ qui soit consistante

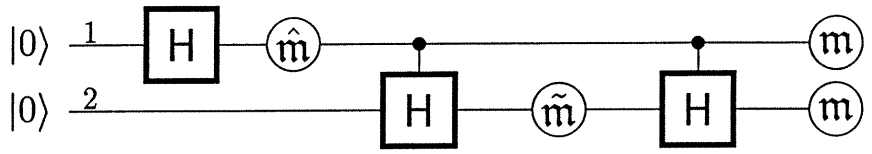

FIG. 3.2 – Mesures consistantes à embranchement.

est la mesure triviale $\{\mathbb{1}\}$. Cependant, en présence de retour d'information, il est possible de faire mieux. Nous effectuons ces mesures de façon séquentielle, c'est-à-dire en effectuant d'abord la mesure $\hat{\mathfrak{m}}$ au temps t_1, suivie de $\tilde{\mathfrak{m}}$ au temps t_2 puis des deux mesures finales $\mathfrak{m}$ au temps t_3. Ainsi, les ensembles de projecteurs suivants forment une famille d'histoires consistantes à embranchement :

$$\begin{aligned} \sigma^{(1)} &= \{|0\rangle\langle 0| \otimes \mathbb{1}, |1\rangle\langle 1| \otimes \mathbb{1}\} \quad \sigma^{(3)} = \{|00\rangle\langle 00|, |01\rangle\langle 01|, |10\rangle\langle 10|, |11\rangle\langle 11|\} \\ \sigma^{(2,0)} &= \{\mathbb{1} \otimes |0\rangle\langle 0|, \mathbb{1} \otimes |1\rangle\langle 1|\} \quad \sigma^{(2,1)} = \{\mathbb{1} \otimes |+\rangle\langle +|, \mathbb{1} \otimes |-\rangle\langle -|\}. \end{aligned}$$

où $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. L'avantage de ces mesures consistantes est qu'elles permettent d'effectuer les transformations de Walsh-Hadamard contrôlées par contrôle classique (c'est-à-dire d'appliquer la transformation ou non selon une décision classique), donc remplacent une interaction à deux corps par une simple rotation d'un qubit. Cette constatation sera établie formellement à la section 4.2. L'exemple donné ici est, de toute évidence, purement académique, comme la plupart des exemples à venir. Un exemple physique de situation où la consistance est uniquement atteinte en présence de retour d'information est donnée dans [71].

Systèmes ouverts

Deuxièmement, bien que cela sorte de la discussion présente, le retour d'information est essentiel à la simulation de dynamique *non unitaire*, c'est-à-dire à la simulation de systèmes en interaction avec un environnement. En effet, un ensemble de portes unitaires universelles accompagnées d'une mesure fixe d'un qubit peuvent reproduire l'évolution d'un système ouvert si et seulement si l'information acquise lors des mesures influence les opérations subséquentes appliquées au système [64]. La simulation de systèmes physiques quantiques forme une des

applications des plus importantes de l'informatique quantique. La possibilité de simuler une dynamique non unitaire, par exemple de pouvoir simuler des systèmes quantiques en contact thermodynamique, est donc d'une importance primordiale.

Retour d'information et implantation physique

Troisièmement, le retour d'information peut faciliter l'implantation physique de calculateurs quantiques. Des exemples de telles implémentations ont déjà été proposées. Par exemple, la proposition de calcul universel avec optique linéaire de Knill, Laflamme et Milburn [60] nécessite un retour d'information. Dans la démonstration de son bon fonctionnement, on ne fait jamais appel à la notion de consistance. L'analyse est formulée en termes d'évolution conditionnelle à l'obtention de certains résultats. Pourtant, il est possible de formuler entièrement cette analyse en terme de circuit unitaire uniquement (circuit de taille infinie malheureusement puisque le temps d'exécution n'est pas borné). [5] D'autres propositions utilisent également le retour d'information, par exemple celle de Gottesman et Chuang [45] et celle de Raussendorf et Briegel [75].

3.5. Analyse

Dans cette section, nous analysons la structure des familles d'histoires consistantes. Les résultats qui y sont présentés ne concernent pas uniquement l'application des histoires consistantes au calcul quantique, mais les histoires consistantes en général. Néanmoins, certains résultats sont mieux motivés par le calcul quantique et c'est pourquoi nous choisissons de présenter cette analyse ici.

[5] La notion de consistance intervient à deux niveaux dans cette proposition. D'abord, pour se débarrasser de l'évolution conditionnelle, nous pouvons remplacer les mesures par des pseudo mesures tel qu'illustré à la figure 3.1. De plus, dans l'analyse du protocole, on doit montrer qu'une certaine mesure peut être devancée dans le temps sans affecter les résultats. On y parvient à l'aide de règles de commutation alors qu'il s'agit simplement de démontrer la consistance d'une mesure.

Notation

Avant d'entreprendre notre analyse, nous devons introduire quelques nouvelles notations. Soit $\mathcal{S} = \{\rho, \sigma^{(1)}, \sigma^{(2)}, \ldots, \sigma^{(n)}\}$ une famille d'histoires consistantes[6]. La famille $\mathcal{S}' = \{\rho, \sigma^{(1)}, \ldots, \sigma^{(k)}, \tau, \sigma^{(k+1)}, \ldots, \sigma^{(n)}\}$ est une extension consistante de la famille $\mathcal{S}$ par l'ensemble de projecteurs $\tau = \{Q_1, Q_2, \ldots, Q_m\}$ si *i)* τ est un ensemble exhaustif de projecteurs exclusifs (éq.2.7) et *ii)* $\mathcal{S}'$ est consistant. Dans ce qui suit, nous considérons uniquement $k < n$, c'est-à-dire que nous n'ajoutons pas de mesures à la suite de la mesure finale.

À l'aide de cette définition, le programme de classicalité du calcul quantique se formule très simplement. Un calcul quantique est la spécification d'un état initial, d'une évolution et d'une mesure finale. Cette unique mesure est automatiquement consistante. *Classicaliser* un calcul quantique consiste donc à en trouver des extensions consistantes locales à cette famille.

Une extension consistante sera dite *triviale* si pour chaque histoire $(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n)$ de la famille $\mathcal{S}$, il y a au plus une histoire $(\alpha_1, \ldots, \alpha_k, \beta, \alpha_{k+1}, \ldots, \alpha_n)$ de la famille $\mathcal{S}'$ qui possède une probabilité non nulle. En d'autres termes, la mesure correspondant à l'ensemble τ n'apporte aucune information supplémentaire puisque le processus $Pr(\beta|\alpha_1, \ldots, \alpha_n)$ est déterministe.

L'ensemble de projecteurs $\sigma = \{P_j\}$ est un raffinement de l'ensemble $\sigma' = \{P'_k\}$ si chaque projecteur de σ' est obtenu en sommant un certain nombre de projecteurs de σ. L'inverse du raffinement est le partitionnement[7]. On montre facilement que le partitionnement conserve la consistance, ce qui n'est pas le cas pour le raffinement en général. Nous dirons d'un ensemble exhaustif de projecteurs exclusifs σ qu'il est raffiné s'il est impossible de le raffiner davantage, en d'autres termes, si tous ses projecteurs sont de rang 1.

[6]Le type de consistance est sans importance pour ces définitions.

[7]Les termes anglophones pour désigner le raffinement et le partitionnement sont le *fine graining* et le *coarse graining* respectivement.

Branches d'Everett

Le programme de classicalité étant maintenant formulé en termes d'extensions consistantes, nous allons ici caractériser ces dernières. Comme nous l'avons démontré à la section 3.2.1, s'il est possible de faire une extension locale raffinée à chaque étape du calcul quantique, alors celui-ci se réduit à un calcul stochastique classique. Existe-t-il une borne sur le nombre d'extensions consistantes possibles d'un processus quantique ? De façon générale, il n'en existe pas. Cependant, le nombre d'extensions consistantes *non triviales* est borné.

Lemme 1. *Étant donné une matrice de densité initiale ρ de rang r, il y a au plus $r\Omega$ histoires consistantes moyennes (éq.2.21) auxquelles sont associées des probabilités non nulles, Ω étant la dimension de l'espace de Hilbert. Toutefois, il existe un nombre infini de familles d'histoires qui atteignent cette borne.*

Preuve. La première partie de ce lemme est due à Diósi [31]. Afin de construire une famille qui atteint cette borne, choisissons $\sigma^{(1)}$ comme l'ensemble de projecteurs de rang 1 qui commutent avec ρ. En d'autres termes, si $\rho = \sum_{j=1}^{r} \lambda_j |\psi_j\rangle\langle\psi_j|$, alors $\sigma^{(1)} = \{|\psi_j\rangle\langle\psi_j|\}_{j=1,\ldots,\Omega}$ où les $|\psi_j\rangle$ $j > r$ forment une base du sous-espace associé à la valeur propre 0 de ρ. Maintenant, choisissons $\sigma^{(2)}$ comme un ensemble de projecteurs de rang 1 $\sigma^{(2)} = \{|\phi_k\rangle\langle\phi_k|\}$ de sorte que $\langle\psi_j|\phi_k\rangle \neq 0 \quad \forall i,j$. Par exemple, cela peut être réalisé si la base $\{|\phi_k\rangle\}$ est la transformée de Fourier de $\{|\psi_j\rangle\}$. Ainsi, on montre facilement que $\mathcal{S} = \{\rho, \sigma^{(1)}, \sigma^{(2)}\}$ respecte la condition de consistance moyenne et possède exactement $r\Omega$ histoires avec probabilité non nulle. À partir de cette construction, il est évident qu'il est possible de construire un nombre infini de telles familles. □

Dans la construction précédente, la borne de Diósi est atteinte puisque $\langle\psi_j|\phi_k\rangle \neq 0 \quad \forall i,j$. Sans cette condition, la borne n'est pas atteinte. Dans ce qui suit, nous montrons, entre autres, que sans cette condition, aucune extension consistante de $\mathcal{S}$ n'atteint cette borne.

Lemme 2. *Soit $\mathcal{S} = \{\rho, \sigma^{(1)}, \sigma^{(2)}\}$ une famille d'histoires où $\sigma^{(1)}$ est un ensemble de projecteurs de rang 1 qui commutent avec ρ et $\sigma^{(2)}$ est n'importe quel ensemble de projecteurs de rang 1. Alors, $\mathcal{S}$ est consistant et il n'existe aucune famille*

d'histoires $\mathcal{S}' = \{\rho, \sigma^{(1)}, \tau^{(1)}, \ldots, \tau^{(n)}, \sigma^{(2)}\}$ *qui soit une extension consistante non triviale de* $\mathcal{S}$.

Preuve. Montrons d'abord que $\mathcal{S}$ est consistante. En utilisant la notation introduite au Lemme 1, la fonction de cohérence (éq.2.12) devient

$$\begin{aligned} D(i,j;k,l) &= Tr\{|\phi_j\rangle\langle\phi_j|\psi_i\rangle\langle\psi_i|\rho|\psi_k\rangle\langle\psi_k|\phi_l\rangle\langle\phi_l|\} \\ &= \lambda_i |\langle\phi_j|\psi_i\rangle|^2 \delta_{ik}\delta_{jl}, \end{aligned}$$

ce qui satisfait à la condition de consistance moyenne (éq.2.21).

Maintenant, supposons que $\tau^{(k)} = \{P^{(k)}_{\alpha_k}\}$ sont des ensembles de projecteurs qui font de $\mathcal{S}'$ une extension consistante de $\mathcal{S}$. Pour un couple fixe $(|\psi_j\rangle, |\phi_k\rangle)$, la fonction de cohérence devient

$$\begin{aligned} & D(j,\alpha_1,\ldots,\alpha_n,k;j,\beta_1,\ldots,\beta_n,k) \\ = \; & \langle\phi_k|P^{(n)}_{\alpha_n}\ldots P^{(1)}_{\alpha_1}|\psi_j\rangle \; \lambda_j \; \langle\psi_j|P^{(1)}_{\beta_1}\ldots P^{(n)}_{\beta_n}|\phi_k\rangle \qquad (3.7) \\ \propto \; & \sqrt{Pr(j,\alpha_1,\ldots,\alpha_n,k)} \times \sqrt{Pr(j,\beta_1,\ldots,\beta_n,k)}. \end{aligned}$$

Afin que la famille soit consistante moyenne, la condition

$$\sqrt{Pr(j,\alpha_1,\ldots,\alpha_n,k)} \times \sqrt{Pr(j,\beta_1,\ldots,\beta_n,k)} \propto \delta_{\alpha_1\beta_1}\ldots\delta_{\alpha_n\beta_n} Pr(j,\alpha_1,\ldots,\alpha_n,k) \qquad (3.8)$$

doit être satisfaite. Il s'en suit qu'une seule de ces histoires peut posséder une probabilité non nulle, donc l'extension est triviale. □

Les deux lemmes précédents n'ont pas d'implications directes sur le calcul quantique puisqu'ils sont formulés en terme de consistance moyenne. Cette condition est trop restrictive pour le calcul quantique. Idéalement, c'est la condition de consistance de calcul qui devrait fixer les bornes. Cependant, puisqu'elle est si peu restrictive, nous ne savons pas s'il existe une borne sur le nombre d'extensions consistantes de calcul non triviales.

De plus, les limitations apportées par ces deux lemmes concernent les extensions non triviales. Elles ne limitent pas le nombre d'extensions consistantes triviales. Pour la classicalité du calcul quantique, le fait que les extensions soient triviales ou non ne nous importe pas.

Le prochain lemme traduit la borne de Diósi à une condition de consistance moins restrictive : la consistance faible (éq.2.14). Cela constitue donc un premier pas dans la direction de la consistance de calcul.

Lemme 3. *Étant une matrice de densité initiale ρ de rang r, il y a au plus $2r\Omega$ histoires consistantes faibles (éq.2.14) auxquelles sont associées des probabilités non nulles. Toutefois, il existe un nombre infini de familles d'histoires qui atteignent cette borne.*

Preuve. La preuve de la première partie est très semblable à celle de Diósi [31]. Soit $\{(\lambda_j, |\psi_j\rangle)\}$ les valeurs et vecteurs propres de ρ. Définissons la purification de ρ :

$$|\Psi\rangle = \sum_{j=1}^{r} \sqrt{\lambda_j}|\psi_j\rangle \otimes |\psi'_j\rangle \tag{3.9}$$

où les vecteurs $\{|\psi'_j\rangle\}_{j=1...r}$ forment une base d'un espace de Hilbert $\mathcal{E}$ de dimension r, de sorte que $Tr_{\mathcal{E}}\{|\Psi\rangle\langle\Psi|\} = \rho$. À l'aide des opérateurs d'histoire C_α, définissons les vecteurs non normalisés $|\Psi_\alpha\rangle = (C_\alpha \otimes \mathbb{1}_{\mathcal{E}})|\Psi\rangle$. La condition de consistance faible devient donc $Re\{\langle\Psi_\alpha|\Psi_\beta\rangle\} = \delta_{\alpha\beta}Pr(\alpha)$. Puisque ces vecteurs reposent dans un espace de Hilbert de dimension $r\Omega$, il peut y avoir au plus $2r\Omega$ vecteurs non nuls satisfaisant cette condition.

Pour la seconde partie de la preuve, nous allons supposer que Ω est pair, le cas impair étant plus technique et de moindre intérêt pour le calcul quantique. Choisissons par exemple $\sigma^{(1)}$ comme un ensemble de projecteurs de rang 1 qui commutent avec ρ, $\sigma^{(2)}$ la transformée de Fourier de $\sigma^{(1)}$ et finalement $\sigma^{(3)}$ est obtenu en appliquant la transformation

$$|j\rangle \mapsto \frac{i|j\rangle + |(j + \Omega/2) \mathrm{mod} \Omega\rangle}{\sqrt{2}} \tag{3.10}$$

aux éléments de $\sigma^{(2)}$. Pour les systèmes composés de qubits, cette transformation correspond à l'application de la porte

$$\frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix} \tag{3.11}$$

sur le qubit le plus significatif. La consistance de cette famille se démontre simplement à l'aide du théorème 3 ; nous y reviendrons. □

La portée de ce lemme va bien au-delà du calcul quantique. Il impose des limitations sur la quantité d'information non redondante qui peut être acquise sur l'évolution d'un système quantique ainsi que sur le nombre maximal de « branches d'Everett » dans l'univers. Rappelons que selon l'interprétation dite d'Everett qui, soit dit en passant, va plus loin que la proposition originale d'Everett, la superposition d'états correspond à un embranchement de l'univers. L'interférence est due à une recombinaison des univers identiques ayant suivi une évolution différente.

C'est afin de valider cette interprétation que Deutsch a proposé son modèle de calcul quantique et son algorithme. Selon lui, si un calculateur quantique peut déterminer si $f(0) = f(1)$ en n'ayant recours qu'une seule fois à f lorsqu'il se trouve en superposition de deux états de base, c'est parce que les calculs sont exécutés dans deux univers parallèles.

Le problème principal de cette interprétation provient de l'indépendance de représentation d'un état quantique. Soit un vecteur $|\psi\rangle$. Dans une certaine représentation, $|\psi\rangle$ est la superposition de plusieurs vecteurs de base alors qu'il peut correspondre à un vecteur de base d'une autre représentation. Il s'en suit une subjectivité de la séparation des univers. Encore une fois, une règle de supersélection s'impose. Selon Paz et Żurek, c'est l'environnement qui choisit cette base : « *decoherence defines branches* » [71].

Sans vouloir entrer dans le fanatisme, cette interprétation se marie bien avec les thèses proposées ici. Chaque branche de l'univers doit posséder sa propre logique consistante. Puisque la condition de consistance faible est la condition minimale pour que les règles de la logique soient respectées, le lemme 3 impose une borne sur le nombre d'embranchements possibles de l'univers.

Analyse systématique

L'analyse de classicalité d'un algorithme quantique est une tâche fort complexe. Les lemmes précédents imposent des limites fondamentales pour différents types

de consistances, mais n'aident en rien l'analyse d'un algorithme concret. Dans ce qui suit, nous développons des outils simplifiant l'analyse d'un circuit. L'analyse systématique d'un algorithme en terme d'histoires consistantes nous permettrait de déceler toutes les interventions quantiques fondamentales, ce qui réglerait un bien grand nombre d'interrogations. Nous ne prétendons pas être en mesure de conduire une telle analyse, mais ce qui suit est, encore une fois, un pas dans cette direction.

Le partitionnement des ensembles de projecteurs d'une famille consistante conserve la consistance. Plus important encore, le partitionnement judicieux d'une famille non consistante peut être consistant. D'ailleurs, selon Gell-Mann et Hartle, le partitionnement est un aspect *nécessaire* à la consistance :

> *Completely fine-grained histories cannot be assigned probabilities; only suitable coarse-grained histories can.* [39] *Except for pathological cases, coarse-graining is necessary for decoherence.* [42] *Maximal sets [...] are those decohering sets for which there is no finer-grained decoherent set.* [39]

Le prochain théorème indique que lorsque l'état initial du système est pur, aucun partitionnement n'est nécessaire à la consistance. On y montre que toute famille d'HC peut être obtenue en partitionnant une famille raffinée consistante.

Théorème 2. *Soit* $\mathcal{S} = \{\rho, \sigma^{(1)}, \ldots, \sigma^{(n)}\}$ *une famille consistante moyenne où* $\rho = |\psi\rangle\langle\psi|$ *est un état pur. Alors il existe une famille* $\mathcal{S}' = \{\rho, \sigma'^{(1)}, \ldots, \sigma'^{(n)}\}$ *où* $\sigma'^{(j)} = \{|\phi_k^{(j)}\rangle\langle\phi_k^{(j)}|\}$ *est un raffinement de* $\sigma^{(j)}$ *pour chaque* j.

Preuve. La preuve est par induction. D'abord, nous montrons que la dernière mesure peut être raffinée de façon consistante. Puis nous montrons que si les ensembles $\sigma^{(j)}$ $j > k$ sont tous raffinés, alors il est possible de raffiner $\sigma^{(k)}$.

Soit les états non normalisés $|\Psi_{\alpha_1,\ldots,\alpha_n}\rangle = P_{\alpha_n}^{(n)} \ldots P_{\alpha_1}^{(1)}|\psi\rangle$. La condition de consistance moyenne (éq.2.21) nous assure que

$$\langle\Psi_{\alpha_1,\ldots,\alpha_n}|\Psi_{\beta_1,\ldots,\beta_n}\rangle = \delta_{\alpha_1\beta_1}\ldots\delta_{\alpha_n\beta_n}Pr(\alpha_1,\ldots,\alpha_n), \tag{3.12}$$

donc ces vecteurs sont orthogonaux. Afin d'alléger la notation, remplaçons le vecteur d'indice $(\alpha_1,\ldots,\alpha_{n-1})$ par un indice unique ℓ donné par ordre décroissant des

probabilités $Pr(\ell, \alpha_n)$. Puisque les projecteurs d'un même ensemble sont orthogonaux (éq.2.7), nous avons $P_{\beta_n}^{(n)}|\Psi_{\ell,\alpha_n}\rangle = \delta_{\alpha_n\beta_n}|\Psi_{\ell,\alpha_n}\rangle$; les vecteurs $|\Psi_{\ell,\alpha_n}\rangle$ sont des vecteurs orthogonaux reposant dans le sous-espace $\mathcal{W}_{\alpha_n}$ associé à $P_{\alpha_n}^{(n)}$. La dimension de $\mathcal{W}_{\alpha_n}$ est donnée par le rang de $P_{\alpha_n}^{(n)}$, soit $r_{\alpha_n}^{(n)}$. Le nombre de vecteurs orthogonaux $|\Psi_{\ell,\alpha_n}\rangle$ non nuls $w_{\alpha_n}^{(n)}$ ne peut excéder la dimension de ce sous-espace. Nous pouvons construire une base pour $\mathcal{W}_{\alpha_n}$ en renormalisant les $w_{\alpha_n}^{(n)}$ vecteurs non nuls $|\Psi_{\ell,\alpha_n}\rangle$ et en complétant si nécessaire

$$|\nu_{\ell,\alpha_n}\rangle = \begin{cases} \frac{|\psi_{\ell,\alpha_n}\rangle}{\sqrt{Pr(\ell,\alpha_n)}} & si\ \ell \leq w_{\alpha_n}^{(n)} \\ |\mu_{\ell-\omega_{\alpha_n}^{(n)}}\rangle & si\ \omega_{\alpha_n}^{(n)} < \ell \leq r_{\alpha_n}^{(n)} \end{cases} \tag{3.13}$$

où les vecteurs $|\mu_j\rangle$ ne servent qu'à compléter la base. Avec cette construction, on vérifie facilement que

$$P_{\alpha_n}^{(n)} = \sum_{\ell=1}^{r_{\alpha_n}^{(n)}} |\nu_{\ell,\alpha_n}\rangle\langle\nu_{\ell,\alpha_n}| \tag{3.14}$$

et que $\mathcal{S}' = \{\rho, \sigma^{(1)}, \ldots, \sigma^{(n-1)}, \sigma'^{(n)}\}$ avec $\sigma'^{(n)} = \{|\nu_{\ell,\alpha_n}\rangle\langle\nu_{\ell,\alpha_n}|\}$ forment une famille consistante.

Afin de compléter le preuve, supposons que la famille consistante soit de la forme $\mathcal{S} = \{\rho, \sigma^{(1)}, \ldots, \sigma^{(n)}, \tau^{(n+1)}, \ldots, \tau^{(f)}\}$ où les $\tau^{(k)}$ sont des ensembles de projecteurs de rang 1. La condition de consistance moyenne nous indique que $\langle\psi|P_{\alpha_1}^{(1)} \ldots P_{\alpha_n}^{(n)} P_{\beta_n}^{(n)} \ldots P_{\beta_1}^{(1)}|\psi\rangle = \delta_{\alpha_a\beta_1} \ldots \delta_{\alpha_n\beta_n} Pr(\alpha_1, \ldots \alpha_n)$, ce qui nous permet de définir les vecteurs $|\Psi_{\alpha_1,\ldots,\alpha_n}\rangle$ et $|\nu_{\ell,\alpha_n}\rangle$ comme nous l'avons fait dans la première partie de cette preuve. Il s'en suit que

$$P_{\alpha_n}^{(n)} = \sum_{\ell=1}^{r_{\alpha_n}^{(n)}} |\nu_{\ell,\alpha_n}\rangle\langle\nu_{\ell,\alpha_n}| \tag{3.15}$$

et que $\mathcal{S}' = \{\rho, \sigma^{(1)}, \ldots, \sigma^{(n-1)}, \sigma'^{(n)}, \tau^{(n+1)}, \ldots, \tau^{(f)}\}$ avec $\sigma'^{(n)} = \{|\nu_{\ell,\alpha_n}\rangle\langle\nu_{\ell,\alpha_n}|\}$ forment une famille consistante, ce qui complète la preuve. □

À l'aide de ce théorème, nous pouvons nous contenter de rechercher parmi les ensemble de projecteurs de rang 1 lorsque nous tentons de faire une extension consistante moyenne, ce qui allège largement la tâche. Encore plus important, les

histoires constituées de projecteurs de rang 1 admettent une analyse de graphe que nous avons décrite à la section 2.5. Encore une fois, le résultat n'est valable que pour la consistance moyenne. Néanmoins, l'idée de trajectoires consistantes de Griffiths peut être adaptée à une condition moins restrictive.

Toujours dans le but de construire une méthode d'analyse systématique des circuits quantiques en terme d'histoires consistantes, voici comment analyser graphiquement la consistance faible. Le graphe est construit de la même façon qu'à la section 2.5. Ici, à chaque arête est associée sa fonction de Green (éq.2.23). La condition de consistance faible peut alors se formuler sous forme de théorème.

Théorème 3. *Si deux trajectoires relient deux sommets distincts, le produit des fonctions de Green autour de cette boucle doit être purement imaginaire afin que l'ensemble des trajectoires forme une famille faiblement consistante.*

Preuve. Il suffit de constater que le produit des fonctions de Green autour d'une boucle correspond à la fonction de cohérence (éq.2.12) pour des projecteurs de rang 1. □

Notons que $G_{jk}(t_j, t_k) = (G_{jk}(t_k, t_j))^*$. En terme de phase de propagateur (ϕ est la phase du nombre complexe $x = Ae^{i\phi}$), la somme des phases de trajectoires formant une boucle dans le graphe doit être un multiple impaire de $\pi/2$.

Par exemple, nous pouvons analyser la famille construite à la preuve du lemme 3 (avec $\Omega = 6$). $\sigma^{(0)}$ est l'ensemble des états initiaux $|\psi_j\rangle$ (si la famille est consistante pour les états $|\psi_j\rangle$ individuellement, elle l'est également pour leur mélange statistique par linéarité de la fonction de cohérence (éq.2.12).) $\sigma^{(1)}$ représente une mesure dans la base $|\psi_j\rangle$; les fonctions de Green sont donc $G_{jk}(t_0, t_1) = \delta_{jk}$. L'ensemble $\sigma^{(2)}$ est une transformée de Fourier de $\sigma^{(1)}$, donc $G_{jk}(t_1, t_2) = \frac{1}{\sqrt{\Omega}} e^{i2\pi jk/\Omega}$ (lignes doubles) par définition de la transformée de Fourier quantique (éq.4.3). Finalement, selon la définition de $\sigma^{(3)}$ (éq.3.10), les arêtes simples (figure 3.3) représentent un nombre réel $\frac{1}{\sqrt{2}}$ alors que les lignes foncées sont purement imaginaires $\frac{i}{\sqrt{2}}$. Le produit des fonctions de Green dans une boucle (sens horaire par exemple) est donc

$$\frac{1}{\sqrt{\Omega}} \exp\left\{\frac{i2\pi jk}{\Omega}\right\} \left(\frac{1}{\sqrt{2}}\right) \left(\frac{i}{\sqrt{2}}\right)^* \frac{1}{\sqrt{\Omega}} \left(\exp\left\{\frac{i2\pi j(k+\Omega/2)}{\Omega}\right\}\right)^* = \frac{i}{2\Omega}, \quad (3.16)$$

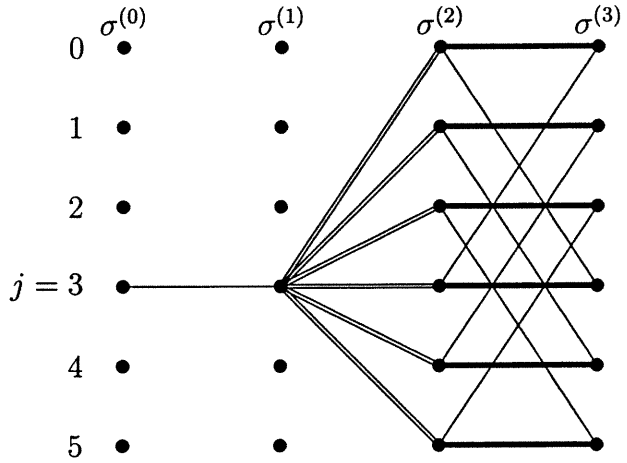

FIG. 3.3 – Analyse de graphe du lemme 3.

purement imaginaire, donc la famille est consistante.

En résumé, l'analyse graphique est complètement générale pour la consistance moyenne avec état initial pur, ce qui avait échappé à Griffiths et qui contredit ce qu'ont postulé Gell-Mann et Hartle, c'est-à-dire que le partitionnement est essentiel à la consistance. Pour la consistance faible, il existe une méthode d'analyse graphique mais qui n'est possiblement pas générale puisque nous ne savons démontrer ou réfuter l'analogue du Théorème 2 pour la consistance faible.

4 — Discussion

Nous avons démontré comment il est possible, en principe, d'utiliser les histoires consistantes afin de caractériser la classicalité de certains processus quantiques. L'analyse d'un algorithme quantique en termes d'histoires consistantes constitue une tâche extrêmement complexe. Les outils développés au chapitre précédent allègent cette tâche qui, somme toute, demeure lourde.

Dans ce qui suit, nous discutons de deux aspects de notre approche. D'abord, nous explorons les conséquences qu'entraînerait une analyse systématique de la classicalité d'un circuit quantique, c'est-à-dire la possibilité de pouvoir déterminer les familles d'histoires consistantes locales d'un processus. Cette partie de la discussion relève de la pure fantaisie puisqu'une analyse complète est à ce jour inaccessible. Deuxièmement mais non le moindre, nous apportons certains éclaircissements sur les fondements du calcul quantique à l'aide des concepts que nous avons établis. La validité de nos conclusions ne repose pas sur la possibilité de conduire une analyse consistante systématique.

4.1. Exemple non trivial

Dans cette section, nous donnons un exemple d'extension consistante non triviale qui nous servira tout au long de notre discussion. L'exemple que nous donnons est purement académique. Il serait évidemment plus intéressant d'analyser un circuit utile mais, comme nous l'avons mentionné à plusieurs reprises, les techniques ne sont pas suffisamment mûres pour une telle entreprise.

Circuit

Le circuit utilisé pour l'exemple est présenté à la figure 4.1. La porte F représente

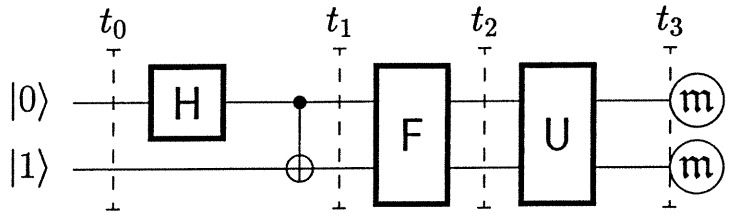

FIG. 4.1 – Circuit quantique.

la transformée de Fourier quantique définie sur n qubits dans la base de calcul par

$$|j\rangle \mapsto \frac{1}{\sqrt{\Omega}} \sum_{k=0}^{\Omega-1} \exp\left\{\frac{i2\pi(kj \bmod \Omega)}{\Omega}\right\} |k\rangle \tag{4.1}$$

où $\Omega = 2^n$ est la dimension de l'espace de Hilbert. Les mesures finales sont réalisées dans la base de calcul et la porte U est définie par

$$\mathsf{U} : \begin{cases} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto \left(|01\rangle + \sqrt{2}|10\rangle + |11\rangle\right)/2 \\ |10\rangle \mapsto \left(|01\rangle - \sqrt{2}|10\rangle + |11\rangle\right)/2 \\ |11\rangle \mapsto \left(|01\rangle - |11\rangle\right)/\sqrt{2} \end{cases} . \tag{4.2}$$

Extensions consistantes

Une extension triviale de cette famille à un seul événement constitue en la mesure des deux qubits dans la base de Bell (éq.1.22) au temps t_1, soit $\hat{\sigma}^{(1)} = \{|\Phi^{\pm}\rangle\langle\Phi^{\pm}|, |\Psi^{\pm}\rangle\}\langle\Psi^{\pm}|\}$. [1] Cette extension est toutefois triviale puisque l'effet des portes appliquées entre t_0 et t_1 sur l'état initial est $|01\rangle \mapsto |\Psi^+\rangle$. Ainsi, la mesure $\hat{\sigma}^{(1)}$ est redondante étant donné l'état initial. De plus, cette mesure ne respecte pas la condition de localité imposée par le calcul classique. En effet, les états de Bell sont maximalement enchevêtrés, donc ne constituent pas des mesures locales.

Une extension non triviale de cette famille est réalisée en mesurant les deux qubits dans la base de calcul au temps t_2, c'est-à-dire $\hat{\sigma}^{(2)} = \{|j\rangle\langle j|\}_{j=0,1,2,3}$.

[1] Nous choisissons de décrire les ensembles de projecteurs dans la représentation de Schrödinger puisqu'ils y sont beaucoup plus simples, se prêtent mieux à l'analyse de graphe et surtout puisqu'ils représentent les mesures *réellement* réalisées en laboratoire.

Afin de s'en convaincre, nous construisons le graphe associé à la famille $\mathcal{S} = \{|01\rangle\langle 01|, \hat{\sigma}^{(1)}, \hat{\sigma}^{(2)}, \hat{\sigma}^{(3)}\}$ où $\hat{\sigma}^{(3)}$ représente la mesure finale, donc identique à $\hat{\sigma}^{(2)}$. L'ensemble $\hat{\sigma}^{(1)}$, les mesures de Bell, est inclus dans l'analyse ; si la famille $\mathcal{S}$ est consistante en sa présence, elle le sera en son absence puisqu'il s'agirait alors d'une partition de $\mathcal{S}$ et que le partitionnement préserve la consistance (une conséquence de la règle de somme des probabilités classiques).

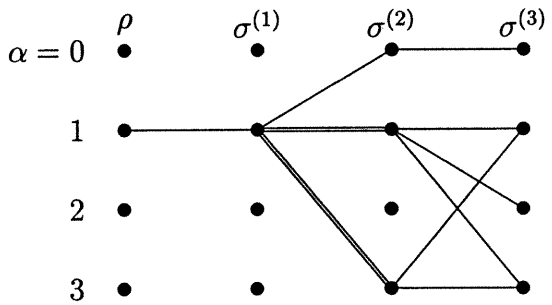

FIG. 4.2 – Analyse de graphe du circuit de la figure 4.1.

Dans ce graphe, nous avons uniquement représenté les arêtes qui sont reliées à l'état initial $|01\rangle$ puisqu'elles sont les seules susceptibles de causer de l'interférence, donc de nuire à la consistance. En raison de la présence de boucles dans le graphe, la famille $\mathcal{S}$ n'est pas consistante moyenne. Afin de vérifier la condition de consistance faible, notons que toutes les fonctions de Green (éq.2.23) associées à ce graphe sont réelles, à l'exception de[2] $G_{11}(t_1, t_2) = -1 + i$ et $G_{13}(t_1, t_2) = -1 - i$, qui sont indiquées par des traits doubles sur le graphe. On vérifie ainsi facilement que le produit des fonctions de Green autour de cette boucle est imaginaire puisque $G_{11}(t_1, t_2)G^*_{13}(t_1, t_2) = -2i$.

4.2. Contrôle classique

La possibilité d'insérer une mesure consistante dans un calcul quantique comporte certains avantages, mais la possibilité de pouvoir répéter cette mesure est

[2]Ces valeurs sont données à une constante multiplicative réelle près.

d'autant plus intéressante. Dowker et Kent ont montré que si un ensemble de projecteurs σ apparaît à deux temps dans une même famille, disons t_a et t_b, alors il peut être inséré à tous les temps entre t_a et t_b [32]. Il est à noter que ce résultat est établi dans la représentation de Heisenberg. Dans la représentation de Schrödinger, plus commune en informatique quantique, sa formulation est plus complexe. Néanmoins, voici la conclusion intéressante que nous en tirons pour le calcul quantique. Soit un circuit composé de n qubits $q_1, \ldots, q_n$ et $|\psi_0\rangle$ et $|\psi_1\rangle$, deux vecteurs orthonormaux dans un espace à deux dimensions. Supposons qu'il soit possible de mesurer le qubit k (q_k) selon la base $\{|\psi_0\rangle, |\psi_1\rangle\}$ à deux temps t_a et t_b dans une famille consistante. Supposons également que les portes appliquées entre les temps t_a et t_b, $U_{a+1}, \ldots, U_b$, n'affectent pas ces deux vecteurs, c'est-à-dire que

$$U_j\left(|\psi_0\rangle \otimes |\Psi\rangle\right) = |\psi_0\rangle \otimes (V_j^0|\Psi\rangle) \quad \text{et} \quad U_j\left(|\psi_1\rangle \otimes |\Psi\rangle\right) = |\psi_1\rangle(V_j^1 \otimes |\Psi\rangle) \qquad (4.3)$$

$\forall\ |\Psi\rangle$ état des autres qubits $q_1, \ldots, q_{k-1}, q_{k+1}, \ldots, q_n$ et $a < j \leq b$. Alors, la mesure de q_k selon la base $\{|\psi\rangle, |\psi_1\rangle\}$ peut être répétée à chaque étape entre t_a et t_b.

Il s'en suit que q_k peut être substitué par un bit classique et une description de la base $\{|\psi_0\rangle, |\psi_1\rangle\}$ pour tout cet intervalle de temps. Le bit agit alors comme contrôle. En effet, on peut voir à (éq.4.3) que l'effet de la porte U_j sur le reste du système est d'implanter la transformation V_j^0 si q_k est dans l'état $|\psi_0\rangle$ et V_j^1 lorsque q_k se trouve dans l'état $|\psi_1\rangle$. Si nous mesurons q_k au temps t_a, nous pouvons exercer ce contrôle classiquement, c'est-à-dire effectuer la première transformation si le résultat obtenu est $|\psi_0\rangle$ et la seconde dans le cas complémentaire. Au temps t_b, l'information est retransférée sur un support quantique.

Retour d'information

À première vue, le protocole décrit plus haut semble invoquer un retour d'information. L'information acquise lors de la mesure est utilisée afin de déterminer quelle opération doit être appliquée au reste du système. Néanmoins, le contrôle exercé ne diffère en rien de celui qu'exercerait le système quantique ayant subit la réduction du paquet d'onde si la mesure avait pris place sans que son résultat

ne soit dévoilé (comme si l'appareil de mesure était dans une boîte noire). Ainsi, l'information classique ne fait que substituer l'information quantique ici, il n'y a pas de réel retour d'information.

Transformée de Fourier semi-classique

Le principe décrit dans cette section a déjà trouvé une application fort importante en informatique quantique : la transformée de Fourier semi-classique de Griffiths et Niu [48]. Leur circuit est une modification du circuit inspiré de Coppersmith [25] basée sur une constatation qui, lorsque interprétée en termes d'histoires consistantes, est très simple. En fait, elle constitue une version plus faible du lemme de Dowker et Kent : si, à partir du temps t, le qubit k agit uniquement comme qubit de contrôle, et ce, jusqu'à la fin du calcul où il sera mesuré dans la base de calcul, alors sa mesure au temps t est automatiquement consistante. Il s'en suit que toutes les opérations contrôlées par q_k à des temps subséquents à t peuvent être contrôlées classiquement.

Le circuit proposé par Coppersmith peut être représenté comme suit. Les

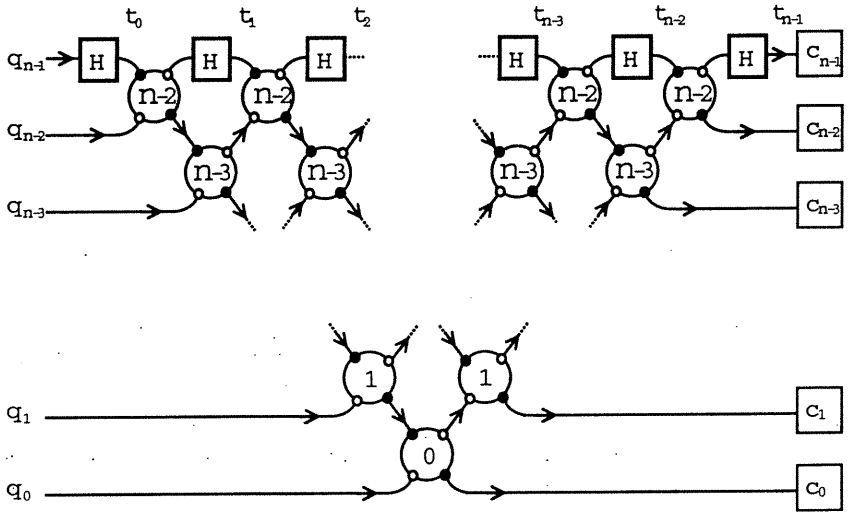

FIG. 4.3 – Circuit réalisant la TFQ inspiré de la description de Coppersmith, tel qu'illustré par Griffiths et Niu [48].

portes binaires indexées d'un entier $m = 0, 1, ..., n-2$ sont définies par

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |10\rangle \\ |11\rangle &\rightarrow \exp\left\{\frac{2\pi i 2^m}{\Omega}\right\}|11\rangle. \end{aligned} \tag{4.4}$$

L'analyse conduite par Griffiths et Niu permet de remplacer ce circuit, lorsqu'il est suivi de mesures dans la base de calcul, par le circuit semi-classique suivant. Dans ce circuit, les fils simples transportent des qubits alors que les fils doubles

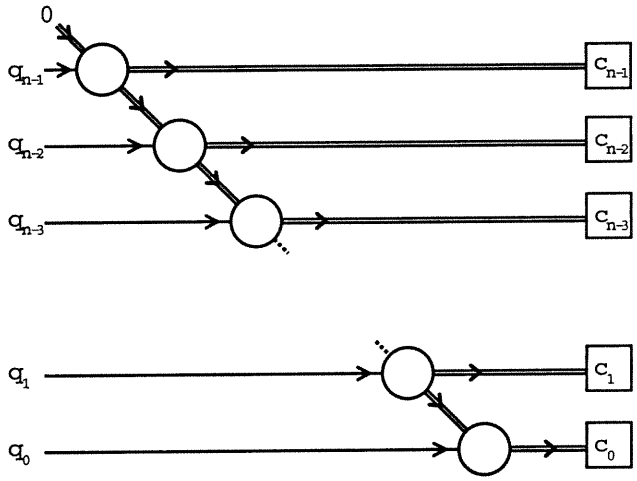

FIG. 4.4 – Circuit réalisant la TFQ semi-classique de Griffiths et Niu [48].

transportent de l'information classique (au plus, une chaîne de n bits). Chaque porte possède une entrée classique, une entrée quantique et deux sorties classiques. L'entrée classique représente une phase ϕ et l'action de la porte est d'abord d'appliquer la transformation unitaire sur l'entrée quantique

$$\begin{aligned} |0\rangle &\rightarrow \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \\ |1\rangle &\rightarrow \frac{\left(|0\rangle + e^{i2\pi\phi}|1\rangle\right)}{\sqrt{2}} \end{aligned} \tag{4.5}$$

puis d'effectuer une mesure ($|0\rangle$ *vs.* $|1\rangle$) du qubit pour obtenir un bit classique b. Les deux sorties classiques sont le bit b mesuré (qui sera le j^e bit de la mesure

finale c) et la nouvelle phase obtenue par l'application

$$\phi \rightarrow \frac{\phi}{2} + \frac{b}{4} \tag{4.6}$$

qui sera l'entrée classique de la $(j+1)^e$ porte.

Avec cette construction, la transformée de Fourier, lorsqu'elle apparaît à la fin d'un calcul, peut être accomplie uniquement à l'aide de portes à un qubit et de contrôle classique. Ce résultat est d'une grande importance étant donné l'omniprésence de la transformée de Fourier en informatique quantique [22]. Il est à noter que, par symétrie d'inversion temporelle de la fonction de cohérence (éq.2.12) pour les états initiaux purs, le résultat s'applique aussi bien à une transformée de Fourier inverse appliquée en début de calcul, également fort utile.

4.3. Résistance au bruit

Ce qui motive l'utilisation, lorsque possible, d'information classique au détriment de l'information quantique est l'extrême difficulté à manipuler cette dernière. L'information classique est robuste et stable alors que l'information quantique est fragile puisqu'elle perd facilement sa cohérence. Ironiquement, ces attributs positifs de l'information classique et négatifs de l'information quantique sont dus à une même cause : l'irréversibilité causée par l'interaction avec l'environnement. En effet, la stabilité de l'information classique est une conséquence d'une dissipation, une sorte de freinage, ce qui ne peut se produire dans un système isolé. De même, la perte de cohérence de l'information quantique est due à une interaction avec l'environnement comme nous en avons discuté à la section 1.5.6.

Dans le reste de cette section, nous montrons comment une analyse de classicalité peut contribuer à augmenter la résistance au bruit des algorithmes quantiques.

Temps de cohérence

L'avantage évident qu'offre l'analyse de classicalité à la résistance au bruit est la stabilité de l'information classique. En effet, lorsque l'information quantique est substituée par de l'information classique, elle devient, à toutes fins pratiques,

insensible à l'environnement. Ultimement, seulement les parties fondamentalement quantiques de l'algorithme demeurent vulnérables au bruit.

De plus, supposons qu'une analyse complète de classicalité nous indique qu'il est possible de mesurer le qubit k d_k fois tout au long du circuit. En principe, un temps de cohérence T—le temps d'exécution de l'algorithme—est requis pour q_k afin que le résultat du calcul soit significatif. Néanmoins, l'analyse de classicalité nous indique que le temps de cohérence nécessaire doit être le plus grand temps séparant deux mesures d'un même qubit. Grossièrement, l'environnement augmente l'entropie du système, mais chaque mesure vient rafraîchir le qubit, donc combat l'effet de l'environnement, comme le font les codes correcteurs. D'ailleurs, en présence de codes correcteurs, l'argument présenté ici doit être modifié puisque le temps T n'est plus le temps d'exécution de l'algorithme mais le temps séparant les vérifications d'erreurs.

Décohérence consistante

La substitution d'information quantique par de l'information classique exige des mesures projectives, c'est-à-dire des mesures du type décrit aux quatrième et cinquième postulats. Malheureusement, de telles mesures sont impossibles à réaliser sur certaines implantations d'ordinateurs quantiques, notamment pour celles basées sur la résonance magnétique nucléaire (RMN) à l'état liquide. Cependant, tout n'est pas perdu.

Introduisons d'abord la notion de mesure faible dans une base orthonormale $\{|\psi_0\rangle, |\psi_1\rangle\}$. Une mesure projective aurait pour effet de transformer l'état du qubit k $|\phi\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle$ en un mélange statistique $\rho_m = |\alpha|^2|\psi_0\rangle\langle\psi_0| + |\beta|^2|\psi_1\rangle\langle\psi_1|$. Cependant, l'interaction avec l'environnement est incontrôlée ; la mesure effective qui en résulte ne se produit donc pas avec certitude. L'état résultant de ce processus incertain est donc le mélange de l'état non mesuré et de l'état mesuré $\epsilon(|\alpha|^2|\psi_0\rangle\langle\psi_0| + |\beta|^2|\psi_1\rangle\langle\psi_1|) + (1-\epsilon)|\phi\rangle\langle\phi|$, où ϵ est la probabilité que la mesure se soit produite. En général, ϵ tend exponentiellement rapidement vers 1 avec le temps.[3]

[3]Cette description des mesures faibles est basée sur une approche par équation maîtresse,

Supposons que la décohérence causée par l'interaction avec l'environnement ait pour effet de mesurer *faiblement* le qubit k dans la base $\{|\psi_0\rangle, |\psi_1\rangle\}$. Si, par coïncidence, la mesure $\{|\psi_0\rangle, |\psi_1\rangle\}$ constitue une extension consistante de la famille originale, alors l'effet de l'environnement ne se fera pas ressentir. Ce fait peut être reformulé sous forme de lemme dont la preuve élémentaire est omise.

Lemme 4. *Si la famille $\mathcal{S} = \{\rho, \sigma^{(1)}, \ldots, \sigma^{(n)}\}$ est consistante, alors les mesures faibles $\sigma^{(k)}$ avec paramètres ϵ_k quelconques sont logiquement compatibles.*

Dans l'énoncé de ce lemme, nous employons «logiquement compatibles» plutôt que «consistantes» puisque le formalisme des HC n'est pas adapté aux mesures faibles.

À moins d'une coïncidence extraordinaire, la situation présentée ci-haut n'est pas réaliste. Cependant, si la mesure faible de l'environnement se produit dans une base locale $\{|\mu_0\rangle, |\mu_1\rangle\}$ différente de la base consistante, alors son effet peut être annulé en appliquant la transformation unitaire

$$U = |\mu_0\rangle\langle\psi_0| + |\mu_1\rangle\langle\psi_1| \tag{4.7}$$

au qubit k. Évidemment, cette transformation altère l'état de q_k, mais de façon réversible. Ainsi, lorsque vient le temps d'utiliser q_k, la transformation U peut être inversée par $U^\dagger$. Pendant le temps qui s'écoule entre ces deux transformations, q_k est complètement à l'abri de l'environnement. Plus précisément, l'environnement détruit la cohérence de q_k et modifie son contenu en information, mais son information *utile*—celle qui mène au résultat final—demeure intacte.

Combattre le feu avec le feu

Dans certaines situations, nous ne savons pas dans quelle base la décohérence agit. Il est donc impossible de faire coïncider la base consistante avec la base de

c'est-à-dire une équation différentielle stochastique décrivant l'évolution du système [63]. Il est également possible de les décrire à l'aide d'une évolution unitaire du système et l'environnement combinés. Dans ce cas, ϵ peut être interprété comme la «qualité» de l'information sur l'état du système laissée dans l'environment [96, 67].

décohérence à tout coup. Par contre, certaines hypothèses raisonnables peuvent êtres émises sur le couplage entre l'environnement et le système. C'est le cas lorsque nous construisons des codes correcteurs. En général, nous supposons que l'environnement agit sur les qubits séparément ; si une erreur à plusieurs qubits se produit, les codes correcteurs pourront faillir à la corriger.

Une caractéristique de la décohérence locale—qui mesure faiblement les qubits individuellement—est qu'elle détruit l'enchevêtrement. L'enchevêtrement est une caractéristique purement quantique ; plusieurs croient qu'elle est essentielle à l'efficacité des algorithmes quantiques (*e.g.* [34]). Ainsi, il est fort possible que la conséquence d'une décohérence locale soit tout à fait tragique !

Pourtant, dans l'exemple de la section 4.1, la mesure consistante détruit tout enchevêtrement présent sans affecter le résultat final. En effet, l'état du système au temps t_2 (figure 4.1) est $|\psi(t_2)\rangle = (2|00\rangle + (-1+i)|01\rangle + (-1-i)|11\rangle)/\sqrt{8}$. Cet état contient 0,4165 paires EPR d'enchevêtrement (*cf.* section 1.4) qui sont complètement détruites par la mesure.

Il est à noter que la destruction «consistante» d'enchevêtrement de cet exemple diffère considérablement de celle présente dans la transformée de Fourier (TF) semi-classique. Les mesures consistantes utilisées afin de classicaliser la TF détruisent l'enchevêtrement présent dans le système, mais seulement *dans une direction du temps.*

Cette remarque mérite certainement quelques éclaircissements. Les mesures introduites dans la TF sont consistantes puisqu'elles constituent simplement un devancement des mesures finales. Ce devancement est possible puisque la mesure finale commute avec toutes les opérations intermédiaires. Ainsi, les mesures consistantes ne font que détruire l'enchevêtrement qui serait détruit de toutes façons lors de la mesure finale. Si le circuit est renversé, c'est-à-dire si nous initialisons le registre de l'ordinateur quantique dans un des états pouvant ressortir de la mesure finale et appliquons les transformations inverses, alors aucun enchevêtrement n'est présent dans le système lorsque les mesures consistantes sont appliquées.

Dans l'exemple de la section 4.1, la destruction d'enchevêtrement par les mesures consistantes ne correspond pas à celle des mesures finales. À preuve, un des

résultats possibles de la mesure finale est $|01\rangle$ qui, à la suite de l'application de $\mathsf{U}^\dagger$ donne $(|01\rangle + |10\rangle + \sqrt{2}|11\rangle)/2$ qui contient $\approx 0,35$ paires EPR d'enchevêtrement. Ainsi, dans cet exemple, l'enchevêtrement est détruit dans les deux directions du temps.

Puisqu'il est parfois possible de détruire l'enchevêtrement sans affecter les résultats du calcul, notre intuition nous indique que cette procédure pourrait adoucir les effets néfastes de la décohérence locale. C'est l'idée de combattre le feu avec le feu. La décohérence locale détruit l'enchevêtrement, alors nous la détruisons à l'aide de mesures consistantes avant même que l'environnement puisse intervenir. Intuitivement, cela laisse moins «d'espace de phase» dans lequel les dégâts de la décohérence peuvent s'étendre.

Nous n'avons pas réussi à prouver cette intuition de façon générale, mais un exemple vient l'appuyer. Si nous laissons la décohérence agir dans une base locale aléatoire entre les portes F et U de la figure 4.1, il en résultera une distribution de probabilité de la mesure finale $\tilde{Pr}$ différente de celle en l'absence de décohérence Pr, la distribution convoitée. La perturbation causée par l'environnement sur les résultats finaux peut être mesurée à l'aide de l'entropie relative $H(Pr||\tilde{Pr}) = \sum_j Pr(j) \log \frac{Pr(j)}{\tilde{Pr}(j)}$ (distance de Kullback-Leibler [26]). Cette entropie est calculée dans deux situations : H_0 mesure la perturbation lorsqu'aucune précaution n'est prise afin de contrer l'effet de la décohérence ; H_m est la mesure de la perturbation causée par l'environnement lorsqu'une mesure consistante locale est réalisée afin de détruire l'enchevêtrement avant que la décohérence agisse. Puisque la base dans laquelle la décohérence agit est inconnue, nous devons considérer la moyenne de ces perturbations sur toutes les bases locales $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$, $\langle H \rangle = \int H(\psi_0, \psi_1, \psi_2, \psi_3) d(\psi_0, \psi_1, \psi_2, \psi_3)$. Une réduction de l'entropie relative d'environ 25% est observée lorsque le système est forcé à un état local avant d'être perturbé par l'environnement.

4.4. Calcul avec états mixtes

Nous sortons ici du cadre général de ce mémoire afin de nous pencher sur la question controversée du calcul avec états mixtes. À l'équilibre thermodynamique,

l'état d'un système à température T est $\rho = e^{-\beta H}/Z$ où $\beta = 1/k_B T$, H est l'Hamiltonien du système et $Z = Tr\{e^{-\beta H}\}$. L'entropie de cette matrice de densité augmente avec la température. Quand la température est infinie, la matrice de densité est proportionnelle à l'identité, donc l'entropie est simplement le logarithme de la dimension de l'espace de Hilbert $\log \Omega$. Idéalement, la première étape d'un calcul quantique serait d'initialiser ce système à un état pur. Cela se réalise à l'aide d'une mesure projective. Toutefois, comme nous en avons discuté à la section 1.4.5, certains systèmes, notamment ceux basés sur la résonance magnétique nucléaire (RMN) à l'état liquide, n'admettent que des mesures d'ensemble qui ne perturbent pas l'état, donc ne permettent pas d'initialiser.

La question soulevée est de savoir si un système à haute entropie admettant uniquement des opérations unitaires et des mesures d'ensemble peut servir de calculateur quantique efficace. Dans ce qui suit, nous décrivons d'abord les techniques générales du calcul avec état mixtes, puis nous commentons sur la nature fondamentalement quantique de sa dynamique.

État pseudo-pur

La première étape d'un calcul à état mixte est la création d'un état pseudo-pur. Il s'agit de transformer l'état $\rho = e^{-\beta H}/Z$ en

$$\rho = \frac{1-\epsilon}{\Omega}\mathbb{1} + \epsilon|\psi\rangle\langle\psi| \tag{4.8}$$

où $|\psi\rangle$ est l'état initial qui serait utilisé dans un système à état pur et ϵ est la polarisation. La préparation d'un tel état n'est certes pas facile, mais théoriquement possible en temps polynomiale dans le nombre de qubits. Avec probabilité ϵ, le système se trouve dans l'état désiré, alors qu'avec probabilité complémentaire, il est dans un mélange uniforme de tous les états (y compris $|\psi\rangle$). Cette dernière partie du mélange n'évolue pas puisque $U\mathbb{1}U^\dagger = \mathbb{1}$. Ainsi, l'évolution peut être décrite en considérant uniquement la partie «pure» du mélange.

Cette dernière remarque est également valable en ce qui concerne la consistance d'une famille dont l'état initial est pseudo-pur, comme le montre le lemme suivant.

Lemme 5. *Soit $\mathcal{S} = \{|\psi\rangle\langle\psi|, \sigma^{(1)}, \ldots, \sigma^{(n)}\}$, une famille d'histoires consistantes.*

(Ce résultat s'applique à toutes les conditions de consistance.) Alors la famille $\mathcal{S}' = \{\rho, \sigma^{(1)}, \ldots, \sigma^{(n)}\}$ *où* $\rho = \frac{1-\epsilon}{\Omega}\mathbb{1} + \epsilon|\psi\rangle\langle\psi|$ *est consistante de calcul (éq.3.2).*

Preuve. Il est général de supposer que la famille $\mathcal{S}$ satisfait à la condition de consistance calculatoire (éq.3.2). On vérifie alors facilement que la famille $\mathcal{S}'$ est consistante de calcul. □

Si une famille d'histoire est consistante pour un ensemble d'états initiaux purs, alors elle le sera pour l'état initial constitué de leur mélange statistique. L'inverse n'est généralement pas vrai. Dans le cas d'un état pseudo-pur, l'analyse de graphe se prête bien à l'étude de consistance mais risque de ne pas être générale. En d'autres termes, si le graphe construit avec l'analogue pur de l'état pseudo-pur indique une consistance, alors il y a consistance avec l'état pseudo-pur. Cependant, si l'analyse de graphe indique que la famille est inconsistante avec l'état initial pur, il est possible qu'elle soit consistante pour l'analogue pseudo-pur.

De plus, l'analyse de graphe fonctionne uniquement avec les projecteurs de rang 1, ce qui est général pour un état initial pur mais peut-être pas pour un état mixte. Ce qui manque est un analogue du Théorème 2 pour état mixte. Nous croyons que les mesures complètes sont générales pour les états mixtes lorsque le retour d'information est possible. L'intuition derrière cette conjecture est la suivante : les états mixtes peuvent être purifiés (éq.3.9) à l'aide de systèmes ancillaires et les histoires consistantes à branchement sont équivalentes à celles sans branchement accompagnées de systèmes ancillaires.

Refroidissement algorithmique

Les valeurs expérimentales de la polarisation sont très basses. L'ordre de grandeur typique est $\epsilon \approx 10^{-5}$. Puisque la RMN liquide constitue une réalisation statistique de l'ensemble, nous pouvons dire que seule une fraction 10^{-5} des sous-systèmes se trouvent véritablement dans l'état analogue pur.

Cette probabilité peut être augmentée si nous sommes prêts à sacrifier certaines composantes de l'ordinateur. Il est possible de partiellement transférer la polarisation d'un sous-système à un autre [80]. Par exemple, si trois qubits sont initialement dans l'état pseudo-pur $\rho_\epsilon = \frac{1-\epsilon}{2}\mathbb{1} + \epsilon|0\rangle\langle 0|$, alors le circuit suivant

augmente la polarisation du qubit supérieur d'un facteur 3/2 au détriment de la

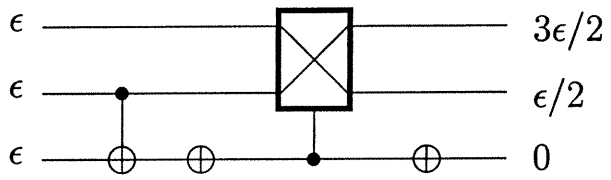

FIG. 4.5 – Routine de base de refroidissement algorithmique.

polarisation des deux autres qubits, dont on disposera. Nous avons introduit dans ce circuit la porte d'échange qui permute ses deux entrées. Sur la figure 4.5, les polarisations sont données au premier ordre en ϵ uniquement. Il est possible de répéter cette routine de base afin d'augmenter davantage la polarisation du premier qubit. L'utilisation d'un bain de chaleur permet, en principe, de refroidir le système à volonté [18]. En fait, la température finie du bain de chaleur signifie qu'il y a un certain ordre ; le refroidissement algorithmique tire avantage de cet ordre. Le désordre total n'est possible qu'à température infinie.

Absence d'enchevêtrement

L'argument principal indiquant que le calcul quantique avec états hautement mélangés est inefficace est l'absence d'enchevêtrement dans ces systèmes [21]. Nous n'avons pas décrit comment se mesure l'enchevêtrement des états mixtes, mais il est évident qu'un mélange statistique d'états non enchevêtrés n'est pas enchevêtré. (Sans quoi le simple fait d'oublier pourrait créer de l'enchevêtrement !) Soit ρ, l'état d'un système bipartie partagé entre Alice et Bob. S'il est possible d'écrire $\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$ où les p_j sont des probabilités et où les états $|\psi_j\rangle = |\phi_j^{\mathcal{A}}\rangle \otimes |\phi_j^{\mathcal{B}}\rangle$ sont séparables, alors il n'y a pas d'enchevêtrement entre $\mathcal{A}$ et $\mathcal{B}$. Comme nous l'avons mentionné, l'enchevêtrement est souvent ciblé comme responsable de la puissance de calcul du monde quantique [34], donc son absence anéantirait tout espoir d'en tirer avantage.

Lorsque $\epsilon \leq 1/3$, tout état pseudo-pur à deux qubits est séparable. Par exemple, lorsque ρ est un état pseudo-pur représentant un des états de Bell

(éq.1.22) : $\rho = \frac{1-\epsilon}{4}\mathbb{1} + \epsilon|\Phi^+\rangle\langle\Phi^+|$ avec $\epsilon \leq \frac{1}{3}$, le mélange $\{(\nwarrow\nwarrow, \frac{\epsilon}{2}), (\nearrow\nearrow, \frac{\epsilon}{2}), (\circlearrowleft\circlearrowleft, \frac{\epsilon}{2}), (\circlearrowright\circlearrowright, \frac{\epsilon}{2}), (\uparrow\uparrow, \frac{1-\epsilon}{4}), (\downarrow\downarrow, \frac{1-\epsilon}{4}), (\uparrow\downarrow, \frac{1-3\epsilon}{4}), (\downarrow\uparrow, \frac{1-3\epsilon}{4})\}$ génère bien ρ.[4] Cette polarisation critique diminue avec la taille du système. Cependant, avec ce que nous pouvons produire en laboratoire aujourd'hui, il est clair qu'aucun enchevêtrement n'est présent. Il est possible qu'en augmentant la taille de l'ordinateur, nous puissions un jour observer de l'enchevêtrement à la température ambiante. Néanmoins, il est à noter qu'un effet compétitionne avec cette diminution de la polarisation critique ; nos techniques actuelles de préparation d'état pseudo-purs font diminuer exponentiellement la polarisation.

Limitations statiques vs limitations dynamiques

Nous croyons qu'un argument visant à démontrer la classicalité du calcul à état hautement mélangé impliquant l'absence d'enchevêtrement n'est pas fondé[5]. L'enchevêtrement est une caractéristique de l'information quantique, pas de la *manipulation* d'information quantique. Ainsi, cet argument enraye toute possibilité d'utiliser des systèmes basés sur la RMN à l'état liquide afin de téléporter ou de réaliser d'autres tâches de communication quantique. Cependant, il n'impose aucune limitation sur la dynamique de tels systèmes.

Par analogie avec la discussion de la section 2.2, l'entropie élevée du système constitue une condition initiale. Ce qui limite le type de dynamique d'un système sont les règles de sélection. Ici, seule la condition d'unitarité du sixième postulat restreint le type d'évolution du système ; la température élevée n'impose aucune règle de sélection.

Les notions de décohérence et de mélange statistique sont très intimement liées. La décohérence transforme un état pur en une mixture en raison de corrélations établies entre le système et l'environnement. Cependant, la mixture d'un état n'implique en rien la présence de décohérence[6]. L'analyse de Aharonov et Ben-

[4]Nous utilisons une notation standard de polarisation : $\uparrow = |0\rangle$, $\downarrow = |1\rangle$, $\nearrow = |0\rangle + |1\rangle$, $\nwarrow = |0\rangle - |1\rangle$, $\circlearrowright = |0\rangle + i|1\rangle$, $\circlearrowleft = |0\rangle - i|1\rangle$ avec normalisation appropriée.

[5]Certains arguments similaires à ceux présentés ici sont avancés dans [62].

[6]Les adeptes de l'Église de l'espace de Hilbert élargi diront qu'une mixture implique une

Or (*cf.* section 3.1.2 et [2]) nous indique qu'une trop forte décohérence anéantit tout espoir de construire un ordinateur quantique plus efficace qu'un calculateur classique. Ceci n'est pas surprenant puisque la décohérence est un processus dynamique, donc impose des limitations sur la manipulation d'information quantique, un processus dynamique. Cependant, les systèmes restreints à une entropie élevée, une limitation statique, possèdent une évolution unitaire ; aucune limitation s'impose sur leur dynamique, donc l'analyse de Aharonov et Ben-Or ne s'applique pas, elle est complètement hors contexte.

En plus de cette distinction fondamentale entre les deux types de limitations, l'absence d'enchevêtrement n'implique pas une classicalité de l'information. Ollivier et Żurek [68] ainsi que Bennett *et al.* [11] ont démontré que certains phénomènes purement quantiques prennent place dans un contexte d'information (statique) où aucun enchevêtrement n'est présent. L'exemple le plus frappant d'information quantique sans enchevêtrement est le protocole de cryptographie quantique de Bennett et Brassard [8]. Bien qu'aucun enchevêtrement ne soit nécessaire à la réalisation de ce protocole, les effets quantiques y sont prépondérants puisque aucun protocole similaire n'est réalisable classiquement. Ce que ces trois exemples partagent en commun est l'existence d'états non orthogonaux, concept absent en mécanique classique.

Système mixte à dynamique quantique

La question du calcul quantique avec états hautement mélangés demeure à ce jour ouverte. Nous croyons que l'argument principal, c'est-à-dire l'absence d'enchevêtrement, n'est pas fondé puisqu'il n'impose pas de limitation pertinente au problème. Certains résultats, en particulier ceux de Knill et Laflamme [58], semblent indiquer quelques avantages du calcul quantique avec états mixtes mais n'apportent pas de preuve. Cela n'est pas surprenant puisque nous ne possédons même pas de preuve de l'avantage du calcul quantique avec états purs, sauf pour les problèmes à oracle !

certaine décohérence dans le passé. De notre point de vue, l'ignorance de l'expérimentateur explique très bien l'entropie finie du système.

Dans ce qui suit, nous n'apportons pas d'argument direct concernant les capacités *calculatoires* des systèmes à états mixtes. Plutôt, nous démontrons qu'ils manifestent un *comportement dynamique sans équivalent classique.* Soit une famille d'histoires à deux événements avec état initial de la forme (éq.4.8). La fonction de cohérence (éq.2.12) associée à cette famille est

$$\begin{aligned} & Tr\left\{P^{(2)}_{\alpha_2}P^{(1)}_{\alpha_1}\rho P^{(1)}_{\beta_1}P^{(2)}_{\beta_2}\right\} \\ = \; & \frac{(1-\epsilon)}{\Omega}\delta_{\alpha_1\beta_1}\delta_{\alpha_2\beta_2}Tr\left\{P^{(2)}_{\alpha_2}P^{(1)}_{\alpha_1}\right\} \\ + \; & \epsilon\delta_{\alpha_2\beta_2}Tr\left\{P^{(2)}_{\alpha_2}P^{(1)}_{\alpha_1}|\psi\rangle\langle\psi|P^{(1)}_{\beta_1}\right\} \end{aligned} \tag{4.9}$$

ou encore

$$D_\epsilon(\alpha_1,\alpha_2;\beta_1,\beta_2) = \frac{(1-\epsilon)}{\Omega}\delta_{\alpha_1\beta_1}\delta_{\alpha_2\beta_2}Tr\left\{P^{(2)}_{\alpha_2}P^{(1)}_{\alpha_1}\right\} + \epsilon D_1(\alpha_1,\alpha_2;\beta_1,\beta_2) \tag{4.10}$$

où l'indice représente la polarisation de l'état initial. Ainsi, la famille est consistante si et seulement si la famille analogue à état initial pur est consistante. Afin de compléter l'argument, il s'agit de trouver une famille d'histoire à deux événements qui, lorsque l'état initial est pur, n'est pas consistante. Sans doute le plus simple exemple provient de l'expérience des fentes de Young. Les deux événements sont le passage des particules dans une des fentes et leur détection sur un écran. Nous savons depuis la petite école que l'inférence statistique tirée des probabilités conditionnelles d'une telle expérience est logiquement incompatible : la famille est inconsistante. L'équation 4.10 nous indique donc que la famille analogue à état initial pseudo-pur n'est pas consistante.

Comme nous le savons, c'est l'interférence qui est responsable de cette violation de la logique classique. *L'interférence est un processus dynamique.* L'entropie initiale du système ne limite pas son évolution (sauf lorsque l'entropie est maximale). Ici, c'est encore l'existence d'états non orthogonaux qui entre en jeu. Lorsque la polarisation est suffisamment petite, l'état du système peut s'exprimer sous forme de mélange statistique d'états purs séparables. Néanmoins, ces états ne sont généralement pas orthogonaux, comme le montre l'exemple de l'état de Bell pseudo-pur (un mélange de huit états dans un espace à quatre dimensions).

Si l'état du système pouvait s'écrire à tout instant du calcul comme un mélange d'états purs séparables mutuellement orthogonaux, il serait possible de simuler sa dynamique à l'aide de spins classiques (simplement des vecteurs dans une sphère unitaire). Puisque tel n'est pas le cas, il semble qu'une simulation classique soit hors de portée sauf, bien entendu, si nous acceptons une décroissance exponentielle de ses performances [79].

4.5. Uniformité

Quoi de mieux pour clore cette discussion qu'une note pessimiste ! Nous avons passé sous silence un aspect très important d'une analyse de classicalité : l'uniformité. Nous devons exiger d'une analyse qu'elle soit valable pour tout le domaine des états initiaux d'un circuit donné et qu'elle se généralise simplement à des circuits de plus grande taille. Si une nouvelle analyse doit être entreprise pour chaque exemplaire du problème, alors ce temps d'analyse doit être inclus dans le temps d'exécution du calcul. En raison de la taille exponentielle des graphes utilisés pour l'analyse, l'espoir d'en tirer avantage est anéanti.

La transformée de Fourier semi-classique est un exemple de processus uniforme : Les mesures à effectuer sont indépendantes de l'entrée et il existe une description simple du procédé pour toute taille du circuit. L'indépendance des mesures envers l'entrée n'est toutefois pas nécessaire, une dépendance simple (polynomialement calculable) suffit.

Il ne serait pas étonnant que la plupart des algorithmes quantiques admettent des mesures consistantes locales au long de leur exécution les rendant semi-classiques. Par contre, le nombre de procédures semi-classique *uniformes* risque d'être beaucoup moins élevé. Ces dernières doivent relever de symétries très particulières du circuit.

5 — Conclusions

Nous avons montré comment les histoires consistantes peuvent êtres adaptées à l'étude de classicalité d'un circuit quantique. Une telle analyse permet, en principe, de substituer une part de l'information quantique par de l'information classique sans affecter les performances du processus de façon considérable. La réalisation d'une analyse complète d'un circuit quantique en termes d'histoires consistantes est une tâche fort complexe.

Certains de nos résultats allègent cette tâche. Notamment, les résultats bornant le nombre d'extensions consistantes non triviales permettent de tirer certaines conclusions sans devoir analyser le processus quantique dans ses détails. L'adaptation de l'analyse de graphe à des conditions moins restrictives constituerait un pas essentiel vers une analyse simplifiée. Nous n'avons malheureusement pas réalisé cet exploit pour la condition de consistance de calcul, mais l'adaptation à la condition faible constitue un premier pas. La possibilité qu'offre le théorème 2 de considérer uniquement les familles constituées de projecteurs de rang 1 allège également la tâche d'analyse de façon considérable.

La possibilité fantaisiste de conduire une analyse de classicalité complète engendrerait un grand nombre de conséquences. Parmi les plus importantes, deux nouveaux types de prévention d'erreurs s'offriraient. Le premier est la possibilité de faire coïncider la base de décohérence avec une base consistante. Ce type de prévention d'erreur s'apparente aux sous-systèmes libres de décohérence. La seconde possibilité, dont l'efficacité n'a pas été démontrée, constitue à détruire l'enchevêtrement de façon consistante avant que le système subisse les effets néfastes d'une décohérence locale, entraînant une destruction d'enchevêtrement.

Finalement, mais de grande importance, l'analyse de classicalité nous a permis d'apporter certaines réflexions sur la question controversée du calcul avec états

mixtes. Nous avons démontré que malgré une absence totale d'enchevêtrement en tout temps, certains systèmes à haute entropie affichent une dynamique sans équivalent classique. Cette constatation ne règle évidemment pas la question portant sur la puissance de calcul, mais forme un argument de poids aux principales objections.

Bibliographie

[1] D. S. Abrams et S. Lloyd. Simulation of many-mody Fermi systems on a universal quantum computer. *Phys. Rev. Lett*, **79** p.2586, 1997.

[2] D. Aharonov et M. Ben-Or. Fault tolerant quantum computation with constant error. *Proc. of the 29th Annual ACM Symposium on Theory of Computing*, p.176, 1997.

[3] A. Aspect, P. Grangier et G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.*, **47** p.460, 1981.

[4] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, **1** p.195, 1964.

[5] P. Benioff. Quantum mechanical Hamiltonian models of Turing machines. *J. of Stat. Phys.*, **29** p.515, 1982.

[6] C. H. Bennett. The thermodynamics of computation—A review. *Int. J. of The. Phys.*, **21** p.905, 1982.

[7] C. H. Bennett, H. J. Bernstein, S. Popescu et B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev.* **A**, **53** p.2046, 1996.

[8] C. H. Bennett et G. Brassard. Quantum cryptography : Public key distribution and coin tossing. *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing*, p.175, 1984.

[9] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual EPR and classical channels. *Phys. Rev. Lett.*, **70** p.1895, 1993.

[10] C. H. Bennett, G. Brassard et N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, **68** p.557, 1992.

[11] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin et W. K. Wootters. Quantum nonlocality without entanglement. *Phys. Rev.* **A**, **59** p.1070, 1999.

[12] C. H. Bennett et P. W. Shor. Quantum information theory. *IEEE Trans. Info. Theo.*, **44** p.2724, 1998.

[13] E. Bernstein et U. Vazirani. Quantum complexity theory. *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing*, page 11, 1993.

[14] E. Bernstein et U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26 p.1411, 1997.

[15] A. Berthiaume. L'ordinateur quantique : Complexité et stabilité des calculs. Thèse de doctorat, Université de Montréal, 1996.
`http ://www.iro.umontreal.ca/~utheorie/.`

[16] A. Blais. Calcul quantique universel sur qubits supraconducteurs. Mémoire de maîtrise, Université de Sherbrooke, 1999.
`http ://www.physique.usherb.ca/~ablais/.`

[17] M. Boyer, G. Brassard, P. Høyer et A. Tapp. Tight bounds on quantum searching. *Fortsch. Phys.*, **46** p.493, 1998.

[18] P. O. Boykin, T. Mor, V. Roychowdhury, F. Vatan et R. Vrijen. Algorithmic cooling and scalable NMR quantum computers. arXiv `quant-ph/0106093`, 2001.

[19] G. Brassard. Quantum communication complexity (a survey). arXiv `quant-ph/0101005`, 2001.

[20] G. Brassard, N. Lütkenhaus, T. Mor et B. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, **85** p.1330, 2000.

[21] S. Braunstein, C. Caves, R. Jozsa, N. Linden, S. Popescu et R. Schack. Separability of very noisy states and implications for NMR quantum computing. *Phys. Rev. Lett.*, **83** p.1054, 1999.

[22] R. Cleve, A. Ekert, C. Macchiavello et M. Mosca. Quantum algorithms revisited. *Proc. Royal Soc. of London* **A**, **454** p.339, 1998.

[23] R. Cleve et J. Watrous. Fast parallel circuit for the quantum Fourier transform. *41th Annual Symposium on Foundations of Computer Science*, page 526, 2000.

[24] C. Cohen-Tannoudji, B. Diu et F. Laloë. *Mécanique Quantique.* Hermann, Paris, 1996.

[25] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. *IBM Research Report RC19642*, 1994.

[26] T. M. Cover et J. A. Thomas. *Elements of Information Theory.* Wiley, 1991.

[27] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. Royal Soc. of London* **A**, **400** p.97, 1985.

[28] D. Deutsch. Quantum computational networks. *Proc. Royal Soc. of London* **A**, **425** p.73, 1989.

[29] D. Deutsch et R. Jozsa. Rapid solution of problems by quantum computation. *Proc. Royal Soc. of London* **A**, **439** p.1992, 553.

[30] D. Dieks. Communication by EPR devices. *Phys. Lett.* **A**, **92** p.271, 1982.

[31] L. Diósi. On maximum number of decoherent histories. *Phys. Lett.* **A**, **203** p.267, 1995.

[32] F. Dowker et A. Kent. On the consistent histories approach to quantum mechanics. *J. Stat. Phys.*, **82** p.1575, 1996.

[33] A. Einstein, B. Podolsky et N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, **47** p.777, 1935.

[34] A. Ekert et R. Jozsa. Quantum algorithms : entanglement-enhanced information processing. *Phil. Trans. Royal Soc. of London* **A**, **356** p.1769, 1998.

[35] H. Everett III. Relative state formulation of quantum mechanics. *Rev. of Mod. Phys.*, **29** p.454, 1957.

[36] E. Farhi, J., Goldstone, S. Gutmann et M. Sipser. Quantum computation by adiabatic evolution. arXiv `quant-ph/0001106`, 2000.

[37] R. P. Feynman. Simulating physics with computers. *Int. J. of The. Phys.*, **21** p.467, 1982.

[38] R. P. Feynman et A. R. Hibbs. *Quantum mechanics and path integrals.* McGraw-Hill, New York, 1965.

[39] M. Gell-Mann et J. B. Hartle. Quantum mechanics in the light of quantum cosmology. Dans W. H. Żurek, éditeur, *Complexity, Entropy and the Physics of Information*, p.425, 1991.

[40] M. Gell-Mann et J. B. Hartle. Classical equations for quantum systems. *Phys. Rev.* **D**, **47** p.3345, 1993.

[41] M. Gell-Mann et J. B. Hartle. Time symmetry and asymmetry in quantum mechanics and quantum cosmology. Dans J. J. Halliwell, J. Pérez-Mercader et W. H. Żurek, éditeurs, *Physical Origins of Time Asymmetry*, p.311, 1994.

[42] M. Gell-Mann et J. B. Hartle. Strong decoherence. arXiv `gr-qc/9509054`, 1995.

[43] D. Giulini, E. Joos, C. Kiefer, I. O. Stamatescu et H. D. Zeh. *Decoherence and the Appearance of a Classical World in Quantum Theory.* Springer, New York, 1996.

[44] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev.* **A**, **54** p.1862, 1996.

[45] D. Gottesman et I. Chuang. Demonstrating the viabilaty of universal quantum computation using teleportation and single-qubit operations. *Nature*, **402** p.390, November 1999.

[46] R. Griffiths. Consistent histories et the interpretation of quantum mechanics. *J. of Stat. Phys*, **36** p.219, 1984.

[47] R. Griffiths. Consistent interpretation of quantum mechanics using quantum trajectories. *Phys. Rev. Lett.*, **70** p.2201, 1993.

[48] R. B. Griffiths et C.-S. Niu. Semiclassical fourier transform for quantum computation. *Phys. Rev. Lett.*, **76** p.3228, 1996.

[49] L. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, p.212, 1996.

[50] J. J. Halliwell. Decoherent histories and the emergent classicality of local densities. *Phys. Rev. Lett.*, **83** p.2481, 1999.

[51] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems of Information Transmission*, **9** p.177, 1973.

[52] E. Joos et H. D. Zeh. The emergence of classical property through interaction with the environment. *Z. Phys.* **B**, **59** p.223, 1985.

[53] R. Jozsa. Quantum algorithms and the Fourier transform. *Proc. Royal Soc. of London* **A**, **454**, 1998.

[54] R. Jozsa et N. Linden. On the role of entanglement in quantum computational speed-up. arXiv `quant-ph/0201143`, 2002.

[55] A. Kent. Quantum histories and their implications. arXiv `gr-qc/9607073`, 2000.

[56] A. Y. Kitaev. *Uspekhi Mat. Nauk.*, **52** p.53, 1997.

[57] E. Knill et R. Laflamme. Theory of quantum error-correcting codes. *Phys. Rev.* **A**, **55** p.900, 1997.

[58] E. Knill et R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, **81** p.5672, 1998.

[59] E. Knill, R. Laflamme, R. Martinez et C. H. Tseng. An algorithmic benchmark for quantum information processing. *Nature*, **404** p.368, 2000.

[60] E. Knill, R. Laflamme et G. J. Milburn. A scheme for efficient linear optics quantum computation. *Nature*, **409** p.46, January 2001.

[61] E. Knill, R. Laflamme et W. H. Żurek. Resilient quantum computation. *Science*, **279** p.342, 1998.

[62] R. Laflamme, D. G. Cory, C. Negrevergne et L. Viola. NMR quantum information processing and entanglement. *Quant. Info. and Comp.*, **2**, 2002.

[63] G. Lindblad. On the generators of quantun dynamical semigroups. *Commun. Math. Phys.*, **48** p.119, 1976.

[64] S. Lloyd et L. Viola. Control of open quantum systems dynamics. arXiv quant-ph/0008101, 2000.

[65] J. M. Martinis, M. H. Devoret et J. Clarke. Experimental tests for the quantum behavior of a macroscopic degree of freedom : The phase difference across a Josephson junction. *Phys. Rev. B*, **35** p.4682, 1987.

[66] M. A. Nielsen et I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, United Kingdom, 2000.

[67] H. Ollivier, D. Poulin et W. H. Żurek. Objectivity through decoherence. En préparation, 2002.

[68] H. Ollivier et W. H. Żurek. Introducing quantum discord. arXiv quant-ph/0105072, 2001.

[69] R. Omnès. Logical reformulation of quantum mechanics, I, II & III. *J. of Stat. Phys.*, **53** p.893, 1988.

[70] R. Omnès. *The Interpretation of Quantum Mechanics.* Princeton University Press, 1994.

[71] J. P. Paz et W. H. Żurek. Environment-induced decoherence, classicality, and consistency of quantum histories. *Phys. Rev.* **D**, **48** p.2728, 1993.

[72] J. P. Paz et W. H. Żurek. Quantum limit of decoherence : Environment induced superselection of energy eigenstates. *Phys. Rev. Lett.*, **82** p.5181, 1999.

[73] D. Poulin. Classicality of quantum information processing. *Phys. Rev.* **A**, **65** p.42319, 2001.

[74] J. Preskill. Reliable quantum computers. *Proc. Roy. Soc. of London* **A**, **454** p.385, 1998.

[75] R. Raussendorf et H. J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, **86** p.5188, 2001.

[76] F. Reif. *Fundamentals of Statistical and Thermal Physics.* McGraw Hill, 1965.

[77] J. J. Sakurai. *Advanced Quantum Mechanics.* Addison-Wesley, 1967.

[78] L. Salvail. Variations sur la transmission inconsciente en cryptographie quantique. Thèse de doctorat, Université de Montréal, 1997.
http ://www.iro.umontreal.ca/~utheorie/.

[79] R. Schack et C. M. Caves. Classical model for bulk-ensemble NMR quantum computation. *Phys. Rev.* **A**, **60** p.4354, 1999.

[80] L.J. Schulman et U.V. Vazirani. Molecular scale heat engines and scalable quantum computation. *Proc. of the 31th Annual ACM Symposium on Theory of Computing*, p.322, 1999.

[81] B. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev.* **A**, **54** p.2614, 1996.

[82] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. $\mathcal{F}$*, **27** p.379, 623, 1948.

[83] P. W. Shor. Algorithms for quantum computation : Discrete logarithms and factoring. *Proceedings of the 35th Annual ACM Symposium on the Theory of Computing*, p.124, 1994.

[84] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev* **A**, **52** p.2493, 1995.

[85] D. R. Simon. On the power of quantum computation. *35th Annual Symposium on Foundations of Computer Science*, page 116, 1994.

[86] R. Somma, G. Ortiz, J. Gubernatis, E. Knill et R. Laflamme. Simulating physical phenomena by quantum networks. arXiv quant-ph/0108146, 2001.

[87] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, **77** p.793, 1996.

[88] A. Tapp. Informatique quantique : Algorithmes et complexité de la communication. Thèse de doctorat, Université de Montréal, 1999.
http ://www.iro.umontreal.ca/~utheorie/.

[89] G. Vidal et J.I. Cirac. When only two thirds of the entanglement can be distilled. arXiv quant-ph/0107051, 2001.

[90] J. von Neumann. *Mathematical Foundations of Quantum Mechanics.* Princeton University Press, 1955.

[91] S. Wiesner. Simulating many-body quantum systems by a quantum computer. arXiv quant-ph/9603028, 1996.

[92] E. P. Wigner. The problem of measurement. *American J. of Phys.*, **31** p.6, 1963.

[93] W. K. Wootters et W. H. Żurek. A single quantum cannot be cloned. *Nature*, **299** p.802, Octber 1982.

[94] P. Zanardi et M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.*, **79** p.3306, 1997.

[95] W. H. Żurek. Pointer basis of quantum apparatus : Into what mixture does the wave packet collapse? *Phys. Rev.* **D**, **24** p.1516, 1981.

[96] W. H. Żurek. Environment-induced superselection rules. *Phys. Rev.* **D**, **26** p.1862, 1982.