Université de Montréal

Intrication & non-localité

par
André Allan Méthot

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Thèse présentée à la Faculté des études supérieures
en vue de l'obtention du grade de Philosophiæ Doctor (Ph.D.)
en informatique

Décembre, 2005

Université de Montréal
Faculté des études supérieures

Cette thèse intitulée:

Intrication & non-localité

présentée par:

André Allan Méthot

a été évaluée par un jury composé des personnes suivantes:

Pierre McKenzie
président-rapporteur

Gilles Brassard
directeur de recherche

Alain Tapp
codirecteur de recherche

Richard MacKenzie
membre du jury

Serge Massar
examinateur externe

Christian Léger
représentant du doyen de la FES

Thèse acceptée le 12 décembre 2005

RÉSUMÉ

Albert Einstein, Boris Podolsky et Nathan Rosen ont publié en 1935 un article maintenant célèbre qui argumente que la mécanique quantique est une théorie incomplète. À leurs yeux la position et la quantité de mouvement d'une particule sont toutes deux des « éléments de réalité », mais elles ne sont pas représentées comme tels dans le formalisme quantique. Une conséquence implicite de leur point de vue est que la nature doit être décrite selon une théorie dite à variables locales cachées. Une telle théorie pourrait en principe prédire totalement le comportement d'un système conditionnellement à la connaissance de ces variables. Les variables locales cachées représentent donc les « éléments de réalité » d'une théorie locale réaliste. Trente ans plus tard, Bell aura démontré qu'un tel projet est voué à l'échec. Il prouvera qu'aucune théorie à variables locales cachées ne peut reproduire les corrélations quantiques de mesures biparties sur un système quantique.

Dans cette thèse, nous examinons en détail l'argument d'Einstein, Podolsky et Rosen ainsi que la réponse immédiate de Niels Bohr. Nous définissons les éléments de réalité, les théories locales réalistes, les variables locales cachées, etc. De plus, nous explicitons le théorème de John S. Bell ainsi que deux autres formes de théorème d'impossibilité pour les variables locales cachées. Ces théorèmes sont centraux au traitement de l'information quantique, car l'intrication, responsable de corrélations non-classiques, est une ressource distribuée très importante à ce paradigme. Cette dernière est responsable, entre autres choses, de la puissance accrue du modèle de communication quantique sur le modèle classique. La compréhension de l'intrication, plus précisément de la puissance de celle-ci, est donc essentielle à son utilisation à des fins de traitement de l'information. Nous croyons qu'afin de bien comprendre l'intrication (la non-localité), la simulation de celle-ci par différentes ressources est une approche novatrice et prometteuse. Nous voyons donc dans cette thèse plusieurs modèles de simulation de l'intrication par des théories à variables locales cachées auxquelles nous ajoutons une ressource supplémentaire, telle la communication, les boîtes non-locales, etc. Nous explici-

tons ensuite les différents liens qui unissent tous ces modèles. La thèse culmine par la démonstration que la non-localité et l'intrication sont des concepts totalement différents. Cette vision va à l'encontre de la perception générale du physicien.

Mots clés : Intrication, non-localité, fondation de la mécanique quantique, informatique quantique, inégalités de Bell, paradoxe d'Einstein-Podolsky-Rosen, complexité de la communication.

ABSTRACT

Einstein, Podolsky and Rosen published in 1935 a now famous paper, which argued that quantum mechanics is an incomplete theory. For them, position and momentum are both "elements of reality", but they are not represented as such in the quantum formalism. An implicit consequence of their point of view is that Nature should be described by a local hidden variable theory. Such a theory would totally predict the behaviour of a system conditioned upon the knowledge of these variables. Therefore, the local hidden variables represent the "elements of reality" of a local realist theory. Thirty years later, Bell showed that such a project was bound to fail. He proved that no local hidden variable theory could reproduce the correlations of bipartite measurements on an entangled quantum state.

We examine here in detail the argument of Einstein, Podolsky and Rosen as well as Bohr's answer. We explain what is meant by elements of reality, local realist theory, local hidden variable, etc. We also describe explicitly the theorem of Bell and give two other local-hidden-variable no-go theorems. These theorems are central to quantum information processing because entanglement, the source of non-classical correlations, is a distributed resource of great significance to this paradigm. Entanglement is responsible for the power difference between quantum and classical communication models, as well as many other things. Therefore, understanding of this resource is essential to its application to quantum information processing protocols. We believe that, in order for us to understand entanglement (non-locality), the simulation of entanglement with different other resources is a novel and promising approach. In this thesis, we examine simulations of entanglement correlations by local hidden variable models supplemented with different resources, such as communication, non-local boxes, etc. We then spin the web of links between these models. The high point of the thesis is the unveiling that entanglement and non-locality are truly really different concepts. This vision is contrary to the general intuition by physicists.

Keywords: **Entanglement, non-locality, fondation of quantum mechanics, quantum information processing, Bell inequalities, Einstein-Podolsky-Rosen paradox, communication complexity.**

TABLE DES MATIÈRES

LISTE DES SIGLES

BKS	Bell-Kochen-Specker
BNL	Boîte non-locale
CHSH	Clauser-Horne-Shimony-Holt
EPR	Einstein-Podolsky-Rosen
GHZ	Greenberger-Horne-Zeilinger
MQ	Mécanique quantique
POVM	Positive operator valued measure
VLC	Variable locale cachée

NOTATION

$\imath$	nombre imaginaire, $\imath = \sqrt{-1}$
$\mathbb{1}$	matrice d'identité
x_i	$i^{\text{ième}}$ symbole de la chaîne x
$\bar{x}$	négation de chaque bit de la chaîne x
$\lg x$	$\log_2 x$
$\texttt{OUX}(x, y)$	$z_i = x_i \oplus y_i = x_i + y_i \mod 2 \equiv x \oplus y$
$\texttt{ET}(x, y)$	opération logique et $(x \wedge y)$
$\texttt{OU}(x, y)$	opération logique ou $(x \vee y)$
$\texttt{CNON}(x, y)$	opération logique contrôle-non $((x, y \oplus x))$
$IP(x, y)$	$\sum_i x_i \cdot y_i \mod 2 = \bigoplus_i x_i \wedge y_i \equiv x \cdot y$
$x^{(i)}$	appartenance du bit x au participant i
$x \in_r X$	élément aléatoire de X selon une distribution uniforme
$\text{Tr}(\rho)$	trace de ρ
$\rho^{(A)} \equiv \text{Tr}_B(\rho^{A \otimes B})$	trace partielle du système $\rho^{A \otimes B}$ sur le sous-système B
$M^{\perp}$	$M + M^{\perp} = \mathbb{1}$
$\vec{\psi}$	$\lvert\psi\rangle = \cos(\theta)\lvert 0\rangle + \sin(\theta)e^{\imath\phi}\lvert 1\rangle \Rightarrow \vec{\psi} = \begin{pmatrix} \sin(2\theta)\cos(\phi) \\ \sin(2\theta)\sin(\phi) \\ \cos(2\theta) \end{pmatrix}$

À Annie et Lucie

REMERCIEMENTS

J'aimerais tout d'abord remercier Gilles Brassard qui m'a donné l'occasion de me joindre à son groupe de recherche très stimulant, qui m'a ouvert la porte d'un domaine fascinant et qui m'a appris plus de choses sur la physique que je ne le croyais possible. Je voudrais aussi remercier Alain Tapp qui a partagé ses connaissances, son savoir-faire ainsi que son amitié généreusement.

Merci à tous les membres du LITQ qui ont fait de ces années une expérience agréable et enrichissante. Merci à Anne Broadbent, co-auteure et amie, qui m'a donné plus d'un coup de pouce.

J'aimerais remercier mes beaux-parents, Ginette et Robert Poirier, pour leur soutien inconditionnel.

Je me dois aussi de grandement remercier ma famille et spécialement mes parents, Lucie Cardinal et Allan Méthot, qui m'ont toujours incité à aller au bout de mes rêves.

Un remerciement spécial doit être fait à l'égard de mon épouse Annie Poirier. Ses encouragements et nos discussions ont été des plus précieux.

J'espère que ces simples remerciements laissent tout de même entrevoir l'ampleur de ma gratitude.

À vous tous, merci.

AVANT-PROPOS

Cette thèse se veut l'étude de propriétés fondamentales et philosophiques de la physique quantique par les outils de l'informatique théorique. Nous utilisons la théorie des jeux, la simulation, des boîtes noires, des mesures de complexité telles que la complexité de la communication, etc. afin d'exhiber certaines propriétés fort intéressantes, et parfois surprenantes et non-intuitives, de la mécanique quantique. Malgré l'aspect un peu physique de la présentation, cette thèse cadre bien dans le domain de l'informatique, car elle vise essentiellement à comprendre les propriétés de l'intrication, en particulier au point de vue de la non-localité, en terme de ressource par la réduction de celle-ci à d'autres ressources informatiques, telles que l'information partagée ou la communication. De plus, l'intrication est une ressource très riche pour le traitement de l'information quantique.

Les travaux originaux à l'auteur sont dispersés un peu partout au travers de la thèse. La Définition 1.3, le Lemme 1.4 et la Proposition 1.2 proviennent de [23]. La discussion sur l'article d'Einstein, Podolsky et Rosen, sur la réponse de Bohr [21] ainsi que sur les variables locales cachées au Chapitre 2 sont dues à l'auteur. La discussion du Chapitre 3 suit [62] en partie. Les résultats des Sections 3.1.1 et 3.4.2 peuvent être trouvés dans [63] et [23] respectivement. La Section 4.1.1 est tirée de [61] et la Section 4.2 de [24]. La discussion de la Section 5.1 provient de [62], celle de la Section 5.2 de [23] et contient du matériel original. Les résultats des Sections 5.8 et 5.9 sont dérivés de [19]. La discussion de la Section 5.10 est une conséquence de [24] et la discussion de la Section 5.11 est présentée dans [22]. La conclusion au Chapitre 6 est tirée ou découle des travaux de l'auteur. D'autres travaux ont été effectués par l'auteur durant le doctorat [25, 26, 64, 65], mais ne sont pas présentés dans cette thèse.

CHAPITRE 1

INTRODUCTION

1.1 Formalisme quantique

La mécanique quantique est une théorie fort bien établie en physique. Elle est aussi une théorie mathématiquement riche. Le formalisme quantique est maintenant très développé et c'est pourquoi nous ne verrons qu'un sous-ensemble approprié au traitement de l'information. De plus, nous ne pourrons couvrir tous les aspects de la théorie de l'information quantique. Pour d'excellents ouvrages sur le sujet, nous recommandons au lecteur de consulter [16, 70].

1.1.1 États purs et transformations unitaires

L'information quantique se représente comme une généralisation de l'information classique. Un état quantique à deux niveaux (qubit) s'exprime comme suit :

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.1}$$

où $\alpha, \beta \in \mathbb{C}$ sont les amplitudes de $|0\rangle$ et $|1\rangle$ respectivement et $|\alpha|^2 + |\beta|^2 = 1$. La notation $|\cdot\rangle$ (prononcé *ket*) est utilisée pour représenter les états dits purs et est appelée notation de Dirac. Le ket symbolise un vecteur de norme 1 dans un espace de Hilbert $\mathcal{H}$, espace vectoriel sur le corps des complexes. On dit d'un qubit qu'il est dans un état classique si la valeur absolue d'une des amplitudes est égale à 1 et que nous connaissons la base dans laquelle cela se produit.

Une transformation $\mathsf{U}\colon \mathcal{H}_2 \to \mathcal{H}_2$ sur un qubit envoie $|0\rangle$ sur $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|1\rangle$ sur $|\Psi'\rangle = \delta|0\rangle + \gamma|1\rangle$ où $|\gamma|^2 + |\delta|^2 = 1$ et $\alpha\delta^\star + \beta\gamma^\star = 0$. Il est à noter qu'il y a donc infiniment plus de portes unaires dans le modèle quantique que dans le modèle classique reversible, qui n'en compte que deux : la négation et l'identité.

Qu'arrive-t-il lorsque nous avons plus qu'un qubit, soit un registre quantique ?

L'espace de Hilbert se trouve agrandi ($\mathcal{H}_{2^n}$ où n est le nombre de qubits). Prenons l'exemple de deux qubits, la généralisation à n qubits est évidente. L'état décrivant les deux qubits $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|\Phi\rangle = \gamma|0\rangle + \delta|1\rangle$ est

$$|\Upsilon\rangle = |\Psi\rangle \otimes |\Phi\rangle = |\Psi\rangle|\Phi\rangle = |\Psi\Phi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle. \quad (1.2)$$

Cet état est dit séparable, car il est possible de mettre les termes en évidence de sorte que $|\Upsilon\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$. Mais est-ce bien toujours le cas ? Qu'en est-il alors de l'état $|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$? Cet état n'est pas séparable ! On dit qu'il est intriqué (il est en fait maximalement intriqué). $|\Psi^-\rangle$ est un des quatre états de Bell, soit

$$\begin{aligned} |\Psi^-\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \\ |\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\Phi^-\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \text{ et} \\ |\Phi^+\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned} \quad (1.3)$$

Les états de Bell forment une base de l'espace de Hilbert $\mathcal{H}_4$. Ils jouent un rôle important dans le traitement de l'information quantique et sont l'un des sujets de l'étude de cette thèse.

Il est à noter que les états de Bell ne sont pas les seuls états maximalement intriqués. Tout état pouvant être produit à partir de transformations unitaires locales sur un état de Bell est aussi un état maximalement intriqué.

La mécanique quantique étant une théorie linéaire, elle peut donc être représentée et manipulée par les outils de l'algèbre linéaire. On peut alors représenter $|0\rangle$ par

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (1.4)$$

et $|1\rangle$ par

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.5}$$

Les opérations permises sont maintenant représentées par des matrices unitaires

$$\mathsf{U} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}, \tag{1.6}$$

où $|\alpha|^2 + |\beta|^2 = 1$, $|\gamma|^2 + |\delta|^2 = 1$ et $\alpha\gamma^\star + \beta\delta^\star = 0$. Pour représenter n qubits, il faut un vecteur de 2^n éléments. Les matrices dans cet espace sont des matrices unitaires ($\mathsf{U}\mathsf{U}^\dagger = \mathsf{U}^\dagger\mathsf{U} = I$) de taille $2^n \times 2^n$ et elles sont les éléments du groupe $SU(2^n)$. On peut, par exemple, représenter l'état de Bell $|\Psi^-\rangle$ comme

$$|\Psi^-\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \tag{1.7}$$

et l'opération non-contrôlé `CNON` par

$$\mathsf{U}_{\texttt{CNON}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.8}$$

Lorsque nous avons deux qubits, l'un dans l'état $\alpha|0\rangle + \beta|1\rangle$ et le deuxième dans l'état $\gamma|0\rangle + \delta|1\rangle$, l'état global du système peut être calculé à l'aide du produit de

Kronecker

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \\ \beta \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix}. \tag{1.9}$$

Pour ce qui est des opérations sur des sous-ensembles de plusieurs qubits, cela fonctionne de la même façon. Soit un système dans l'état $|\psi\rangle|\phi\rangle$. On veut effectuer les transformations U sur le premier qubit et V sur le deuxième qubit $\mathsf{U}|\psi\rangle \otimes \mathsf{V}|\phi\rangle$, l'opération sur le système global sera donnée par la matrice $\mathsf{U} \otimes \mathsf{V}$, définie de façon similaire aux vecteurs.

Rappelons-nous que les *kets* peuvent être représentés par des vecteurs colonnes. Il existe un analogue pour les vecteurs lignes. Le *bra* (dénoté $\langle\cdot|$) est l'équivalent du *ket* transposé conjugué $\langle\psi| = |\psi\rangle^\dagger$.

On peut aussi définir les transformations unitaires en ces termes. Soit une transformation unitaire U qui envoie $|0\rangle$ sur $|\psi\rangle$ et $|1\rangle$ sur $|\phi\rangle$, où $|\psi\rangle$ et $|\phi\rangle$ sont orthogonaux. Cette transformation unitaire s'écrit :

$$\mathsf{U} = |\psi\rangle\langle 0| + |\phi\rangle\langle 1|. \tag{1.10}$$

1.1.2 Matrices de densité et trace partielle

Il est aussi possible de créer des mélanges statistiques. Nous pouvons, par exemple, concevoir une machine qui produirait un état $|\psi\rangle$, pouvant aussi s'exprimer sous la forme $|\psi\rangle\langle\psi|$, avec probabilité p et un état $|\phi\rangle$, $|\phi\rangle\langle\phi|$, avec probabilité $1-p$. Auquel cas, nous décririons l'état par une matrice de densité

$$\rho = p|\psi\rangle\langle\psi| + (1-p)|\phi\rangle\langle\phi|. \tag{1.11}$$

En général, nous pouvons donc décrire tout état σ par une matrice de densité

$$\sigma = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{1.12}$$

où $p_i > 0$ et $\sum_i p_i = 1$.

Le résultat de l'application de la transformation unitaire U sur un mélange statistique ρ donne

$$\rho' = \mathsf{U}\rho\mathsf{U}^\dagger. \tag{1.13}$$

Lorsque nous voulons décrire un sous-système A d'un plus grand système $A \otimes B$, nous prenons la trace partielle. La trace partielle sera dénotée dans cette thèse comme

$$\rho^{(A)} \equiv \mathrm{Tr}_B(\rho^{A\otimes B}). \tag{1.14}$$

Une représentation fort intéressante du qubit est celle de la sphère de Bloch. Prenons un qubit dans un état pur

$$|\psi\rangle = \cos(\theta)|0\rangle + \sin(\theta)e^{\imath\phi}|1\rangle, \tag{1.15}$$

pour $0 \leq \theta \leq \pi/2$ et $0 \leq \phi < 2\pi$. Nous pouvons représenter ce qubit comme un unique vecteur à la surface d'une sphère

$$\vec{\psi} = \begin{pmatrix} \sin(2\theta)\cos(\phi) \\ \sin(2\theta)\sin(\phi) \\ \cos(2\theta) \end{pmatrix} \tag{1.16}$$

en trois dimensions. Nous retrouvons le point sur la sphère en prenant d'abord un vecteur pointant vers le haut. Puis nous le penchons vers nous d'un angle 2θ, en continuant vers le bas pour $2\theta \geq \pi/2$. Ensuite, nous appliquons une rotation *sinistrorsum* d'un angle de ϕ. Une propriété intéressante de la sphère de Bloch est que les états orthogonaux sont représentés comme des vecteurs avec des directions opposées. Les matrices de densité peuvent aussi être représentées dans ce formalisme. Prenons la matrice de densité $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, sa représentation est $\vec{\rho} = \sum_i p_i\vec{\psi}_i$. La sphère de Bloch est donc une sphère pleine avec l'état $\mathbb{1}/2$ au centre, aussi appelé l'état complètement mélangé, les états purs sur la sphère de rayon unitaire et le reste des états quantiques à l'intérieur.

1.1.3 Mesures

1.1.3.1 Mesures de von Neumann

Une des différences frappantes entre l'information classique et l'information quantique se situe au niveau de la mesure de l'information. En effet, la mesure de l'information classique est simple : nous n'avons qu'à regarder et nous obtenons toute l'information qu'il y a à avoir. Par contre, la mesure de l'information quantique est différente. Lorsque l'on mesure un qubit dans une base, ce dernier donne comme réponse l'un des éléments de la base avec une probabilité égale au carré de la norme de l'amplitude de cet élément et le qubit prend l'état classique de cet élément. Ce type de mesure est appelée mesure de von Neumann. Prenons par exemple le qubit $\frac{\sqrt{3}}{2}|0\rangle - \frac{i}{2}|1\rangle$. Lorsque l'on mesure ce qubit dans la base de calcul on obtient 0 avec une probabilité de 3/4 et le qubit est maintenant dans l'état $|0\rangle$. Avec une probabilité de 1/4, on obtient 1 et le qubit est maintenant dans l'état $|1\rangle$. Cette mesure est aussi appelée mesure projective, ou PVM (Projective Valued Measure), car elle projette l'état quantique dans un des états classiques de la base de mesure. La généralisation vers n qubits est évidente.

On peut aussi penser de façon géométrique et interpréter le produit interne comme une projection. Soient deux états orthogonaux $|\psi\rangle$ et $|\phi\rangle$ et un autre état $|\chi\rangle = \alpha|\psi\rangle + \beta|\phi\rangle$. Si nous multiplions $\langle\psi|$ par $|\chi\rangle$ nous obtenons

$$\langle\psi|\chi\rangle = \alpha\langle\psi|\psi\rangle + \beta\langle\psi|\phi\rangle = \alpha. \tag{1.17}$$

Nous pouvons donc réécrire $|\chi\rangle$ comme

$$|\chi\rangle = \langle\psi|\chi\rangle|\psi\rangle + \langle\phi|\chi\rangle|\phi\rangle. \tag{1.18}$$

En d'autres mots, $\langle\psi|\chi\rangle|\psi\rangle$ est la projection de $|\chi\rangle$ sur $|\psi\rangle$. Étant donné que $\langle\psi|\chi\rangle$ est un scalaire et que la mécanique quantique est une théorie linéaire et associative,

$$\langle\psi|\chi\rangle|\psi\rangle = |\psi\rangle\langle\psi|\chi\rangle = (|\psi\rangle\langle\psi|)|\chi\rangle. \tag{1.19}$$

On peut donc dire que $|\psi\rangle\langle\psi|$ est l'opérateur de projection sur $|\psi\rangle$ et $|\langle\psi|\chi\rangle|^2$ est la probabilité d'obtenir $|\psi\rangle$ lorsque l'on mesure $|\chi\rangle$.

Il existe deux façons naturelles et équivalentes pour représenter les projecteurs sur un qubit.

Représentation 1.1. *La représentation ket-bra est donnée par une matrice positive $P = |\psi\rangle\langle\psi|$, pour un état pur $|\psi\rangle$ sur lequel la projection est effectuée. Dans ce cas, nous pouvons toujours réécrire le projecteur sous la forme*

$$P = \begin{pmatrix} \cos^2\theta & e^{-\imath\phi}\sin\theta\cos\theta \\ e^{\imath\phi}\sin\theta\cos\theta & \sin^2\theta \end{pmatrix} \tag{1.20}$$

pour les angles appropriés $0 \leq \theta \leq \pi/2$ et $0 \leq \phi \leq 2\pi$. Nous permettons que $\phi = 2\pi$ pour des raisons qui seront apparentes à la Section 3.4.2.

Représentation 1.2. *La représentation comme vecteur est donnée par un vecteur de norme unitaire dans un espace tridimensionnel :*

$$\vec{\psi} = (x, y, z) = \big(\sin(2\theta)\cos(\phi), \sin(2\theta)\sin(\phi), \cos(2\theta)\big) \tag{1.21}$$

ce qui peut être considéré comme un point sur la sphère de rayon unitaire (sphère de Bloch).

Il est à noter que les θ et ϕ des Représentations 1.1 et 1.2 sont les mêmes et que la probabilité d'obtenir $|\psi\rangle$ en mesurant $|\chi\rangle$ est

$$|\langle\psi|\chi\rangle|^2 = \frac{1 + \vec{\psi}\cdot\vec{\chi}}{2}, \tag{1.22}$$

où $\vec{\psi}\cdot\vec{\chi}$ est le produit scalaire de deux vecteurs.

Définition 1.3. *Nous disons qu'un projecteur est dans l'*hémisphère est *si $0 \leq \phi < \pi$ et dans l'*hémisphère ouest *si $\pi < \phi \leq 2\pi$, excepté lorsque $\theta = 0$ où le projecteur est dans les deux hémisphères et lorsque $\theta = \pi/2$ où le projecteur n'est dans aucun hémisphère.*

Il est important de noter que, pour tout θ, le point à $\phi = 2\pi$ est le même qu'à $\phi = 0$, ce qui implique que les points ayant comme coordonnées $(x, 0, z)$, pour un x positif, appartiennent aux deux hémisphères. Cette double appartenance est volontaire et sera exploitée à la Section 3.4.2. Il est aussi à noter que nous avons exclu $\phi = \pi$ des deux hémisphères. Les pôles sont des points singuliers qui méritent un traitement spécial. Pour nos besoins, nous dirons que le pôle Nord ($\theta = 0$) appartient aux deux hémisphères alors que le pôle Sud ($\theta = \pi/2$) n'appartient à aucun hémisphère.

1.1.3.2 POVM

Lorsque l'on désire extraire de l'information classique d'un système quantique, il est possible de lui joindre un registre quantique supplémentaire dans un état connu, d'effectuer une transformation unitaire sur le système conjoint pour finalement mesurer les deux systèmes en totalité ou en partie. Les qubits ajoutés sont communément appelés un *système ancillaire* ou *ancilla*. L'ensemble de ces opérations peuvent être regroupées conceptuellement dans une construction mathématique appellée POVM (Positive-Operator-Valued Measure). Plus formellement, les éléments M_i d'un POVM $\{M_i\}$ sont des matrices carrées et positives qui respectent les conditions

$$M_i = A_i^\dagger A_i \quad ; \quad \sum_{i=1}^{k} M_i = \mathbb{1}, \tag{1.23}$$

où les A_i sont des matrices carrées quelconques. Il est à noter qu'il existe en général une infinité de choix pour les A_i. Sur une entrée ρ, le POVM produira comme résultat une valeur classique i avec probabilité $\mathrm{Tr}(\rho M_i)$ et un résidu quantique

$$\frac{1}{\mathrm{Tr}(\rho M_i)} A_i \rho A_i^\dagger. \tag{1.24}$$

Définition 1.4. *Nous dénoterons par $M^\perp$ la matrice telle que $M + M^\perp = \mathbb{1}$.*

1.1.3.3 Raffinement des POVM

Malgré que les POVM soient composés de matrices positives quelconques, quelques résultats peuvent être dérivés plus facilement si nous restreignons les éléments des POVM à être proportionnels à des projecteurs. Le prochain lemme montre que nous pouvons adopter cette simplification sans perte de généralité [32].

Lemme 1.1. *Tout POVM peut être étandu à un POVM au moins aussi informatif dont tous les éléments sont proportionnels à des projecteurs.*

Démonstration. Considérons un POVM ayant comme éléments la collection $\{M_i\}$. À partir du théorème de la décomposition spectrale, chaque M_i peut être réécrit comme $M_i = \sum_j \gamma_{ij} P_{ij}$, où les γ_{ij} sont des constantes réelles, $0 < \gamma_{ij} \leq 1$, et les P_{ij} sont des projecteurs. Nous pouvons alors construire un nouveau POVM ayant la collection $\{\gamma_{ij} P_{ij}\}$ comme éléments. Il est clair que ces nouveaux éléments sont des matrices positives et que $\sum_{ij} \gamma_{ij} P_{ij} = \sum_i M_i = \mathbb{1}$. Afin d'obtenir précisément l'effet du POVM original avec le nouveau POVM, nous devons interpréter les résultats du nouveau POVM comme suit : si le résultat ij est obtenu lorsque le nouveau POVM est appliqué, nous faisons comme si le POVM original avait obtenu simplement i. □

Proposition 1.2. *Nous étendons la notion d'hémisphère aux éléments de POVM proportionnels à des projecteurs en disant que γP appartient au même hémisphère que P, pour tout $0 < \gamma \leq 1$.*

De [32], nous avons aussi le lemme suivant :

Lemme 1.3. *Considérons une collection de projecteurs P_i et de nombres positifs γ_i. Pour chaque i, prenons $\vec{v}_i$ comme le point sur la sphère de Bloch qui correspond à P_i, selon l'Équation 1.21. La condition $\sum_i \gamma_i P_i = \mathbb{1}$ est équivalente à $\sum_i \gamma_i \vec{v}_i = 0$ et $\sum_i \gamma_i = 2$.*

Lemme 1.4. *Tout POVM ayant des éléments proportionnels à des projecteurs contient au moins un élément dans chaque hémisphère.*

Il est important de noter que l'élément de l'hémisphère ouest peut être le même que celui de l'hémisphère est.

Démonstration. Considérons un POVM $\{\gamma_i P_i\}$, où chaque P_i est un projecteur et $0 < \gamma_i \leq 1$. Pour chaque i, prenons θ_i, ϕ_i et $\vec{v}_i = (x_i, y_i, z_i)$ correspondant à P_i selon les Équations 1.20 et 1.21. Si au moins un des P_i correspond au pôle nord ($\theta_i = 0$), ou si $\phi_i = 0$ (de façon équivalente $\phi_i = 2\pi$), ce $\gamma_i P_i$ est un élément qui appartient aux deux hémisphères et on a fini. Autrement, la condition $\sum_i \gamma_i \vec{v}_i = 0$ implique qu'il doit y avoir un i tel que $y_i \neq 0$. Si $y_i > 0$ ($y_i < 0$), alors $\gamma_i P_i$ appartient à l'hémisphère est (ouest). Dans tous les cas, nous utilisons de nouveau la condition $\sum_k \gamma_k \vec{v}_k = 0$ afin de conclure qu'il existe aussi un projecteur P_j tel que le signe de y_j est l'opposé du signe de y_i, et $\gamma_j P_j$ appartient à l'autre hémisphère. □

1.1.4 Théorème de Holevo et théorème d'impossibilité de clonage

Du théorème de Holevo [51], il est possible de déduire le théorème suivant :

Théorème 1.5. *Il est impossible d'obtenir plus d'un bit d'information à la mesure d'un qubit.*

Le théorème suivant est prouvé dans [83].

Théorème 1.6. *Il est impossible de faire une réplique parfaite d'un état quantique inconnu.*

Le fait qu'un qubit $\alpha|0\rangle + \beta|1\rangle$ ne peut être mesuré que par des mesures projectives ou des POVM, combiné au fait que l'information quantique ne peut être clonée, rend impossible d'obtenir α et β exactement. On n'obtient qu'un seul bit d'information sur l'état, alors que α et β sont des nombres complexes, donc des variables continues ayant une quantité d'information infinie.

1.1.5 Intrication en tant que ressource

L'intrication peut être utilisée pour accomplir des tâches surprenantes. Nous en verrons quelques exemples. Il est important de noter que dans la plupart des

applications de l'intrication, la quantité de ressources nécessaires afin d'accomplir la tâche est comptée en terme du nombre d'états de Bell requis.

1.1.5.1 Téléportation et codage superdense

La téléportation quantique a été inventée en 1992 par Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres et William K. Wootters [10] afin de caractériser combien d'information deux participants peuvent obtenir sur un état à l'aide d'opérations locales et de communication classique. Elle n'est pas un transfert instantané d'un système physique entre des points séparés dans l'espace. Il s'agit en fait de simuler une utilisation d'un canal quantique par deux utilisations d'un canal classique en consommant un bit d'intrication. Plus précisement, Alice et Bob partagent un état $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et Alice désire transmettre un qubit dans l'état $\alpha|0\rangle + \beta|1\rangle$. Il est important de noter qu'Alice n'a pas besoin de connaître cet état. Ils possèdent donc l'état

$$(\alpha|0\rangle + \beta|1\rangle) \otimes \left(\tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) \tag{1.25}$$

où les deux premiers qubits appartiennent à Alice et le troisième appartient à Bob. Alice exécute ensuite un `CNOT` sur ses deux qubits (le premier qubit étant le qubit de contrôle) et elle applique un Walsh-Hadamard

$$\mathsf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.26}$$

sur son premier qubit. L'état est maintenant

$$\begin{aligned}
&\frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle)+ \\
&\frac{1}{2}|01\rangle(\beta|0\rangle + \alpha|1\rangle)+ \\
&\frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle)+ \\
&\frac{1}{2}|11\rangle(\beta|0\rangle - \alpha|1\rangle).
\end{aligned} \tag{1.27}$$

Alice mesure ensuite ses deux qubits et envoie le résultat (deux bits obtenus selon une distribution uniforme) à Bob, qui peut retrouver l'état $\alpha|0\rangle+\beta|1\rangle$ en appliquant les transformations nécessaires (changement de phase ou/et négation). Il est à noter que Bob n'a aucune information sur $|\psi\rangle$ tant et aussi longtemps qu'il n'a pas reçu le résultat de la mesure d'Alice. En effet, la matrice de densité décrivant l'état de Bob reste l'état complètement mélangé $\mathbb{1}/2$ tout au long des opérations d'Alice.

Le codage superdense est lié à la téléportation quantique. En effet, le codage superdense simule deux utilisations d'un canal classique par une utilisation d'un canal quantique avec la consommation d'un bit d'intrication [11]. Si Alice et Bob partagent un $|\Phi^+\rangle$, Alice (respectivement Bob) peut transmettre deux bits à Bob (Alice) en éxecutant la procédure suivante. Si le premier bit d'Alice est $a_1 = 1$, elle applique un changement de phase sur son qubit. Si son deuxième bit est $a_2 = 1$, elle applique une négation sur son qubit. Ensuite, elle envoie son qubit à Bob, qui possède alors l'un des quatre états de Bell $|\phi_{a_1 a_2}\rangle$:

$$\begin{aligned}
|\phi_{00}\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\phi_{01}\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\phi_{10}\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\phi_{11}\rangle &= \tfrac{1}{\sqrt{2}}(|10\rangle - |01\rangle).
\end{aligned} \tag{1.28}$$

Bob peut alors distinguer lequel des quatre états il possède.

1.2 Formalisme classique

Nous utilisons cette section pour définir quelques concepts non-quantiques dont nous aurons besoin.

1.2.1 Théorie des jeux

La définition de jeux classiques présentée ici est beaucoup moins générale que le permet le cadre habituel de la théorie des jeux, mais seulement ce type de jeux sera considéré dans cette thèse.

Définition 1.5. *Un* jeu $G = (X, Y, R)$ *est un ensemble d'entrées* $X = X^{(A)} \times X^{(B)} \times \ldots$, *un ensemble de sorties* $Y = Y^{(A)} \times Y^{(B)} \times \ldots$ *et une relation* $R \subseteq X^{(A)} \times X^{(B)} \times \cdots \times Y^{(A)} \times Y^{(B)} \times \ldots$.

Définition 1.6. *Une* stratégie gagnante *pour un jeu biparti* $G = (X, Y, R)$ *est une stratégie selon laquelle pour tout* $x^{(i)} \in X^{(i)}$, *le participant* i *produit* $y^{(i)} \in Y^{(i)}$ *tel que* $(x^{(A)}, x^{(B)}, \ldots, y^{(A)}, y^{(B)}, \ldots) \in R$.

1.2.2 Boîtes non-locales

Une *boîte non-locale* (BNL) est un engin imaginaire [73] qui a un port d'entrée et de sortie chez Alice et un autre chez Bob, même si ces derniers sont séparés d'une quelconque façon. Lorsqu'Alice entre un bit $x^{(A)}$ dans son port d'entrée, elle obtient de la BNL un bit aléatoire $y^{(A)}$ uniformément distribué, non-corrélé avec son entrée ou celle de Bob. De même pour Bob, dont l'entrée sera nommée $x^{(B)}$ et la sortie $y^{(B)}$. La « magie » apparaît sous la forme de corrélations entre la paire d'entrées et la paire de sorties : le ou-exclusif `OUX` (somme modulo deux) des sorties est toujours égal au et logique `ET` des entrées. Autrement dit, $x^{(A)} \wedge x^{(B)} = y^{(A)} \oplus y^{(B)}$. Tout comme les corrélations qui peuvent être établies par de l'intrication, cet engin est intemporel : Alice reçoit sa sortie dès qu'elle insère son entrée, sans égard à ce qui se passe chez Bob, et *vice versa*. Toujours inspirée par l'intrication, la BNL est un engin à utilisation unique : les corrélations n'apparaissent qu'à la première

utilisation de la BNL et tout usage subséquent entraîne des sorties non-correlées. Il est évidemment possible pour Alice et Bob de partager plusieurs BNL. Dans ce cas, les BNL sont considérées comme des ressources quantifiables par le nombre de BNL nécessaires pour accomplir une tâche.

Une propriété importante des BNL est qu'elle ne permet pas par elle-même à Alice et Bob de communiquer. La raison est que les sorties sont purement aléatoires localement. En d'autres mots, les BNL sont non-locales, mais causales : elles ne permettent pas aux effets de précéder les causes dans le contexte de la relativité.

1.3 Complexité de la communication

1.3.1 Complexité de la communication classique

Soient deux participants, Alice et Bob, voulant collaborer à l'accomplissement d'une tâche distribuée, c'est-à-dire calculer une fonction sur leurs entrées distribuées. Plus formellement, Alice reçoit $x^{(A)} \in X^{(A)}$ et Bob $x^{(B)} \in X^{(B)}$, où $X^{(A)} = \{0,1\}^n$ et $X^{(B)} = \{0,1\}^k$, et ils veulent calculer $y = f(x^{(A)}, x^{(B)})$, où $y \in Y = \{0,1\}^m$ et $f\colon X^{(A)} \times X^{(B)} \to Y$. Afin de compléter cette tâche, Alice et Bob doivent, en général, s'échanger un certain nombre de bits. Dans ce modèle classique, proposé par Harold Abelson en 1978 [1] et par Andrew C.-C. Yao en 1979 [84], Alice et Bob doivent accomplir cette tâche distribuée en communiquant le moins de bits possible. La complexité est donnée en terme de la quantité minimale de bits de communication nécessaires pour le résoudre. La complexité des calculs locaux effectués par les participants n'est pas comptabilisée.

Définition 1.7. *Le coût déterministe d'un protocole est le nombre total de bits de communication pour la pire des entrées possibles de taille n.*

La complexité de la communication est la science vouée à l'étude des bornes de complexité dans ce modèle, souvent appelé modèle classique. Nous noterons par $C(f)$ la complexité déterministe de la fonction f dans ce modèle.

Définition 1.8. *La complexité $C(f)$ de la fonction f est le coût du protocole calculant f avec le plus faible coût.*

La complexité de la communication classique a été et est encore grandement étudiée pour son intérêt fondamental et ses multiples applications [55].

Plusieurs variantes du modèle existent :

- Modèle probabiliste avec erreur bornée : Alice et Bob peuvent tirer à pile ou face et doivent produire y tel que $\Pr[y = f(x^{(A)}, x^{(B)})] \geq 1 - \varepsilon$ où ε est la probabilité d'erreur. Nous noterons par $C_\varepsilon(f)$ la complexité de la fonction f dans ce modèle.
- Modèle probabiliste avec erreur bornée et variables aléatoires préalablement partagées[1] : nous supposons qu'Alice produit une chaîne de bits aléatoires (parfois même un nombre réel aléatoire) puis en donne une copie à Bob. Il convient de ne pas tenir compte de cet échange, car il aura été fait avant qu'Alice reçoive $x^{(A)}$ et Bob $x^{(B)}$, donc avant même que le protocole ait débuté. L'analyse du protocole pour une entrée donnée est effectuée en prenant une distribution de probabilité uniforme sur tous les choix de variables aléatoires partagées possibles. Alice et Bob partagent donc un ensemble infini de variables aléatoires (aussi appelées variables locales). Ils doivent produire y tel que $\Pr[y = f(x^{(A)}, x^{(B)})] \geq 1 - \varepsilon$, où ε est la probabilité d'erreur sur le choix des variables aléatoires partagées. Nous noterons par $C^\star_\varepsilon(f)$ la complexité de la fonction f dans ce modèle.

Il existe aussi plusieurs autres modèles, voir [55], mais seulement ces dernières variantes seront considérées dans cette thèse.

De façon générale, n bits de communication suffisent ($n + m$ si les deux participants doivent connaître la réponse). En effet, Alice n'a qu'à envoyer x à Bob qui, lui, peut calculer $f(x^{(A)}, x^{(B)})$ (et envoyer la réponse à Alice si elle doit la connaître). Afin d'éviter une notation lourde, nous supposerons que seulement un

[1] Les variables aléatoires partagées sont supposées inconnues de l'entité qui fournit les entrées aux participants.

des deux participants doit connaître la réponse, en l'occurrence Bob. Il est possible de faire mieux pour certaines fonctions.

Soit la fonction suivante :

$$f(x^{(A)}, x^{(B)}) = PARITY(x^{(A)}, x^{(B)}) = \bigoplus_i x_i^{(A)} \oplus x_i^{(B)}. \tag{1.29}$$

Il suffit d'un seul bit de communication pour accomplir la tâche :

- Alice calcule $z = \bigoplus_i x_i^{(A)}$
- Alice envoie ensuite z (un bit) à Bob
- Bob calcule $z \oplus (\bigoplus_i x_i^{(B)})$.

Par contre, la plupart des fonctions booléenes, telles que $IP(x^{(A)}, x^{(B)}) = x^{(A)} \cdot x^{(B)} = \sum_i x_i y_i \mod 2$, requièrent n bits de communication. Plusieurs techniques ont été développées afin de prouver de telles affirmations [55].

Lorsque l'on permet au protocole de tirer à pile ou face et de commettre des erreurs, la situation peut changer de façon significative. Pour la plupart des fonctions la complexité de la communication restera $\Theta(n)$, mais certaines fonctions présentent un gain exponentiel dans cette variante. Soit la fonction EQ définie comme étant égale à 1 si $x^{(A)} = x^{(B)}$ et 0 autrement :

$$EQ = \bigwedge_i \neg(x_i^{(A)} \oplus x_i^{(B)}). \tag{1.30}$$

EQ prend n bits de communication dans la variante sans erreur, mais seulement $O(\lg \frac{n}{\varepsilon})$ bits de communication si on permet une probabilité d'erreur ε qui ne dépend pas de n [55], $C(EQ) \in \Theta(n) \supsetneq C_{\frac{1}{3}}(EQ) \in \Theta(\lg n)$.

Dans la variante où l'on permet à Alice et Bob de partager des variables aléatoires, il est suffisant, et nécessaire, de communiquer $\lceil \lg \frac{1}{\varepsilon} \rceil$ bits d'information pour résoudre EQ [55], $C^{\star}_{\frac{1}{3}}(EQ) \in \theta(1) \subsetneq C_{\frac{1}{3}}(EQ) \in \theta(\lg n) \subsetneq C(EQ) \in \theta(n)$.

Il est à noter que quel que soit f [55] :

$$C^{\star}_{\varepsilon}(f) \leq C_{\varepsilon}(f) \leq C(f) \tag{1.31}$$

et que $C^*_\varepsilon(f)$ permet, dans le meilleur des cas, une diminution d'un facteur logarithmique par rapport à C_ε [68].

Définition 1.9. *La complexité de la communication de f, $C(f)$, $C_\varepsilon(f)$ ou $C^*_\varepsilon(f)$, est dite* triviale *si le problème peut être résolu avec* un seul bit *de communication.*

1.3.2 Complexité de la communication quantique

1.3.2.1 Modèle de Yao

Le modèle pour la complexité de la communication quantique dans un monde quantique proposé par Yao en 1993 [85] est l'extension naturelle de son modèle classique. L'innovation de ce modèle de communication quantique est qu'Alice et Bob ne s'échangent plus des bits, mais des qubits. Nous noterons cette complexité par $Q(f)$. Les variantes du modèle classique s'appliquent avec la même notation à ce modèle.

De prime abord, il peut sembler étrange, voire inutile, de considérer ce nouveau modèle de communication suite à l'apparition, 20 ans plus tôt, du théorème de Holevo [51]. En effet, ce théorème établit qu'il est impossible de communiquer plus de n bits d'information en transmettant n qubits si les participants ne disposent pas d'intrication. De plus, Charles H. Bennett et Stephen J. Wiesner ont découvert le *codage superdense*, voir Section 1.1.5.1, avec lequel il est possible de transmettre deux bits d'information en envoyant un qubit et en consommant un bit d'intrication. Richard Cleve, Wim van Dam, Michael Nielsen et Alain Tapp ont démontré la généralisation suivante : [37] :

Théorème 1.7. *Si Alice veut communiquer n bits d'information à Bob à travers un canal quantique mais qu'ils ne partagent pas d'intrication, alors ils ont besoin de s'échanger au moins n qubits, dont au moins $\lceil n/2 \rceil$ doivent provenir d'Alice. S'ils possèdent de l'intrication, alors Alice doit envoyer $\lceil n/2 \rceil$ qubits, peu importe combien de qubits Bob envoie.*

En somme, l'utilisation de la mécanique quantique afin de transmettre de l'information ne paraissait guère prometteuse au début des années 90, car elle ne sem-

blait donner qu'un simple coefficient de 2 par rapport à l'information classique et nécessitait pour cela un canal quantique et un partage d'intrication afin de pouvoir utiliser le codage superdense. Heureusement, ces résultats ne s'appliquent pas à la complexité de la communication, car le but premier ici n'est pas de communiquer, mais d'accomplir une tâche distribuée.

Le premier protocole dans le modèle quantique de Yao à donner un avantage sur le monde classique a été proposé par Cleve, van Dam, Nielsen et Tapp [37]. Dans ce protocole, il est possible de calculer IP (où les deux participants doivent savoir la réponse) sur des entrées de deux bits avec une probabilité de 80% en envoyant seulement deux qubits, alors que la meilleure probabilité possible avec deux bits est de 78%.

La première grande séparation entre la complexité classique et la complexité quantique est survenue en 1998 avec Harry Buhrman, Richard Cleve et Avi Wigderson [28]. Un protocole calculant

$$EQ'(x^{(A)}, x^{(B)}) = \begin{cases} 1 & \text{si } \Delta(x^{(A)}, x^{(B)}) = 0 \\ 0 & \text{si } \Delta(x^{(A)}, x^{(B)}) = 2^{n-1} \end{cases} \tag{1.32}$$

(où $\Delta(x^{(A)}, x^{(B)})$ est la distance de Hamming) y est donné, dans le cas exact, avec complexité $Q(EQ') \in O(\lg n)$, alors que $C(EQ') \in \Omega(n)$.

Pour ce qui est du modèle où l'on tolère une erreur bornée ε, le premier protocole à avoir une séparation exponentielle est celui de Ran Raz [74]. Le problème étudié par Raz est une modification d'un problème d'abord défini par Ilan Kremer [54]. Alice reçoit un vecteur de norme unitaire $\vec{x} \in \mathbb{R}^n$, où $\mathbb{R}^n$ est un espace vectoriel de dimension n sur les réels, et deux espaces vectoriels orthogonaux $M_0, M_1 \subset \mathbb{R}^n$, chacun de dimension $n/2$. Bob reçoit une matrice unitaire $T\colon \mathbb{R}^n \to \mathbb{R}^n$. Le but est de répondre 0 si la distance entre $T(x)$ et M_0 est plus petite que ϑ et de répondre 1 si la distance entre $T(x)$ et M_1 est plus petite que ϑ. Classiquement, il faut $\Omega(\sqrt{n})$ bits de communication, alors qu'à l'aide de la mécanique quantique, il en faut $\Theta(\lg n)$. L'efficacité de son protocole vient du fait que l'on peut représenter un vecteur de

dimension m par $\lg m$ qubits, ce qui n'est pas possible classiquement. Il faut donc envoyer $\vec{x}$ par un canal classique, ce qui demande beaucoup de communication.

1.3.2.2 Modèle de Cleve-Buhrman

La deuxième façon de « quantifier » le modèle classique de communication est de revenir à la communication classique, mais de permettre aux participants de partager de l'intrication [36]. Nous noterons cette complexité par $E(f)$. Les variantes du modèle classique s'appliquent avec la même notation à ce modèle.

Le fait que l'intrication ne permette pas de signaler par elle-même peut sembler donner une réduction de ce modèle vers le modèle classique. Toutefois, comme dans le cas du modèle avec communication quantique, ces arguments ne s'appliquent que dans le cas où l'on désire communiquer et non dans le cas où l'on veut accomplir une tâche distribuée.

Dans l'article proposant ce modèle de communication, Cleve et Buhrman ont aussi trouvé un protocole à trois participants permettant de sauver un bit de communication par rapport au modèle classique [36]. Ce protocole fut, en fait, le tout premier protocole où une tâche distribuée pouvait se faire plus efficacement dans un monde quantique que dans un monde classique.

Le premier exemple d'un gain non constant est aussi survenu dans ce modèle. Harry Buhrman, Wim van Dam, Peter Høyer et Alain Tapp [29] ont donné une tâche f à k participants nécessitant $C(f) \in \Theta(k \lg k)$ bits de communication dans le modèle classique, alors que $E(f) \in O(k)$ bits de communication suffisent si les participants partagent de l'intrication.

Maintenant que nous avons vu les deux modèles de complexité de la communication quantique, une question intéressante apparaît : existe-t-il une différence entre les deux modèles ou sont-ils équivalents ? Une partie de la réponse est déjà connue : on peut simuler tout protocole dans le modèle avec un canal quantique à l'aide du modèle à canal classique supplémenté d'intrication. La téléportation quantique nous permet de simuler une utilisation du canal quantique par deux utilisations du canal classique en consommant un bit d'intrication [10]. De plus, si l'on

tolère des erreurs, nous savons que $Q_\varepsilon(EQ) \in \Omega(\lg n)$ et que $E_\varepsilon(EQ) \in O(1)$, pour une constante ε. Cette comparaison est toutefois malhonnête. Afin qu'Alice et Bob puisse partager de l'intrication dans le modèle de Cleve-Buhrman, il est nécessaire qu'ils aient interagi avant de recevoir leurs questions. Il faudrait donc permettre à Alice et Bob de partager des variables aléatoires dans le modèle de Yao. Par contre, l'existence d'une réduction du modèle de Cleve-Buhrman au modèle de Yao dans le cas exact est toujours un problème ouvert. Il existe un troisième modèle de communication quantique dans lequel les participants partagent de l'intrication et communiquent par un canal quantique, mais ce modèle se réduit au modèle de Cleve-Buhrman par l'utilisation de la téléportation quantique, voir Section 1.1.5.1. Ces deux modèles sont donc équivalents.

1.3.3 Calcul distribué

Nous présentons ici un nouveau modèle de calcul proposé par van Dam [39]. Nous avons d'abord besoin de quelques définitions [19], puis nous établirons quelques lemmes faciles à dériver [19]. Les résultats intéressants concernant ce modèle seront dévoilés aux Sections 4.2, 5.8 et 5.9.

Définition 1.10. *Un bit x est* distribué *si Alice a un bit $x^{(A)}$ et Bob a un bit $x^{(B)}$ tel que $x = x^{(A)} \oplus x^{(B)}$.*

Définition 1.11. *Une fonction booléenne $f(x^{(A)}, x^{(B)})$, $f\colon \{0,1\}^{2n} \to \{0,1\}$, est* calculée distributivement *par Alice et Bob si, étant donné $x^{(A)}$ et $x^{(B)}$ en entrée respectivement, ils produisent un bit distribué égal à $f(x^{(A)}, x^{(B)})$. La communication est interdite lors d'un calcul distribué.*

Définition 1.12. *Une fonction booléenne $f(x^{(A)}, x^{(B)})$ a un* biais *si elle peut être calculée distributivement avec probabilité strictement plus grande que $1/2$.*

Définition 1.13. *Une fonction booléenne $f(x^{(A)}, x^{(B)})$ a un* biais borné *si elle peut être calculée distributivement avec une probabilité plus grande que $1/2+\varepsilon$, pour une constante $\varepsilon > 0$, et ce peu importe la longueur des entrées.*

Lemme 1.8. *Pourvu qu'Alice et Bob aient accès à des variables aléatoires partagées, toute fonction booléenne est biaisée.*

Démonstration. Alice et Bob partagent une variable aléatoire uniformément distribuée z de la même longueur que l'entrée de Bob $x^{(B)}$. Lorsqu'elle reçoit son entrée $x^{(A)}$, Alice produit $a = f(x^{(A)}, z)$. La stratégie de Bob est de vérifier si $x^{(B)} = z$. Si oui, il produit $b = 0$; si non, il produit un bit aléatoire uniformément distribué b. Dans le cas où $x^{(B)} = z$, le bit distribué entre Alice et Bob est correct puisque $a \oplus b = f(x^{(A)}, z) \oplus 0 = f(x^{(A)}, x^{(B)})$. Ceci se produit avec probabilité 2^{-n} si n est la longueur de l'entrée de Bob. Dans tout autre cas, le bit distribué est uniformément aléatoire, donc correct avec probabilité $1/2$. En somme, le bit distribué est correct avec probabilité

$$\Pr[a \oplus b = f(x^{(A)}, x^{(B)})] = \frac{1}{2^n} + \Big(1 - \frac{1}{2^n}\Big)\frac{1}{2} = \frac{1}{2} + \frac{1}{2^{n+1}},$$

qui est bel et bien plus grand que $1/2$. □

Lemme 1.9. *Toute fonction booléenne qui a un biais borné a une complexité probabiliste de la communication triviale, $\exists \varepsilon < 1/2$ tel que $C_\varepsilon(f) = 1$.*

Démonstration. Prenons f avec un biais borné. Alors pour toutes entrées $x^{(A)}$ et $x^{(B)}$, Alice et Bob peuvent respectivement produire des bits a et b sans communication tels que $f(x^{(A)}, x^{(B)}) = a \oplus b$ avec probabilité d'erreur d'au plus $\varepsilon < 1/2$. Envoyer a à Bob donne un protocole pour f, avec un seul bit de communication. □

Décrivons maintenant une contruction mathématique quelque peu technique qui nous sera utile aux Sections 4.2.4 et 5.8. Si Alice et Bob ont deux bits chacun, $x_1^{(A)}, x_2^{(A)}$ et $x_1^{(B)}, x_2^{(B)}$ respectivement, alors l'usage de deux BNL leur permet de calculer $y^{(A)}$ pour Alice et $y^{(B)}$ pour Bob, tel que $y^{(A)} \oplus y^{(B)} = f(x_1^{(A)}, x_2^{(A)}, x_1^{(B)}, x_2^{(B)}) = (x_1^{(A)} \oplus x_1^{(B)}) \wedge (x_2^{(A)} \oplus x_2^{(B)})$. Cette observation provient du fait que $f(x_1^{(A)}, x_2^{(A)}, x_1^{(B)}, x_2^{(B)}) = x_1^{(A)}x_2^{(A)} \oplus x_1^{(B)}x_2^{(B)} \oplus x_1^{(A)}x_2^{(B)} \oplus x_2^{(A)}x_1^{(B)}$, où les deux premiers termes peuvent être calculés localement alors que les deux derniers requièrent une BNL chacun. Alice calcule $A_1 = x_1^{(A)}x_2^{(A)}$ et Bob $B_1 = x_1^{(B)}x_2^{(B)}$. Alice

entre $x_1^{(A)}$ dans la première BNL alors que Bob entre $x_2^{(B)}$. Ils obtiennent alors A_2 et B_2 respectivement. Alice entre $x_2^{(A)}$ dans la deuxième BNL alors que Bob entre $x_1^{(B)}$, d'où ils obtiennent A_3 et B_3. Avec $y^{(A)} = A_1 \oplus A_2 \oplus A_3$ et $y^{(B)} = B_1 \oplus B_2 \oplus B_3$, Alice et Bob ont $y^{(A)} \oplus y^{(B)} = (x_1^{(A)} \oplus x_1^{(B)}) \wedge (x_2^{(A)} \oplus x_2^{(B)})$. Nous appelons une telle opération le calcul *distribué* de la fonction f, ce qui revient à calculer le ET de deux bits distribués, $x_1 = x_1^{(A)} \oplus x_1^{(B)}$ et $x_2 = x_2^{(A)} \oplus x_2^{(B)}$.

CHAPITRE 2

ARGUMENT D'EINSTEIN-PODOLSKY-ROSEN ET RÉPONSE DE BOHR

2.1 Contexte historique

En 1935, Albert Einstein, Boris Podolsky et Nathan Rosen (EPR) ont publié un article qui a ébranlé la communauté des physiciens [43], particulièrement à Copenhague. Leon Rosenfeld décrit l'impact de l'article sur Niels Bohr, l'un des pères de la mécanique quantique et le plus grand défenseur de cette dernière, de la manière suivante : « This onslaught came down to us as a bolt from the blue » [76].

À cette époque, la mécanique quantique (MQ) était encore une théorie relativement jeune et fondée sur plusieurs faits empiriques. Elle exhibait tellement de propriétés exotiques que Bohr a déjà dit à son sujet : « Anyone who is not shocked by quantum theory has not understood it. »[1] Parmi les effets non-classiques de la MQ, notons sa nature fondamentalement probabiliste[2] et le fait qu'il y est impossible de déterminer simultanément la position et la quantité de mouvement d'une particule avec une précision arbitraire. En fait, la MQ nous dit que deux variables conjuguées, telles que la position et la quantité de mouvement, n'ont pas d'*existences* simultanées[3]. Ces propriétés excentriques n'étaient pas attrayantes à la totalité de la communauté physicienne. D'aucuns prétendent qu'il s'agissait d'indications que la MQ était incapable de décrire pleinement la réalité physique. Avec cette pensée à l'esprit, EPR publièrent l'article intitulé « Can quantum-mechanical description of physical reality be considered complete ? » [43], dans lequel ils avancent un argument qui, soi-disant, leur permettait de répondre par la négative. Soixante-dix

[1] Il n'est pas clair quelle fut l'expression exacte énoncée par Bohr. Plusieurs citations similaires peuvent être trouvées sur `http://en.wikiquote.org/wiki/Niels_Bohr`.

[2] Du moins dans l'interprétation de Copenhague, interprétation généralement acceptée à l'époque.

[3] Toujours selon l'interprétation de Copenhague.

ans après sa publication, il s'agit toujours de l'article le plus téléchargé du site de l'American Physical Society `www.aps.org`.

Même s'il existe des indices permettant de croire qu'Einstein y pensait depuis 1931 [46, 52], la notion d'intrication fut publiée en premier lieu dans l'article d'EPR. Les auteurs utilisent les corrélations obtenues de mesures biparties sur un état intriqué pour prétendre qu'il est possible, pour la position et la quantité de mouvement, d'avoir des existences simultanées. Étant donné que le formalisme de la MQ interdit cette possibilité, EPR concluent que la MQ ne peut offrir une description complète de la réalité. Même si la terminologie de « variables locales cachées » (VLC) n'existait pas encore, une conséquence directe de leur opinion est que la nature possède ces VLC. Ces VLC ne peuvent être collectivement connues par une expérience—car dans le cas contraire une violation du principe d'incertitude d'Heisenberg serait obtenue—mais elles permettent de déterminer la réaction du système physique sous n'importe quelle mesure. Nous y reviendrons à la Section 2.4. Einstein a d'ailleurs passé le reste de sa vie à chercher une telle théorie, en vain.

Deux mois après la publication de l'article de EPR, Bohr a soumis une réponse à l'article d'EPR au même journal avec le même titre que ces derniers [14]. De toute évidence, Einstein n'a guère été convaincu par cette réplique.

Dans ce chapitre, nous présentons une discussion sur l'argument d'EPR, ainsi que sur la réponse de Bohr, suivant les lignes de [21]. Le but est de montrer des faiblesses de l'article d'EPR, et ce, sans faire référence aux inégalités de Bell qui seront traitées au Chapitre 3. Les points que nous soulevons ne sont pas aussi fatals que le théorème de Bell, mais ils nous permettent de questionner l'argument de EPR, indépendamment de la réponse de Bohr. Il est important de noter que nous ne démontrons pas l'impossibilité d'une description à VLC de la nature. Nous montrons plutôt que l'argument d'EPR aurait pu être plus soigné, car il est rempli d'erreurs logiques.

2.2 Argument d'Einstein-Podolsky-Rosen

Afin de caractériser ce que nous devrions considérer comme une théorie valide de la nature, EPR proposent les deux critères suivants : la théorie devrait être *correcte* et la théorie devrait être *complète*. Évidemment, le paradigme scientifique demande aussi que la théorie soit falsifiable, mais l'argument d'EPR repose sur la complétude de la MQ. Spécifiquement, les auteurs proposent la définition suivante.[4]

Définition 2.1 (Complétude). *Every element of the physical reality must have a counterpart in the physical theory.*

La définition de la *réalité physique* donnée par EPR, qu'ils « regard as reasonable » sans plus de justifications, est donnée par une citation célèbre.

Définition 2.2 (Réalité physique). *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*

Comme nous allons voir, l'argument d'EPR gravite autour de deux énoncés.

Énoncé A. *La description de la réalité physique par la mécanique quantique n'est pas complète.*

Énoncé B. *Des opérateurs qui ne commutent pas ne peuvent pas avoir de réalités simultanées.*

EPR utilisent ces deux énoncés de façon labyrinthique pour en arriver à la « conclusion » que l'Énoncé A doit être vrai. La structure de leur preuve peut être établie par les deux citations suivantes, qui apparaissent à la fin de la première section de leur article.

[4]Les comptes rendus *in extenso* de l'article d'EPR et de la réponse de Bohr seront présentés en format sans sérif et respecteront les caractères italiques.

(a) From this it follows that either (1) *the quantum-mechanical description of reality given by the wave function is not complete* or (2) *when operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality.*

(b) In quantum mechanics it is usually assumed that the wave function *does* contain a complete description of the physical reality of the system in the state to which it corresponds. [...] We shall show, however, that this assumption, together with the criterion of reality given above, leads to a contradiction.

L'argument culmine dans leur conclusion :

(c) Starting then with the assumption that the wave function does give a complete description of the physical reality, we arrived at the conclusion that two physical quantities, with noncommuting operators, can have simultaneous reality. [...] We are thus forced to conclude that the quantum-mechanical description of physical reality given by wave functions is not complete.

Pour extraire la substance de l'argument d'EPR, rephrasons sa structure dans le langage de la logique mathématique. Dans ce langage, la Citation (a) se traduit par : « soit Énoncé A ou Énoncé B ». L'usage normal de « *soit* p ou q » correspond mathématiquement au *ou-exclusif* de p et q. Autrement dit, soit que p est vrai, soit que q est vrai, mais pas les deux. Il est usuel d'écrire cela par $p \oplus q$ en mathématiques modernes. La première citation se traduit donc par

$$\mathrm{A} \oplus \mathrm{B}\,. \tag{2.1}$$

La Citation (b) est plus difficile à traduire. Nous devons d'abord comprendre que « the criterion of reality given above », à la fin de la citation, signifie que l'Énoncé B est vrai. La Citation (b) se traduit alors par $\neg \mathrm{A} \wedge \mathrm{B} \Rightarrow$ faux, qui est équivalent à

$$\neg \mathrm{A} \Rightarrow \neg \mathrm{B}\,. \tag{2.2}$$

La proposition (2.2) est énoncée plus clairement par la première phrase de la Ci-

tation (c).

Étant donné qu'EPR dérivent leur conclusion, nommément Énoncé A, après avoir « établi » la véracité des deux citations, l'argument final—Citation (c)—repose sur la tautologie

$$(A \oplus B) \wedge (\neg A \Rightarrow \neg B) \Rightarrow A\,. \tag{2.3}$$

Maintenant que nous avons reformulé l'argument d'EPR en termes de la logique mathématique, discutons de chacune des trois propositions.

Dans le but d'établir la véracité de $A \oplus B$, nous devons montrer soit que l'Énoncé A est vrai, soit que l'Énoncé B est vrai. Pour ce faire, EPR utilisent le fait que la MQ ne permet pas à la position et à la quantité de mouvement d'une particule d'être simultanément définies. Donc, si la position et la quantité de mouvement ont véritablement des réalités simultanées (négation de l'Énoncé B), alors la MQ ne peut être complète selon leurs critères (Énoncé A). En d'autres mots, $\neg B \Rightarrow A$. De plus, ils argumentent que si la MQ est une théorie complète (négation de l'Énoncé A), alors la position et la quantité de mouvement ne peuvent pas avoir de réalités simultanées (Énoncé B). En d'autres mots, $\neg A \Rightarrow B$.

À ce point, il est intéressant de remarquer la redondance des deux implications décrites ci-haut, puisqu'elles sont logiquement équivalentes, chacune étant la contraposée de l'autre. Un problème plus sérieux est que la conclusion désirée (1) ne peut être faite. En effet, $\neg A \Rightarrow B$ est logiquement équivalent à $A \vee B$, qui ne peut être utilisé afin de conclure $A \oplus B$. Pire encore, aucun raisonnement logique ne peut corriger cette erreur puisqu'à aucun moment EPR n'argumentent que les Énoncés A et B ne peuvent être vrais en même temps. Il est tout à fait possible de concevoir que la MQ pourrait être incomplète pour une toute autre raison.

Nous croyons que le problème pourrait venir de notre interprétation linguistiquement correcte du mot « either » dans la citation (a) : Sans doute qu'EPR n'avait pas 2.1 en tête, mais bien

$$A \vee B\,, \tag{2.4}$$

qui est bel et bien correct, même avec les connaissances actuelles. Cette confusion est soit le fruit d'une négligence dans l'écriture de leur article, soit la conséquence du changement de la signification du mot « either » durant les soixante-dix dernières années. Il n'est cependant pas utile de se soucier plus de ce détail, car nous verrons qu'il n'a aucun impact sur les conclusions d'EPR.

Afin de « prouver » que $\neg A \Rightarrow \neg B$, Einstein, Podolsky et Rosen ont utilisé un état biparti intriqué de deux particules, où deux physiciens, Alice et Bob, prennent une particule chacun et sortent du cône de lumière de l'autre. Supposons qu'Alice mesure la quantité de mouvement de sa particule. Selon la MQ, elle est maintenant parfaitement capable de prédire avec certitude et précision arbitraire le résultat d'une mesure de la quantité de mouvement chez Bob. Puisqu'aucun des participants n'est dans le cône de lumière de l'autre, il est impossible, selon la théorie de la relativité, que la mesure chez Alice perturbe l'état du système chez Bob. Selon la Définition 2.2, la quantité de mouvement est donc un élément de réalité. Changeons maintenant de scénario et supposons qu'Alice mesure la position de sa particule. Encore une fois, elle pourrait maintenant prédire avec certitude le résultat d'une mesure de la position de la particule de Bob sans l'avoir perturbée. La position correspond donc elle aussi à un élément de réalité. Il « en découle » que la position et la quantité de mouvement (deux opérateurs qui ne commutent pas) avaient des réalités simultanées *avant* d'être mesurées. Ce qui « prouve » que B est faux.

Bien entendu, l'erreur est que l'argumention d'EPR est contrefactuelle, « le physicien peut faire ceci ou le physicien peut faire cela » alors qu'il ne peut clairement pas faire les deux. Personne n'a mis cette erreur en évidence mieux qu'Asher Peres dans son célèbre aphorisme : « Unperformed experiments have no results » [71]. Puisqu'Alice ne peut faire les deux mesures, il est incorrect de conclure que les deux résultats sont définis simultanément. Sachant très bien qu'Einstein n'aurait pas été convaincu par cet argument, nous continuons sur une ligne d'attaque différente, basée sur la logique plutôt que la physique.

Rappelons-nous que nous étions supposés prouver que $\neg A \Rightarrow \neg B$. Le lecteur attentif aura sûrement remarqué qu'EPR sont arrivés à la conclusion désirée $\neg B$

sans faire appel à aucun moment à l'hypothèse $\neg A$. En effet, le raisonnement n'était aucunement lié à la complétude de la mécanique quantique. Il était plutôt fondé sur l'exactitude de la MQ, en particulier sur la validité du postulat de la mesure. Si nous sommes prêts à accepter que les prédictions de la MQ sont correctes—ce que nous croyons être le point de vue d'EPR—alors l'argument qui soi-disant prouve $\neg A \Rightarrow \neg B$, « prouve » directement $\neg B$. Il est vrai que $\neg A \Rightarrow \neg B$ a été « prouvé » en démontrant $\neg B$, mais l'énoncé $\neg A \Rightarrow \neg B$ est plus complexe que ce qui est nécessaire.

D'un point de vue purement logique, il n'y rien de catastrophique dans l'argumentation précédente ... du moins au premier coup d'oeil. L'équation 2.3 est bel et bien une tautologie, comme il peut être facilement démontré par une table de vérité ou un simple argument de logique[5]. Par contre, cette tautologie n'est pas pertinente à l'argument d'EPR. Nous devons remplacer 2.1 par 2.4 à l'intérieur de la tautologie :

$$(A \vee B) \wedge (\neg A \Rightarrow \neg B) \Rightarrow A\,. \tag{2.5}$$

L'Équation 2.5 est aussi une tautologie, d'où le fait que la signification exacte de « either...or » n'est pas importante, tel que mentionné ci-haut.

Rappelons-nous maintenant que, sans tenir compte de la Citation (b), le raisonnement d'EPR ne prouve pas 2.2, puisqu'ils n'ont pas utilisé l'hypothèse $\neg A$ selon laquelle la MQ est complète. Ils ont plutôt « prouvé » directement $\neg B$, sous la seule condition que la MQ est correcte. Cette hypothèse est tellement prise pour acquis tout au long de l'article qu'il est en fait presque impossible de la qualifier d'hypothèse. En somme, la tautologie quelque peu compliquée que nous avons écrite à l'Équation 2.3, pour traduire le texte d'EPR, n'est en fait rien d'autre que :

$$(A \vee B) \wedge \neg B \Rightarrow A\,. \tag{2.6}$$

[5]Supposons que A est faux. B est alors vrai puisque $A \oplus B$ est vrai. Par contre, A serait alors vrai puisque $\neg A \Rightarrow \neg B$ est équivalent à $B \Rightarrow A$ et B est vrai. Puisque ceci contredit l'hypothèse que A est faux, il faut donc conclure que A est vrai.

Cet énoncé est tellement plus simple[6] que la tautologie originale qu'il est tentant de croire que la tautologie originale n'était qu'un écran de fumée.

En somme, la conclusion d'EPR aurait pu être correcte si nous permettions un argument contrefactuel, mais la logique utilisée par les auteurs est beaucoup plus compliquée, et parfois même fausse, qu'il n'était nécessaire.

Prenons la citation suivante d'EPR, qui correspond à la situation après qu'une interaction ait transformé l'état des deux systèmes en un état intriqué.

> We can then calculate with the help of Schrödinger's equation the state of the combined system [...]. We cannot, however, calculate the state in which either one of the two systems is left after the interaction. This, according to quantum mechanics, can be done only with the help of further measurements, by a process known as the *reduction of the wave packet.*

D'un point de vue contemporain, cette phrase est dépourvue de sens. Nous pouvons évidemment calculer l'état de l'un des deux sous-systèmes en prenant la trace partielle. De toute évidence, EPR considéraient que seuls les états purs méritaient d'être appelés « états ». Étant donné leur obsession avec les éléments de réalité, cette position n'est guère surprenante. Néanmoins, il est intéressant de noter que von Neumann avait déjà introduit la notion de matrice de densité quelques années auparavant [67].

Si nous prenons le point de vue épistémologique selon lequel la matrice de densité qui correspond à la connaissance possible de l'état est en fait une description complète de l'état, la mesure d'Alice n'a donc aucun effet sur cet état. C'est seulement si cette dernière révèle le résultat de sa mesure à Bob que l'état de la particule change pour ce dernier. Par contre, cette communication ne peut être plus rapide que la vitesse de la lumière, détruisant ainsi le besoin d'une *spukhafte Fernwirkungen.*

Nous mentionnons ceci pour le lecteur qui pourrait rester sous la fausse impression que la mesure d'Alice a une influence instantanée sur l'état de la particule de

[6] Si A ou B est vrai et ce n'est pas B, c'est alors A.

Bob. Par contre, nous sommes conscients qu'il ne s'agit pas d'une question centrale à la discussion de l'article d'EPR puisque les auteurs ont pris la position sans équivoque (et correcte) qu'une telle influence n'aurait pas lieu. Leur erreur fut de prendre une perspective ontique où tout état est pur, duquel découle le point de vue incorrect selon lequel l'état de Bob est défini indépendamment de la connaissance d'Alice et Bob.

2.3 Réponse de Bohr

Dans sa réponse, Bohr [14] considère peu la question de l'intrication. Pour lui, le phénomène décrit par EPR n'est rien de plus que ce qu'il appelle la *complémentarité*. Il prétend qu'en MQ, tout comme en relativité générale, nous devons considérer l'appareil de mesure afin de pouvoir faire des prédictions. Essentiellement, Bohr affirme que la position et la quantité de mouvement ne peuvent être tous deux mesurés simultanément avec une précision arbitraire parce qu'il est *expérimentalement impossible de faire ainsi*, même en principe. Une mesure de la quantité de mouvement d'une particule peut seulement être réalisée expérimentalement par un transfert de quantité de mouvement de la particule vers l'appareil de mesure, créant ainsi un déplacement et renonçant à tout jamais à la connaissance précise de la position. Dans la vision de Bohr sur l'argument d'EPR, lorsqu'Alice mesure la quantité de mouvement de sa particule, elle apprend celle de Bob, renonçant alors de sa propre volonté à la connaissance de la position de la particule de Bob. Ce sacrifice est basé sur le fait que l'on ne peut prédire le résultat d'une mesure. Dans l'exemple précédent, si nous voulons mesurer la quantité de mouvement de la particule d'Alice, puisqu'il nous est impossible de prévoir le transfert de quantité de mouvement ou le déplacement causé par la mesure, il nous est aussi impossible de savoir avec certitude où la particule a interagi avec l'appareil de mesure. La citation suivante résume bien la position de Bohr :

> In fact, the renunciation in each experimental arrangement of the one or the other of two aspects of the description of physical phenomena,—the

> combination of which characterizes the method of classical physics, and which therefore in this sense may be considered as *complementary* to one another,—depends essentially on the impossibility, in the field of quantum theory, of accurately controlling the reaction of the object on the measuring instruments, i.e., the transfer of momentum in case of position measurements, and the displacement in case of momentum measurements.

Le problème avec la réponse de Bohr est évidemment qu'EPR n'avaient rien contre le principe de complémentarité. Ils ne prétendaient pas qu'il était possible de connaître la position et la quantité de mouvement simultanément. En effet, s'ils n'avaient pas été d'accord avec cette manifestation du principe d'incertitude d'Heisenberg, ils auraient prétendu directement que la MQ est *incorrecte* et non pas seulement incomplète. Leur différend avec la mécanique quantique est résumé dans la citation suivante :

> The usual conclusion from this[7] in quantum mechanics is that *when the momentum of a particle is known, its coordinate has no physical reality.*

Par contre, ceci n'a aucun lien avec l'affirmation que la MQ est incomplète.

Du point de vue d'EPR, l'incomplétude de la MQ est donc liée au fait qu'elle ne permet pas l'existence simultanée de deux observables qui ne commutent pas. Que l'on puisse connaître ou pas ces deux réalités simultanément n'est pas pertinent à leur argument. Le fait que la MQ nous permette de prédire soit la quantité de mouvement, soit la position d'une particule sans avoir interagi avec cette dernière semble montrer que, selon la Définition 2.2, ces deux observables ont des réalités physiques. Selon le critère de la Définition 2.1, la MQ fait donc preuve d'incomplétude.

2.4 Variables locales cachées et réalisme local

Le paradigme des variables locales cachées (VLC) est une conséquence mathématique directe du réalisme local. En effet, le réalisme implique que la valeur d'un

[7] Mesurer la position d'une particule change son état.

opérateur représentant un élément de réalité existe, ou du moins peut être déduite directement de la valeur d'un autre élément de réalité, et ce même avant la mesure. Dans un modèle à VLC, les variables secrètes sont établies selon une distribution de probabilités lors de la création de l'état et représentent une valeur réelle d'un élément de réalité. Elles peuvent seulement être accédées expérimentalement, ce qui en retour perturbe l'état et change possiblement les valeurs des autres VLC. Il est très important de noter qu'elles sont cachées aux physiciens qui créent l'état jusqu'à ce que ces derniers effectuent une mesure. Une description *totale* de l'état inclurait directement la variable, bien en vue, mais la description de la connaissance de l'état fait usage d'une moyenne sur les valeurs possibles de la VLC. Si nous connaissions les valeurs réelles de toutes les VLC, nous pourrions prédire totalement le comportement du système sous n'importe quelle opération, incluant la mesure de n'importe quel élément de réalité. C'est d'ailleurs ce manque de connaissances qui nous forcerait à prendre la moyenne sur les valeurs possibles de ces VLC. Le principe d'incertitude d'Heisenberg et la structure probabiliste de la MQ restent ainsi intacts. Le critère de localité implique que tout événement sur un système à l'extérieur du cône de lumière passé d'un autre système ne peut influencer d'aucune façon les valeurs originales des VLC du système considéré. Les valeurs sont fixées à la création de l'état et ne peuvent être modifiées que par des opérations situées dans le cône de lumière passé du système.

CHAPITRE 3

THÉORÈMES D'IMPOSSIBILITÉ POUR LES VARIABLES LOCALES CACHÉES

Presque trente ans se sont écoulés entre l'article d'Einstein, Podolsky et Rosen et l'article qui vint finalement mettre fin aux théories à VLC. C'est en 1964 que John S. Bell publia un article [8] démontrant qu'aucune théorie à VLC ne peut reproduire les prédictions de la MQ. Plus précisément, Bell exhiba des corrélations entre des mesures sur un état intriqué, proposé par David Bohm lors de sa version de l'argument d'EPR [12, 13], prouvant ainsi qu'EPR ne pouvait avoir démontré l'incomplétude de la MQ. La situation aurait pu être pire pour la MQ : elle aurait pu être incorrecte ! Par la suite, plusieurs expérimentations [6, 45] ont établi la supériorité de la MQ sur les théories à VLC, un ricochet ironique de l'intention de l'article d'EPR.

Au cours de ce chapitre, nous donnerons les définitions formelles de trois formes de théorème d'impossibilité relativement aux modèles à VLC [62] et une forme de théorème qui place certaines contraintes sur les théories à VLC, soit les inégalités de Bell, les théorèmes de Bell sans inégalités [1], la pseudo-télépathie et les théorèmes de Bell-Kochen-Specker (BKS). Nous débutons avec les théorèmes de BKS. Nous les généralisons ensuite à l'utilisation de POVM [31, 63, 80]. Nous présenterons ensuite les théorèmes de Bell à la Section 3.2, les théorèmes de Bell sans inégalités à la Section 3.3 et la pseudo-télépathie à la Section 3.4. Finalement, la Section 3.4.2 décrira quelques résultats intéressants quant aux limites de la pseudo-télépathie [23].

[1] Aussi appelées inégalités de Bell sans probabilités, inégalités de Bell sans inégalités ou réfutation d'EPR de type tout ou rien.

3.1 Théorèmes de Bell-Kochen-Specker

Durant plus de trente ans, l'existence de théories à VLC a été débattue. Certains remettaient même en doute la pertinence de cette question pour la science. Indépendamment, John S. Bell [9] et Simon Kochen et Ernst P. Specker [53] ont montré que si une telle théorie existait, elle devait être contextuelle. Nous nommerons ce type d'arguments des théorèmes de BKS.

Définition 3.1. *On dit d'une théorie qu'elle est contextuelle si la valeur d'un opérateur physique dépend du contexte où elle est mesurée.*

Remarque 3.2. *La mécanique quantique est non-contextuelle.*

En effet, lors d'une mesure, que ce soit une mesure de von Neumann ou un POVM, la probabilité d'obtenir un résultat i, $\mathrm{Tr}(\rho M_i)$, ne dépend pas des autres éléments de la mesure, M_j pour $j \neq i$.

Dans l'article de Kochen-Specker, il a été prouvé qu'un état quantique à trois niveaux, un qutrit, ne peut être décrit par une théorie non-contextuelle réaliste. Selon cette preuve, aucune théorie ne peut exister où l'on peut assigner une valeur binaire (« oui », « non ») à chaque élément de mesure de façon à ce que toute mesure de von Neumann faite sur le qutrit ait un et un seul élément de la base ayant une valeur « oui » et que cette valeur ne dépende pas de la mesure utilisée. Autrement dit, une fois la valeur « oui »/« non » assignée, elle reste la même pour cet élément dans n'importe quelle mesure. Leur preuve est équivalente, se réduit, à trouver un graphe tel qu'il est impossible de le colorier par deux couleurs de façon à ce que tout sous-graphe complet de trois sommets contient un et un seul sommet de la première couleur. Il est par contre impossible d'adapter leur preuve à un système à un qubit, preuve qui repose sur l'usage de mesure de von Neumann. Une question se pose alors d'elle-même : faut-il considérer les POVM afin de montrer la non-contextualité d'un qubit ?

3.1.1 Théorème de Bell-Kochen-Specker avec POVMs

Il est intéressant de noter qu'il existe plusieurs propositions de ce que pourrait être un théorème de BKS utilisant les POVM et qu'il n'existe pas de consensus à savoir laquelle correspond à un rejet des théories à VLC sous-entendues par l'article d'EPR.

Proposition 3.1. *Une preuve de BKS que la mécanique quantique ne peut être décrite par une théorie à VLC non-contextuelle peut être formulée en considérant que deux éléments mathématiquement identiques sont physiquement équivalents.*

Lemme 3.2. *Aucune théorie classique à VLC non-contextuelle n'existe selon la Proposition 3.1.*

Démonstration. Dans le POVM $\{\mathbb{1}/2, \mathbb{1}/2\}$, on ne peut assigner une et une seule valeur « oui » puisque les deux éléments sont le même. □

Théorème 3.3. *La preuve du Lemme 3.2 contenant le moins d'éléments requiert un POVM de deux éléments.*

Démonstration. Une preuve contenant moins d'éléments n'aurait qu'un POVM d'un seul élément, $\{\mathbb{1}\}$. Il est toujours possible d'assigner la valeur « oui » à un et un seul élément de la mesure. □

Proposition 3.4. *Une preuve de BKS que la mécanique quantique ne peut être décrite par une théorie à VLC non-contextuelle n'a de sens qui si les éléments des mesures sont distincts.*

Lemme 3.5. *Aucune théorie classique à VLC non-contextuelle n'existe selon la Proposition 3.4.*

Démonstration. La preuve de cet énoncé a d'abord été présentée dans un article d'Adan Cabello [31], qui donne tout le crédit à Masahiro Nakamura. Prenons les POVM

$$\begin{aligned} &\{A/2, A^{\perp}/2, B/2, B^{\perp}/2\}, \\ &\{A/2, A^{\perp}/2, C/2, C^{\perp}/2\} \text{ et} \\ &\{B/2, B^{\perp}/2, C/2, C^{\perp}/2\}, \end{aligned} \tag{3.1}$$

où A, B et C sont des projecteurs distincts quelconques. Puisque chaque élément apparaît deux fois et que le nombre de « oui » requis est impair (trois), il est impossible d'assigner non-contextuellement un et un seul « oui » par POVM. □

Théorème 3.6. *La preuve du Lemme 3.5 contenant le moins d'éléments requiert trois POVM de quatre éléments chacun.*

Démonstration. Tentons d'abord de réduire le nombre de POVM. Si nous avons seulement un POVM avec des éléments distincts, il est facile d'assigner un et un seul « oui » à un élément. Dans le cas où nous avons deux POVM, soit un élément apparaît dans les deux POVM et nous lui attribuons le « oui » et la valeur « non » à tous les autres éléments, soit tous les éléments sont distincts et nous assignons la valeur « oui » à un élément de chaque POVM au hasard. Nous voyons donc que trois POVM sont nécessaires.

Pour l'instant, il est établi que nous avons besoin de trois POVM et que trois POVM de quatre éléments chacun sont suffisants. Essayons maintenant de réduire le nombre d'éléments des POVM. Le cas à un élément chacun est simple et les POVM à deux éléments sont en fait des mesures de von Neumann. Nous savons qu'elles ne sont pas suffisantes pour relever la non-contextualité d'un qubit. En fait, du moment où nous avons moins de trois éléments dans un POVM, ce POVM est inutile pour la construction d'un théorème de BKS selon la Proposition 3.4, car l'élément A doit soit toujours être seul, soit toujours être accompagné de l'unique élément $A^{\perp}$.

Examinons maintenant le cas de trois POVM de trois éléments chacun. Nous pouvons les exprimer sous la forme $\{A_1, B_1, C_1\}$, $\{A_2, B_2, C_2\}$ et $\{A_3, B_3, C_3\}$, sans perte de généralité, avec $A_i \neq B_j$ et $A_i \neq C_j$ pour tout (i, j). Portons notre attention sur les éléments A_1, A_2 et A_3. Soit que ces trois éléments sont les mêmes, soit que deux d'entre eux sont pareils ou bien ils sont tous différents. Dans tous les cas, nous pouvons assigner « oui » aux éléments A_i et « non » aux autres éléments sans créer de contradiction. Pour ce qui est d'une construction à quatre POVM de trois éléments chacun, celle-ci engendrerait une preuve avec le même

nombre d'éléments que celle de trois POVM avec quatre éléments chacun. Une telle construction est par contre impossible. Écrivons cet ensemble sous la forme $\{A_1, B_1, C_1\}$, $\{A_2, B_2, C_2\}$, $\{A_3, B_3, C_3\}$ et $\{A_4, B_4, C_4\}$. Nous pouvons toujours réécrire les POVM avec $A_i \neq B_j$ et $A_i \neq C_j$ pour tout (i, j), ou encore avec un ensemble de POVM isomorphe à l'ensemble $\{A_1, B_1, C_1\}$, $\{A_1, B_2, C_2\}$, $\{A_1, B_3, C_3\}$ et $\{B_1, B_2, B_3\}$. Dans les deux cas, nous pouvons facilement assigner des valeurs « oui » non-contextuellement sans créer de contradiction. □

Proposition 3.7. *Une preuve de BKS où la mécanique quantique ne peut être décrite par une théorie à VLC non-contextuelle doit être formulée à l'aide de mesures dont les éléments M_i ne sont pas proportionnels entre eux, $M_j \neq \gamma M_i$ pour $j \neq i$ et $\gamma > 0$.*

Autrement dit, les directions de mesures doivent être distinctes.

Lemme 3.8. *Aucune théorie classique à VLC non-contextuelle n'existe selon la Proposition 3.7.*

Démonstration. Nous pouvons utiliser l'ensemble de l'Équation 3.1 tel que nous l'avons fait pour le Lemme 3.5. □

Théorème 3.9. *La preuve du Lemme 3.8 contenant le moins d'éléments requiert trois POVM de quatre éléments chacun.*

Démonstration. La preuve est la même que celle du Théorème 3.6. □

Proposition 3.10. *Une preuve de BKS où la mécanique quantique ne peut être décrite par une théorie à VLC non-contextuelle doit assigner des valeurs « oui »/« non » seulement aux éléments de mesure M_i qui ne peuvent pas apparaître deux fois dans un POVM, $|M_i| > \frac{1}{2}$ [80].*

Benjamin F. Toner, David Bacon et Michael Ben-Or [80] ont prouvé que l'on ne peut avoir une théorie à VLC non-contextuelle selon la Proposition 3.10. Leur preuve contient 9 POVM avec entre 3 et 4 éléments chacun pour un total de 31 éléments.

Même si les preuves minimales des Lemmes 3.5 et 3.8 sont les mêmes, il est important de noter que ces deux types d'arguments sont fondamentalement différents. Alors que la Proposition 3.4 requiert seulement que les éléments soient distincts, la Proposition 3.7 requiert que les directions des sorties de la mesure soient distinctes.

3.2 Théorèmes de Bell

Les travaux de Bell ont été qualifiés par Henry P. Stapp de : « most profound discovery of science » [78]. Du moins, il est facile d'argumenter que le théorème de Bell a changé notre perspective de la nature, tout comme les travaux de Newton sur la mécanique classique ou d'Einstein sur la relativité. Grâce à ce théorème, nous *savons* maintenant qu'il existe des observables, dont les opérateurs ne commutent pas, qui n'ont pas d'existences simultanées et que seule une mesure peut forcer un état qui n'est pas un état propre de l'observable à prendre une valeur. Ceci dépend évidemment de la correctitude de la mécanique quantique.

La première preuve que le monde physique ne peut être décrit par une théorie à VLC a été formulée par Bell en 1964 sous la forme d'une inégalité [8]. Bell a borné la valeur absolue de la valeur espérée d'un opérateur spécifique pour *n'importe quelle* théorie à VLC et il a démontré que la MQ peut en fait violer cette borne. Il est donc approprié de définir les théorèmes de Bell sous la forme suivante.

Définition 3.3. *Un* théorème de Bell *est un ensemble de mesures multi-parties sur un état intriqué où les corrélations obtenues par les mesures ne peuvent pas être reproduites par quelque modèle à VLC que ce soit où aucune communication entre les parties n'est permise.*

3.2.1 Théorème de Clauser-Horne-Shimony-Holt

Le théorème de Bell discuté dans cette section est souvent considéré comme l'exemple canonique et a été proposé comme expérience réalisable par John F. Clauser, Michael A. Horne, Abner Shimony et Richard A. Holt (CHSH) [35]. Prenons A_1 et A_2 comme étant des mesures binaires sur le système d'Alice avec comme

résultat a_1 et a_2 respectivement, et B_1 et B_2 comme étant des mesures binaires sur le système de Bob avec comme résultat b_1 et b_2 respectivement. Nous pouvons alors borner classiquement

$$\Pr[a_1 = b_1] + \Pr[a_1 = b_2] + \Pr[a_2 = b_1] + \Pr[a_2 \neq b_2] \leq 3. \tag{3.2}$$

La preuve consiste simplement à analyser toutes les stratégies déterministes. Chacune est bornée par la valeur 3. Il ne peut donc pas exister une stratégie probabiliste qui viole cette borne, la première étant un mélange statistique de stratégies déterministes. Par contre, il existe une stratégie quantique, pour laquelle Alice et Bob font des mesures locales spécifiques sur un $|\Psi^-\rangle$, qui peut atteindre $2+\sqrt{2} > 3$. Le fait qu'aucune théorie à VLC ne puisse obtenir une valeur espérée plus grande que 3 alors que la MQ le permet est une preuve claire qu'il est impossible d'obtenir les corrélations quantiques avec une théorie à VLC. Du coup, si nous prenons les prédictions de la MQ comme étant correctes, nous devons abandonner la recherche d'une théorie locale réaliste de la nature.

3.3 Théorèmes de Bell sans inégalités

Un théorème de Bell dans toute sa généralité peut faire appel à un argument statistique afin de prouver l'impossibilité pour les théories à VLC de simuler la MQ. Pour cette raison, ils ne sont pas attrayantes aux yeux de plusieurs. Une preuve plus directe a donc été recherchée. Le premier exemple vient de Peter Heywood et Michael L. G. Redhead [50], où les auteurs ont proposé une « vérification expérimentale »[2] du théorème de BKS afin de rejeter le réalisme local[3]. Il est important de noter que les théorèmes de Bell sans inégalités ne sont pas des propositions d'expérimentation qui invalident les théories à VLC en un seul événement, contrairement aux théorèmes de Bell ordinaires qui requièrent plusieurs événements afin

[2]Voir la Section 5.2 pour en connaître d'avantage sur le sujet.

[3]Le premier exemple est souvent attribué faussement à Daniel M. Greenberger, Michael A. Horne et Anton Zeilinger [48].

de pouvoir faire une étude statistique. Comme l'a si bien dit Peres [71] : « The list of authors [qui ont fait cette erreur] is too long to give explicitly, and it would be unfair to give only a partial list. » Nous reviendrons sur ce sujet à la Section 5.1.

Définition 3.4. *Un* théorème de Bell sans inégalités *est un ensemble de mesures multiparties sur un état intriqué pour lequel n'importe quelle théorie à VLC voulant simuler la distribution de probabilités des résultats donnée par la MQ assignera une probabilité non-zéro à certains résultats de mesures interdits par la MQ* ou *ne produira jamais certains résultats de mesures prédits avec probabilité non-zéro par la MQ.*

3.3.1 Théorème de Hardy

Pour cet exemple, nous donnerons la version de Brassard [16] de la preuve de Lucien Hardy [49]. Les participants, Alice et Bob, partagent un état $(|01\rangle + |10\rangle + |11\rangle)/\sqrt{3}$. Disons qu'Alice et Bob ont maintenant le choix de mesurer individuellement l'état dans la base standard $|0\rangle, |1\rangle$, que nous nommerons ici $\mathbb{1}$, ou dans la base de Walsh-Hadamard H, qui est une transformation unitaire de Walsh-Hadamard (Équation 1.26) suivie d'une mesure dans la base standard. Selon la MQ, si les deux participants mesurent dans la base de Walsh-Hadamard, ils obtiendront le résultat $1 \otimes 1$ avec probabilité $1/12$. Il faut donc que n'importe quelle théorie à VLC voulant simuler les prédictions de la MQ prépare l'état de façon à ce qu'il produise parfois $1 \otimes 1$, lorsque les deux participants mesureront dans la base de Walsh-Hadamard. Supposons maintenant que l'état *est* décrit en fonction de VLC qui produiront $1 \otimes 1$ lorsque mesuré dans la base $\mathsf{H} \otimes \mathsf{H}$. Selon les critères des théories locales réalistes, nous savons maintenant que nous obtiendrons 1 lors d'une mesure locale H, indépendamment du choix de l'autre mesure. Voyons maintenant ce qui arrive lorsqu'Alice et Bob mesurent $\mathbb{1} \otimes \mathsf{H}$ ou $\mathsf{H} \otimes \mathbb{1}$. Selon les prédictions de la MQ, la théorie à VLC ne peut produire le résultat $1 \otimes 1$. Nous devons donc conclure, une fois de plus selon les critères des théories locales réalistes, qu'une mesure locale $\mathbb{1}$ de l'état produira la valeur 0. Une mesure $\mathbb{1} \otimes \mathbb{1}$ produira donc $0 \otimes 0$, ce qui n'est

pas permis selon la MQ. En somme, afin qu'une théorie à VLC produise $1 \otimes 1$ avec probabilité non-nulle lors d'une mesure $\mathsf{H} \otimes \mathsf{H}$, ce qui est prédit par la MQ, elle produira aussi $0 \otimes 0$ avec probabilité non-nulle lors d'une mesure $\mathbb{1} \otimes \mathbb{1}$, ce qui est interdit par la MQ.

3.4 Pseudo-télépathie

La pseudo-télépathie fut d'abord définie, mais pas encore baptisée comme telle, par Brassard, Cleve et Tapp[4]. Ils ont transformé l'algorithme de David Deutsch et Richard Jozsa [41] en format distribué afin de montrer qu'un nombre exponentiel de bits de communication est requis pour simuler les corrélations d'un certain nombre d'états de Bell [20]. Pour un article de survol complet sur la pseudo-télépathie, veuillez consulter [17].

Définition 3.5. *Nous disons qu'un jeu biparti G, Section 1.2.1, exhibe de la* pseudo-télépathie *si des mesures biparties d'un état intriqué peuvent donner une stratégie gagnante alors qu'aucune stratégie classique qui ne fait pas usage de communication ne peut être une stratégie gagnante.*

La généralisation aux cas multipartis est naturelle. Le terme pseudo-télépathie a été introduit afin de souligner un comportement qui ne peut être expliqué classiquement sans une communication quelconque. Imaginons deux physiciens qui ne connaissent pas la MQ (ou qui n'y croient absolument pas) et qui observent ce phénomène. Imaginons aussi qu'ils aient placé chaque participant à l'extérieur du cône de lumière de l'autre. Ceci peut être accompli en questionnant les deux participants avec un tel synchronisme, et en demandant des réponses tellement rapidement, qu'un signal allant à la vitesse de la lumière ne pourrait pas se rendre d'un participant à l'autre à temps pour influencer leurs réponses. Le fait que les participants continuent de répondre correctement à tous les coups, même si cela

[4]Un argument pourrait être formulé en faveur de Mermin [60] qui savait clairement ce qu'il faisait, mais n'a pas donné de définition formelle.

est incroyablement peu probable classiquement, étant donné qu'ils ne peuvent communiquer par aucun moyen physique connu par un physicien classique, serait pour le moins intrigant. Si intrigant que la *seule* explication convenable serait que les participants communiquent par un moyen encore inconnu à la physique. Pourquoi pas alors la télépathie ? Encore mieux, s'agirait-il même d'une preuve que la communication télépathique est instantanée ? Évidement, la vraie réponse est donnée par la MQ et non la télépathie.

Définition 3.6. *Nous disons que G est un jeu de pseudo-télépathie de dimension $d_A \times d_B$ s'il n'existe aucune stratégie classique, alors qu'une stratégie quantique utilisant un état intriqué de dimension $d_A \times d_B$ existe.*

3.4.1 Jeu du carré magique

Nous présentons ici le jeu de pseudo-télépathie connu sous le nom du carré magique dû à Padmanabhan K. Aravind [5]. Les participants, Alice et Bob, reçoivent un trit comme question, $x^{(A)} \in \{0,1,2\}$ et $x^{(B)} \in \{0,1,2\}$. Afin de gagner au jeu, ils doivent produire trois bits chacun, $y_1^{(A)}$, $y_2^{(A)}$, $y_3^{(A)}$ et $y_1^{(B)}$, $y_2^{(B)}$, $y_3^{(B)}$, de telle sorte que $y_1^{(A)} + y_2^{(A)} + y_3^{(A)}$ doit être pair, $y_1^{(B)} + y_2^{(B)} + y_3^{(B)}$ doit être impair et $y_{x^{(B)}}^{(A)}$ doit égaler $y_{x^{(A)}}^{(B)}$. Afin d'avoir une stratégie gagnante sans avoir recours à la MQ ou à la communication, Alice et Bob doivent partager une stratégie qui donne une réponse acceptable à tout coup. Cela revient à partager un tableau 3×3 de 0 et de 1 de telle sorte que la somme de chaque rangée, represantant les sorties d'Alice pour chaque entrée, est paire et la somme de chaque colonne, *idem* pour Bob, est impaire. Un simple argument de parité montre qu'il est en fait impossible de construire un tel tableau et donc impossible d'avoir une stratégie classique gagnante au jeu du carré magique. D'un autre côté, si Alice et Bob partagent de l'intrication, il existe une stratégie gagnante. Il doit être noté qu'il est toujours impossible pour Alice et Bob de construire un carré magique, mais les corrélations des mesures de l'état intriqué leur permettent tout de même de répondre correctement aux questions à tous les coups.

3.4.2 Limites de la pseudo-télépathie

Dans cette section, nous présentons les limites connues de la pseudo-télépathie en fonction de la dimension de la stratégie quantique gagnante.

Théorème 3.11. *Il n'existe pas de jeu de pseudo-télépathie dont la dimension de l'ensemble des réponses est de* 2×2 *[38].*

Théorème 3.12. *Il existe un jeu de pseudo-télépathie dont la dimension de l'ensemble des réponses est de* 2×3 *[38, 50].*

Corollaire 3.13. *Le plus petit jeu de pseudo-télépathie possible, en terme de la dimension de l'ensemble des réponses, est* 2×3.

Démonstration. Il ne peut exister un jeu de pseudo-télépathie de dimension 2×2. Deux solutions sont envisageables, nous ajoutons un troisième participant ou nous augmentons la dimension de l'ensemble de réponses. Si nous augmentons le nombre de participants, afin que le nouveau jeu ait un sens, la cardinalité k de l'ensemble de réponses du nouveau joueur doit être plus grande ou égale à deux. Nous avons donc un nouveau jeu pour lequel la dimension de l'ensemble des réponses est de $2 \times 2 \times k \geq 8$. L'autre possibilité est d'incrémenter la cardinalité de l'ensemble des réponses de l'un des participants déjà existant. La plus petite incrémentation possible est un ensemble $2 \times 3 = 6 < 8$. □

Théorème 3.14. *Il existe un jeu de pseudo-télépathie dont la dimension de l'ensemble des questions est de* 3×3 *[5].*

Théorème 3.15. *Il existe un jeu de pseudo-télépathie dont la dimension de l'ensemble des questions est de* $2 \times 2 \times 2$ *[60].*

Conjecture 3.16. *Il n'existe pas de jeu de pseudo-télépathie dont l'ensemble des questions est de dimension* 2×2.

Pour un ensemble de questions de dimension 2×3, la question est aussi ouverte. Il n'existe malheureusement pas plus de résultats quant à la dimension minimale de

l'ensemble des questions. Par contre, la dimension minimale de l'état intriqué requis pour l'existence d'un jeu de pseudo-télépathie est connue [23]. Nous prouverons ici en détail ces résultats. Commençons d'abord par quelques lemmes techniques.

Lemme 3.17. *Prenons n'importe quel jeu à deux participants dont la stratégie quantique gagnante utilise un état* $|\Phi\rangle$ *de dimension* 2×2. *Le même jeu a aussi une stratégie gagnante si les joueurs sont restreints à partager un état biparti* $|\Psi\rangle = \alpha|00\rangle + \beta|11\rangle$, *où* α *et* β *sont des nombres réels positifs bien choisis.*

Démonstration. Nous savons du théorème de décomposition de Schmidt qu'il existe une base orthonormale $\{|A_0\rangle, |A_1\rangle\}$ pour Alice et $\{|B_0\rangle, |B_1\rangle\}$ pour Bob telle que $|\Phi\rangle$ peut être réécrit comme

$$|\Phi\rangle = \alpha|A_0\rangle|B_0\rangle + \beta|A_1\rangle|B_1\rangle$$

pour des nombres réels positifs appropriés α et β. Si Alice et Bob partagent un état intriqué $|\Psi\rangle = \alpha|00\rangle + \beta|11\rangle$ au lieu de $|\Phi\rangle$, Alice applique une transformation unitaire $|A_0\rangle\langle 0| + |A_1\rangle\langle 1|$ sur son qubit et Bob fait de même avec $|B_0\rangle\langle 0| + |B_1\rangle\langle 1|$. L'effet de ces opérations locales est de transformer $|\Psi\rangle$ en $|\Phi\rangle$. De là, Alice et Bob peuvent appliquer la stratégie quantique dont nous avons supposé l'existence. □

Lemme 3.18. *Tout jeu de pseudo-télépathie de dimension* $d_A \times d_B$ *est aussi un jeu de pseudo-télépathie de dimension* $d \times d$, *où* $d = \min(d_A, d_B)$.

Démonstration. Il n'y a évidement rien à prouver si $d_A = d_B$. Supposons sans perte de généralité que $d = d_A < d_B$. Nous savons du théorème de décomposition de Schmidt que n'importe quel système quantique de dimension $d_A \times d_B$ peut être écrit comme $\sum_i^d \alpha_i|A_i\rangle|B_i\rangle$ dans une base orthonormale appropriée, $\{|A_i\rangle\}_{i=1}^{d_A}$ pour Alice et $\{|B_i\rangle\}_{i=1}^{d_B}$ pour Bob, où la sous-base de Bob $\{|B_i\rangle\}_{i=1}^{d}$ génère un sous-espace de dimension d_A de l'espace de Hilbert de dimension d_B d'origine. Le reste de la preuve suit exactement celle du Lemme 3.17. □

Lemme 3.19. *Pour tous nombres réels* a *et* b, $a^2 + b^2 \geq 2ab$, *avec égalité si et seulement si* $a = b$.

Démonstration. La moyenne géométrique de a^2 et b^2 est $\sqrt{a^2b^2} = ab$ et la moyenne arithmétique est $(a^2 + b^2)/2$. Le lemme est une conséquence directe du fait bien connu que la moyenne géométrique est une borne inférieure à la moyenne arithmétique, l'égalité étant remplie si et seulement si les deux nombres sont égaux. □

Théorème 3.20. *Il n'y a pas de jeu de pseudo-télépathie de dimension* 2×2.

Démonstration. Prenons n'importe quel jeu biparti $(X^{(A)}, X^{(B)}, Y^{(A)}, Y^{(B)}, R)$ pour lequel Alice et Bob ont une stratégie quantique gagnante où ils utilisent un état intriqué de dimension 2×2. Notre but est de montrer une stratégie purement classique qui est aussi une stratégie gagnante. Par définition, ceci implique que ce jeu n'est pas un jeu de pseudo-télépathie, ce qui prouve le théorème.

Il est important de noter que nous ne tentons pas de simuler les probabilités des réponses de la stratégie quantique, ce qui est impossible sans communication. Qui plus est, nous ne tentons pas de trouver une stratégie classique qui produit, avec une probabilité non-nulle, l'ensemble exact des réponses que la stratégie quantique peut produire. Tout ce que nous désirons de notre stratégie classique est de ne *jamais* produire une réponse interdite par le jeu de pseudo-télépathie. Cette condition sera automatiquement remplie si nous créons une stratégie classique qui ne produit jamais de réponse ayant une probabilité nulle d'être produite par la stratégie quantique.

Selon la MQ, la stratégie la plus générale qu'Alice et Bob peuvent confectionner consiste à ce que chacun choisisse un POVM en fonction de sa question, applique le POVM à sa partie de l'état partagé et interprète le résultat en terme des éléments de l'ensemble des réponses. Plus formellement, soit $\mathcal{P}$ l'ensemble de tous les POVM sur un qubit. Pour chaque $M \in \mathcal{P}$ possédant un ensemble de matrices positives $\{M_i\}$, notons l'ensemble de réponses possibles par O_M. L'indice i dans $\{M_i\}$ prend donc comme valeur un élément de l'ensemble O_M. Prenons O comme l'union de tous les O_M pour les $M \in \mathcal{P}$.

Toute stratégie quantique peut être définie en termes de l'état intriqué $|\Psi\rangle$ et

des correspondances suivantes.

$$\begin{aligned} \mathcal{X}^{(A)} &: X^{(A)} \to \mathcal{P} \quad ; \quad \mathcal{X}^{(B)} : X^{(B)} \to \mathcal{P} \\ \mathcal{Y}^{(A)} &: X^{(A)} \times O \to Y^{(A)} \quad ; \quad \mathcal{Y}^{(B)} : X^{(B)} \times O \to Y^{(B)} \end{aligned}$$

Lorsqu'elle reçoit sa question $x^{(A)} \in X^{(A)}$, Alice détermine sa mesure $M^{x^{(A)}} = \mathcal{X}^{(A)}(x^{(A)})$ et l'applique sur sa partie de $|\Psi\rangle$. Elle obtient un résultat $i \in O_{M^{x^{(A)}}}$ et elle produit $\mathcal{Y}^{(A)}(x, i)$ comme réponse. Lorsqu'il reçoit sa question $x^{(B)} \in X^{(B)}$, Bob fait de même, *mutatis mutandis*.

Sans perte de généralité, selon le Lemme 3.17, nous pouvons supposer que l'état intriqué utilisé par Alice et Bob est de la forme $|\Psi\rangle = \alpha|00\rangle + \beta|11\rangle$, où α et β sont des nombres réels positifs. Nous pouvons aussi supposer que α et β sont strictement positifs, car sinon l'état est un état produit et les mesures locales sur les états produits sont facilement simulables classiquement. Nous pouvons aussi, grâce au Lemme 1.1, nous permettre sans perte de généralité de ne considérer que les POVM dont les éléments sont proportionnels à des projecteurs.

Considérons une ronde du jeu dans laquelle Alice et Bob reçoivent des questions $x^{(A)} \in X^{(A)}$ et $x^{(B)} \in X^{(B)}$ respectivement. Selon la stratégie quantique gagnante, $M^{x^{(A)}} = \mathcal{X}^{(A)}(x^{(A)}) = \{\gamma_i^{x^{(A)}} P_i^{x^{(A)}}\}$ et $N^{x^{(B)}} = \mathcal{X}^{(B)}(x^{(B)}) = \{\gamma_j^{y^{(B)}} Q_j^{x^{(B)}}\}$ sont les POVM appliqués par Alice et Bob, respectivement, sur leur partie de l'état intriqué. Soit $\theta_i^{(A)}$ et $\phi_i^{(A)}$ les angles qui caractérisent le projecteur $P_i^{x^{(A)}}$ selon l'Équation 1.20, et similairement $\theta_j^{(B)}$ et $\phi_j^{(B)}$ pour $Q_j^{x^{(B)}}$. Pour tout i et j, la probabilité conjointe $\Pr[i, j]$ que le résultat de la mesure d'Alice soit i et que celui de Bob soit j est

$$\begin{aligned} \Pr[i,j] &= \langle\Psi|(\gamma_i^{x^{(A)}} P_i^{x^{(A)}}) \otimes (\gamma_j^{x^{(B)}} Q_j^{x^{(B)}})|\Psi\rangle \\ &= \gamma_i^{x^{(A)}} \gamma_j^{x^{(B)}} \big[\alpha^2 \cos(\theta_i^{(A)})^2 \cos(\theta_j^{(B)})^2 + \beta^2 \sin(\theta_i^{(A)})^2 \sin(\theta_j^{(B)})^2 \\ &\quad + 2\alpha\beta \cos(\theta_i^{(A)}) \cos(\theta_j^{(B)}) \cos(\phi_i^{(A)} + \phi_j^{(B)}) \sin(\theta_i^{(A)}) \sin(\theta_j^{(B)})\big]. \end{aligned} \tag{3.3}$$

Prenons $a = \alpha \cos(\theta_i^{(A)}) \cos(\theta_j^{(B)})$, $b = \beta \sin(\theta_i^{(A)}) \sin(\theta_j^{(B)})$ et $c = \cos(\phi_i^{(A)} + \phi_j^{(B)})$. Il est important de noter que $a \geq 0$ et $b \geq 0$, car $\alpha > 0$, $\beta > 0$, $0 \leq \theta_i^x \leq \pi/2$

et $0 \leq \theta_j^y \leq \pi/2$, et évidement $-1 \leq c \leq 1$. Puisque $\gamma_i^{x^{(A)}}$ et $\gamma_j^{x^{(B)}}$ sont non-nuls, il découle directement du Lemme 3.19 que la probabilité conjointe d'Alice et Bob est $\Pr[i,j] = \gamma_i^{x^{(A)}}\gamma_j^{x^{(B)}}(a^2+b^2+2abc)$, qui ne peut être nulle que si $a=b=0$ ou si $a=b$ et $c=-1$. Le premier cas requiert que $\theta_i^{(A)} = 0$ et $\theta_j^{(B)} = \pi/2$ ou *vice versa*, ce qui implique que $P_i^{x^{(A)}}$ ou $Q_j^{x^{(B)}}$ n'appartient à aucun hémisphère, étant proportionnel au pôle Sud. La condition $c=-1$ dans le second cas implique que $\phi_i^{(A)} + \phi_j^{(B)} = \pi$ ou $\phi_i^{(A)} + \phi_j^{(B)} = 3\pi$, car $0 \leq \phi_i^{(A)} + \phi_j^{(B)} \leq 4\pi$.

Rappelons-nous que notre but est d'établir une stratégie classique entre Alice et Bob qui ne produira jamais un résultat qui n'aurait pu être produit par la stratégie quantique. Pour cela, il suffit à Alice de choisir un i tel que $\gamma_i^{x^{(A)}} P_i^{x^{(A)}}$ appartient à l'hémisphère *est* et pour Bob de choisir un j tel que $\gamma_j^{x^{(B)}} Q_j^{x^{(B)}}$ appartient à l'hémisphère *ouest*. Ceci est toujours possible selon le Lemme 1.4. De cette façon, ni Alice, ni Bob ne choisiront un élément de POVM proportionnel au pôle Sud, évitant donc $a=b=0$, et $\pi < \phi_i^{(A)} + \phi_j^{(B)} < 3\pi$ puisque $0 \leq \phi_i^{(A)} < \pi$. De plus, $\pi < \phi_j^{(B)} \leq 2\pi$, évitant ainsi $c=-1$. Il en découle que les choix indépendants d'Alice et Bob selon la stratégie classique sont des choix qui auraient pu être faits lors de la stratégie quantique. Puisque la stratégie quantique est une stratégie gagnante, elle produit donc une réponse valide, tout comme la stratégie classique. □

Corollaire 3.21. *Il n'y a pas de jeu de pseudo-télépathie à deux participants de dimension* $2 \times n$*, peut importe le nombre* n*.*

Démonstration. Selon le Lemme 3.18, tout jeu de pseudo-télépathie de dimension $2 \times n$ serait un jeu de pseudo-télépathie de dimension 2×2. Selon le Théorème 3.20, il ne peut exister un tel jeu. □

Corollaire 3.22. *Le jeu de pseudo-télépathie à deux participants ayant la plus petite dimension est de dimension* 3×3*.*

Démonstration. Ceci découle directement du Corollaire 3.21 et du fait qu'un jeu de pseudo-télépathie de dimensions 3×3 existe [38, 50]. □

Corollaire 3.23. *Le jeu de pseudo-télépathie ayant la plus petite dimension est de dimension* $2 \times 2 \times 2$*.*

Démonstration. Un jeu de pseudo-télépathie requiert que chaque participant ait au moins un qubit d'intrication avec les autres participants. Il en découle donc qu'un jeu à n participants doit être de dimension totale d'au moins 2^n si tous les joueurs participent au jeu. Selon le Corollaire 3.22, le meilleur jeu à deux participants est de dimension $3 \times 3 = 9$. Selon la discussion ci-haut, le jeu à trois joueurs Mermin-GHZ [48,60], qui est de dimension $2 \times 2 \times 2 = 8$, est optimal parmi les jeux à trois joueurs. Du fait que $8 < 9 < 16$, on obtient le corollaire. □

CHAPITRE 4

SIMULATION DE L'INTRICATION

Ce qui nous intéresse lors de la simulation de l'intrication est de reproduire les corrélations produites par des mesures multiparties sur un état intriqué. Alice et Bob partagent un état $|\psi\rangle_{AB}$ et reçoivent la description d'un POVM $\{X_i^{(A)}\}$ et $\{X_j^{(B)}\}$ respectivement. S'ils mesurent localement leur partie de l'état $|\psi\rangle_{AB}$ selon la description de leur POVM, la probabilité conjointe est

$$\Pr[y^{(A)} = i, y^{(B)} = j] = \langle\psi_{AB}| \left(X_i^{(A)} \otimes X_j^{(B)}\right) |\psi_{AB}\rangle. \tag{4.1}$$

Dans le cas où l'état est $|\Psi^-\rangle$ et que nous utilisons la Représentation 1.2 ainsi que le Lemme 1.1, la probabilité conjointe est

$$\Pr[y^{(A)} = i, y^{(B)} = j] = (|\vec{x}_i^{(A)}||\vec{x}_j^{(B)}| - \vec{x}_i^{(A)} \cdot \vec{x}_j^{(B)})/4. \tag{4.2}$$

Dans cette situation, nous voulons reproduire ces corrélations avec des théories à VLC augmentées d'une autre ressource car nous savons que les théories à VLC ne sont pas suffisantes [8]. La mesure de complexité sera simplement la quantité de ressources ajoutées aux VLC afin de pouvoir reproduire les corrélations quantiques. Cette approche est très intéressante, autant pour les physiciens que pour les informaticiens. En effet, nous croyons qu'elle est une bonne mesure de non-localité[1] et que nous apprendrons beaucoup sur le monde quantique par ces études, en particulier sur les expériences tentant d'invalider les théories à VLC. De plus, comme nous le verrons aux Sections 5.7 et 5.8, ces mesures ont des impacts sur la complexité de la communication et elles nous permettent de mieux comprendre ce qui nous est possible d'accomplir avec de l'intrication.

[1]Plus de détails à la Section 5.11

4.1 Simulation de l'intrication par la communication

Le problème de la simulation de l'intrication par la communication peut être défini plus précisément.

Définition 4.1. *Soit un triplet* $(|\Psi\rangle_{AB}\ ,\ X^{(A)},\ X^{(B)})$ *où* $|\Psi\rangle_{AB}$ *est un état intriqué,* $X^{(A)}$ *est un ensemble de mesures sur la première partie et* $X^{(B)}$ *est un ensemble de mesures sur la deuxième partie. Le coût de la simulation de l'intrication est le protocole purement classique étant capable de reproduire les mêmes corrélations avec le moins de communication possible entre Alice et Bob.*

La simulation de l'intrication par la communication a été introduite par un article de Tim W. Maudlin publié dans un journal de philosophie en 1992 [59]. Dans son article, il propose une simulation d'un état de Bell avec de la communication espérée et des variables locales cachées et il prétend qu'une simulation avec une communication bornée en pire cas est impossible. Cette dernière affirmation a été contredite par Brassard, Cleve et Tapp [20] où les auteurs ont trouvé la première simulation en pire cas. Nous savons maintenant qu'il est possible de simuler des mesures de von Neumann sur un état de Bell avec un bit de communication et une VLC continue [79]. En fait, ce bit n'est pas d'entropie maximale, et si nous faisons le protocole plusieurs fois en parallèle, nous pouvons utiliser le codage en blocs pour réduire la communication à $\cos^2(\pi/8) \approx 0,85$ bit par état simulé. La simulation d'un état de Bell avec des variables aléatoires partagées, $C^\star(|\Psi^-\rangle)$, est donc $C^\star(|\Psi^-\rangle) \leq 0,85$. Nous savons aussi que si nous voulons simuler des mesures de von Neumann sur n états de Bell, et non faire n simulations d'*un* état, $\Omega(2^n)$ bits de communication sont nécessaires en pire cas [20].

Tous ces protocoles utilisent des variables aléatoires partagées. Sont-elles nécessaires ? Serge Massar, David Bacon, Nicolas Cerf et Richard Cleve ont démontré que, si la communication était bornée de façon absolue, alors un nombre de bits fini de variables aléatoires partagées n'est pas suffisant pour simuler de l'intrication [57]. Par contre, dans le cas d'une quantité de communication espérée, les variables aléatoires partagées ne sont pas nécessaires. En effet, un protocole est présenté

dans [57] pour simuler des POVM sur n bits d'intrication avec $O(n2^n)$ bits de communication espérée sans variables aléatoires partagées (20 pour un état de Bell). La simulation de POVM sur un état de Bell, $C(|\Psi^-\rangle|\text{POVM})$, est donc $C_{\text{espérée}}(|\Psi^-\rangle|\text{POVM}) \leq 20$.

4.1.1 Simulation de POVM

Nous présenterons ici un protocole basé sur [79] et [32] afin de simuler des *POVM* sur un état de Bell. Le protocole utilise *5,7 bits de communication espérée* et une quantité infinie de VLC [61], $C_{\text{espérée}}(|\Psi^-\rangle|\text{POVM}) \leq 5,7$.

- Alice et Bob partagent deux vecteurs de norme unitaire $\vec{v}_1, \vec{v}_2 \in \mathbb{R}^3$.
- Alice et Bob se font donner la description de leur POVM $\{X_i^{(A)}\}$ et $\{X_i^{(B)}\}$ respectivement.
- Alice choisit le $i^{\text{ème}}$ résultat de son POVM selon la distribution de probabilité $\Pr[y^{(A)} = i] = |\vec{x}_i^{(A)}|/2$.
- Alice envoie $c = \Theta(-\vec{x}_i^{(A)} \cdot \vec{v}_1)$ et $d = \Theta(-\vec{x}_i^{(A)} \cdot \vec{v}_2)$, où $\Theta(x) = \begin{cases} 1 \text{ si } x \geq 0 \\ 0 \text{ si } x < 0 \end{cases}$.
- Bob choisit le $j^{\text{ème}}$ résultat de son POVM selon la distribution de probabilité $\Pr[y^{(B)} = j] = |\vec{x}_j^{(B)}|/2$.
- Bob vérifie si $-\vec{x}_j^{(B)} \cdot ((-1)^c\vec{v}_1 + (-1)^d\vec{v}_2) < 0$. Si c'est le cas, il envoie 0 à Alice et ils recommencent le protocole avec de nouvelles variables aléatoires $\vec{v}_1$ et $\vec{v}_2$.
- Autrement, Bob envoie 1 à Alice et ils produisent leurs sorties i et j respectivement.

L'analyse du protocole est simple. La probabilité pour Alice d'obtenir le résultat i du POVM est, tel qu'énoncé, $\Pr[y^{(A)} = i] = |\vec{x}_i^{(A)}|/2$. Pour ce qui est de la probabilité marginale de Bob, le vecteur $(-1)^c\vec{v}_1 + (-1)^d\vec{v}_2$ peut être considéré comme un vecteur pointant dans une direction aléatoire. La probabilité qu'il rejette le vecteur $\vec{x}_j^{(B)}$ est donc $1/2$. Puisque la probabilité de rejeter le vecteur est indépendante d'une ronde à l'autre, la probabilité marginale de Bob est $Pr[y^{(B)} = j] = |\vec{x}_j^{(B)}|/2$.

Pour la probabilité conjointe, le calcul est un peu plus difficile, mais tout de même assez direct. Afin que les équations entrent sur une ligne, prenons les définitions $\vec{a}_i \equiv \vec{x}_i^{(A)}$ et $\vec{b}_i \equiv \vec{x}_i^{(B)}$.

$$\begin{aligned}
\Pr[y^{(A)} = i, y^{(B)} = j] &= \frac{|\vec{a}_i||\vec{b}_j|}{4(4\pi)^2} \iint \Theta(-\vec{b}_j \cdot ((-1)^c \vec{v}_1 + (-1)^d \vec{v}_2)) d\vec{v}_1 d\vec{v}_2 \\
&= \frac{|\vec{a}_i||\vec{b}_j|}{8} - \frac{|\vec{a}_i||\vec{b}_j|}{8(4\pi)^2} \iint sgn(\vec{a}_i \cdot \vec{v}_1) sgn(\vec{b}_j \cdot (\vec{v}_1 + sgn(\vec{a}_i \cdot \vec{v}_1) sgn(\vec{a}_i \cdot \vec{v}_2) \vec{v}_2)) d\vec{v}_1 d\vec{v}_2 \\
&= \frac{|\vec{a}_i||\vec{b}_j| - \vec{a}_i \cdot \vec{b}_j}{8},
\end{aligned} \tag{4.3}$$

où $sgn(x) = 2\Theta(x) - 1$.

Le facteur de $1/2$ dans l'Équation 4.3 par rapport à l'Équation 4.2 n'est qu'un artefact de la façon dont nous avons calculé la probabilité conjointe. Il représente en fait la probabilité d'échouer lors d'une ronde et peut être éliminé par renormalisation [32]—qui est permis étant donné que les rondes sont indépendantes l'une de l'autre—ou par calcul formel passant par la série géométrique. Nommons

$$p \equiv \frac{|\vec{x}_i^{(A)}||\vec{x}_j^{(B)}| - \vec{x}_i^{(A)} \cdot \vec{x}_j^{(B)}}{4}. \tag{4.4}$$

Lors de la première ronde, Alice et Bob produisent des résultats qui ont une distribution de probabilité p avec probabilité $1/2$ et ils passent à la ronde suivante avec probabilité $1/2$, ainsi de suite. La distribution de probabilité totale est donc

$$\frac{1}{2}p + \frac{1}{2} \cdot \frac{1}{2}p + \cdots = \sum_{n=1}^{\infty} \frac{1}{2^n} p = p. \tag{4.5}$$

Puisque chaque ronde est indépendante de la ronde précédente et que chacune a une probabilité de mettre un terme au protocole de $1/2$, le protocole prend en moyenne deux rondes et donc $2(2 + 1) = 6$ bits de communication espérée. S'il nous est permis d'utiliser le codage en blocs, nous pouvons réduire la communication. Alice envoie toujours c tel que décrit par le protocole original, mais au lieu d'envoyer d, elle envoie $d' = \Theta(\vec{x}_i^{(A)} \cdot \vec{v}_1) \oplus \Theta(\vec{x}_i^{(A)} \cdot \vec{v}_2)$, duquel il est possible de retrouver

facilement d à l'aide de c. Nous savons de [79] que d' peut être comprimé à $0,85$ bit en moyenne. La communication devient alors de $2(1+0,85+1)=5,7$ bits.

4.2 Simulation de jeux de pseudo-télépathie

Cette section est vouée à la simulation de certaines corrélations quantiques qui peuvent survenir lors de jeu de pseudo-télépathie [24]. Nous utilisons ici deux différentes ressources afin de simuler la MQ : la communication et les BNL.

Récemment, Nicolas Cerf, Nicolas Gisin, Serge Massar et Sandu Popescu ont transformé le protocole de Toner et Bacon [79] afin de pouvoir utiliser les BNL pour simuler les corrélations obtenues par des mesures de von Neumann biparties sur un état de Bell $|\Psi^-\rangle$, et ce sans communication [33]. Ce résultat démontre qu'il n'est pas nécessaire de signaler de l'information sur les mesures afin de pouvoir réussir une simulation parfaite des corrélations quantiques. Le but à long terme de cette étude est de caractériser les BNL afin de nous donner une intuition sur la non-localité de la nature.

La BNL a été inspirée de l'inégalité de CHSH [35], qui est souvent considérée comme l'inégalité canonique pour la non-localité d'un état de Bell. Il peut donc être tentant de tracer une analogie entre les BNL et les états de Bell. Nous allons par contre montrer des tâches distribuées qui ne peuvent pas être accomplies par un seul état de Bell, alors qu'un protocole non-local utilisant seulement une BNL peut accomplir la tâche.

Définition 4.2. *Un protocole* non-local *est un protocole purement classique dans lequel les participants peuvent utiliser des BNL.*

Définition 4.3. *Un protocole* simule *les* corrélations *d'un jeu de pseudo-télépathie si, en plus d'être une stratégie gagnante, les réponses données par le protocole sont uniformément distribuées parmi toutes les réponses qui satisfont la relation.*

En particulier, nous étudierons dans les Sections 4.2.1 et 4.2.2 la pseudo-télépathie et démontrerons certains jeux de pseudo-télépathie pour lesquels une

seule BNL suffit pour simuler le jeu, alors que plus d'un état de Bell est requis pour réussir la tâche. Nous démontrerons aussi une limite à la puissance de la BNL dans les Sections 4.2.3 et 4.2.4.

4.2.1 Jeu du carré magique

Nous avons vu qu'une BNL peut simuler les corrélations de mesures de von Neumann sur un état de Bell $|\Psi^-\rangle$ sans communication. Une question évidente serait de se demander si les BNL peuvent nous en donner plus. En particulier, existe-t-il des corrélations quantiques qui peuvent être simulées par une seule BNL alors que plusieurs états de Bell seraient nécessaires ? Dans cette section, nous répondons à cette question par l'affirmative en démontrant que le jeu de pseudo-télépathie du carré magique [5] peut être simulé par un protocole non-local utilisant seulement une BNL, alors que plus d'un état de Bell est requis pour confectionner une stratégie gagnante. Alors que nous avons déjà défini le jeu du carré magique à la Section 3.4, nous donnons ici une définition plus formelle et mieux adaptée aux besoins de cette section.

Définition 4.4. *Dans le jeu du* carré magique, *Alice et Bob reçoivent* $x^{(A)} \in \{1,2,3\}$ *et* $x^{(B)} \in \{1,2,3\}$, *respectivement. Ils produisent ensuite trois bits chacun,* $(y_1^{(A)}, y_2^{(A)}, y_3^{(A)})$ *et* $(y_1^{(B)}, y_2^{(B)}, y_3^{(B)})$, *tel que :*

$$\begin{aligned} y_1^{(A)} \oplus y_2^{(A)} \oplus y_3^{(A)} &= 0, \\ y_1^{(B)} \oplus y_2^{(B)} \oplus y_3^{(B)} &= 1, \\ y_{x^{(B)}}^{(A)} &= y_{x^{(A)}}^{(B)}. \end{aligned} \tag{4.6}$$

Dans cette définition, de même que pour toutes les futures définitions de jeux de pseudo-télépathie, il est sous-entendu que $(x^{(A)}, x^{(B)}, y^{(A)}, y^{(B)}) \in R$ si et seulement si les équations données sont satisfaites.

Il est connu que le jeu du carré magique est un jeu de pseudo-télépathie dont la meilleure probabilité de gagner pour des joueurs classiques est de 8/9 alors que des joueurs partageant l'état $|\psi\rangle = \frac{1}{2}|0011\rangle - \frac{1}{2}|0110\rangle - \frac{1}{2}|1001\rangle + \frac{1}{2}|1100\rangle$ (deux

états de Bell), où Alice a les deux premiers qubits et Bob les deux derniers, ont une stratégie gagnante [17].

Lemme 4.1. *Aucune stratégie quantique pour le jeu du carré magique n'est une stratégie gagnante si les participants ne partagent qu'une paire de qubits intriqués* $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$.

Démonstration. Il s'agit d'une conséquence directe du Théorème 3.20. □

Théorème 4.2. *Il existe une stratégie classique gagnante au jeu du carré magique si les participants peuvent communiquer un bit.*

Démonstration. Alice et Bob se mettent d'accord à l'avance sur deux stratégies, 0 et 1. La stratégie 0 donnera une réponse satisfaisante à toutes les questions sauf lorsque $x^{(A)} = x^{(B)} = 3$, et la stratégie 1 donnera une bonne réponse lorsque $x^{(A)} = 3$. De plus, les stratégies 0 et 1 peuvent être choisies de telle sorte que les réponses d'Alice sont les mêmes lors des deux stratégies. La stratégie finale d'Alice et Bob sera simplement l'envoi d'un bit par Alice signalant si $x^{(A)} = 3$ ou pas. Si $x^{(A)} \neq 3$, Bob agit selon la stratégie 0, sinon la stratégie 1. Il est maintenant facile de vérifier qu'il s'agit bien d'une stratégie gagnante. □

Théorème 4.3. *Des participants classiques qui peuvent se transmettre un bit de communication peuvent simuler le jeu du carré magique.*

Démonstration. Alice et Bob choisissent maintenant les stratégies 0 et 1, comme dans la preuve du Théorème 4.2, mais en utilisant cette fois une variable aléatoire partagée afin de choisir uniformément parmi toutes les stratégies qui peuvent être construites ainsi. Avec cette nouvelle stratégie, les réponses d'Alice et de Bob sont maintenant uniformément distribuées parmi toutes les réponses gagnantes possibles. □

Théorème 4.4. *Il existe une stratégie non-locale gagnante pour le jeu du carré magique qui utilise une seule BNL.*

Démonstration. Alice et Bob ont chacun deux stratégies, $A0$ et $A1$ pour Alice et $B0$ et $B1$ pour Bob. Les deux stratégies d'Alice respectent la condition $y_1^{(A)} \oplus y_2^{(A)} \oplus y_3^{(A)} = 0$ et celles de Bob, $y_1^{(B)} \oplus y_2^{(B)} \oplus y_3^{(B)} = 1$. Chaque paire de stratégies $(A0, B0)$ et $(A1, B1)$ produit des réponses valides, $y_{x^{(B)}}^{(A)} = y_{x^{(A)}}^{(B)}$, pour toutes les questions, sauf lorsque $x^{(A)} = x^{(B)} = 3$. De plus, les stratégies $A0$ et $B1$, ainsi que $A1$ et $B0$, sont coordonnées de telle sorte que si Alice répond selon la stratégie Ai $(i \in 0, 1)$ et Bob selon la stratégie Bj $(j = i \oplus 1)$, alors nous avons $y_3^{(A)} = y_3^{(B)}$ pour les questions $x^{(A)} = x^{(B)} = 3$. De telles stratégies se trouvent aisément.

Alice et Bob utilisent une BNL afin de déterminer quelles stratégies ils utiliseront. Ils entrent tous deux un bit dans la BNL représentant s'ils ont, ou pas, eu $x^{(A)} = 3$ ou $x^{(B)} = 3$. Ils utilisent ensuite les sorties de la BNL, $z^{(A)}$ et $z^{(B)}$, afin de déterminer quelle stratégie ils doivent suivre ($Az^{(A)}$ pour Alice, $Bz^{(B)}$ pour Bob).

Prenons note que, par les propriétés de la BNL, Alice et Bob auront $z^{(A)} = z^{(B)}$ tant et aussi longtemps que $x_A \neq 3$ ou $x_B \neq 3$. Les stratégies $(A0, B0)$ et $(A1, B1)$ produiront des résultats valides dans ce cas. Si, par contre, $x^{(A)} = 3$ et $x^{(B)} = 3$, alors Alice et Bob répondront selon les stratégies $(A0, B1)$ ou $(A1, B0)$. Ces stratégies ont justement été coordonnées pour s'assurer que $y_3^{(A)} = y_3^{(B)}$ dans ce cas. □

Théorème 4.5. *Des participants classiques qui peuvent utiliser une seule BNL peuvent simuler le jeu du carré magique.*

Démonstration. La preuve est similaire à celle du Théorème 4.3. Tout ce qu'Alice et Bob ont à faire pour simuler les corrélations du carré magique est d'appliquer la stratégie de la preuve du Théorème 4.4, mais avec les stratégies $A0$, $A1$, $B0$ et $B1$ choisies selon une distribution uniforme parmi toutes les stratégies qui satisfont la construction donnée à la preuve du Théorème 4.4. Les réponses d'Alice et Bob sont alors uniformément distribuées parmi toutes les réponses qui satisfont la Définition 4.4. □

Du Lemme 4.1 et du Théorème 4.4, nous trouvons le corollaire suivant :

Corollaire 4.6. *Une seule BNL peut simuler des corrélations quantiques biparties qu'une seule paire de qubits intriqués, $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$, ne peut simuler.*

4.2.2 Jeu de Mermin-GHZ

Dans cette section, nous continuerons de démontrer la puissance des BNL en montrant qu'elles peuvent aussi simuler des corrélations quantiques triparties.

Définition 4.5. *Lors du jeu de* Mermin-GHZ *à trois participants [48, 60], Alice, Bob et Charlie reçoivent chacun un bit tel que $x^{(A)} + x^{(B)} + x^{(C)} \equiv 0 \pmod 2$ et ils doivent produire chacun un bit tel que*

$$y^{(A)} \oplus y^{(B)} \oplus y^{(C)} = \frac{x^{(A)} + x^{(B)} + x^{(C)}}{2}. \tag{4.7}$$

Il est bien connu que ce jeu est un jeu de pseudo-télépathie. Pour la stratégie quantique gagnante, Alice, Bob et Charlie partagent un état GHZ $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle$.

Lemme 4.7. *Aucune stratégie quantique où les participants ne partagent qu'un état intriqué de deux qubits $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$ ne peut être une stratégie gagnante.*

Démonstration. Tel que dans la preuve du Lemme 4.1, la démonstration du théorème est une conséquence directe du Théorème 3.20. □

Théorème 4.8. *Il existe une stratégie classique gagnante si les participants peuvent envoyer un bit de communication entre seulement deux des trois participants.*

Démonstration. La stratégie est la suivante : Bob et Charlie produisent $y^{(B)} = b$ et $y^{(C)} = c$ respectivement, où b et c sont des bits arbitraires connus de tous les participants. Bob envoie $x^{(B)}$ à Alice, qui calcule $y = x^{(A)} \vee x^{(B)}$ et produit $y^{(A)} = b \oplus c \oplus y$. Il est facile de vérifier que cette stratégie fonctionne. □

Théorème 4.9. *Des participants classiques qui peuvent communiquer un bit entre deux participants peuvent simuler le jeu de Mermin-GHZ.*

Démonstration. Alice, Bob et Charlie peuvent choisir uniformément parmi toutes les stratégies énoncées dans la preuve du Théorème 4.8, ce qui est une simulation des corrélations du jeu de Mermin-GHZ. □

Théorème 4.10. *Il existe une stratégie classique gagnante si les participants peuvent utiliser une seule BNL entre seulement deux des trois participants.*

Démonstration. Encore une fois, nous utiliserons la BNL pour remplacer la communication dans le protocole de la preuve du Théorème 4.8. Tout d'abord, prenons note de la relation entre le OU et le ET :

$$\overline{x^{(A)} \vee x^{(B)}} = \bar{x}^{(A)} \wedge \bar{x}^{(B)}. \tag{4.8}$$

La stratégie est simple. Alice et Bob inversent leurs bits de question et les entrent dans la BNL, qui retourne $y^{(A)}$ et $y^{(B)}$ tel que

$$y^{(A)} \oplus y^{(B)} = \overline{x^{(A)} \vee x^{(B)}}. \tag{4.9}$$

Puisque $x^{(A)} + x^{(B)} + x^{(C)} \equiv 0 \pmod 2$,

$$\overline{x^{(A)} \vee x^{(B)}} = \left(\frac{x^{(A)} + x^{(B)} + x^{(C)}}{2} \right) \oplus 1. \tag{4.10}$$

Si Charlie répond $y^{(C)} = 1$, le protocole satisfait la Définition 4.5. □

Théorème 4.11. *Des participants classiques qui peuvent utiliser une seule BNL entre deux participants peuvent simuler les corrélations de la stratégie quantique pour le jeu de Mermin-GHZ.*

Démonstration. Comme lors de la preuve du Théorème 4.9, nous pouvons choisir selon une distribution parmi tous les protocoles donnés lors de la preuve du Théorème 4.10. Nous avons seulement besoin d'un bit aléatoire partagé de plus disant à Bob et à Charlie s'ils doivent simultanément inverser leurs bits de réponse. Nous avons donc un nouveau protocole qui satisfait la Définition 4.5 et qui simule les corrélations de la stratégie quantique. □

Du Lemme 4.7 et du Théorème 4.10, nous obtenons le corollaire suivant :

Corollaire 4.12. *Une seule BNL peut simuler des corrélations quantiques tripartites qu'aucune paire de qubits intriqués* $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$ *ne peut simuler.*

4.2.3 Jeu de Mermin-GHZ multiparti

Est-ce que toutes les corrélations quantiques se réduisent à une simple utilisation d'une BNL ? La réponse est non. Nicolas Brunner, Nicolas Gisin et Valerio Scarani [27] ont démontré qu'une BNL n'est pas suffisante pour simuler toutes les corrélations obtenues par des mesures de von Neumann arbitraires sur une paire de qubits non-maximalement intriqués. Nous montrerons ici qu'il existe des jeux de pseudo-télépathie dont les corrélations ne peuvent être simulées par une seule BNL. Premièrement, nous démontrerons ceci dans un contexte multiparti. Nous utiliserons par la suite le jeu de Deutsch-Jozsa distribué afin de démontrer, à la Section 4.2.4, qu'il en est de même dans un contexte biparti. Une conséquence importante de ce travail sera expliqué à la Section 5.10. Tout d'abord, nous donnons la définition du jeu de Mermin-GHZ de [18].

Définition 4.6. *Le jeu de* Mermin-GHZ multiparti *est défini comme suit. Chaque participant* $i \in \{1, \ldots, n\}$ $(n \geq 3)$ *reçoit un bit* $x^{(i)}$ *tel que* $\sum_i x^{(i)} \equiv 0 \pmod 2$. *Chaque participant doit répondre un bit* $y^{(i)}$ *tel que :*

$$\sum_i y^{(i)} \equiv \left(\frac{\sum_i x^{(i)}}{2} \right) \pmod 2. \tag{4.11}$$

Théorème 4.13. $\binom{n}{2} \in O(n^2)$ *BNL sont suffisantes pour simuler le jeu de Mermin-GHZ multiparti.*

Démonstration. Chaque participant partage une BNL avec chaque autre participant, pour un total de $\binom{n}{2}$ BNL. Lorsqu'il reçoit sa question $x^{(i)}$, le participant i introduit $x^{(i)}$ dans chaque BNL qu'il partage. Prenons $y^{(i,j)}$ comme étant la sortie de la BNL que le participant i partage avec le participant j. Le participant i cal-

cule alors la parité de tous les bits $y^{(i,j)}$: $y^{(i)} = \sum_{j \neq i} y^{(i,j)} \pmod 2$ qui servira de réponse au participant i.

Afin de montrer que cette stratégie fonctionne, prenons note que

$$\sum_i y^{(i)} \equiv \sum_i \sum_{j \neq i} y^{(i,j)} \pmod 2, \tag{4.12}$$

et que $\forall i, j$ où $i \neq j$

$$y^{(i,j)} + y^{(j,i)} \pmod 2 \equiv \begin{cases} 0, & x^{(i)} \wedge x^{(j)} = 0 \\ 1, & x^{(i)} \wedge x^{(j)} = 1. \end{cases} \tag{4.13}$$

Donc, si $\sum_i x^{(i)} = 4k$ pour un nombre entier k, (et donc $\left(\frac{\sum_i x^{(i)}}{2}\right) \equiv 0 \pmod 2$), alors $\sum_i y^{(i)} \equiv \binom{4k}{2} \equiv 0 \pmod 2$. Si $\sum_i x^{(i)} = 4k + 2$ pour un nombre entier k, (et donc $\left(\frac{\sum_i x^{(i)}}{2}\right) \equiv 1 \pmod 2$), alors $\sum_i y^{(i)} \equiv \binom{4k+2}{2} \equiv 1 \pmod 2$. □

Théorème 4.14. *Tout protocole non-local qui est une stratégie gagnante pour le jeu de Mermin-GHZ multiparti pour $n \geq 4$ participants requiert plus d'une BNL.*

Démonstration. Considérons le cas où $n = 4$. Supposons pour une contradiction qu'une seule BNL suffit à implanter une stratégie gagnante. Sans perte de généralité, disons que les participants 1 et 2 partagent la BNL. Disons même qu'ils peuvent communiquer sans limites entre eux, rendant ainsi la BNL inutile. Nous montrerons que, même sous ce modèle plus fort, il est impossible d'avoir une stratégie gagnante pour le jeu de Mermin-GHZ multiparti. Il s'en suit donc qu'une stratégie gagnante pour le jeu de Mermin-GHZ multiparti requiert plus d'une BNL.

Prenons un sous-ensemble de toutes les questions possibles $X^{(1)} \times X^{(2)} \times X^{(3)} \times X^{(4)}$: $\{(0,0,0,0), (0,0,1,1), (0,1,0,1), (0,1,1,0)\}$. Si nous considérons les participants 1 et 2 comme une seule entité, nous avons, après avoir renommé les questions, l'ensemble : $\{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$. Cet ensemble est exactement l'ensemble de questions du jeu de Mermin-GHZ (Définition 4.5). Puisqu'une stratégie gagnante pour le jeu de Mermin-GHZ multiparti qui permet aux seuls deux pre-

miers participants de communiquer peut être facilement transformée en stratégie *classique* gagnante pour le jeu de Mermin-GHZ, ce qui est impossible, la contradiction prouve notre énoncé.

Ce résultat s'étend facilement au cas où $n > 4$. Même si nous permettons une communication sans limites entre les $n-2$ premiers participants, nous pouvons trouver un sous-ensemble de questions où les participants doivent avoir une stratégie classique gagnante pour le jeu de Mermin-GHZ afin d'avoir une stratégie non-locale gagnante pour le jeu de Mermin-GHZ multiparti. □

Théorème 4.15. $\Omega(n)$ *BNL sont nécessaires pour avoir une stratégie non-locale gagnante pour le jeu de Mermin-GHZ multiparti.*

Démonstration. Tel que nous l'avons vu lors de la preuve du Théorème 4.14, il ne peut y avoir deux participants, ou plus, qui ne sont pas reliés aux autres participants par au moins une BNL. Afin qu'au moins $n-1$ participants soient reliés, $\lfloor n/2 \rfloor \in \Omega(n)$ BNL sont nécessaires. □

Il est intéressant de noter qu'une séparation existe pour l'instant entre la borne inférieure que nous avons prouvée $\Omega(n)$ et la borne supérieurs que nous avons trouvée $O(n^2)$.

4.2.4 Jeu de Deutsch-Jozsa distribué

Nous allons maintenant nous intéresser au scénario biparti et montrer qu'il existe des corrélations quantiques biparties qui requièrent plus d'une BNL afin de les simuler.

Définition 4.7. *Lors du jeu de pseudo-télépathie* Deutsch-Jozsa distribué *[20], Alice et Bob reçoivent comme question des chaînes de* 2^n *bits* $x^{(A)}$ *et* $x^{(B)}$ *respectivement, tel que*

$$\Delta(x^{(A)}, x^{(B)}) \in \{0, 2^{n-1}\} \tag{4.14}$$

où $\Delta(x^{(A)}, x^{(B)})$ *est dénomée la* distance de Hamming *entre les deux chaînes. L'Équation 4.14 implique que les deux chaînes sont soit égales soit différentes*

en exactement la moitié des positions. Les participants doivent alors produire des chaînes de n bits $y^{(A)}$ et $y^{(B)}$ respectivement tel que :

$$[y^{(A)} = y^{(B)}] \Leftrightarrow [x^{(A)} = x^{(B)}]. \tag{4.15}$$

Nous savons que, pour tout $n \geq 4$, ce jeu est un jeu de pseudo-télépathie [69], et qu'il existe une stratégie quantique gagnante dans laquelle l'état intriqué est en fait n états de Bell $\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle|j\rangle$ [20]. De plus, nous avons le lemme suivant [20] :

Lemme 4.16. *Toute stratégie classique gagnante pour le jeu de Deutsch-Jozsa distribué requiert $\Omega(2^n)$ bits de communication.*

Théorème 4.17. *Aucun protocole non-local qui utilise moins de $\Omega(2^n)$ BNL n'est une stratégie gagnante.*

Démonstration. Puisque nous savons comment simuler une BNL avec un bit de communication [82], il ne peut exister une stratégie gagnante avec moins de $\Omega(2^n)$ BNL. Une telle stratégie contredirait le Lemme 4.16. □

Théorème 4.18. *Il existe une stratégie non-locale gagnante pour le jeu de Deutsch-Jozsa distribué qui utilise $O(2^n)$ BNL.*

Démonstration. Nous utilisons ici des concepts et construction introduits à la Section 1.3.3. Premièrement, Alice inverse ses bits. Appelons cette chaîne $\bar{x}^{(A)}$. En utilisant cette nouvelle question, Alice et Bob exécutent une série de rondes. Chaque ronde i a la propriété suivante. Au début de la ronde, Alice détient la chaîne $a^{(i)} \in \{0,1\}^{2^{n-i}}$ et Bob $b^{(i)} \in \{0,1\}^{2^{n-i}}$ telle que soit la condition *diamétrique* ($\Delta(a^{(i)}, b^{(i)}) = 2^{n-i}$), soit la condition de *disparité* ($\Delta(a^{(i)}, b^{(i)}) < 2^{n-i}$) est valide. À la fin de la ronde, Alice détient la chaîne $a^{(i+1)} \in \{0,1\}^{2^{n-i-1}}$ et Bob $b^{(i+1)} \in \{0,1\}^{2^{n-i-1}}$ et la condition, diamétrique ou disparité, est inchangée.

Afin d'exécuter la ronde i, les participants font une séquence de 2^{n-i-1} calculs distribués de la fonction $f(a_1, a_2, b_1, b_2) = (a_1 \oplus b_1) \wedge (a_2 \oplus b_2)$: pour chaque entier $j \in \{0, \ldots 2^{n-i-1}\}$, prenons $a_j^{(i+1)}$ et $b_j^{(i+1)}$ comme le résultat du calcul distribué de

$f(a_{2j}^{(i)}, a_{2j+1}^{(i)}, b_{2j}^{(i)}, b_{2j+1}^{(i)})$. Alice et Bob finissent la ronde i avec les chaînes $a^{(i+1)}$ et $b^{(i+1)}$ respectivement. Il est facile de voir que la fonction f maintient les conditions diamétriques et de disparité au travers la ronde.

Alice et Bob commencent la ronde 0 avec une chaîne de 2^n bits chacun, $a^{(0)} = \bar{x}^{(A)}$ et $b^{(0)} = x^{(B)}$. Ils répètent plusieurs rondes jusqu'à ce qu'ils aient des chaînes de n bits. Ils peuvent ajouter des bits diamétriques à la fin de la dernière ronde pour avoir le bon nombre de bits sans changer la condition diamétrique ou de disparité. Il y a donc $n - \lfloor \lg n \rfloor$ rondes, pour un total de $2(\sum_{i=0}^{n-\lfloor \lg n \rfloor - 1} 2^{n-i-1}) = 2^{n+1} - 2^{\lfloor \lg n \rfloor + 1} \in O(2^n)$ BNL. À la fin de la séquence de rondes, Alice inverse à nouveau ses bits. Alice et Bob finissent donc avec les chaînes $y^{(A)}$ et $y^{(B)}$ respectivement, tel que $[y^{(A)} = y^{(B)}] \Leftrightarrow [x^{(A)} = x^{(B)}]$. □

4.3 Modèles avec erreurs

Une autre façon de permettre aux VLC de jouer sur le même terrain que la MQ est de rendre la MQ un peu plus réaliste, c'est-à-dire de tenir compte des erreurs et des imperfections. Le but premier de ce genre de modèle est de voir si, dans une situation d'expérimentation réelle, nous pouvons toujours conclure que la nature n'est pas locale réaliste.

4.3.1 Bruit blanc

Le premier modèle que nous examinons fut proposé par Reinhard F. Werner en 1989 [81]. Le modèle tente de répondre à la question suivante : qu'arrive-t-il si l'état créé est imparfait ? Nous demandons donc à nos théories à VLC d'être capables de simuler parfaitement des mesures sur un état de Werner

$$W = p|\psi^-\rangle\langle\psi^-| + (1-p)\frac{\mathbb{1}}{4}. \tag{4.16}$$

Nous savons que, pour $p \leq 1/3$, et seulement pour ces valeurs, l'état est séparable. Nous pouvons donc le simuler à l'aide de VLC. À partir des travaux de Clauser, Horne, Shimony et Holt [35], nous pouvons dériver que, lorsque $p \geq 1/\sqrt{2}$, l'état

ne peut plus être simulé par une théorie à VLC. L'intérêt de ce modèle est que Werner a démontré que, pour $p \leq 1/2$, nous pouvons simuler l'état. Il existe donc des états non-séparables qui peuvent être simulée par des VLC! Il s'agit de la première preuve que l'intrication n'implique pas nécessairement la non-localité. Ce résultat fut généralisé par Jonathan Barrett [7]. Nous savons maintenant que nous pouvons même simuler des POVM pour $p \leq 5/12$.

4.3.2 Bruit noir

L'autre modèle d'intérêt est celui où les détecteurs ne sont pas parfaits. Supposons que chaque détecteur a une probabilité indépendante η de répondre. Nous noterons alors l'événement où le détecteur ne répond pas, probabilité $1-\eta$, par $\perp$. L'idée est maintenant de savoir quelle est la plus grande valeur $\eta^\star$ pour laquelle il nous est toujours possible d'avoir une théorie à VLC qui reproduit parfaitement les probabilités de la MQ. Serge Massar et Stefano Pironio [58] ont montré que

$$\eta^\star \geq \frac{X^{(A)} + X^{(B)} - 2}{X^{(A)} X^{(B)} - 1}, \tag{4.17}$$

où $X^{(A)}$ et $X^{(B)}$ sont le nombre de mesures disponibles à Alice et Bob respectivement. Ils ont aussi montré que, lorsque N participants peuvent choisir parmi M mesures, alors

$$\eta^\star \geq \frac{1}{M^{(N-1)/N}}. \tag{4.18}$$

CHAPITRE 5

LIENS ENTRE LES DIFFÉRENTS MODÈLES

5.1 Théorèmes de Bell, théorèmes de Bell sans inégalités et pseudo-télépathie

Le lien évident entre les théorèmes de Bell, les théorèmes de Bell sans inégalités et la pseudo-télépathie est qu'ils rejettent tous la possibilité d'une description du monde physique par une théorie à VLC. De là découle l'impossibilité d'adopter le point de vue local réaliste. Il est par contre bien important de ne pas ajouter de contraintes non-nécessaires et de respecter les structures établies au Chapitre 3 afin d'avoir une réfutation valide du point de vue local réaliste [25, 26]. Tel que mentionné au Chapitre 3, les trois formes de théorème requièrent plusieurs répétitions de l'expérience avec des paramètres aléatoires à chaque répétition ainsi qu'une analyse statistique afin de conclure que l'univers n'est probablement pas local réaliste. Un modèle à VLC pourrait être chanceux et répondre correctement pour plusieurs répétitions. Étant donné qu'un modèle à VLC ne peut réussir à la longue qu'avec une incroyablement faible probabilité, mais qu'il peut tout de même réussir, nous ne pouvons que collectionner des indices considérablement forts contre les théories à VLC. En une seule expérimentation des théorèmes d'impossibilité, nous ne pourrions que rejeter la MQ. En effet, si nous considérons les appareils comme étant parfaits et que nous obtenons un résultat incompatible avec les prédictions d'un théorème de Bell sans inégalités ou d'un jeu de pseudo-télépathie, c'est alors que cette dernière est fausse.

Il est intéressant de noter que, selon les définitions du Chapitre 3, tous les jeux de pseudo-télépathie sont des théorèmes de Bell sans inégalités et que tous les théorèmes de Bell sans inégalités sont des théorèmes de Bell. En pseudo-télépathie, le fait qu'aucune stratégie à VLC ne peut produire un résultat appartenant à tout coup à la relation (Définition 3.5) peut être interprété comme le fait d'attribuer

une probabilité non-nulle à un résultat interdit par la MQ (Définition 3.4). De plus, il est évident, par définition, que la pseudo-télépathie et les théorèmes de Bell sans inégalités sont des preuves que la MQ ne peut être représentée par une théorie à VLC, ce qui fait d'eux des théorèmes de Bell.

Les théorèmes de Bell connus (sauf les théorèmes de Bell sans inégalités) et la pseudo-télépathie ne sont que quantitativement différents. Un jeu de pseudo-télépathie est en fait une inégalité de Bell ou la violation quantique de l'inégalité atteint la valeur algébrique maximale. Autrement dit, l'expression mathématique de l'inégalité peut facilement être interprétée comme la condition de la relation du jeu de pseudo-télépathie et le fait que la relation soit toujours respectée en pseudo-télépathie implique une violation maximale des inégalités.

La généralisation à plusieurs participants de la Définition 3.5 peut être réécrite comme un ensemble de mesures sur un état intriqué où tout modèle à VLC voulant produire des résultats qui ne sont pas incompatibles avec les prédictions de la MQ échouera. Il peut dont être tentant de penser que les théorèmes de Bell sans inégalités sont des jeux de pseudo-télépathie déguisés. En fait, la liste de personnes qui ont fait l'erreur de penser ainsi serait probablement trop longue pour être incluse. La raison est que, dans ces deux paradigmes, nous voulons prouver l'impossibilité d'une description de la nature par une théorie à VLC à l'aide d'une contradiction. Toutefois, nous avons démontré récemment qu'il ne peut exister un jeu de pseudo-télépathie dans lequel les participants ne partagent qu'un système de dimension 2×2 [23]. Afin que des corrélations suffisamment fortes soient produites, un système de dimensions d'au moins 3×3 [50] ou $2 \times 2 \times 2$ est requis [60]. Il est donc impossible que l'état utilisé par Hardy pour son théorème d'impossibilité puisse être utilisé pour confectionner un jeu de pseudo-télépathie. Les théorèmes de Bell sans inégalités et la pseudo-télépathie sont donc différents. Cette différence est subtilement cachée dans les Définitions 3.4 et 3.5. Dans le premier cas, nous demandons au modèle à VLC d'être capable de produire tous les résultats possibles selon la MQ, et seulement ceux-ci, alors que dans le deuxième cas, le critère est plus faible : nous ne demandons au modèle à VLC que de produire des résultats

admis par la MQ. En d'autres mots, il nous suffit de systématiquement produire des résultats permis par la MQ pour avoir une stratégie gagnante en pseudo-télépathie, mais nous n'avons pas besoin de produire *tous* les résultats possibles. La preuve de Hardy repose justement sur le fait que le modèle doit être capable de produire $1 \otimes 1$ lorsque les deux participants mesurent dans la base de Hadarmard.

5.2 Théorèmes de Bell-Kochen-Specker et théorèmes d'impossibilité

Il existe une technique, utilisée par Peter Heywood et Michael L. G. Redhead [50], Padmanabhan K. Aravind [4] et Richard Cleve, Peter Høyer, Benjamin F. Toner et John Watrous [38], pour transformer un argument de BKS traditionnel, où toutes les mesures sont des mesures de von Neumann sur un système de dimension d, en un jeu de pseudo-télépathie de dimension $d \times d$ qui ne demande pas à Alice et Bob de faire des POVM. On pourrait être tenté de croire que ceci provient du fait que la formulation originale des théorèmes de BKS a été construite à l'aide de mesures projectives [9,53]. Par contre, il a été proposé d'étendre les théorèmes de BKS pour inclure les POVM [31,63,77,80]. En particulier, il est alors possible de confectionner des théorèmes de BKS sur un qubit, ce qui est évidement impossible avec la formulation originale. Est-il possible que la technique d'Heywood et Redhead, de Aravind et de Cleve, Høyer, Toner et Watrous s'étende aussi aux théorèmes de BKS basés sur les POVM afin d'en faire des jeux de pseudo-télépathie ? Malheureusement, nous avons démontré qu'il est impossible d'avoir un jeu de pseudo-télépathie 2×2, alors qu'un théorème de BKS avec POVM de dimension 2 existe.

Il est intéressant de noter que la technique inverse existe aussi. En effet, Renato Renner et Stefan Wolf [75] ont trouvé une technique permettant de transformer n'importe quel jeu de pseudo-télépathie, dont la stratégie quantique gagnante utilise un état maximalement intriqué $d \times d$ et des mesures de von Neumann, pour en faire une théorème de BKS sur un système de dimension d. Cette technique est aussi dépourvue de POVM et, encore une fois, [23] implique qu'elle ne pourra pas être adaptée à ceux-ci.

Le fait qu'un théorème de BKS avec des mesures de von Neumann implique l'existence d'un théorème de Bell ayant une structure similaire ne veut pas dire que ce théorème de Bell soit une proposition de vérification expérimentale du théorème de BKS. En effet, le théorème de BKS ne peut pas être vérifié expérimentalement. L'énoncé du théorème implique simplement que, si nous voulons avoir une description à VLC de la nature, alors cette dernière doit être contextuelle. Elle ne rejette pas à proprement dit l'existence de VLC. Une vérification expérimentale de violation de l'inégalité de Bell qui découle du théorème de BKS invaliderait ou pas l'existence des VLC, mais ne changerait rien à la véracité du théorème de BKS. Examinons la situation d'un monde imaginaire suivante : l'intrication ne peut survivre une séparation des deux sous-systèmes à l'extérieur des cônes de lumière respectifs. L'état intriqué se dégraderait en état séparable. Il pourrait maintenant exister une théorie à VLC (du moins aucun théorème de la physique ne l'empêcherait), mais cette théorie devrait être contextuelle.

5.3 Bruit blanc et bruit noir

Il est intéressant de noter qu'il existe un lien entre les modèles de simulation de l'intrication avec bruit blanc et avec bruit noir. En effet, une simulation d'un état maximalement intriqué *biparti* $|\psi\rangle$ où les détecteurs fonctionnent avec probabilité p peut être aisément transformée en protocole qui simule l'état $p^2|\psi\rangle\langle\psi|+(1-p^2)\mathbb{1}/D$, où D est la dimension totale de l'état. Il suffit de changer les stratégies des participants en changeant « répondre $\perp$ » par « répondre n'importe quoi » avec les bonnes distributions marginales. Il est important de noter que cette stratégie ne peut fonctionner que si la trace partielle de l'état $|\psi\rangle$ est l'état complètement mélangé. Par contre, l'inverse n'est pas vrai. En général, une stratégie pour simuler un état intriqué $|\psi\rangle$ dans le modèle avec bruit blanc demande aux participants de toujours répondre quelque chose. Les participants ne savent donc pas nécessairement quand il aurait été mieux de s'abstenir. D'un autre côté, la construction mentionnée cihaut peut aussi servir à faire des implications à partir du modèle avec bruit blanc

sur le modèle avec bruit noir. En effet, s'il nous est impossible de simuler un état biparti $|\psi\rangle$ avec une probabilité au-dessus de q dans le modèle avec bruit blanc, alors il est impossible de simuler le même état dans le modèle avec bruit noir où les détecteurs fonctionnent avec une probabilité au-dessus de $\sqrt{q}$.

5.4 Bruit blanc, bruit noir et pseudo-télépathie

Une mesure intéressante d'intrication de l'état $|\psi\rangle$ est la probabilité maximale ω de la meilleure stratégie classique pour gagner à un jeu de pseudo-télépathie minimisée sur tous les jeux de pseudo-télépathie dont la stratégie quantique gagnante utilise $|\psi\rangle$. Cette probabilité est en fait reliée au $\eta^\star$ du modèle avec bruit noir et p du modèle avec bruit blanc par

$$\begin{aligned} \omega &\geq (\eta^\star)^n \\ \omega &\geq p, \end{aligned} \tag{5.1}$$

où n est le nombre de participants. En effet, des simulations qui violeraient les bornes de l'Équation 5.1 pourraient être utilisées afin de construire des stratégies classiques qui gagneraient avec probabilité plus grande que ω, ce que nous présumons impossible.

5.5 Simulation par la communication et modèles avec bruit

Il existe aussi un lien entre le nombre de bits de communication que deux participants, Alice et Bob, doivent s'échanger afin de simuler les corrélations de mesures biparties et l'efficacité minimum des détecteurs requise afin d'éviter une description des corrélations par une théorie à VLC (bruit noir). En effet, Massar [56] a trouvé une technique qui permet à Alice et Bob de transformer un protocole où chacun répond avec probabilité η en un protocole où ils s'échangent $2/\eta^2$ bits de communication espérée. Nous avons donc, pour un état biparti $|\psi\rangle$,

$$\eta^\star(|\psi\rangle) \leq \sqrt{\frac{2}{C^\star_{\text{espérée}}(|\psi_{AB}\rangle)}}. \tag{5.2}$$

Dans un tout autre ordre d'idée, Alice et Bob peuvent tenter de deviner la communication qu'ils devraient s'échanger, dans une simulation par communication à sens unique bornée en pire cas, afin de simuler $p|\psi\rangle\langle\psi| + (1-p)\mathbb{1}/(D)$. Alice et Bob tirent préalablement au hasard une chaîne de bits qui pourrait être produite lors de la simulation avec la communication. S'ils ont bien deviné, ils répondent selon le protocole avec communication, sinon Alice répond n'importe quoi, ce qui entraîne

$$\frac{1}{2^{C^*(|\psi\rangle)}} \leq p. \tag{5.3}$$

Il est intéressant de noter que cette construction ne peut pas fonctionner dans le modèle avec bruit noir, car la probabilité de se tromper est trop grande et, par conséquent, on ne peut pas construire un protocole.

5.6 Théorèmes de Bell et simulation par la communication

Afin de pouvoir discuter sur les théorèmes de Bell, nous devons formaliser ceux-ci de façon uniforme. Pour cela, nous aurons besoin de quelques définitions. Tout d'abord, prenons un état $|\psi\rangle_{AB}$ et définissons $p_{y^{(A)}y^{(B)}|x^{(A)}x^{(B)}}$ comme étant la probabilité pour Alice et Bob d'obtenir les résultats $y^{(A)}$ et $y^{(B)}$ respectivement, étant donné les mesures $x^{(A)} \in X^{(A)}$ et $x^{(B)} \in X^{(B)}$ pour des ensembles $X^{(A)}$ et $X^{(B)}$ finis. Prenons $\vec{p}$ comme étant le vecteur ayant comme valeurs $p_i = p_{y^{(A)}y^{(B)}|x^{(A)}x^{(B)}}$ pour un ordre quelconque sur les $x^{(A)}$, $x^{(B)}$, $y^{(A)}$ et $y^{(B)}$. Il s'agit donc du vecteur représentant les différentes probabilités étant donné les paramètres de mesure choisis. Définissons maintenant les quantités $B(\vec{p}) = \vec{b}\cdot\vec{p}$, pour un vecteur $\vec{b}$ quelconque et $B_i = \vec{b}\cdot\vec{p}_{\text{classique}}$, où $\vec{p}_{\text{classique}}$ est le vecteur des probabilités du modèle à VLC, où il est permis de communiquer i bits entre Alice et Bob, qui maximise l'expression $\vec{b}\cdot\vec{p}$. Pironio [72] a alors démontré que

$$C^*_{\text{espérée}}(|\psi_{AB}\rangle) \geq \frac{B(\vec{p}) - B_0}{B_{i^*} - B_0} i^*, \tag{5.4}$$

où i^* est la quantité de communication qui permet de violer maximalement la borne classique par bit de communication, $\max_{i\neq 0}(B_i - B_0)/i$. L'intuition derrière l'Équation 5.4 est que la communication espérée est bornée par la valeur de la violation de la limite des théories à VLC divisée par la valeur de la violation maximale par bit de communication. Dans le cas des inégalités de CHSH, nous déduisons donc que la communication espérée nécessaire afin de simuler les corrélations de CHSH est $\sqrt{2}-1 \approx 0,41$ bits de communication. Cette borne s'applique directement à la simulation de n'importe quelle mesure sur un état de Bell $C^*_{\text{espérée}}(|\Psi^-\rangle) \geq \sqrt{2}-1 \approx 0,41$. Nous avons donc

$$\cos^2(\pi/8) \geq C^*(|\Psi^-\rangle) \geq C^*_{\text{espérée}}(|\Psi^-\rangle) \geq \sqrt{2}-1. \tag{5.5}$$

5.7 Simulation par la communication et complexité de la communication quantique

Étant donné que l'intrication peut servir à réduire la complexité d'une tâche distribuée, l'étude de la simulation de l'intrication est centrale au domaine de la complexité de la communication quantique. En fait, une borne supérieure sur la simulation par la communication d'un état intriqué (ou n copies de ce dernier) nous donne une borne supérieure sur le gain potentiel en complexité de la communication entre le modèle quantique, lorsque les participants partagent cet état (ou n copies), et le modèle classique.

5.8 Complexité de la communication quantique et non-localité

Nous sommes intéressés à savoir jusqu'à quel point nous pouvons simuler de façon approximative la BNL en respectant les lois de la physique.

Même si le travail original [35] a été écrit dans une terminologie différente, il est fort simple de reformuler l'inégalité de CHSH dans le langage des BNL imparfaites. La disponibilité d'intrication entre Alice et Bob leur permet de simuler la BNL

avec probabilité

$$\wp = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.854\,. \tag{5.6}$$

Ceci peut être utilisé afin de tester les théories à VLC, car CHSH ont démontré que ces dernières ne pouvaient réussir avec une probabilité meilleure que 3/4 si Alice et Bob ne peuvent communiquer. Ultérieurement, Boris Tsirelson a démontré que l'inégalité de CHSH était optimale, ce qui implique que la meilleure simulation d'une BNL par la MQ a une probabilité de succès de $\wp$ [34] (voir aussi [30] pour une preuve plus simple).

Deux questions d'intérêt se posent dans cette section. (1) *Étant donné que les BNL parfaites ne violent pas la causalité, pourquoi les lois de la physique nous permettent-elles de les simuler mieux que n'importe quel modèle à VLC, mais pas parfaitement ?* (2) *Pourquoi nous permettent-elles de les simuler avec probabilité $\wp$ et pas plus ?*

Comme nous l'avons vu à la Section 1.3.3, van Dam [39] a prouvé que la disponibilité de BNL parfaites rend la complexité de la communication de toutes fonctions booléennes triviale ! Ceci répond à la première question : si nous prenons comme axiome que la complexité de la communication ne devrait pas être triviale, il doit être impossible pour la MQ de pouvoir simuler les BNL parfaitement. En effet, un monde où la complexité de la communication est triviale serait étonnant pour tous ceux qui étudient ce domaine, car nous savons que presque toutes les fonctions ont une complexité de $\Theta(n)$. La plupart des informaticiens considéreraient un tel monde aussi surprenant qu'un physicien moderne considérerait la violation de la causalité.

Notre théorème [19] répond partiellement à la deuxième question.

Théorème 5.1. *Dans tout monde où il est possible de simuler les BNL avec une probabilité plus grande que $\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 90.9\%$,* toutes *les fonctions booléennes ont une complexité de la communication triviale selon la Définition 1.9.*

Nous allons démontrer comment augmenter le biais naturel de n'importe quelle fonction booléenne en la calculant plusieurs fois et en prenant la majorité. Nous

déterminons ensuite jusqu'à quel point la porte de majorité distribuée peut être imparfaite et encore augmenter le biais. Finalement, nous construirons la porte de majorité distribuée à partir de BNL et nous déterminerons jusqu'à quel point ces dernières peuvent être imparfaites.

Définition 5.1. *Le problème de la* majorité distribuée *consiste à calculer localement la majorité de trois bits distribués. Plus précisément, disons qu'Alice a les bits x_1, x_2, x_3 et Bob a les bit y_1, y_2, y_3. Le but est de calculer a et b respectivement tel que*

$$a \oplus b = MAJ(x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3)\,, \tag{5.7}$$

où $MAJ(u, v, w) = \lfloor (u + v + w)/2 \rfloor$.

Théorème 5.2. *Pour tout q tel que $5/6 < q \leq 1$, si Alice et Bob peuvent calculer localement la majorité distribuée avec probabilité au moins q, alors toutes les fonctions booléennes ont un biais borné selon la Définition 1.13.*

Démonstration. Prenons une fonction booléenne arbitraire f et disons qu'Alice et Bob peuvent calculer distributivement, pour une longueur d'entrée donnée, la fonction f avec une probabilité au moins $p > 1/2$. Grâce au Lemme 1.8, nous savons que p existe (même s'il peut dépendre de la taille des entrées). Alice et Bob calculent distributivement la fonction trois fois, avec des choix aléatoires indépendants d'une fois à l'autre. Ceci produit trois bits distribués, chacun étant correct avec probabilité au moins p. Alice et Bob calculent maintenant la majorité distribuée de ces trois bits avec une probabilité q de calculer correctement la majorité. Puisque le résultat final sera correct si la porte de majorité distribuée a fonctionné correctement et qu'au moins deux des trois résultats sont exacts, ou si la porte n'a pas fonctionné correctement et qu'au plus un des trois résultats est exact, la probabilité que la porte de majorité distribuée ait obtenu le bon résultat final est

$$h(p) = q(p^3 + 3p^2(1-p)) + (1-q)(3p(1-p)^2 + (1-p)^3)\,. \tag{5.8}$$

Définissons

$$\delta = q - 5/6 > 0 \quad \text{et} \quad s = \frac{1}{2} + \frac{3\sqrt{\delta}}{2\sqrt{1+3\delta}} > \frac{1}{2}. \tag{5.9}$$

Il peut être montré que $p < h(p) < s$ si $1/2 < p < s$. Ceci, une fois jumelé au fait que $h(p)$ est continu sur tout l'intervalle $1/2 < p < s$, implique qu'une répétition de ce processus peut augmenter la probabilité de calculer localement la bonne réponse arbitrairement proche de s. Ce qui prouve que f a un biais borné puisque, pour une valeur de $q > 5/6$, nous pouvons choisir une constante $t < s$ tel que $t > 1/2$ et calculer distributivement f avec une probabilité au moins t d'être exact, et ce indépendamment de la taille des entrées. □

Définition 5.2. *Le problème de* l'égalité distribuée *consiste à déterminer localement si trois bits sont égaux. Plus précisément, disons qu'Alice détient les bits* x_1, x_2, x_3 *et Bob, les bits* y_1, y_2, y_3. *Le but est de calculer* a *et* b *respectivement tel que*

$$a \oplus b = \begin{cases} 1 \text{ } si \text{ } x_1 \oplus y_1 = x_2 \oplus y_2 = x_3 \oplus y_3 \\ 0 \text{ } autrement. \end{cases} \tag{5.10}$$

Lemme 5.3. *L'égalité distribuée peut être calculée avec deux BNL parfaites.*

Démonstration. Le but est d'obtenir a et b tels que :

$$a \oplus b \;=\; (x_1 \oplus y_1 = x_2 \oplus y_2) \wedge (x_2 \oplus y_2 = x_3 \oplus y_3). \tag{5.11}$$

Alice et Bob calculent localement $x' = x_1 \oplus x_2 \oplus 1$, $y' = y_1 \oplus y_2$, $x'' = x_2 \oplus x_3 \oplus 1$ et $y'' = y_2 \oplus y_3$. Puis l'Équation 5.11 devient équivalente à $(x' \oplus y') \wedge (x'' \oplus y'') = a \oplus b$. Il est alors suffisant de montrer à Alice et Bob comment calculer le ET de deux bits distribués, $x' \oplus y'$ et $x'' \oplus y''$.

Notons que $(x' \oplus y') \wedge (x'' \oplus y'') = (x' \wedge x'') \oplus (x' \wedge y'') \oplus (x'' \wedge y') \oplus (y' \wedge y'')$. Tel que nous l'avons vu à la Section 1.3.3, en utilisant deux BNL, Alice et Bob peuvent obtenir des bits distribués $a' \oplus b'$ et $a'' \oplus b''$ avec $a' \oplus b' = x' \wedge y''$ et $a'' \oplus b'' = x'' \wedge y'$. Prenant $a = (x' \wedge x'') \oplus a' \oplus a''$ et $b = (y' \wedge y'') \oplus b' \oplus b''$, nous avons l'Équation 5.11. □

Lemme 5.4. *La majorité distribuée peut être calculée avec deux BNL.*

Démonstration. Prenons x_1, x_2, x_3 comme étant les bits d'entrée d'Alice et y_1, y_2, y_3 ceux de Bob. Pour $i \in \{1, 2, 3\}$, prenons $z_i = x_i \oplus y_i$ comme le $i^{\text{ième}}$ bit d'entrée distribué. En vertu du Lemme 5.3, Alice et Bob utilisent deux BNL pour calculer l'égalité distribuée des entrées, produisant a et b tel que $a \oplus b = 1$ si et seulement si z_1, z_2 et z_3 sont égaux. Finalement, Alice produit $a' = \overline{a} \oplus x_1 \oplus x_2 \oplus x_3$ et Bob $b' = b \oplus y_1 \oplus y_2 \oplus y_3$. Prenons

$$z = a' \oplus b' = (\overline{a} \oplus b) \oplus (z_1 \oplus z_2 \oplus z_3) \tag{5.12}$$

comme étant le bit distribué calculé par ce protocole. Quatre cas doivent être examinés, dépendant du nombre ℓ de 1 parmi les z_i :

1. si $\ell = 0$, alors $a \oplus b = 1$ et $z_1 \oplus z_2 \oplus z_3 = 0$;
2. si $\ell = 1$, alors $a \oplus b = 0$ et $z_1 \oplus z_2 \oplus z_3 = 1$;
3. si $\ell = 2$, alors $a \oplus b = 0$ et $z_1 \oplus z_2 \oplus z_3 = 0$;
4. si $\ell = 3$, alors $a \oplus b = 1$ et $z_1 \oplus z_2 \oplus z_3 = 1$.

Notons que $z = 0$ dans les deux premiers cas et $z = 1$ dans les deux derniers cas, donc $z = \text{MAJ}(z_1, z_2, z_3)$ dans tous les cas. □

Nous sommes maintenant prêts à prouver le théorème principal.

Preuve du Théorème 5.1. Disons que les BNL peuvent être simulées avec probabilité p. En les utilisant, nous pouvons calculer la majorité distribuée avec probabilité $q = p^2 + (1-p)^2$ d'être corrects puisque le protocole donné dans la preuve du Lemme 5.4 réussit précisément lorsqu'aucune des BNL, ou les deux, fonctionnent correctement. Le résultat découle donc du Théorème 5.2 et du Lemme 1.9, car $q > 5/6$ lorsque $p > \frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.909$. Un calcul plus précis, basé sur la preuve du Théorème 5.2, montre que le calcul biparti de n'importe quelle fonction booléenne peut être accompli en utilisant un seul bit de communication, avec la probabilité

d'être correct près de

$$\frac{1}{2} + \frac{\sqrt{3p^2 - 3p + 1/4}}{2p - 1} \tag{5.13}$$

si $p > \frac{1}{2} + \frac{1}{\sqrt{6}}$, le rendant trivial par définition. □

Corollaire 5.5. *Dans n'importe quel monde où la complexité de la communication n'est pas triviale, les BNL ne peuvent être simulées sans communication avec probabilité plus grande que* $\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 90.9\%$.

Notons que ni la majorité distribuée, ni l'égalité distribuée ne peut être calculée avec une seule BNL. Sinon, l'intrication nous permettrait de simuler la BNL assez bien pour résoudre la majorité distribuée avec probabilité $\wp \approx 0.854 > 5/6$. Il découlerait du Théorème 5.2 et du Lemme 1.9 que toutes les fonctions booléennes ont une complexité de la communication quantique probabiliste triviale. Or, nous savons que tel n'est pas le cas [37].

5.9 Non-localité et calcul tolérant aux erreurs

Le résultat de la Section 5.8 donne aussi une borne sur la probabilité d'erreurs tolérable pour les circuits tolérants aux erreurs. Dans la preuve du Lemme 5.3, nous avons montré comment simuler une porte ET distribuée. En utilisant les BNL qui fonctionnent avec probabilité $\wp$—ce qui est permis par la MQ—un tel ET distribué serait correct avec probabilité $(1-\wp)^2 + \wp^2 = 3/4$. De plus, la porte NON distribué peut être calculée distributivement de façon parfaite : il suffit à un participant (disons Alice) d'inverser son bit. Il est bien connu que le NON et le ET sont suffisants pour le calcul classique universel. Le produit interne de deux chaînes $IP(x,y) = \bigoplus_i (x_i \wedge y_i)$ peut donc être calculé avec cet ensemble de portes. De plus, la complexité de la communication quantique de IP est $E^\star_\epsilon(IP) = \Omega(n)$ [37]. Donc, même si nous permettons à Alice et Bob de communiquer un nombre de bits constant et que nous leur permettons d'utiliser un nombre arbitraire de BNL qui fonctionnent avec probabilité $\wp$, ils ne peuvent toujours pas calculer le produit interne.

Ceci implique qu'aucune famille de circuits, formés à partir de portes NON parfaites et de portes ET indépendamment imparfaites avec probabilité d'au plus 1/4, ne peut calculer le produit interne. Par contre, ce résultat est loin de la borne optimale connue de 0,089 [44].

5.10 Intrication et boîtes non-locales

Nous avons vu aux Sections 4.2.1 et 4.2.2 qu'une seule BNL peut simuler des corrélations quantiques qui ne peuvent être générées par un seul état de Bell. Est-ce qu'une BNL peut faire encore plus ? Dans cette section, nous discutons du résultat connu qu'une BNL peut générer des corrélations que la MQ ne peut atteindre quelle que soit la quantité d'intrication disponible. Nous démontrerons ceci en montrant un jeu pour lequel il existe une stratégie gagnante qui utilise une seule BNL, alors qu'aucune stratégie quantique ne peut être gagnante. Nous mettrons aussi ce résultat en contexte avec le Théorème 4.17.

Définition 5.3. *Un jeu de* BNL-pseudo-télépathie *est un jeu qui admet une stratégie non-locale gagnante alors qu'aucune stratégie quantique ne peut être gagnante.*

Lemme 5.6. *Il existe un jeu de BNL-pseudo-télépathie pour lequel la stratégie non-locale gagnante n'utilise qu'une seule BNL.*

Démonstration. Le jeu qui nous intéresse est en fait le jeu qui définit la BNL. Par définition, lorsqu'Alice et Bob utilisent une BNL, ils peuvent obtenir des réponses telles que le OUX de ces réponses est égal au ET des questions. Lorsque Sandu Popescu et Daniel Rohrlich [73] ont proposé la BNL, il était déjà connu, mais en d'autres termes, que la BNL pouvait servir à un jeu de BNL-pseudo-télépathie. En fait, Tsirelson a montré en 1980 que la MQ ne pouvait pas violer pleinement les inégalités de CHSH alors que la BNL est précisément construite à ce dessein [34]. □

Lorsque considérée comme une ressource bipartie, l'intrication est quantifiée par le nombre d'états de Bell utilisés. Le fait qu'il existe des corrélations quantiques qui requièrent un nombre exponentiel de BNL par rapport au nombre d'états de Bell, combiné avec le fait que la BNL-pseudo-télépathie existe, est une preuve que ces deux resources sont différentes et incomparables. Dans [27], il est démontré que certaines corrélations générées par un état non-maximalement intriqué de deux qubits ne peuvent pas être simulées par une seule BNL. Il est important de noter qu'il ne s'agit pas d'une preuve que ces deux ressources sont différentes, car nous pourrions toujours envisager un monde où toutes les corrélations générées par n paires de qubits intriquées pourraient être simulées par cn BNL, pour une constante $c > 1$. Dans un tel monde, les BNL seraient considérées comme une ressource strictement plus forte que l'intrication, puisque lorsque nous étudions la complexité de problèmes sous différentes ressources, les constantes multiplicatives n'ont aucune signification. Dans ce monde, l'intrication et les BNL seraient donc comparables : les BNL étant la plus forte ressource. Seul un résultat asymptotique tel que le Théorème 4.17, combiné à l'existence de la BNL-pseudo-télépathie, peut nous permettre de conclure que l'intrication et la non-localité sont des ressources différentes.

5.11 Anomalies des mesures des différents modèles

Une approche intéressante à la quantification de l'intrication est de caractériser l'intrication d'un état $|\psi\rangle$ par la quantité de ressources nécessaires afin de simuler l'état. Nous pouvons donc voir le nombre de bits de communication échangés entre les participants, le nombre de BNL utilisées par les participants, l'efficacité requise des détecteurs pour éviter une description locale réaliste de l'expérience, le bruit blanc que l'on doit ajouter afin de rendre classiques les corrélations ainsi que la violation d'une inégalité de Bell comme des mesures de l'intrication.

Alors qu'il est possible de simuler un état de Bell $|\Psi^-\rangle$ avec un seul bit de communication, le mieux que nous savons faire pour un état intriqué biparti général,

$\alpha|00\rangle + \beta|11\rangle$ pour certains $\alpha, \beta \neq 0, 1/\sqrt{2}$, est deux bits [79]. Pour le cas des BNL, il est également possible de simuler un état de Bell avec une seule BNL, alors qu'il existe des états $\alpha|00\rangle + \beta|11\rangle$, pour certains $\alpha, \beta \neq 0, 1/\sqrt{2}$, pour lesquels il n'existe pas de simulation utilisant une seule BNL [27]. Une efficacité des détecteurs de 3/4 est requise pour éviter une description locale réaliste d'une expérience avec un état de Bell et des mesures de von Neumann, alors que pour une paire de qubits générale, 2/3 est suffisant [42]. Considérons maintenant une inégalité de Bell sur une paire de qutrits où Alice et Bob ont tous deux le choix entre deux mesures chacun $x_1^{(A)}$, $x_2^{(A)}$, $x_1^{(B)}$ et $x_2^{(B)}$ respectivement, pour lesquels ils reçoivent comme résultats $y_1^{(A)}$, $y_2^{(A)}$, $y_1^{(B)}$ et $y_2^{(B)}$ respectivement. Nous pouvons alors borner classiquement l'opérateur

$$\begin{aligned} & P(y_1^{(A)} = y_1^{(B)}) + P(y_1^{(B)} = y_2^{(A)} + 1) + P(y_2^{(A)} = y_2^{(B)}) \\ & + P(y_2^{(B)} = y_1^{(A)}) - P(y_1^{(A)} + 1 = y_1^{(B)}) - P(y_1^{(B)} = y_2^{(A)}) \\ & - P(y_2^{(A)} + 1 = y_2^{(B)}) - P(y_2^{(B)} + 1 = y_1^{(A)}) \leq 2, \end{aligned} \tag{5.14}$$

où la somme à l'intérieur des P est modulo 3. S'il est possible pour les participants de partager une paire de qutrits maximalement intriqués, ils peuvent alors violer cette inégalité jusqu'à la valeur $4(2\sqrt{3}+3)/9 > 2$. Par contre, il existe une paire de qutrits non-maximalement intriqués pour laquelle les participants peuvent violer l'inégalité jusqu'à la valeur $1 + \sqrt{11/3} > 4(2\sqrt{3}+3)/9$ [2].

Un autre fait intéressant est que la construction de Hardy, présentée à la Section 3.3.1, ne fonctionne pas seulement pour l'état $(|01\rangle + |10\rangle + |11\rangle)/\sqrt{3}$, mais pour presque tous les états bipartis. Les états séparables et les états maximalement intriqués sont des exceptions [49].

Tout expérimentateur devrait connaître une mesure très importante, soit la distance de Kullback-Leibler (ou entropie relative). Appliquée dans notre cas, il s'agit du support moyen en faveur de la mécanique quantique contre les théories à VLC par prise de données probabilistes, lorsque les données viennent effectivement

de la distribution de probabilité quantique

$$D(\mathrm{MQ}, \mathrm{VLC}) = \sum_z p_{\mathrm{MQ}}(z) \log \left(\frac{p_{\mathrm{MQ}}(z)}{p_{\mathrm{VLC}}(z)} \right). \tag{5.15}$$

Pour un état biparti maximalement intriqué, nous pouvons atteindre la valeur maximum de 0,058, alors que pour un état biparti non-maximalement intriqué, nous pouvons atteindre 0,077 [3].

CHAPITRE 6

CONCLUSION

Dans le Chapitre 2, nous avons revisité, avec le bénéfice de 70 ans de recul, les arguments d'EPR et la réponse de Bohr. Nous avons démontré que, lorsque vu au travers des yeux de la logique mathématique, l'argument d'Einstein, Podolsky et Rosen est quelque peu fautif, et ce, même sans faire appel aux théorèmes de Bell. Nous questionnons aussi la vision quelque peu étroite qu'EPR portent sur ce qu'est vraiment un « état ». Cette vision n'est par contre pas surprenante chez des avocats de la défense des « éléments de réalité ». Par ailleurs, nous aimerions ajouter que la définition des « éléments de réalité » est laissée très vague dans l'article d'EPR. Néanmoins, nous avons été encore plus sévères envers la réponse de Bohr qui, selon nous, a complètement manqué le point soulevé par EPR. En rétrospective, malgré notre critique de l'article d'EPR, nous aurions sûrement pris la défense de ces derniers face à Bohr, à condition d'avoir une preuve satisfaisante que la position et la quantité de mouvement ne sont pas des éléments de réalité selon la MQ. Une telle preuve doit être construite avec attention afin de ne pas « montrer » par accident que la MQ est incorrecte [64]. Nous aurions donc favorisé EPR, du moins jusqu'à ce que l'éclair laisse place au tonnerre de l'article de Bell.

La Section 3.1 contient plusieurs définitions de théorèmes de BKS avec POVM et nous y avons exposé les preuves minimales pour certaines d'entre-elles. Davantage de travaux doivent être effectués afin d'établir la preuve minimale, contenant le moins d'éléments de POVM, du théorème de BKS avec des POVM sur un qubit selon la Définition 3.10. De plus, une question plus fondamentale reste à explorer. Nous n'avons toujours pas cerné quelle est la définition de la non-contextualité devant être adoptée par la communauté, ou plutôt quelle est la classe des théories à VLC raisonnables. Une argumentation pourrait être avancée en faveur de la Définition 3.1, selon laquelle il est facile de démontrer que la mécanique quantique ne peut pas être substituée par une théorie à VLC non-contextuelle. D'autres

peuvent prétendre qu'il est évident que le fait d'utiliser le même élément (ou un élément proportionnel à ce dernier) lors d'une preuve de BKS amènera une contradiction, mais qu'il n'y a pas de problèmes si nous sommes prêts à croire que la nature assigne un indice à chacun de ces éléments, et que cet indice nous est inaccessible. Une argumentation similaire peut être soulevée pour chaque définition donnée ici. La question demeure : Quelle est la définition de non-contextualité qui représente vraiment la nature ? Cette question est peut-être du ressort de la philosophie, mais comme Bell nous l'a si bien démontré en répondant à l'article d'EPR[1], il ne faut pas laisser tomber une question seulement parce qu'il semble difficile d'y répondre.

Nous avons aussi énoncé trois formes de théorème d'impossibilité pour les théories à VLC. Les limites de l'une d'elles, la pseudo-télépathie, ont été étudiées en détail. Nous avons prouvé que le jeu de pseudo-télépathie de [38], qui utilise deux qutrits intriqués et qui produit un bit et un trit, est le plus petit jeu possible à deux participants. Par contre, en terme de la dimension du système global, ce jeu à deux participants est battu par le jeu de Mermin-GHZ à trois participants [60]. Nous avons donc établi que les POVM ne donnaient aucun avantage aux stratégies quantiques en pseudo-télépathie, comparativement aux stratégies avec des mesures de von Neumann, lorsque le système quantique partagé est restreint en dimension 2×2. Quelle est la situation en plus haute dimension ou avec plus de participants ? Est-ce que tout jeu de pseudo-télépathie de dimension $d \times d$ peut avoir une stratégie gagnante qui utilise seulement des mesures projectives ? Une mesure de non-localité d'un jeu de pseudo-télépathie est la meilleure probabilité de succès possible pour toutes les stratégies classiques [17]. Plus la probabilité est petite, plus le jeu est classiquement difficile, et plus un physicien classique serait surpris de voir le succès systématique des participants quantiques. Cette probabilité doit être strictement plus petite que 1 par définition, mais il existe des jeux pour lesquels cette probabilité approche ridiculement de 1 [47]. Pour tout entier positif

[1] Wolfgang Pauli avait qualifié le problème d'EPR comme étant un problème similaire à « Combien d'anges peuvent s'asseoir sur la pointe d'une aiguille ? » [15]

d, prenons p_d comme étant la probabilité de succès du meilleur protocole classique pour le jeu de pseudo-télépathie le plus difficile de dimension $d \times d$. Est-ce que p_d peut être plus petit si nous permettons l'usage de POVM, contrairement à limiter les participants à des mesures de von Neumann ? Dans quel contexte ?

Nous avons vu la définition formelle de trois formes de théorème d'impossibilité pour les VLC, les théorèmes de BKS ainsi que la façon dont ils sont différents les uns des autres. Nous avons par le fait même soulevé le fait qu'il est important d'examiner de près les modèles étudiés lorsque nous décrivons la nature, car nous aurions pu voir il y a longtemps une différence qualitative entre le théorème de Hardy et les autres théorèmes de Bell sans inégalités connus. Dans cette hiérarchie de théorèmes d'impossibilité, la pseudo-télépathie est une réfutation plus forte du point de vue local réaliste. Il existe des théorèmes de Bell qui ne sont pas des théorèmes de Bell sans inégalités et des théorèmes de Bell sans inégalités qui ne sont pas des jeux de pseudo-télépathie, alors que les inclusions contraires sont vraies. Il existe des états qui peuvent générer des corrélations assez puissantes pour construire un théorème de Bell sans inégalités alors que le même état ne peut servir par lui-même à un jeu de pseudo-télépathie [23].

Nous avons aussi montré une simulation d'un état de Bell qui utilisait 5,7 bits de communication espérée. Même si ce résultat est une amélioration et une simplification de [32], il reste encore beaucoup à faire. Même s'il est possible de simuler des mesures de von Neumann avec une communication bornée (ou encore à sens unique), il n'est pas clair que l'on puisse faire de même pour les POVM. Les mesures de von Neumann ont toujours un nombre de résultats possibles borné par la dimension du système alors que les POVM peuvent avoir un nombre arbitraire de résultats. Est-ce qu'un protocole avec une communication bornée peut nous permettre de choisir parmi un nombre non-borné de possibilités ? Dans un autre ordre d'idée, peut-on généraliser ce type de protocole pour simuler des POVM sur n états de Bell ? Pour les états GHZ et autres états intriqués ? Combien de bits de communication espérée sont nécessaires pour simuler n bits d'intrication ? Qu'en est-il de tous ces résultats lorsque l'on tolère des erreurs ? Comment peut-on comparer

ces mesures d'intrication aux mesures déjà existantes, telles que l'intrication de formation et de distillation ? Combien de bits de communication sont nécessaires et suffisants dans tous ces scénarios pour des états GHZ et autres états intriqués ?

Nous avons aussi fait du progrès vers la compréhension du pouvoir remarquable des BNL. Une simple BNL peut simuler des corrélations quantiques qu'aucune paire de qubits intriqués ne peut faire, dans le scénario biparti (Théorème 4.5) et dans le scénario multiparti (Théorème 4.11). Dans la Section 5.10, nous avons aussi montré qu'une seule BNL peut générer des corrélations qui ne peuvent pas être obtenues à l'aide de la MQ, peu importe l'état, et nous avons défini la pseudo-télépathie à BNL (Définition 5.3). Finalement, nous avons démontré, avec les Théorèmes 4.14 et 4.17, qu'une seule boîte non-locale ne peut pas reproduire toutes les corrélations de la MQ. En montrant que la simulation de certaines corrélations quantiques requiert une quantité *exponentielle* de BNL dans le nombre d'états de Bell utilisés pour établir les corrélations (Théorème 4.17) et du fait que la pseudo-télépathie à BNL existe, nous avons démontré que les BNL et l'intrication sont en fait des ressources différentes et incomparables. Ceci est dû, selon nous, au fait que les BNL sont fondamentalement classiques et ne peuvent être "intriquées" entre elles.

Le lecteur très minutieux aura peut-être vu un lien entre le Théorème 4.2 et le Théorème 4.5, entre le Théorème 4.8 et le Théorème 4.11, et entre le Lemme 4.16 et le Théorème 4.17 : nous avons transformé une stratégie classique gagnante utilisant n bits de communication en une stratégie gagnante qui utilise n BNL. Peut-on toujours faire cette substitution ? Ce n'est évidemment pas le cas. Par exemple, en complexité de la communication, il est impératif de signaler à ses partenaires de l'information sur son entrée si la fonction dépend de l'entrée (le cas contraire n'a aucun sens). Nous savons qu'il est impossible de signaler à l'aide des BNL. Il est donc impossible de substituer toute la communication par des BNL, du moins en complexité de la communication, mais que se passe-t-il si nous ne voulons que simuler des corrélations quantiques ? Nous savons aussi que l'intrication ne peut être utilisée afin de communiquer. Est-il possible qu'afin de simuler n'importe quelles corrélations quantiques, il soit inutile de signaler ? Il pourrait aussi être vrai que

toutes les corrélations quantiques soient simulables par les BNL. Une réponse partielle a été présentée dans [27]. Les auteurs ont prouvé qu'il existe des corrélations qui peuvent être générées à partir d'un modèle à VLC augmenté d'un bit de communication qui ne signale pas d'information sur la mesure, mais qui ne peuvent être simulées par un modèle à VLC qui utilise une BNL. Même s'il n'existe pas de correspondance un pour un, est-ce que le paradigme des BNL, sans considération du nombre de boîtes, peut toujours remplacer la communication qui ne signale pas ? La réponse peut être difficile à trouver. Julien Degorre, Sophie Laplante et Jérémie Roland ont récemment généralisé les travaux de Méthot [61] et de Cerf, Gisin, Massar et Popescu [33] afin de créer une simulation de POVM sur un état de Bell à l'aide de deux BNL et de quatre bits de communication en moyenne [40]. Dans leur construction, il peut être difficile de nous débarrasser de la communication étant donné que toutes les simulations connues de POVM sur des états intriqués utilisent le principe du *test* [32,57,61] : Bob reçoit de l'information d'Alice et lui dit si cette information est pertinente étant donné sa mesure, sinon ils recommencent. Afin qu'Alice puisse savoir quand recommencer, continuer ou arrêter, Bob doit lui signaler que c'est le cas, ou *vice versa*. La façon de sortir de ce paradigme n'est pas évidente.

Des simulations d'autres jeux de pseudo-télépathie ou d'états quantiques à l'aide de BNL doivent être trouvées avant que nous puissions affirmer que nous comprenons parfaitement celles-ci. En particulier, une question ouverte de grand intérêt, tel que souligné lors du paragraphe précédent, est : « Est-il possible de simuler toutes les corrélations quantiques à l'aide de BNL ? » Nous aimerions aussi voir des bornes inférieures non-triviales sur le nombre de BNL nécessaires aux simulations du jeu de Mermin-GHZ multiparti.

Nous avons aussi démontré que dans n'importe quel monde où la complexité de la communication n'est pas triviale, il existe une limite sur la non-localité de ce monde. Pour ce faire, nous avons développé un protocole qui calcule de façon distribuée avec un biais borné n'importe quelle fonction booléenne, si nous pouvons simuler la BNL avec une probabilité d'au moins $\frac{1}{2} + \frac{1}{\sqrt{6}} \approx 0.909$. Cette borne,

qui est une grande amélioration sur le fait qu'une BNL ne peut pas être simulée parfaitement [39], s'approche de la vraie valeur de $\wp \approx 0.854$ imposée par la MQ. Nous avons aussi montré qu'en dépit du fait que les BNL et l'intrication soient des ressources différentes [24], les BNL sont toujours un sujet d'étude intéressant. Le problème ouvert évident est de réduire l'écart entre les deux probabilités. Une preuve qu'une complexité de la communication non-triviale empêche une meilleure approximation que $\wp$ de la BNL par la MQ serait vraiment intéressante, car elle rendrait la borne de Tsirelson [34] inévitable.

Nous avons aussi esquissé les liens très forts qui unissent tous les modèles présentés dans cette thèse et relevé une anomalie qui est présente dans plusieurs mesures d'intrication. En effet, pour plusieurs de ces mesures, nous avons vu que certains états non-maximalement intriqués obtiennent une valeur plus grande que pour les états maximalement intriqués. Nous croyons que cette anomalie provient du fait que nous utilisons des mesures de non-localité, qui sont intuitivement tout-à-fait appropriées pour cela, afin de mesurer l'intrication. Serait-ce un autre indice voulant que l'intrication et la non-localité soient deux phénomènes différents ? Nous croyons fermement que oui.

BIBLIOGRAPHIE

[1] H. Abelson, "Lower bounds on information transfer in distributed computation", *Proceedings of the 19th IEEE Symposium on Foundations of Computer Science*: 151–158, 1978.

[2] A. Acín, T. Durt, N. Gisin et J. I. Latorre, "Quantum nonlocality in two three-level systems", *Physical Review A* **65**: 052325, 2002.

[3] A. Acín, R. Gill et N. Gisin, "Optimal Bell tests do not require maximally entangled states", disponible sur `http://arxiv.org/quant-ph/0506225`.

[4] P. K. Aravind, "Impossible colorings and Bell's theorem", *Physics Letters A* **262**: 282–286, 1999.

[5] P. K. Aravind, "Bell's theorem without inequalities and only two distant observers", *Foundations of Physics Letters* **15**: 397–405, 2001.

[6] A. Aspect, P. Grangier et G. Roger, "Experimental tests of realistic local theories via Bell's theorem", *Physical Review Letters* **47**: 460–463, 1981.

[7] J. Barrett, "Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a Bell inequality", *Physical Review A* **65**: 042302, 2002.

[8] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox", *Physics* **1**: 195–200, 1964.

[9] J. S. Bell, "On the problem of hidden variables in quantum mechanics", *Reviews of Modern Physics* **38**: 447–452, 1966.

[10] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres et W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Physical Review Letters* **70**: 1895–1899, 1993.

[11] C. H. Bennett et S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states", *Physical Review Letters* **69**: 2881–2884, 1992.

[12] D. Bohm, "A suggested interpretation of the quantum theory in terms of 'hidden' variables. I", *Physical Review* **85**: 166–179, 1952.

[13] D. Bohm, "A suggested interpretation of the quantum theory in terms of 'hidden' variables. II", *Physical Review* **85**: 180–193, 1952.

[14] N. Bohr, "Can quantum-mechanical description of physical reality be considered complete?", *Physical Review* **48**: 696–702, 1935.

[15] M. Born et H. Born, *The Born-Einstein Letters: Correspondence Between Albert Einstein and Max and Hedwig Born from 1916 to 1955*, Walker, New York, 1971.

[16] G. Brassard, *Quantum Information Processing for Computer Scientist*, MIT Press, Cambridge, à paraître.

[17] G. Brassard, A. Broadbent et A. Tapp, "Quantum pseudo-telepathy", *Foundations of Physics* **35**, 2005.

[18] G. Brassard, A. Broadbent et A. Tapp, "Recasting Mermin's multi-player game into the framework of pseudo-telepathy", *Quantum Information and Computation* **5**: 538–550, 2005.

[19] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp et F. Unger, "A limit on non-local correlations in any world where communication complexity is not trivial", disponible sur `http://arxiv.org/quant-ph/0508042`.

[20] G. Brassard, R. Cleve et A. Tapp, "Cost of exactly simulating quantum entanglement with classical communication", *Physical Review Letters* **83**: 1874–1877, 1999.

[21] G. Brassard et A. A. Méthot, "Can quantum-mechanical description of physical reality be considered *in*complete?", *International Journal on Quantum Information*, à paraître.

[22] G. Brassard, A. A. Méthot et V. Scarani, "Is a maximally entangled state maximally entangled?", en préparation.

[23] G. Brassard, A. A. Méthot et A. Tapp, "Minimal bipartite state dimension required for pseudo-telepathy", *Quantum Information and Computation* **5**: 275–284, 2005.

[24] A. Broadbent et A. A. Méthot, "On the power of non-local boxes", *Theoretical Computer Science C*, à paraître.

[25] A. Broadbent et A. A. Méthot, "Entanglement swapping, light cones and elements of reality", disponible sur `http://arxiv.org/quant-ph/0511047`.

[26] A. Broadbent, A. A. Méthot et J. Walgate, "On classical strategies", en préparation.

[27] N. Brunner, N. Gisin et V. Scarani, "Entanglement and non-locality are different resources", *New Journal of Physics* **7**: 88, 2005.

[28] H. Buhrman, R. Cleve et A. Wigderson, "Quantum vs. classical communication and computation", *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*: 63–68, 1998.

[29] H. Buhrman, W. van Dam, P. Høyer et A. Tapp, "Multiparty quantum communication complexity", *Physical Review A* **60**: 2737–2741, 1999.

[30] H. Buhrman et S. Massar, "Causality and Cirel'son bounds", disponible sur `http://arxiv.org/quant-ph/0409066`.

[31] A. Cabello, "Kochen-Specker theorem for a single qubit using positive operator-valued measures", *Physical Review Letters* **90**: 190401, 2003.

[32] N. Cerf, N. Gisin et S. Massar, "Classical teleportation of a quantum bit", *Physical Review Letters* **84**: 2521–2524, 2000.

[33] N. Cerf, N. Gisin, S. Massar et S. Popescu, "Simulating maximal quantum entanglement without communication", *Physical Review Letters* **94**: 220403, 2005.

[34] B. S. Cirel'son, "Quantum generalizations of Bell's inequality", *Letters in Mathematical Physics* **4**: 93–100, 1980.

[35] J. F. Clauser, M. A. Horne, A. Shimony et R. A. Holt, "Proposed experiment to test local hidden-variable theories", *Physical Review Letters* **23**: 880–884, 1969.

[36] R. Cleve et H. Buhrman, "Substituting quantum entanglement for communication", *Physical Review A* **56**: 1201–1204, 1997.

[37] R. Cleve, W. van Dam, M. Nielsen et A. Tapp, "Quantum entanglement and the communication complexity of the inner-product function", *Quantum Computing and Quantum Communication: Proceedings of First NASA International Conference (QCQC'98), Lecture Notes in Computer Science 1509 (Springer-Verlag)*: 61–74, 1998.

[38] R. Cleve, P. Høyer, B. Toner et J. Watrous, "Consequences and limits of nonlocal strategies", *Proceedings of 19th IEEE Conference on Computational Complexity*: 236–249, 2004.

[39] W. van Dam, *Nonlocality & Communication Complexity*, Thèse de Ph.D., Université d'Oxford, 2000.

[40] J. Degorre, S. Laplante et J. Roland, "Simulating quantum correlations as a distributed sampling problem", *Physical Review A*, à paraître.

[41] D. Deutsch et R. Jozsa, "Rapid solution of problems by quantum computation", *Proceedings of the Royal Society of London, Series A* **439**: 553–558, 1992.

[42] P. Eberhard, "Background level and counter efficiencies required for a loophole free Einstein-Podolsky-Rosen experiment", *Physical Review A* **47**: R747–R750, 1993.

[43] A. Einstein, B. Podolsky et N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Physical Review* **47**: 777–780, 1935.

[44] W. Evans et N. Pippenger, "On the maximum tolerable noise for reliable computation by formulas", *IEEE Transactions on Information Theory* **44**: 1299–1305, 1998.

[45] J. S. Freedman et J. F. Clauser, "Experimental test of local hidden-variable theories", *Physical Review Letters* **28**: 938–941, 1972.

[46] C. A. Fuchs, *Notes on a Paulian Idea: Foundational, Historical, Anecdotal & Forward-Looking Thoughts on the Quantum*, Växjö University Press, Växjö, Sweden, 2003, disponible sur `http://arxiv.org/quant-ph/0105039`.

[47] V. Gaillard, A. Tapp et S. Wolf, "The impossibility of pseudo-telepathy without quantum entanglement", *Proceedings of IEEE International Symposium on Information Theory*: 457, 2003, version complète disponible sur `http://arxiv.org/quant-ph/0211011`.

[48] D. M. Greenberger, M. A. Horne et A. Zeilinger, "Going beyond Bell's theorem", dans *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edité par M. Kafatos (Kluwer Academic, Dordrecht), pages 69–72, 1989.

[49] L. Hardy, "Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories", *Physical Review Letters* **68**: 2981–2984, 1992.

[50] P. Heywood et M. L. G. Redhead, "Nonlocality and the Kochen-Specker paradox", *Foundations of Physics* **13**: 481–499, 1983.

[51] A. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel", *Problemy Peredachi Informatsii* **9**: 177–183, 1973.

[52] M. Jammer, "The EPR problem in its historical development", dans *Symposium on the Foundations of Modern Physics: 50 Years of the Einstein-Podolsky-Rosen Gedankenexperiment*, edité par P. Lahti et P. Mittelstaedt (World Scientific, Singapore), pages 129–149, 1985.

[53] S. Kochen et E. Specker, "The problem of hidden variables in quantum mechanics", *Journal of Mathematical Mechanics* **17**: 59–87, 1967.

[54] I. Kremer, *Quantum Communication*, thèse de M.Sc., Université Hébraïque, 1995.

[55] E. Kushilevitz et N. Nisan, *Communication Complexity*, Cambridge University Press, Cambridge, 1997.

[56] S. Massar, "Non locality, closing the detection loophole and communication complexity", *Physical Review A* **65**: 032121, 2002.

[57] S. Massar, D. Bacon, N. Cerf et R. Cleve, "Classical simulation of quantum entanglement without local hidden variables", *Physical Review A* **63**: 052305, 2001.

[58] S. Massar et S. Pironio, "Violation of local realism vs. detection efficiency", *Physical Review A* **68**: 062109, 2003.

[59] T. Maudlin, "Bell's inequality, information transmission, and prism models", *PSA: Proceedings of the Biennial Meeting of the Philosophy of Science Association* **1**: 404–417, 1992.

[60] N. D. Mermin, "Quantum mysteries revisited", *American Journal of Physics* **58**: 731–743, 1990.

[61] A. A. Méthot, "Simulating POVMs on EPR pairs with 5.7 bits of expected communication", *European Physical Journal D* **29**: 445–446, 2004.

[62] A. A. Méthot, "On local-hidden-variable no-go theorems", *Canadian Journal of Physics*, à paraître.

[63] A. A. Méthot, "Minimal Bell-Kochen-Specker proofs with POVMs on qubits", disponible sur `http://arxiv.org/quant-ph/0509199`.

[64] A. A. Méthot, "Can quantum-mechanical description of physical reality be considered *correct*?", en préparation.

[65] A. A. Méthot et K. Wicker, "Interaction-free measurement applied to quantum computation: a new 'cnot' gate", disponible sur `http://arxiv.org/quant-ph/0109105`.

[66] A. Nayak, "Optimal lower bounds for quantum automata and random access codes", *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science*: 369–376, 1999.

[67] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer Verlag, Berlin, 1932.

[68] I. Newman, "Private vs. common random bits in communication complexity", *Information Processing Letters* **39**: 67–71, 1991.

[69] M. W. Newman, *Independent Sets and Eigenspaces*, Thèse de Ph.D., Université de Waterloo, 2004.

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

[71] A. Peres, "Unperformed experiments have no results", *American Journal of Physics* **46**: 745–747, 1978.

[72] S. Pironio, "Violation of Bell inequalities as lower bounds on the communication cost of non-local correlations", *Physical Review A* **68**: 062102, 2003.

[73] S. Popescu et D. Rohrlich, "Quantum nonlocality as an axiom", *Foundations of Physics* **24**: 379–385, 1994.

[74] R. Raz, "Exponential separation of quantum and classical communication complexity", *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*: 358–367, 1999.

[75] R. Renner et S. Wolf, "Quantum pseudo-telepathy and the Kochen-Specker theorem", *Proceedings of 2004 IEEE International Symposium on Information Theory*: 322, 2004.

[76] L. Rosenfeld, "Niels Bohr in the thirties", dans *Niels Bohr: His Life and Work Seen by his Friends and Colleagues*, editié par S. Rozental (Interscience), 1964.

[77] R. Spekkens, "Contextuality for preparations, transformations, and unsharp measurements", *Physical Review A* **71**: 052108, 2005.

[78] H. R. Stapp, "Are superluminal connections necessary?", *Nuovo Cimento B* **40**: 191–204, 1977.

[79] B. F. Toner et D. Bacon, "The communication cost of simulating Bell correlations", *Physical Review Letters* **91**: 187904, 2003.

[80] B. F. Toner, D. Bacon et M. Ben-Or, "Kochen-Specker theorem for generalized measurements", en préparation.

[81] R. F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model", *Physical Review A* **40**: 4277–4281, 1989.

[82] S. Wolf et J. Wullschleger, "Oblivious transfer and quantum non-locality", *Proceedings of the 2005 IEEE International Symposium on Information Theory*, à paraître.

[83] W. K. Wootters et W. H. Żurek, "A single quantum cannot be cloned", *Nature* **299**: 802–803, 1982.

[84] A. C.-C. Yao, "Some complexity questions related to distributed computing", *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*: 209–213, 1979.

[85] A. C.-C. Yao, "Quantum circuit complexity", *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*: 352–361, 1993.