Université de Montréal

Effet de l'intrication brouillée sur la téléportation quantique

par
Xavier Coiteux-Roy

Département de physique
Faculté des arts et des sciences

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

Décembre, 2016

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

Effet de l'intrication brouillée sur la téléportation quantique

présenté par:

Xavier Coiteux-Roy

a été évalué par un jury composé des personnes suivantes:

Richard Leonelli,	président-rapporteur
Gilles Brassard,	directeur de recherche
Louis Salvail,	membre du jury

Mémoire accepté le: . . . . . .

RÉSUMÉ

La téléportation quantique promet d'être centrale à de nombreuses applications du futur tels la cryptographique quantique et l'ordinateur quantique. Comme toute mise en œuvre physique s'accompagne inévitablement d'imperfections expérimentales, on étudie la téléportation dans un contexte où la ressource quantique, c'est-à-dire l'intrication, que l'on consomme est brouillée. Pour ce faire, on introduit en premier lieu le formalisme de l'informatique quantique. En seconde partie, on approche les protocoles de téléportation quantique standard, de téléportation avec relais quantiques et de téléportation multi-ports. Notre analyse de la téléportation standard et de la téléportation multi-ports poursuit trois objectifs principaux. Le premier est de comparer l'emploi d'un canal brouillé pour la téléportation d'un état quantique avec l'utilisation de ce même canal pour l'envoi direct de l'état. On trouve ainsi les conditions pour lesquelles les deux protocoles de transmission sont équivalents. Le second but est d'observer le caractère non-local de l'intrication brouillée en regardant quand et comment Alice peut réduire le bruit chez elle à un bruit exclusivement chez Bob. En troisième, on quantifie par une borne inférieure la qualité d'un canal de téléportation en réduisant l'effet de toute intrication brouillée à celui d'un bruit de Pauli à un seul paramètre. On accomplit cette tâche en effaçant au moment approprié l'information classique superflue et en appliquant la wernerisation. Finalement, on analyse la composition de bruits de Pauli et l'effet du taux d'effacement sur la téléportation avec relais quantiques pour mieux comprendre comment se combinent les effets de l'intrication brouillée dans un réseau de téléportation quantique. La suite logique est d'établir des protocoles plus robustes de téléportation quantique qui prennent en compte l'effet de l'intrication brouillée.

Mots clés: Informatique quantique, Communications quantiques, Décohérence, Canaux brouillés, Téléportation multi-ports, Relais quantiques.

ABSTRACT

Quantum teleportation will be a centerpiece of practical quantum cryptography and quantum computing in a soon to be future. As no physical implementation is perfect, we study quantum teleportation in the context of impaired quantum resources which we call noisy entanglement. In a first part, we introduce how quantum mechanics is formalized by quantum information theory. In the second part, we study standard quantum teleportation, in both the absence and presence of quantum repeaters, as well as port-based teleportation. Our analysis of standard quantum teleportation and port-based teleportation follows three main directions. The first goal is to compare the use of a noisy channel for teleportation to the one of the same channel for direct transmission. We thus find the conditions under which the two cases are equivalent. Our second objective is to observe the non-local properties of noisy entanglement by finding when and how Alice can blame Bob for her noise. Thirdly, we quantify, in the worst-case scenario, the quality of a teleportation channel by reducing the effect of any noisy entanglement to the one of a one-parameter Pauli channel that can be interpreted as a depolarizing channel in most instances. We achieve this task by erasing unneeded classical information at the appropriate time and by twirling either the entanglement or the teleported state. Finally, we analyze the composition of Pauli noises and the impact of the erasure channel parameter on the protocol of teleportation with quantum repeaters. We thus aim to understand how the effects of noisy entanglement cumulate in a teleportation network. The next logical step is to create robust teleportation schemes that take into account the effects of noisy entanglement.

Keywords: Quantum information, Quantum communications, Decoherence, Noisy channels, Port-based teleportation, Quantum repeaters.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ANNEXES

LISTE DES SIGLES

TQMP	Téléportation quantique multi-ports
qubit	Bit quantique
qudit	Généralisation du bit quantique à d dimensions
EPR	Einstein-Podelsky-Rosen
CNOT	Non-contrôlé
POVM	« Positive-operator valued measure » (en anglais)
t. q.	tel que
SPG	Sans perdre de généralité

NOTATION

$\mathbb{N}$	Ensemble des entiers naturels
$\mathbb{C}$	Corps des complexes
$\mathbb{C}^{n\times n}$	Espace euclidien complexe de taille $n \times n$
$\mathcal{A}, \mathcal{B}$	Espaces euclidiens complexes
M et V	Matrice et vecteur
T, D et H	Matrice triangulaire supérieure, matrice diagonale et matrice hermitienne
$\langle\psi\|$ et $\|\psi\rangle$	Bra et ket
^{T}, * et †	Transposée, conjuguée et transposée-conjuguée
$^{-1}$	Inverse
ρ	Opérateur de densité
tr, tr_A	Trace et trace partielle
$\times$, $\otimes$, $\circ$	Multiplication, produit tensoriel et composition
$\cdot$	Produit scalaire ou marque substitutive
I	Identité
σ_i, X, Y, Z	Opérateurs de Pauli
H	Opérateur d'Hadamard
A, B, C, E	Registres
$\mathcal{C}$	Canal quantique
$\mathbb{P}$	Projecteur

U	Opérateur unitaire
A	Opérateur de Kraus
$\|\phi^+\rangle, \|\phi^-\rangle, \|\psi^+\rangle, \|\psi^-\rangle$	États de Bell
$\|\phi_d^+\rangle$	Généralisation de $\|\phi^+\rangle$ à d dimensions
π	État complètement mélangé
$F, \bar{F}, F_{\text{intr}}$	Fidélité, fidélité espérée et fidélité d'intrication
$p_{\mathsf{X}},\ p_{\mathsf{Y}},\ p_{\mathsf{Z}}$	Paramètres des bruits de Pauli
p_e, P	Paramètres des bruits d'effacement et de dépolarisation
p_W	Pureté d'un état de Werner
p	Probabilité générique
det	Déterminant
braf et brass	Brafication et brassage
mod	Modulo
$\lfloor\ \rfloor$ et $\lceil\ \rceil$	Partie entière par défaut et partie entière par excès
$:=$, $\sim$ et $\approx$	est défini, est similaire, est environ
δ_{ij} et ε_{ijk}	Delta de Kronecker et symbole de Levi-Civita
S	Nombre quantique associé au spin total
S_z	Nombre quantique associé à la projection du spin sur l'axe $\hat{z}$
$\|$	Symbole de conditionnement
$\|\ \|$	Norme ou valeur absolue
dim	Dimension de
#	Nombre de

$\{\}$	Ensemble ou variante des parenthèses
$\in$	Appartient
$\Rightarrow$	Implique
$\Leftrightarrow$	Si et seulement si
$\forall, \exists, \nexists$	Pour tout, il existe et il n'existe pas
$\sum_i$	Sommation
$\prod_i$ et $\bigotimes_i$	Produit scalaire d'une séquence et produit tensoriel d'une séquence
e	Exponentielle
i	Indice ou $\sqrt{-1}$
!	Factorielle
lim	Limite
$\longrightarrow$	Tend vers ou flèche générique
$\tilde{x}, x'$	Variantes d'un symbole quelconque x

À Gabrielle et Alexis, ainsi qu'à Alice et Bob,

REMERCIEMENTS

Je tiens tout d'abord à remercier mon directeur de recherche Gilles Brassard, puisque sans son enseignement plein d'humour, non seulement je n'aurais pas compléter de maîtrise en informatique quantique, mais je n'aurais même pas su ce que je manquais. Faire de l'informatique sans ordinateur : je n'imaginais pas cela possible quand je suis rentré à l'université en « math-phys » ! Gilles en partageant avec moi sa passion pour l'informatique théorique a, collatéralement, transformé globalement ma vision de la physique et des mathématiques. Sans aucune exagération. Alors merci énormément ! Je veux dire un gros merci ensuite à toute la gang du LITQ : avec vos « backgrounds » tous différents, j'ai découvert, appris, apprécié tellement de nouvelles choses ! Merci notamment à Philippe, Charles, Serge-O, Maxime et Alexandre pour les discussions de bar et les énigmes, à Sara et Rébecca pour leurs points de vue encourageants, et aussi à Paul, pour m'avoir amener à réfléchir sur le processus d'apprentissage et fait changer d'idée sur l'importance de la mémorisation en mathématiques. Je veux remercier Louis Salvail aussi, pour ses conseils et sa bonne humeur stimulante, de même qu'Evelyn et Anne Broadbent à Ottawa pour m'avoir présenté leur groupe de recherche. Finalement, je prends le temps de remercier mes amis à l'extérieur qui, même s'ils ne comprennent pas vraiment ce que j'étudie, croient constamment en moi et me font chérir chaque instant. Même message à ma famille dont le soutien est inconditionnel. Je termine en soulignant l'appui financier du FRQNT qui m'a permis de me consacrer entièrement à ma maîtrise.

-Xavier

CHAPITRE 1

INTRODUCTION

Le phénomène de la téléportation quantique est, comme son nom le laisse présager, totalement fascinant. En elle-même, la téléportation [9] est une manifestation frappante de ce qu'on appelle communément la non-localité de la mécanique quantique. Elle permet de transmettre de l'information quantique directement d'un port A à un port B, sans passer par aucun point intermédiaire. Du point de vue technologique, elle se révèle primordiale pour tout ce qui a trait aux communications quantiques. On peut l'imaginer notamment au cœur de plusieurs protocoles de cryptographie quantique et comme composante essentielle du futur ordinateur quantique. La cryptographie quantique permet, entre autres, d'établir, en théorie et conditionnellement à la validité de la mécanique quantique, des canaux de communication (classique ou quantique) dont l'écoute indiscrète est absolument impossible [8] ! L'ordinateur quantique peut, quant à lui, résoudre certains problèmes insolubles en temps raisonnable pour l'ordinateur classique, celui qu'on utilise aujourd'hui. L'algorithme de Shor pour factoriser des grands nombres premiers en est un exemple puissant [33], mais l'ordinateur quantique devrait aller au-delà de ça : si l'on en croit la thèse de Church-Turing-Deutsch, l'ordinateur quantique permettrait de simuler efficacement n'importe quel phénomène physique [28, 26] ! Cette tâche fondamentale est actuellement impossible pour l'ordinateur classique, puisque simuler un système quantique semble, au meilleur des connaissances actuelles, demander des ressources classiques exponentielles.

Il est important de mentionner que, même si la mécanique quantique est très déstabilisante à première vue, elle est une théorie physique qui repose sur une base expérimentale extrêmement solide. Par exemple, les inégalités de Bell [6], lesquelles constituent une démonstration du phénomène d'intrication, ont été vérifiées et revérifiées maintes fois [2, 38, 21], peut-être justement à cause de leur caractère si contre-intuitif. La téléportation quantique est, dans les dernières années, elle-aussi sortie du rang des curiosités

théoriques : elle a été réalisée, pour ne donner que quelques exemples, entre des photons sur des distances de 600 m en-dessous du Danube [39] et de 143 km aux Îles Canaries [27], ainsi que sur une distance de 3 m entre des centres NV de deux diamants [29].

Un point commun à toutes les implémentations physiques de la téléportation quantique est la fatalité du bruit. On entend par là que toute réalisation concrète de protocoles théoriques souffre nécessairement d'imperfections. En informatique quantique, cette difficulté est accentuée par le fait que l'on ne peut pas cloner l'information quantique. Celle-ci est très fragile et se dégrade lors de toute interaction avec son environnement. Le problème est tel qu'avant l'invention des codes correcteurs quantiques [34], certains scientifiques doutaient que l'ordinateur quantique puisse être jamais bâti. L'espoir est depuis revenu, mais comme en témoigne l'absence actuelle d'ordinateur quantique, la lutte contre le bruit n'est pas encore gagnée et beaucoup reste à apprendre. C'est la motivation principale de ce mémoire.

Dans ce contexte, on étudiera l'effet de l'intrication brouillée sur la téléportation quantique. L'intrication est la ressource principale composant le téléporteur quantique. Elle est un phénomène purement quantique qui caractérise d'une façon rigoureusement définie certains états de la matière. Dans ce mémoire, on traitera l'intrication brouillée comme le résultat de diverses opérations dégradant, ou modifiant, de l'intrication initialement parfaite. On appellera donc *intrication* toute ressource avec laquelle on tente l'opération de téléportation, même si elle est tellement brouillée qu'elle ne respecte plus la définition formelle de l'intrication. Dans le même ordre d'idée, on qualifiera de *bruit* toute opération transformant l'intrication, sans égard pour l'irréversibilité du processus. On note que la téléportation quantique nécessite une étape de communication classique, mais que l'on n'analysera pas l'effet du bruit dans cette dernière, puisque l'information classique peut être copiée impunément et est généralement moins fragile que l'information quantique. De plus, on pourrait réduire facilement tout bruit dans la communication classique à un bruit dans l'intrication.

Ce mémoire est divisé en deux parties majeures. Au chapitre 2, on approche la mécanique quantique d'un système physique sous l'angle de l'informatique quantique. Pour ce faire, on commence par la notion formelle d'état quantique d'un système. On formule après la notion d'évolution quantique pour modéliser la dynamique de ce système, c'est-à-dire comment il passe d'un état à un autre. On explique ensuite brièvement comment on peut acquérir de l'information sur un système en modélisant la mesure. Enfin, on examine de plus près l'évolution quantique dans un contexte brouillé en examinant plusieurs modèles de bruit et en regardant comment les quantifier.

Au chapitre 3, on rentre dans le vif du sujet. On explore l'effet de l'intrication brouillée sur trois méthodes de téléportation quantique. On commence par la téléportation quantique telle que découverte en 1993 [9], laquelle on qualifie de *standard*. On enchaîne avec la téléportation standard en présence de relais quantiques et on termine avec la téléportation multi-ports : une téléportation d'un genre nouveau découverte en 2008 [24]. Pour ces trois sections, on commence par décrire le procédé idéal de téléportation. Ensuite, pour la téléportation standard, on modélise, aux différentes sous-sections, divers modèles d'intrication brouillée en partant des cas les plus restreints et en allant progressivement vers les plus généraux. On s'attaque en passant à trois problématiques principales : comparer l'effet du bruit sur l'intrication à l'effet d'un bruit équivalent appliqué directement sur l'état téléporté ; étudier les propriétés non-locales du bruit ; qualifier de manière pratique la qualité de la téléportation. On passe après à la section sur la téléportation avec relais quantiques où on examine comment se cumule le bruit dans un réseau d'intrication brouillée et on quantifie par rapport au taux d'effacement l'avantage que procure le recours à des relais quantiques. Finalement, dans la dernière section, on analyse la téléportation multi-ports en reprenant les modèles et les questions de la section sur la téléportation quantique standard et en en soulignant les différences.

CHAPITRE 2

FORMALISME DE L'INFORMATIQUE QUANTIQUE

> *The introduction of Alice and Bob is the greatest contribution from quantum information theory to physics.*
>
> — N. David Mermin *[16]*

Le physicien N. David Mermin n'était avec sa moquerie en fait possiblement pas si loin de la vérité. Peut-être qu'Einstein, s'il avait connu Alice, Bob et tout le langage de l'informatique quantique, aurait découvert la téléportation quantique en même temps qu'il découvrit l'intrication en 1935 [17]. Au lieu de cela, la téléportation ne fut découverte que presque 60 ans plus tard, en 1993 [9] ! Le grand apport de l'informatique quantique est ainsi son formalisme : sa façon claire et concise de parler de mécanique quantique.

Ce chapitre est consacré à ce formalisme. Comme le sujet de ce mémoire est l'intrication brouillée, on approche tout de suite les états quantiques comme des mélanges statistiques, donc des matrices densité, plutôt que comme des états purs (donc non-brouillés). On voit ensuite comment se modélise l'évolution quantique à l'aide de la notion de canal quantique. On approche les mesures projective et de type POVM. Puis, on finit avec la notion de canal de transmission pour expliciter divers modèles de bruit et les quantifier selon quelques mesures de fidélité. On donne au fur et à mesure les références sur lesquelles sont bâties ce chapitre.

2.1 États quantiques

L'informatique quantique présente une formalisation puissante de la notion d'état quantique. La signification formelle d'un état quantique repose principalement sur deux des quatre postulats de la mécanique quantique traités dans ce document. Ceux-ci permettent de représenter des états quantiques à l'aide de matrices particulières. On énonce

ces postulats immédiatement, puis on clarifie les notions mathématiques nécessaires à leur compréhension. On relègue les deux autres postulats aux prochaines sections, car ils concernent les phénomènes de l'évolution quantique et de la mesure. La formulation de la mécanique quantique par postulats provient de l'excellent livre de Nielsen et Chuang [28]. On l'a ici considérablement adaptée afin de rendre l'ensemble du travail plus cohérent.

2.1.1 Systèmes physiques, registres et matrices densité

L'hypothèse physique la plus fondamentale en informatique quantique est que tout système physique descriptible par la mécanique quantique peut l'être en termes d'information quantique abstraite.

Postulat 1. *On peut associer un registre à tout système physique isolé. Le système peut alors être entièrement décrit par une matrice densité appartenant à ce registre. Inversement, toute matrice densité représente un état physiquement possible dans un registre de dimension appropriée.*

Cette modélisation implique que l'on peut toujours effectuer de la même manière le traitement formel d'un qubit, qu'il soit associé au spin d'un électron, à la polarisation d'un photon ou bien à n'importe quel autre système quantique !

On rappelle qu'un qubit est un système quantique à 2 dimensions et qu'on peut exprimer tout système quantique de dimension d finie par une composition de $\lceil \log_2 d \rceil$ qubits.

2.1.2 Composition d'états

Le deuxième postulat exprime comment combiner des registres et en composer les matrices densité pour représenter des systèmes physiques conjoints.

Postulat 2. *Soit les registres A et B de deux systèmes physiques différents dont les espaces euclidiens complexes correspondants sont $\mathcal{A}$ et $\mathcal{B}$, alors l'espace euclidien complexe*

associé au registre AB du système physique conjoint est $\mathcal{A} \otimes \mathcal{B}$. L'état conjoint de deux systèmes dont les états ρ_A et ρ_B sont indépendants est quant à lui $\rho_A \otimes \rho_B$.

Il est à noter que certains états conjoints ne peuvent s'écrire comme le produit tensoriel de matrices densité séparées : ils sont classiquement ou quantiquement corrélés. On donne la différence entre ces deux types de corrélation à la sous-section 2.1.5 plus bas. À cause de l'existence de ces états corrélés, l'opération inverse à la composition, c'est-à-dire l'expression d'un système conjoint AB en le produit tensoriel de ses composantes A et B, n'existe pas dans notre formalisme dans le cas général.

L'opération la plus proche est la trace partielle, laquelle consiste intuitivement à ignorer totalement un sous-système. Dans le cas spécifique où ρ_{AB} peut s'écrire comme produit tensoriel de deux sous-systèmes indépendants, alors la trace partielle permet de retrouver les états $\rho_A = \mathrm{tr}_B \rho_{AB}$ et $\rho_B = \mathrm{tr}_A \rho_{AB}$.

La trace partielle est une opération utile dans de nombreux contextes. Par exemple, on peut faire la trace partielle de AB sur B lorsque l'on ne veut considérer que ce qu'Alice peut connaître localement parce que le registre de Bob lui est momentanément, ou ultimement, inaccessible. Cela peut arriver si Bob ne peut/veut communiquer avec Alice, s'il a perdu son état dans l'environnement ou bien si, de manière encore plus extrême, Bob est une construction mathématique sans existence physique nécessaire (voir le concept de purification à la section 2.1.7).

2.1.3 Registres et espaces euclidiens complexes

Pour donner un sens aux notions formelles d'états quantiques énoncées par les postulats 1 et 2, il convient d'établir la notion de registre, laquelle est dérivée de celle d'espace euclidien complexe. On les prend généralement finis et souvent carrés en informatique quantique.

Définition 1. *$\mathbb{C}^{n \times n}$ est un espace euclidien complexe de taille $n \times n$.*

On ne rentre pas dans les détails de ce qu'est formellement un espace euclidien complexe. On se contente de dire que concrètement, c'est l'ensemble des matrices carrées de n^2 valeurs complexes.

Cela suffit pour introduire la notion de registre, laquelle est importante pour faire le pont entre systèmes physiques et entités purement mathématiques tel que l'énonce le postulat 1.

Définition 2. *On appelle registre des espaces euclidiens complexes finis auxquels on a adjoint une étiquette.*

Cette distinction a de l'importance, car souvent on ne s'intéresse pas simultanément à tous les attributs physiques d'un système. Deux systèmes dont l'état étudié est le même ne sont donc pas nécessairement indistinguables, puisque de l'information additionnelle, qu'on pourrait obtenir en examinant d'autres caractéristiques de ces systèmes, pourrait permettre de les départager. Un exemple direct est celui de deux systèmes quantiques identiques mais spatialement distincts. L'étiquette contient alors l'information relative à l'emplacement.

Afin de rendre les expressions plus faciles à suivre, on personnifie souvent en informatique ces étiquettes en faisant appel aux personnages d'Alice et Bob. Par exemple, $\mathcal{A}$ et $\mathcal{B}$ sont respectivement les espaces euclidiens complexes associés aux registres A et B d'Alice et Bob.

2.1.4 États et matrices densité

Chaque registre contient un état quantique formalisé par un opérateur densité. Ce dernier est représentable à l'aide d'une matrice densité ρ (en pratique les termes opérateur et matrice densité sont interchangeables). On note que ρ_A et ρ_B sont les états quantiques (ou plutôt leurs représentations) dans les registres respectifs d'Alice et de Bob. ρ_{AB} est l'état quantique global sur le registre conjoint $A \otimes B$. Comme mentionné précédemment, $\rho_{AB} \neq \rho_A \otimes \rho_B$ dans le cas général. L'état maximalement intriqué $\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$ en est

le meilleur contre-exemple, puisque dans ce cas si l'on prend la trace partielle sur l'un ou l'autre des deux sous-systèmes on obtient l'état complètement mélangé : $\rho_A = \rho_B = \pi$. Or, la composition de l'état complètement mélangé avec lui-même ne donne pas un état maximalement intriqué : $\pi \otimes \pi \neq \rho_{AB}$ (ces deux états particuliers sont décrits dans la section 2.1.6).

Sur ce, on énonce maintenant les conditions nécessaires à une matrice pour qu'elle soit une matrice densité, puis on rappelle les définitions formelles des deux premières conditions.

Définition 3. *Une matrice densité $\rho \in \mathbb{C}^{n \times n}$ est telle que :*

- *ρ est hermitienne*
- *ρ est semi-définie positive*
- *ρ est de trace 1*

On clarifie ces conditions.

Définition 4. *Une matrice $\mathsf{M} \in \mathbb{C}^{n \times n}$ est hermitienne si $\mathsf{M}^\dagger = \mathsf{M}$. Les valeurs propres d'une matrice hermitienne sont réelles.*

Définition 5. *On note par $\mathsf{M}^\dagger$ la matrice transposée conjuguée de M et on réserve M^* à la matrice conjuguée non-transposée.*

Définition 6. *Une matrice H hermitienne $\in \mathbb{C}^{n \times n}$ est semi-définie positive si $\forall x \in \mathbb{C}^n$, $x^\dagger H x \geq 0$. On le note $H \geq 0$. Toute matrice hermitienne dont les valeurs propres sont non-négatives est semi-définie positive. On met l'emphase sur l'hermicité*[1] *de H, car la notion de positivité semi-définie pourrait aussi être définie pour des matrices symétriques.*

Bien qu'on ait introduit directement la notation des matrices densité pour les états quantiques, on utilisera parfois la notation bra-ket pour exprimer ces opérateurs densité ou pour représenter des vecteurs d'états quantiques purs. On part du principe que le lecteur

[1] est la propriété de ce qui est hermitien.

est familier avec cette notation. Dans le cas contraire, on l'invite à consulter [28]. On rappelle que $|x\rangle^\dagger = \langle x|$.

Tester si une matrice densité est idempotente permet de savoir rapidement si l'état qu'elle représente est pur.

Définition 7. *Une matrice* M *est idempotente si* $\mathsf{M}^2=\mathsf{M}$.

Définition 8. *On dit qu'une matrice densité représente un état pur si elle est idempotente. Elle peut alors aussi bien être représentée par un ket que par une matrice densité. Un état qui n'est pas pur est un mélange statistique.*

Il est facile de représenter un état pur quelconque $|\phi\rangle$ par une matrice densité ρ : c'est simplement $\rho = |\phi\rangle\langle\phi|$. Faire l'inverse, c'est-à-dire représenter un mélange statistique quelconque par une somme probabiliste d'états purs, est moins direct mais néanmoins possible et en général fort utile, voire inévitable. Pour cela on aura recours au très important théorème de décomposition spectrale. Ce dernier est en fait le théorème de décomposition de Schur appliqué à des matrices normales. On définit d'abord ces deux notions. L'opérateur unitaire U est au cœur de la notion d'évolution d'un système en mécanique quantique ; c'est pourquoi il n'est défini qu'à la prochaine section. On invite toutefois le lecteur non-familier à en lire tout de suite la définition à la sous-section 2.2.2 avant de poursuivre sa lecture.

Théorème 1. *Le théorème de décomposition de Schur énonce que pour toute matrice carrée* $\mathsf{M} \in \mathbb{C}^{n\times n}$*, il existe une matrice unitaire* $\mathsf{U} \in \mathbb{C}^{n\times n}$ *et une matrice triangulaire supérieure* $\mathsf{T} \in \mathbb{C}^{n\times n}$ *telles que*

$$\mathsf{M} = \mathsf{U}\mathsf{T}\mathsf{U}^\dagger$$

Démonstration. Le théorème de décomposition de Schur peut être prouvé par induction en exhibant une construction récursive de U et T. La preuve est faite dans les notes de cours de Louis Salvail [32]. ■

T a les mêmes valeurs propres que M, puisque le polynôme caractéristique est invariant

sous $\mathsf{U}(\cdot)\mathsf{U}^\dagger$:

$$\begin{aligned}\det \mathsf{U}(M-\lambda I)\mathsf{U}^\dagger &= \det \mathsf{U}(\mathsf{M}-\lambda I)\mathsf{U}^{-1} \\ &= \det(\mathsf{U})\det(\mathsf{M}-\lambda I)\det(\mathsf{U}^{-1}) \\ &= \det(\mathsf{U})\det\frac{1}{(\mathsf{U})}\det(\mathsf{M}-\lambda I) = \det(\mathsf{M}-\lambda I)\end{aligned}$$

Comme T est triangulaire, ces valeurs sont les éléments de sa diagonale.

On définit maintenant la notion de normalité d'une matrice.

Définition 9. *Un opérateur représenté par* $\mathsf{M} \in \mathbb{C}^{n\times n}$ *est dit normal si* M *commute avec sa transposée conjuguée.*

$$\mathsf{M}\mathsf{M}^\dagger - \mathsf{M}^\dagger\mathsf{M} = 0$$

Notamment, un opérateur est normal dès qu'il appartient à l'une des classes suivantes :

- M est hermitien
- M est unitaire
- M est semi-défini positif

La condition de normalité est donc omniprésente en informatique quantique : c'est une caractéristique partagée par les opérateurs densité, les opérateurs POVM, les opérateurs unitaires et tout canal dans la représentation de Choi-Jamiołkowski. (Tous ces concepts seront abordés dans les sections suivantes.)

On peut maintenant s'attaquer au théorème de décomposition spectrale.

Théorème 2. *Le théorème de décomposition spectrale affirme que pour toute matrice carrée normale* $\mathsf{M} \in \mathbb{C}^{n\times n}$*, il existe une matrice unitaire* $\mathsf{U} \in \mathbb{C}^{n\times n}$ *et une matrice diagonale* $\mathsf{D} \in \mathbb{C}^{n\times n}$ *telles que*

$$\mathsf{M} = \mathsf{U}\mathsf{D}\mathsf{U}^\dagger$$

En informatique quantique, la forme équivalente suivante de la décomposition spectrale est utilisée :

$$\mathsf{M} = \sum_j \lambda_j \, |j\rangle\langle j|$$

où $|j\rangle := \mathsf{U}\,|i\rangle$ *et* $\{|i\rangle\}$ *est la base orthogonale.*

Démonstration. La décomposition spectrale est le cas particulier de la décomposition de Schur augmenté de la condition de normalité pour M. Si on explicite cette condition sur la forme de Schur de la matrice M, on obtient la condition suivante sur T :

$$\begin{aligned}
\mathsf{M}\mathsf{M}^\dagger = \mathsf{M}^\dagger\mathsf{M} &\Leftrightarrow (\mathsf{U}\mathsf{T}\mathsf{U}^\dagger)(\mathsf{U}\mathsf{T}\mathsf{U}^\dagger)^\dagger = (\mathsf{U}\mathsf{T}\mathsf{U}^\dagger)^\dagger(\mathsf{U}\mathsf{T}\mathsf{U}^\dagger) \\
&\Leftrightarrow (\mathsf{U}\mathsf{T}\mathsf{U}^\dagger)(\mathsf{U}\mathsf{T}^\dagger\mathsf{U}^\dagger) = (\mathsf{U}\mathsf{T}^\dagger\mathsf{U}^\dagger)(\mathsf{U}\mathsf{T}\mathsf{U}^\dagger) \\
&\Leftrightarrow \mathsf{U}\mathsf{T}\mathsf{T}^\dagger\mathsf{U}^\dagger = \mathsf{U}\mathsf{T}^\dagger\mathsf{T}\mathsf{U}^\dagger \\
&\Leftrightarrow \mathsf{T}\mathsf{T}^\dagger = \mathsf{T}^\dagger\mathsf{T} \qquad (2.1)
\end{aligned}$$

Or, T est triangulaire supérieure. La condition (2.1) ci-dessus implique donc que tous ses éléments non-diagonaux sont nuls. T est diagonal. On le renomme alors D et la preuve de la décomposition spectrale découle directement de celle de Schur. ■

Le théorème de décomposition spectrale a une grande importance physique. Par exemple, lorsqu'on l'applique aux matrices densité (hermitiennes donc normales), la matrice diagonale D de sa décomposition spectrale donne les probabilités d'obtenir chaque état pur composant le mélange statistique (ces probabilités somment bien à 1 car $\mathrm{tr}\,\rho = 1$). Les matrices densité peuvent donc toujours être décomposées en une somme probabiliste d'états purs et la décomposition spectrale indique même comment le réaliser physiquement. Il ne faut cependant pas oublier que la décomposition spectrale d'une matrice densité n'est pas unique (sauf si l'état est pur) et qu'il y a plusieurs façons de réaliser une même matrice densité en mélangeant des états purs.

2.1.5 Intrication

Les deux parties d'un état biparti peuvent être corrélées de manière classique ou quantique. Ce qu'on nomme intrication est la présence d'une corrélation strictement quantique. On compare les deux types de corrélation.

Définition 10. *Soit deux parties éloignées Alice et Bob, un état classiquement corrélé ρ_{AB} est un état qui peut être créé localement par Alice et Bob à l'aide d'un ensemble de variables aléatoires communes, mais qui ne peut pas être écrit directement comme le produit tensoriel d'états locaux chez Alice et chez Bob. Formellement, ces deux critères doivent être respectés :*

- $\exists\{p_i, \rho_{A_i}, \rho_{B_i}\}$ *t.q.* $\rho_{AB} = \sum_i p_i \rho_{A_i} \otimes \rho_{B_i}$
- $\rho_{AB} \neq (\mathrm{tr}_A \rho_{AB}) \otimes (\mathrm{tr}_B \rho_{AB})$

Définition 11. *Soit deux parties éloignées Alice et Bob, un état intriqué ρ_{AB} est un état qui ne peut être créé localement par Alice et Bob, et ce même à l'aide d'un ensemble de variables aléatoires communes. Formellement :*

- $\nexists\{p_i, \rho_{A_i}, \rho_{B_i}\}$ *t.q.* $\rho_{AB} = \sum_i p_i \rho_{A_i} \otimes \rho_{B_i}$

L'introduction de bruit dans un état intriqué peut le faire changer de catégorie en rendant ses parties simplement classiquement corrélées, voir indépendantes. Toutefois, on abusera souvent dans ce travail du mot intrication en l'utilisant pour désigner la ressource qu'on utilise pour tenter le protocole de téléportation, même dans le cas où l'intrication est tellement brouillée que l'état résultant n'est plus formellement intriqué.

2.1.6 États quantiques importants

On explicite ici quelques-uns des états quantiques les plus remarquables ainsi que certaines de leurs propriétés notables.

Un des effets les plus spectaculaires décrits par la mécanique quantique est l'intrication. Celle-ci s'incarne notamment dans les quatre états de Bell. Lorsque deux qubits sont dans un de ces états, on dit qu'ils forment une paire EPR (Einstein-Podolsky-Rosen, en l'honneur des auteurs du premier article mentionnant l'étrangeté de l'intrication [17]).

Définition 12. *On définit les quatre états de Bell par :*

$$|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\psi^+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\phi^-\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Ils sont maximalement intriqués et forment une base de l'espace à 2 qubits.

Le phénomène de l'intrication ne se limite pas aux qubits. On peut l'observer sur un espace de taille arbitraire : tout système de dimension paire peut être dans un état maximalement intriqué.

Définition 13. *Pour 2 qudits (un qudit est la généralisation à d dimensions d'un qubit), on définit l'état maximalement intriqué $|\phi_d^+\rangle$ par :*

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle\,|i\rangle$$

L'état maximalement intriqué tel que défini ci-dessus a une intéressante propriété non-locale. Cette propriété fait toutefois référence encore une fois à l'opérateur unitaire U, lequel n'est défini qu'à la sous-section 2.2.2.

Proposition 1.

$$(\mathsf{U}_d \otimes I_d)\,|\phi_d^+\rangle = (I_d \otimes \mathsf{U}_d^T)\,|\phi_d^+\rangle$$

Démonstration.

$$
\begin{aligned}
\text{Soit SPG} : \mathsf{U}_d &= \sum_{jk} a_{jk} \left|k\right\rangle \left\langle j\right| \\
(\mathsf{U}_d \otimes I_d) \left|\phi_d^+\right\rangle &= \frac{1}{\sqrt{d}} \sum_i (\mathsf{U}_d \left|i\right\rangle)(I_d \left|i\right\rangle) \\
&= \frac{1}{\sqrt{d}} \sum_i (\sum_{jk} a_{jk} \left|k\right\rangle \left\langle j\right| \left|i\right\rangle) \left|i\right\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{ijk} (a_{jk} \left|k\right\rangle \delta_{ij}) \left|i\right\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{jk} a_{jk} \left|k\right\rangle \left|j\right\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{ijk} \left|i\right\rangle (a_{jk} \left|j\right\rangle \delta_{ik}) \\
&= \frac{1}{\sqrt{d}} \sum_i \left|i\right\rangle (\sum_{jk} a_{jk} \left|j\right\rangle \left\langle k\right| \left|i\right\rangle) \\
&= \frac{1}{\sqrt{d}} \sum_i (I_d \left|i\right\rangle)(\mathsf{U}_d^T \left|i\right\rangle) \\
&= (I_d \otimes \mathsf{U}_d^T) \left|\phi_d^+\right\rangle
\end{aligned}
$$

■

Cette propriété sera cruciale dans notre étude du bruit, puisqu'elle permet de traiter toute opération unitaire sur l'intrication du côté d'Alice comme une transformation exclusivement chez Bob.

Dans le cas spécifique à 2 qubits cette propriété a un corollaire également très utile. L'état de Bell $\left|\psi^-\right\rangle$ est invariant sous toutes les transformations unitaires bilatérales et donc effectuer une unitaire sur une moitié est complètement équivalent à réaliser l'unitaire inverse sur l'autre moitié.

Proposition 2.

$$(\mathsf{U} \otimes I) \left|\psi^-\right\rangle = (I \otimes \mathsf{U}^\dagger) \left|\psi^-\right\rangle$$

Démonstration. Conséquence de

$$\begin{aligned}(\mathsf{U}\otimes\mathsf{U})\,|\psi^-\rangle &= (\mathsf{U}\otimes\mathsf{U})(\mathsf{ZX}\otimes I)\,|\phi^+\rangle \\ &= (I\otimes\mathsf{U})(I\otimes(\mathsf{UZX})^T)\,|\phi^+\rangle \\ &= (I\otimes\mathsf{UXZU}^T)\,|\phi^+\rangle \\ &= (I\otimes\mathsf{UXZU}^T\mathsf{ZX})\,|\psi^-\rangle = (I\otimes I)\,|\psi^-\rangle\end{aligned}$$

Les opérateurs X,Z sont les opérateurs de Pauli. Ce sont les premiers opérateurs qu'on décrits à la sous-section 2.2.2.1 sur les opérateurs unitaires importants. ■

Parce que les deux dernières propriétés sont importantes, on invite le lecteur non-familier avec le concept d'opérateur unitaire à y revenir plus tard, après avoir pris connaissance de ce dernier à la section suivante.

L'état complètement mélangé est l'état dont toutes les valeurs ont probabilité égale d'être mesurées peu importe la base choisie par l'observateur.

Définition 14. *L'état complètement mélangé $\pi_n \in \mathbb{C}^{n\times n}$ s'écrit :*

$$\pi_n := \frac{I_n}{n}$$

On omet l'indice n lorsque la dimension du registre est évidente ou arbitraire.

Un état est un mélange statistique lorsqu'il est intriqué avec un autre état inaccessible. (Selon l'interprétation appelée « Church of the larger Hilbert space », c'est d'ailleurs la seule explication d'un mélange statistique.) Lorsque cette intrication est maximale, alors le mélange statistique est complètement mélangé. C'est par exemple le cas d'une moitié de paire EPR dont on aurait perdu l'autre moitié dans l'environnement. Un état n'est pas nécessairement mélangé de manière objective pour tous les observateurs. En effet, un observateur ayant déjà fait la mesure est complètement intriqué avec l'état et pour lui, l'état est pur (tant qu'il est sûr de sa mesure et que rien n'a encore perturbé l'état), alors qu'un observateur qui n'a aucune connaissance a priori sur cet état va le considé-

rer comme complètement mélangé (en utilisant un argument de symétrie). Cela reste vrai même si cet observateur connaît a priori la base de l'état (mais qu'il n'a rien mesuré) !

Finalement, on donne la définition de l'état de Werner [41], sur 2 qubits, parce que celui-ci sera utile lorsque l'on utilisera la notion de wernerisation aux passages 3.1.5.2 et 3.3.6.

Définition 15. *L'état de Werner de pureté p_W est défini par*

$$W_{p_W} = p_W |\psi^-\rangle\langle\psi^-| + \frac{1-p_W}{3}(|\phi^-\rangle\langle\phi^-| + |\phi^+\rangle\langle\phi^+| + |\psi^+\rangle\langle\psi^+|)$$

On note que tout état de Werner n'est pas nécessairement intriqué.

Proposition 3. *Un état de Werner est séparable si sa pureté $p_W \leq \frac{1}{2}$.*

2.1.7 Purification

La purification offre une vision alternative, mais physiquement équivalente, d'un mélange statistique. En effet, on peut traiter tout mélange statistique sur un registre A comme un état pur sur un registre élargi AE, dont la partie E est inaccessible. En d'autres mots, on ajoute un registre fictif E au mélange statistique A de manière à ce que ρ_{AE} soit pur.

Définition 16. *Une purification d'un mélange statistique ρ_A est un état pur $\rho_{AE} = |\phi\rangle\langle\phi|_{AE}$ sur un registre conjoint tel que $\mathrm{tr}_E\, \rho_{AE} = \rho_A$. La purification n'est pas unique, mais tous les états purifiés sont équivalents à une isométrie[2] sur E près.*

On montre comment obtenir une purification valide du mélange statistique ρ_A à partir de sa décomposition spectrale.

$$\rho_A = \sum_i p_i |i\rangle\langle i|$$
$$\Rightarrow |\phi\rangle_{AE} = \sum_i |i\rangle_A \otimes (\sqrt{p_i}\,|j\rangle_E)$$

[2]Une isométrie sur un système est une transformation unitaire agissant conjointement sur ce système et un système ancillaire.

Ici, $\{|j\rangle_E\}_j$ est une base orthonormée de E. Prendre E de dimension égale à A est suffisant pour purifier tout état sur A. L'état $|\phi\rangle_{AE}$ est bel et bien une purification de ρ_A, car

$$\mathrm{tr}_E \sum_i |i\rangle\langle i|_A \otimes (p_i\,|j\rangle\langle j|_E) = \sum_i p_i\,|i\rangle\langle i|_A = \rho_A$$

Comme tout opérateur densité peut être purifié, le premier postulat pourrait s'énoncer en termes d'états purs seulement. Cette vision, nommée « Church of the larger Hilbert space » par John Smolin, est souvent très utile en informatique quantique. La question méta-physique à savoir si le registre de purification existe réellement physiquement ou s'il n'est qu'un artifice mathématique est laissée ouverte.

2.2 Évolution quantique

Maintenant qu'on a établi la correspondance entre la description d'un système physique et un état quantique, on formalise la dynamique du système, c'est-à-dire l'évolution de son état quantique, à l'aide de la notion d'opérateur unitaire et de canal quantique. Ces deux concepts donnent lieu à deux versions physiquement équivalentes du troisième postulats. On donne d'abord ces deux versions, puis les définitions mathématiques nécessaires correspondantes. L'usage de la notion de canal quantique pour caractériser toute évolution quantique provient des notes de cours de John Watrous [40].

2.2.1 Évolutions d'un système fermé et d'un système ouvert

La première version du postulat d'évolution d'un état quantique concerne les systèmes fermés.

Postulat 3 (Première version). *L'évolution d'un système fermé sur un temps t est entièrement descriptible par un opérateur unitaire* U. *Un état quantique* ρ *évolue en* $\mathsf{U}\rho\mathsf{U}^\dagger$ *sous l'influence de cet opérateur unitaire.*

Un corollaire notable est que l'évolution de tout système fermé est a priori complètement réversible. Cette propriété ne tient pas en général pour les systèmes ouverts, lesquels

peuvent aussi être utilisés pour décrire l'évolution d'un système quantique. C'est ce que dit la deuxième version du postulat d'évolution. On clarifiera bientôt comment ces deux formulations peuvent être équivalentes.

Postulat 3 (Seconde version). *L'évolution d'un système ouvert est entièrement descriptible par un canal quantique.*

Bien sûr, ce postulat ne prendra un sens que lorsque l'on aura définit ce qu'est un canal quantique. On verra qu'un tel canal peut être explicité de différentes façons, notamment à l'aide de ses opérateurs de Kraus, de sa matrice d'évolution de Choi-Jamiołkowski ou bien de sa représentation de Stinespring. Cette dernière forme justifie l'équivalence entre les deux versions du postulat, puisqu'elle montre qu'à l'instar d'un état purifié, on peut toujours traiter l'évolution d'un système ouvert A comme celle d'un système conjoint AE fermé mais dont la sous-partie E est inaccessible. On appelle souvent E l'*environnement* ou le *système ancillaire*.

2.2.2 Opérateurs unitaires

On formalise maintenant la notion d'unitarité telle qu'utilisée dans le postulat 3 (Première version).

Définition 17. *Un opérateur* $\mathsf{U} \in \mathbb{C}^{n\times n}$ *est unitaire si* $\mathsf{U}\mathsf{U}^\dagger = I$.

La condition d'unitarité implique que les lignes et colonnes d'une matrice unitaire $n \times n$ sont linéairement indépendantes et normalisées ; elles forment une base orthonormée de l'espace $\mathbb{C}^{n\times n}$. La réciproque est également vraie : on peut construire une matrice unitaire $n \times n$ en choisissant une base orthonormée de l'espace $\mathbb{C}^{n\times n}$.

En informatique quantique, on considère l'évolution comme discrète. Autrement dit, on fixe t dans l'opérateur d'évolution $\mathsf{U}(t)$ et on appelle la nouvelle expression simplement U. Au temps $2t$, l'opérateur d'évolution sera ainsi U^2. L'opérateur unitaire et l'ajout d'un système ancillaire suffisent en principe pour décrire toute la mécanique d'un système quantique. Comme on va le voir, il existe cependant d'autres façons de voir l'évolution

quantique, lesquelles offrent parfois un éclairage différent ou un formalisme plus facile à manipuler.

2.2.2.1 Opérateurs unitaires importants

Un opérateur unitaire appliqué sur un état quantique est parfois appelé porte quantique. Il en existe une large gamme (une infinité en fait !) et on ne s'attardera pas à les énumérer. On va cependant en présenter quelques-uns à cause de leur ubiquité générale et de leur utilité spécifique aux protocoles de téléportation quantique standard et de téléportation multi-ports. Ce sont les opérateurs de Pauli (ainsi que leurs généralisations), de Hadamard, du non-contrôle quantique (CNOT) et de la permutation de deux qubits.

Définition 18. *Pour un qubit, on définit les trois matrices de Pauli par :*

$$\mathsf{X} := \sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \mathsf{Y} := \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \mathsf{Z} := \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

X correspond à l'inversion de bit et Z à l'inversion de phase. Y est l'inversion des deux.

Ces matrices ont de nombreuses propriétés mathématiques particulières. Notamment, les trois matrices de Pauli sont auto-inverses. C'est-à-dire qu'au carré elles donnent l'identité :

$$\sigma_i^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Elles suivent la relation suivante lorsque multipliées entre-elles :

$$\sigma_i \sigma_j = i\varepsilon_{ijk}\sigma_k$$

Les matrices de Pauli anti-commutent :

$$\{\sigma_i, \sigma_j\} := \sigma_i\sigma_j + \sigma_j\sigma_i = 2\delta_{ij}I_2$$

Cela veut dire notamment que pour $\forall i \neq j$:

$$\sigma_i\sigma_j = -\sigma_j\sigma_i$$

L'identité I_2 est parfois appelée quatrième matrice de Pauli (évidemment, elle commute plutôt qu'anti-commute avec les autres).

On peut généraliser la notion des portes de Pauli X et Z à tout espace d-dimensionnel.

Définition 19. *Les opérateurs de décalage cyclique* $\mathsf{X}(x)$ *sont donnés par :*

$$\mathsf{X}(x)\,|j\rangle := |(x+j) \mod d\rangle \text{ où } x, j \in \{0, \ldots, d-1\}$$

C'est-à-dire que $\mathsf{X}(x)_{ab} = \delta_{a,(b+x \mod d)}$.

Définition 20. *Les opérateurs de phase* $\mathsf{Z}(z)$ *sont des opérateurs diagonaux tels que :*

$$\mathsf{Z}(z)\,|j\rangle := e^{\frac{2\pi i \cdot zj}{d}}\,|j\rangle \text{ où } z, j \in \{0, \ldots, d-1\}$$

C'est-à-dire que $\mathsf{Z}(z)_{ab} = e^{\frac{2\pi i \cdot zb}{d}}\delta_{ab}$.

Définition 21. *Les* d^2 *opérateurs de Pauli généralisés sont donc* $\{\mathsf{X}(x) \cdot \mathsf{Z}(z)\}_{x,z}$.

La porte de Hadamard est elle-aussi utilisée presque partout en informatique quantique.

Définition 22. *L'opération d'Hadamard est définie sur un qubit par :*

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

Le non-contrôlé quantique agit sur deux qubits et intrique ces derniers lorsque le qubit source est en superposition d'états.

Définition 23. *Le non-contrôlé quantique est défini par la matrice :*

$$CNOT_{AB} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

L'opérateur de transposition (12) agit sur deux qubits et en échange simplement les valeurs.

Définition 24. *L'opérateur de transposition* (12) *est défini par la matrice :*

$$(12)_{AB} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

2.2.3 Canaux quantiques

On étudiera surtout l'évolution quantique à travers la notion de canal. Un canal quantique est une application linéaire transformant une matrice densité en une nouvelle matrice densité. C'est l'opérateur d'évolution le plus général (à ne pas confondre avec le *canal de transmission* tel que l'on le définit à la section 2.4). Formellement,

Définition 25. *Un canal quantique $\mathcal{C}^{\mathcal{A}\to\mathcal{B}}$ est une application linéaire de l'espace euclidien complexe du registre $\mathcal{A}$ vers celui du registre $\mathcal{B}$ telle que :*

- *$\mathcal{C}$ préserve la trace*
- *$\mathcal{C}$ est une application complètement positive (au sens hermitien)*

Avant d'expliciter la dernière condition, il faut passer par la notion de positivité d'une application.

Définition 26. *Une application $\mathcal{M}(\cdot)$ est positive si $\mathcal{M}(\mathsf{M}) \geq 0$ pour $\forall \mathsf{M} \geq 0$.*

La notion de positivité complète est plus forte :

Définition 27. *Une application $\mathcal{M}(\cdot)$ est complètement positive si $(I^k \otimes \mathcal{M})(\cdot)$ est positive pour $\forall k \in \mathbb{N}$.*

Voir la téléportation et l'intrication brouillée sous l'angle des canaux sera essentiel dans notre analyse. Un canal quantique peut modéliser presque toute opération quantique (voir le bémol dans la note ci-dessous). Ceci inclut notamment les opérations quantiques locales architecturées et souhaitées (comme les portes logiques) et les opérations collatérales non-désirées (comme le bruit provenant de l'environnement). Un canal quantique peut aussi modéliser le déplacement de l'information quantique d'un endroit à un autre, lequel peut survenir suite au transport local d'un registre d'information ou bien suite à la téléportation de l'information d'un registre à un autre.

Note. *On utilise l'approximation de Markov, c'est-à-dire qu'on considère l'environnement comme constant au sens où l'information qui s'y échappe est rapidement dissipée. Les canaux sont ainsi sans mémoire. Certaines opérations quantiques qui ne respectent pas cette approximation ne peuvent pas s'écrire sous forme de canal. Un exemple est l'opération renversant le canal à inversion-de-bit (voir 2.4.2.1 pour la définition de ce dernier). En effet, soit deux canaux, $\mathcal{C}_{inversion}$ et $\mathcal{C}_{inversion^{-1}}$. Si $\mathcal{C}_{inversion}$ effectue une inversion de bit avec probabilité p, alors il n'existe aucun canal $\mathcal{C}_{inversion^{-1}}$ tel que $\mathcal{C}_{inversion^{-1}} \circ \mathcal{C}_{inversion} = \mathcal{C}_{identité}$. C'est pourtant une opération quantique physiquement*

envisageable. Cet exemple illustre une limite du formalisme standard de l'informatique quantique, lequel ne permet pas de recombiner deux systèmes intriqués une fois qu'on les a représentés de manière séparée. On ignorera toutefois dans ce travail toute opération quantique de ce genre.

2.2.3.1 Représentation de Kraus

On examine maintenant trois manières de représenter[3] ces canaux. La première utilise les opérateurs de Kraus.

Définition 28. *Toute application complètement positive peut être décrite par un ensemble d'opérateurs* $\{\mathsf{A}_i\}$[4]. *En ajoutant la condition* $\forall i, \sum_i \mathsf{A}_i^\dagger \mathsf{A}_i = I$, *on assure la préservation de la trace et ces opérateurs* $\{\mathsf{A}_i\}$ *dits de Kraus déterminent un canal quantique. Plus précisément :*

$$\mathcal{C}(\cdot) := \sum_i \mathsf{A}_i(\cdot)\mathsf{A}_i^\dagger$$

La réciproque est vraie : tout ensemble d'opérateurs de Kraus peut a priori représenter un canal.

La représentation d'un canal par ses opérateurs de Kraus n'est pas unique et plusieurs ensembles d'opérateurs de Kraus peuvent être équivalents. C'est le cas par exemple de $\{\frac{I}{2}, \frac{\mathsf{X}}{2}, \frac{\mathsf{Y}}{2}, \frac{\mathsf{Z}}{2}\}$ et $\{\frac{\mathsf{X}+\mathsf{Z}}{2\sqrt{2}}, \frac{\mathsf{X}-\mathsf{Z}}{2\sqrt{2}}, \frac{I+\mathsf{Y}}{2\sqrt{2}}, \frac{I-\mathsf{Y}}{2\sqrt{2}}\}$ qui représentent tous deux le canal complètement dépolarisant (voir 2.4.2.1 pour une définition du canal dépolarisant), c'est-à-dire que l'état sortant est trivialement toujours complètement mélangé.

Les opérateurs de Kraus permettent d'expliciter une caractéristique importante de certains canaux : l'unitalité. Celle-ci peut être vue de manière intuitive comme la préservation de l'identité.

[3] Par abus de langage, on confondra souvent représentation du canal (ou du bruit) avec le canal.
[4] Cette description serait analogue à celle explicitée par l'équation suivante pour les canaux.

Définition 29. *Un canal est unital si sa représentation de Kraus suit la condition :*

$$\sum_i \mathsf{A}_i \mathsf{A}_i^\dagger = I$$

Par linéarité, la condition d'invariance de l'identité à travers un canal unital est équivalente à la préservation de l'état complètement mélangé au travers de ce canal. La sortie d'un canal unital ne peut jamais être plus pure que l'entrée. Toute évolution unitaire sur un système fermé est unitale.

2.2.3.2 Représentation de Stinespring

La représentation la plus naturelle d'un canal quantique est celle de Stinespring, parfois nommée représentation environnementale à cause de l'explicitation du rôle que joue l'environnement. C'est l'analogue pour les canaux sur des systèmes ouverts de la purification pour les mélanges statistiques. On l'explicite.

Définition 30. *On peut spécifier un canal agissant sur un état ρ_A dans la représentation de Stinespring par une unitaire U_{AE} telle que :*

$$\mathcal{C}(\rho_A) = \mathsf{Tr}_E\{\mathsf{U}_{AE}\,(\rho_A \otimes |0\rangle\langle 0|_E)\,\mathsf{U}_{AE}^\dagger\}$$

où $|0\rangle\langle 0|_E$ est l'état pur « zéro » de dimension correspondante à celle de l'environnement.

En adoptant ce point de vue, on remarque tout de suite que le bruit introduit dans le système A vient de la fuite d'information vers l'environnement et que si l'on considérait le système dans son ensemble, l'évolution serait unitaire et sans bruit, donc réversible. L'environnement ici peut avoir une signification physique ou bien n'être qu'un artifice mathématique. Comme pour les ensembles d'opérateurs de Kraus, plusieurs opérateurs U_{AE} peuvent représenter le même canal.

2.2.3.3 Représentation de Choi-Jamiołkowski

On introduit maintenant la représentation de Choi-Jamiołkowski d'un canal quantique en se basant sur le livre de Bengtsson et Życzkowski [7]. Moins utilisée que les deux

dernières, cette forme a l'avantage d'être en bijection avec les canaux quantiques (les représentations précédentes n'étaient pas injectives). En d'autres mots, deux canaux ayant des représentations de Choi-Jamiołkowski distinctes sont nécessairement différents. On expliquera tout de suite après ce qu'on veut dire par les opérations de brafication et de brassage[5] et comme la notation est un peu lourde, des exemples simples seront donnés.

Définition 31. *On définit la représentation de Choi-Jamiołkowski par l'opérateur linéaire complexe* J *de dimension* $n^2 \times n^2$ *agissant sur un état* ρ *de dimension* $n \times n$*, tel que :*

$$\mathcal{C}(\rho) = \text{braf}^{-1}\left[\mathsf{J} \cdot \text{braf}\left[\rho\right]\right]$$

Bien sûr, toute matrice de l'espace $\mathbb{C}^{n^2 \times n^2}$ n'est pas une représentation valable d'un canal. J doit respecter quelques conditions pour que l'état de sortie $\mathcal{C}(\rho)$ soit une matrice densité quand ρ est une matrice densité. Pour expliciter ces conditions, on fait appel à la matrice dynamique D associée en bijection à l'opérateur J. Celle-ci sera bientôt définie, mais on fait d'abord un détour pour décrire les manipulations algébriques que sont la brafication et le brassage.

Définition 32. *Soit* $\{\mathsf{M}_{ij}\}$ *les éléments d'une matrice* M *de dimension* $m \times n$*, alors on appelle brafication (« reshaping » en anglais) l'opération qui transforme* M *en* V *où* V *est un vecteur de taille* $m \cdot n$ *qui s'exprime selon :*

$$V_k = \mathsf{M}_{ij} \text{ où } k = (i-1)n + j$$

En fait, on bâtit un vecteur à partir de la matrice originale, lue de gauche à droite, de haut en bas[6]*. On appellera l'opération inverse simplement débrafication.*

[5] Ces deux termes francophones sont inventés par l'auteur.

[6] À ne pas confondre avec l'opération de vectorisation, laquelle transforme habituellement aussi une matrice en vecteur, mais selon une énumération de haut en bas, de gauche à droite. (La brafication est donc la vectorisation de la matrice transposée.)

Exemple 1. braf $\left[\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}\right] = \begin{pmatrix} a & b & c & d & e & f & g & h & i \end{pmatrix}^T$

Définition 33. *L'opération de brassage* $\text{brass}^{m,n}$ *(« reshuffling » en anglais) est définie par son effet sur une matrice* M *carrée de dimension* $m^2 \times n^2$ *:*

$$(\text{brass}^{m,n}[\mathsf{M}])_{ab} = \mathsf{M}_{ij} \text{ avec :}$$
$$i = (a - a\%m)\frac{n}{m} + b - b\%n + 1$$
$$j = (a\%m - 1)n + b\%n$$

et où l'opération x%y est définie comme :

$$x\%y = \begin{cases} (x \mod y) & \text{if } (x \mod y) \neq 0 \\ y & \text{if } (x \mod y) = 0 \end{cases}$$

Intuitivement, l'opération de brassage peut se voir comme la suite de manipulations suivantes. On effectue d'abord une brafication de la matrice M. On obtient alors un vecteur de longueur $(m \cdot n)^2$. On sépare ensuite ce vecteur en une suite de m^2 sous-vecteurs de longueur n^2. On débrafique ensuite ces sous-vecteurs de longueur n^2 pour former une liste de sous-matrices carrées $n \times n$. Finalement, on débrafique cette liste de sous-matrices débrafiquées pour former une matrice carrée $(m \times n)^2$.

Exemple 2. *On veut effectuer l'opération* $\text{brass}^{(2,3)}\left[\mathsf{M} \in \mathbb{C}^{6\times 6}\right]$. *On l'effectue étape par étape pour donner l'intuition derrière la manipulation. Après cet exemple, on appliquera*

directement la formule. On commence par brafiquer M *:*

$$\mathsf{M} = \begin{pmatrix} 11 & 12 & 13 & 14 & 15 & 16 \\ 21 & 22 & 23 & 24 & 25 & 26 \\ 31 & 32 & 33 & 34 & 35 & 36 \\ 41 & 42 & 43 & 44 & 45 & 46 \\ 51 & 52 & 53 & 54 & 55 & 56 \\ 61 & 62 & 63 & 64 & 65 & 66 \end{pmatrix} \rightarrow \begin{pmatrix} 11 & 12 & 13 & 14 & 15 & 16 & 21 & 22 & \dots & 66 \end{pmatrix}^T$$

Ensuite on débrafique les $2 \cdot 2 = 4$ *sous-vecteurs en matrices* 3×3 *et on en fait une liste :*

$$\rightarrow \left\{ \begin{pmatrix} 11 & 12 & 13 \\ 14 & 15 & 16 \\ 21 & 22 & 23 \end{pmatrix}, \begin{pmatrix} 24 & 25 & 26 \\ 31 & 32 & 33 \\ 34 & 35 & 36 \end{pmatrix}, \begin{pmatrix} 41 & 42 & 43 \\ 44 & 45 & 46 \\ 51 & 52 & 53 \end{pmatrix}, \begin{pmatrix} 54 & 55 & 56 \\ 61 & 62 & 63 \\ 64 & 65 & 66 \end{pmatrix} \right\}$$

Finalement, on débrafique les sous-matrices pour obtenir la matrice finale.

$$\rightarrow \begin{pmatrix} \begin{pmatrix} 11 & 12 & 13 \\ 14 & 15 & 16 \\ 21 & 22 & 23 \end{pmatrix} & \begin{pmatrix} 24 & 25 & 26 \\ 31 & 32 & 33 \\ 34 & 35 & 36 \end{pmatrix} \\ \begin{pmatrix} 41 & 42 & 43 \\ 44 & 45 & 46 \\ 51 & 52 & 53 \end{pmatrix} & \begin{pmatrix} 54 & 55 & 56 \\ 61 & 62 & 63 \\ 64 & 65 & 66 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 11 & 12 & 13 & 24 & 25 & 26 \\ 14 & 15 & 16 & 31 & 32 & 33 \\ 21 & 22 & 23 & 34 & 35 & 36 \\ 41 & 42 & 43 & 54 & 55 & 56 \\ 44 & 45 & 46 & 61 & 62 & 63 \\ 51 & 52 & 53 & 64 & 65 & 66 \end{pmatrix} = \text{brass}^{(2,3)}\,[\mathsf{M}]$$

Pour simplifier l'expression algébrique de la brafication et du brassage, on peut faire appel à une notation à indices doubles.

Définition 34. *Soit une matrice de taille $mn \times mn$,*

$$\mathsf{M}_{\substack{a,b\\c,d}} := \mathsf{M}_{a(m-1)+b,c(m-1)+d}$$

Dans cette notation, le brassage n'est que la permutation des indices b et c.

$$\mathrm{brass}^{n,n}\left[\mathsf{M}_{\substack{a,b\\c,d}}\right] = \mathsf{M}_{\substack{a,c\\b,d}}$$

Armé de ces deux nouveaux outils, on peut désormais définir la matrice dynamique d'une application J.

Définition 35. *La matrice dynamique* D *associée à l'opérateur* J *de dimension* $n^2 \times n^2$ *est définie par :*

$$\mathsf{D} := \mathrm{brass}^{n,n}[\mathsf{J}]$$

Les opérateurs J et D sont évidemment en bijection.

Enfin, on donne à l'aide de D les critères explicites que J doit respecter pour être un canal[7].

Proposition 4. J *est un canal si et seulement si :*

- D *est hermitienne*
- D *est positive*
- $\mathsf{D}_{\substack{a,b\\a,d}} = \delta_{bd}$ *(préservation de la trace)*

La dernière condition est celle qui assure la conservation de la trace par l'application J. Elle est équivalent à la condition suivante :

Proposition 5. *Soit* D_{AB} *appartenant à l'espace euclidien complexe* $\mathcal{A}\otimes\mathcal{B}$ *correspondant au registre conjoint AB, si* $\mathrm{tr}_A\,\mathsf{D}_{AB} = I$*, alors* J *préserve la trace.*

[7] La preuve est faite dans le livre de Bengtsson et Życzkowski [7].

Proposition 6. *On peut passer de la représentation de Kraus à la représentation de Choi-Jamiołkowski en utilisant la formule suivante :*

$$\mathsf{J} = \sum_i A_i \otimes A_i^*$$

2.2.3.4 Précisions sur la notation

En dernier lieu, on clarifie la notation en lien avec les canaux et le transfert d'information entre différents registres. On a précédemment défini un canal comme une application d'un espace euclidien complexe à un autre (noté $\mathcal{C}^{\mathcal{A}\to\mathcal{B}}$). Cependant, il est souvent préférable d'expliciter les registres des espaces euclidiens complexes plutôt que les espaces eux-mêmes (noté $\mathcal{C}^{A\to B}$). L'apposition d'étiquettes permet de départager deux espaces mathématiquement isomorphes, mais physiquement différents. Cette distinction pratique est utile pour localiser l'information quantique (envoyer de l'information de Alice vers Alice est différent physiquement de l'envoyer de Alice vers Bob) et pour décrire les cas où les supports physiques sont de nature différente (le traitement mathématique de l'information quantique du spin d'un électron est le même que celui de la polarisation d'un photon, mais expérimentalement il peut être souhaitable de transférer l'information d'un système à l'autre). Lorsqu'un seul registre est explicitée ($\mathcal{C}^A$), alors on suppose que les registres d'entrée et de sortie sont le même ($\mathcal{C}^A := \mathcal{C}^{A\to A}$).

On complémentera souvent les canaux quantiques par un canal classique (ce dernier est d'ailleurs nécessaire à la téléportation). Pour simplifier la notation, on pourrait représenter sans perdre de généralité les bits classiques par une matrice densité ρ diagonale de dimension adéquate. Pour ne pas s'attarder au problème de correction d'erreurs classique, on suppose que cette dernière est implicite et que le canal résultant est sans bruit. Un canal classique envoyant $2^{\dim(\rho_A)}$ bits de Alice vers Bob est formellement :

$$\mathcal{C}^{A\to B}_{\text{classique}}(\rho_A) = \rho_B \ , \quad \text{où } \rho_A, \rho_B \text{ sont diagonales et } \rho_A = \rho_B$$

ou bien encore plus simplement $\mathcal{C}^{A\to B}_{\text{classique}}$.

Enfin, on définit le symbole $\sim$ et la notion de similarité entre deux canaux.

Définition 36. *Deux canaux $\mathcal{C}(\cdot)$ et $\mathcal{C}'(\cdot)$ sont similaires si quand on leur donne le même état à l'entrée, à la fin des protocoles qu'ils désignent, leurs deux états à la sortie sont indistinguables l'un de l'autre. La méthode et les états ancillaires nécessaires à la production de l'état final peuvent toutefois être différents. On note alors :*

$$\mathcal{C}(\cdot) \sim \mathcal{C}'(\cdot)$$

2.3 Mesure

2.3.1 Mesure projective

Pour clore le sujet de l'évolution des états quantiques, on s'attarde au cas particulier de la mesure. Le postulat physique correspondant s'énonce ainsi :

Postulat 4. *Toute observation directe d'un système quantique peut se faire à l'aide d'une mesure projective complète. Celle-ci retourne la valeur classique i avec probabilité $p_i = \mathrm{tr}(\mathbb{P}_i\rho)$. L'état quantique résultant est $\rho' = \frac{\mathbb{P}_i\rho\mathbb{P}_i}{p_i}$.*

Lors d'une mesure, le registre (et l'état quantique qu'il contient) est parfois détruit. C'est le cas par exemple lors de la détection photonique (du moins pour la plupart des techniques de détection).

La mesure physique d'un système repose sur la notion mathématique de projection.

Définition 37. *Un projecteur $\mathbb{P}$ est un opérateur sur un espace euclidien complexe tel que :*

- $\mathbb{P}$ *est idempotent*
- $\mathbb{P}$ *est hermitien*

Définition 38. *Une mesure projective complète $\mathbb{M}$ sur un espace $\mathbb{C}^{n\times n}$ est un ensemble de projecteurs $\{\mathbb{P}_i\}$ de dimension $n \times n$ tel que :*

- $\sum_i \mathbb{P}_i = I_n$
- $\mathbb{P}_i \mathbb{P}_j = 0$ *si* $i \neq j$

Les résultats d'une mesure sont tels que décrits par le postulat 3.

2.3.2 Mesure généralisée

Pour mesurer un registre sur un espace $\mathbb{C}^{n\times n}$, il existe un type de mesure plus puissant que d'effectuer directement une mesure projective complète sur cet espace. C'est la mesure de type POVM (de l'anglais « Positive-Operator Valued Measure »). Le postulat correspondant est :

Postulat 4′. *Toute observation d'un système quantique peut se faire à l'aide d'une mesure de type POVM. Celle-ci retourne la valeur classique i avec probabilité* $p_i = \mathrm{tr}(\Pi_i \rho)$*, où* $\alpha_{j_i} \geq 0$*. L'état quantique résultant est* $\rho' = \frac{\Pi_i \rho \Pi_i}{p_i}$.

On explicite le formalisme de cette mesure.

Définition 39. *Un POVM* Π *sur un espace* $\mathbb{C}^{n\times n}$ *est un ensemble de combinaisons linéaires de projecteurs* $\{\Pi_i := \sum_{j_i} \alpha_{j_i} \mathbb{P}_{j_i}\}_i$ *de dimensions* $n \times n$ *telles que* $\sum_i \Pi_i = I_n$.

À l'instar du postulat d'évolution, on peut ramener le postulat de la mesure généralisée à celui de mesure projective en supplémentant l'état à mesurer d'un système ancillaire (c'est le théorème de dilatation de Naimark.) Passer par un système ancillaire est toujours nécessaire à l'implémentation physique, mais le vide quantique (« vacuum state » en anglais), lequel est facilement accessible, peut suffire comme système ancillaire. Une telle expérience a d'ailleurs été réalisée en 1996 par un groupe de chercheurs à Genève [22].

2.4 Canaux de transmission

Dans la section précédente, on a eu un bref aperçu de la manière dont évolue les états quantiques et de la riche classe de canaux sous-jacente. On se concentre maintenant

sur une catégorie informelle de ces canaux quantiques qu'on appellera les canaux de transmission. On regroupe tout simplement dans cette classe tout canal quantique dont l'*intention* est le transfert d'un registre à un autre d'information quantique (par opposition par exemple à un calcul quantique dont l'état sortant est volontairement différent de l'état d'entrée). On inclut aussi dans cette catégorie le canal représentant l'évolution d'un état gardé en mémoire, c'est-à-dire quand la transmission d'un état quantique se fait d'un registre vers lui-même à un temps postérieur. On commence par regarder quelques-uns de ces canaux de transmission, puis on regarde comment analyser formellement leur qualité de transmission. Dans les sections suivantes, on examinera le cas du canal de transmission que constitue la téléportation quantique. On a utilisé comme référence le livre de Mark M. Wilde [42] pour les définitions et les propriétés.

2.4.1 Canal de transmission parfait

Le canal identité est le canal de transmission parfait, au sens que le bruit est inexistant et que tout état quantique y passe sans modification. Il est donc un idéal mathématique et sert de référence. Il peut être défini sur n'importe quelle taille de registre.

Définition 40. *Le canal identité est défini par :*

$$\mathcal{C}_{identité}(\rho) = \rho$$

2.4.2 Canaux brouillés

Physiquement, les canaux de transmission ne sont jamais parfaits et l'état à la sortie est souvent une version brouillée de l'état à l'entrée. C'est à travers cette notion que l'on approchera l'intrication brouillée, laquelle on définit comme la caractéristique d'un état intriqué une fois passé à travers un canal de transmission brouillé. Voici quelques modèles de bruit, c'est-à-dire une opération non-désirée, pouvant agir sur un qubit (d=2) lors de sa transmission.

2.4.2.1 Bruits de Pauli

Les bruits de Pauli surviennent lorsque l'état quantique subit potentiellement l'effet non-désiré d'une porte de Pauli lors de sa transmission. On sépare les cas où cette porte est X, Z et le mélange probabiliste des deux.

2.4.2.1.1 Canal à inversion-de-bit (d=2) (« bit-flip »)

Comme son équivalent classique, le canal à inversion-de-bit quantique de paramètre p_X est un canal agissant sur un qubit et ayant probabilité p_X de transformer $|0\rangle$ en $|1\rangle$ et vice versa. Par linéarité, $\alpha|0\rangle + \beta|1\rangle$ devient $\alpha|1\rangle + \beta|0\rangle$ avec probabilité p_X et demeure inchangé sinon. Il peut être causé par une interaction avec l'environnement qui inverse la valeur du bit (en appliquant X).

Définition 41. *Le canal à inversion-de-bit est défini par :*

$$\mathcal{C}_{inversion}(p_X, \rho) = p_X X\rho X + (1 - p_X)\rho$$

2.4.2.1.2 Canal déphasant (d=2) (aussi inversion-de-phase, ou bien « phase-flip »)

Sans homologue classique, le canal déphasant de paramètre p_Z agit aussi sur un qubit, mais affecte avec probabilité p_Z la différence de phase entre $|0\rangle$ et $|1\rangle$ en la décalant d'une demi-période, c'est-à-dire d'un facteur $e^{i\pi} = -1$. En plus de pouvoir être causé par une interaction avec l'environnement, le déphasage peut être dû expérimentalement par l'imprécision lors de la correction du décalage de phase intrinsèque à un système dont les niveaux d'énergie sont différents (voir l'annexe I).

Définition 42. *Le canal déphasant est défini par :*

$$\mathcal{C}_{déphasant}(p_Z, \rho) = p_Z Z\rho Z + (1 - p_Z)\rho$$

De manière générale, un bruit de Pauli quelconque est défini en fonctions des paramètres $\{p_X,\ p_Y,\ p_Z\}$, où p_Y est la probabilité que les erreurs X et Z surviennent simultanément.

2.4.2.1.3 Canal dépolarisant

Le canal dépolarisant est le modèle de bruit le plus simple et le plus répandu (avec le canal à effacement, que l'on introduit subséquemment à la sous-section 2.4.2.3). Il correspond au bruit de Pauli dont les trois probabilités $\{p_{\mathsf{X}},\ p_{\mathsf{Y}},\ p_{\mathsf{Z}}\}$ sont égales (et dont la somme $p_{\mathsf{X}}+p_{\mathsf{Y}}+p_{\mathsf{Z}} \leq \frac{3}{4}$). Soit $P = \frac{4}{3}(p_{\mathsf{X}}+p_{\mathsf{Y}}+p_{\mathsf{Z}})$, alors le canal dépolarisant de facteur dépolarisant P remplace avec probabilité P tout état par l'état complètement mélangé de dimension correspondante. Il peut être défini sur un espace d-dimensionnel quelconque.

Définition 43. *Le canal dépolarisant est défini par :*

$$\mathcal{C}_{dépolarisant}(P,\rho) = P\pi + (1-P)\rho$$

2.4.2.2 Bruits composés d'unitaires mélangés

Les canaux composés d'unitaires mélangés sont des canaux qui appliquent un opérateur unitaire U_i choisi au hasard avec probabilité p_i parmi un ensemble d'unitaires $\{\mathsf{U}_i\}$. On peut les voir comme étant le résultat de l'action d'un environnement inconnu.

Définition 44. *Les canaux composés d'unitaires mélangés sont définis par :*

$$\mathcal{C}_{u.\text{-}m.}(p,\rho) = \sum_i p_i \mathsf{U}_i \rho \mathsf{U}_i^\dagger$$

Ces canaux sont une sous-classe des canaux unitaux, puisque

$$\sum_i p_i \mathsf{U}_i \mathsf{U}_i^\dagger = I$$

Les bruits de Pauli appartiennent au groupe des bruits composés d'unitaires mélangés.

2.4.2.3 Canal à effacement

L'effacement d'un état quantique est la perte complète de cet état et l'avis de cette perte. Expérimentalement, il pourrait par exemple survenir dans une expérience physique

lorsque aucun des détecteurs de photons ne détecte le photon attendu. L'état quantique du photon ainsi effacé est alors nécessairement perdu.

Définition 45. *Soit $|1\rangle_E$ le résultat correspondant à l'effacement, le canal à effacement est défini par :*

$$\mathcal{C}^A_{effacement}(p_e, \rho) = p_e\,|1\rangle\langle 1|_E \otimes \pi_A + (1-p_e)\,|0\rangle\langle 0|_E \otimes \rho_A$$

Le registre de sortie est ici accompagné de l'état $|0\rangle\langle 0|_E$ ou $|1\rangle\langle 1|_E$, lesquels annoncent respectivement la transmission réussie de l'état quantique ou son effacement. Le canal à effacement est un bon exemple de canal dont le registre de sortie est de dimension supérieure à celui d'entrée. Lorsque Bob peut valider (par communication classique) la réception réussie à Alice et que l'usage répété du canal est possible, le canal à effacement est le canal bruité pour lequel la téléportation est la plus utile. On voit pourquoi à la sous-section 3.1.9

2.4.2.4 Canal atténuant l'amplitude (« amplitude damping »)

L'atténuation d'amplitude est un bruit très courant lors d'expériences physiques. Elle dépend directement de la façon dont est encodé le qubit. Par exemple, si $|1\rangle$ correspond à la présence d'un photon et $|0\rangle$ à son absence, alors il y a perte d'amplitude quand le photon se perd dans l'environnement. Un autre exemple est celui d'un système à deux niveaux d'énergie. Si $|0\rangle$ est le niveau fondamental d'un électron et $|1\rangle$ son niveau excité, alors lors de l'émission spontanée l'électron retombe au niveau fondamental en émettant un photon qu'on ne détecte (probablement) pas. Dans un tel cas, on assiste aussi à une perte d'amplitude.

Définition 46. *Le canal atténuant l'amplitude est défini par :*

$$\mathcal{C}_{\text{atténuant-amplitude}}(p, \rho) = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \rho \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} + \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix} \rho \begin{pmatrix} 0 & 0 \\ \sqrt{p} & 0 \end{pmatrix}$$

Le canal atténuant l'amplitude n'est pas unital : il y a asymétrie entre $|0\rangle \leftrightarrow |1\rangle$ et l'état complètement mélangé ne reste pas complètement mélangé. La façon la plus simple de le voir est de constater que dans la limite où l'on utilise le canal en série $n \to \infty$ fois, on se retrouve avec l'état pur $|0\rangle$ peu importe l'état d'entrée.

2.4.3 Mesurer la qualité d'un canal de transmission

Intuitivement, on peut juger de la qualité d'une canal de transmission en comparant l'état à l'entrée et l'état à la sortie. Plus ces deux états sont similaires, meilleur est le canal. Cette ressemblance (ou différence) se formalise par la notion mathématique de distance et on peut définir celle-ci de plusieurs manières. On introduit ici les distances appelées fidélité, fidélité espérée et fidélité d'intrication et on voit pourquoi ces deux dernières sont appropriées à l'étude du bruit dans l'intrication. On finit en en précisant des bornes intéressantes, telle la limite supérieure que l'on peut atteindre sans intrication.

La fidélité F est une mesure de distance entre deux états quantiques. Elle a comme image $[0,1]$. On la définit d'abord comme une distance entre deux mélanges statistiques et on donne ensuite les cas particuliers lorsqu'un ou tous les arguments sont des états purs.

Définition 47. *La fidélité entre ρ et σ, deux états quantiques représentés par des matrices densité, est donnée par*[8] *:*

$$F(\rho,\sigma) := \left(\operatorname{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2$$

Cette expression est dure à manipuler et lorsque c'est possible, on privilégie les deux formes suivantes.

Définition 48. *Si on peut exprimer ρ comme un état pur, alors la fidélité entre $\rho = |\psi\rangle\langle\psi|$ et σ se simplifie et la fidélité s'exprime :*

$$F(|\psi\rangle,\sigma) = \langle\psi|\,\sigma\,|\psi\rangle$$

[8] Il faut être prudent. Parfois on définit la fidélité comme la racine carrée de la fidélité ici définie (par exemple dans [28]).

Définition 49. *Si on peut exprimer ρ et σ comme des états purs, alors la fidélité entre $\rho = |\psi\rangle\langle\psi|$ et $\sigma = |\phi\rangle\langle\phi|$ devient simplement la norme de leur produit scalaire.*

$$F\left(|\psi\rangle, |\phi\rangle\right) = |\langle\psi|\phi\rangle|^2$$

Les formules précédentes nous informent sur la similitude entre deux états quantiques. Pour étendre cette notion de fidélité à un canal, on compare l'état ρ à l'entrée et l'état $\mathcal{C}(\rho)$ à la sortie en posant $\sigma = \mathcal{C}(\rho)$ dans les trois définitions précédentes. Une difficulté que l'on rencontre alors est que la fidélité dépend du choix de l'état ρ à l'entrée et qu'on ne peut pas poser directement $F_{\mathcal{C}} := F(\rho, \mathcal{C}(\rho))$.

Exemple 3. *Si on prend le canal à inversion-de-bit, $F(|0\rangle, \mathcal{C}_{inversion}(p, |0\rangle)) = 1 - p$, mais $F(|+\rangle, \mathcal{C}_{inversion}(p, |+\rangle)) = 1$.*

Comment alors définir $F_{\mathcal{C}}$? Une solution est de prendre la fidélité moyenne sur tous les états purs de la dimension appropriée lorsqu'ils sont distribués uniformément (formellement, on effectue cette intégration par rapport à la mesure de Haar [4]).

Définition 50. *La fidélité espérée d'un canal de transmission quantique est donnée par :*

$$\bar{F}_{\mathcal{C}} := \int_{\forall \mathsf{U}} F(\mathsf{U}|0\rangle, \mathcal{C}(\mathsf{U}|0\rangle)) d\mathsf{U}$$

Une autre solution est de prendre un état précis comme référence : l'état maximalement intriqué. Ce qu'on mesure alors est la capacité d'un canal à transférer l'intrication. Comme la qualité de l'intrication est ce qui limite théoriquement celle de la téléportation quantique (l'information classique peut-être répétée et donc être prise arbitrairement bonne et en théorie les manipulations locales quantiques peuvent être sans défaut) et que la téléportation quantique permet de communiquer n'importe quel état quantique, la capacité à bien envoyer un état intriqué implique celle à transférer de manière fidèle toute l'information quantique d'un état. On appelle cette mesure de distance la fidélité d'intrication.

Définition 51. *La fidélité d'intrication F_{intr} d'un canal $\mathcal{C}^A$ appartenant à Alice est définie*

comme :

$$F_{intr}\left(\mathcal{C}^A\right) := F\left(|\phi^+\rangle\langle\phi^+|_{AB}, (\mathcal{C}^A \otimes I_B)(|\phi^+\rangle\langle\phi^+|_{AB})\right) = \langle\phi^+|_{AB}(\mathcal{C}^A \otimes I_B)(|\phi^+\rangle\langle\phi^+|_{AB})|\phi^+\rangle_{AB}$$

Bob n'est ici qu'un outil pour mesurer la fidélité d'intrication.

On peut également exprimer cette fidélité directement avec les opérateurs de Kraus.

Définition 52. *Soit $\mathcal{C}^A$ un canal quantique agissant sur des états de dimension d et soit $\{\mathsf{A}_i\}$ ses opérateurs de Kraus, alors la fidélité d'intrication de $\mathcal{C}^A$ est donnée par :*

$$F_{intr}\left(\mathcal{C}^A\right) = \sum_i |\operatorname{tr}(\pi_A \mathsf{A}_i)|^2 = \sum_i \frac{1}{d^2} |\operatorname{tr}(\mathsf{A}_i)|^2 \tag{2.2}$$

On a invoqué la téléportation précédemment pour justifier l'utilisation de la fidélité d'intrication comme indice du transfert correct de l'information quantique. En fait, on peut affermir cet argument.

Proposition 7. *La fidélité d'intrication est une borne inférieure sur la capacité d'un canal à envoyer l'information quantique.*

$$\forall \rho,\ F_{intr}\left(\mathcal{C}^A\right) \leq F\left(\rho, \mathcal{C}^A(\rho)\right)$$

Démonstration. La preuve est faite dans l'ouvrage de référence de Mark M. Wilde [42]. ■

Bornée inférieurement un canal quantique est pertinent puisqu'en général Bob ne sait pas quel état Alice va lui envoyer.

Finalement, la fidélité espérée et la fidélité d'intrication sont quantitativement équivalentes et on peut facilement passer de l'une à l'autre.

Proposition 8. *Pour un canal quantique dont l'état à l'entré et à la sortie sont de dimension d, la fidélité espérée et la fidélité d'intrication sont reliées par l'égalité*

suivante :

$$\bar{F}_{\mathcal{C}} = \frac{d \cdot F_{intr}\left(\mathcal{C}^{A}\right) + 1}{d+1}$$

Somme toute, on utilise surtout la fidélité d'intrication puisqu'elle est plus facile à manipuler : elle ne requiert pas de faire la moyenne sur tous les états purs possibles.

Une borne significative dans le contexte de téléportation quantique est la limite supérieure classique. C'est la fidélité espérée de l'état obtenu quand Alice mesure simplement l'état dans une base uniformément aléatoire commune à Bob et qu'elle lui communique le résultat par voie classique afin qu'il recrée une (pâle) copie de l'état[9]. Alice et Bob ne peuvent faire mieux sans partage d'intrication.

Proposition 9. *La borne supérieure pour la fidélité espérée d'un état téléporté classiquement est donnée par :*

$$\bar{F}^{classique} \leq \frac{2}{3}$$

La borne classique pour la fidélité d'intrication s'obtient à partir de ce résultat en appliquant la proposition 8.

Proposition 10. *La borne supérieure pour la fidélité d'intrication d'un état téléporté classiquement est donnée par :*

$$F_{intr}^{classique} \leq \frac{1}{2}$$

Bien qu'on appelle par abus de langage *téléportation quantique* dans ce travail toute *tentative* de téléportation quantique, il faut au moins battre cette borne pour réellement parler de téléportation quantique.

Une dernière valeur à laquelle il peut être intéressant de se comparer est la fidélité d'intrication d'un canal complètement dépolarisant et dont la sortie est donc purement aléatoire.

[9] C'est la variante-téléportation du résultat bien connu sur la borne supérieure de la fidélité lors d'un pseudo-clonage quantique local, lequel est énoncé par exemple dans [15].

Proposition 11. *La fidélité d'intrication d'un canal dont la sortie est l'état complètement mélangé est donnée par :*

$$F_{intr}^{aléatoire} = \frac{1}{4}$$

CHAPITRE 3

EFFET DE L'INTRICATION BROUILLÉE SUR LA TÉLÉPORTATION QUANTIQUE

Redline on the transporter, Mister Scott !
— Technicien du *USS Enterprise*, peu avant une téléportation particulièrement brouillée *[31]*.

Il est maintenant temps d'aborder notre sujet principal : la téléportation quantique. On commence par expliquer ce qu'on appelle *téléportation quantique*, puis on se penche sur l'effet de l'intrication brouillée pour trois protocoles : la téléportation standard (l'originale de 1993 [9]), la téléportation standard avec relais quantiques et la téléportation multi-ports (« port-based teleportation »). Sauf brièvement à la fin de la section sur la téléportation standard, on se concentre exclusivement sur la téléportation d'un seul qubit.

3.1 Téléportation quantique standard

On débute en clarifiant la notion générale de téléportation quantique, puis on donne un protocole formel pour la téléportation quantique standard à un qubit et on s'attaque à l'effet du bruit dans l'intrication en considérant différents scénarios. On limite d'abord la gamme de bruits à des bruits agissant localement simplement sur la moitié intriquée de Bob (la sortie du téléporteur) et on constate que ces bruits commutent avec l'opération de téléportation seulement dans le cas des bruits de Pauli. Ensuite, on généralise notre modèle en permettant des bruits locaux aussi du côté de la moitié intriquée d'Alice. La propriété 1 non-locale d'une transformation unitaire sur une paire EPR, telle que décrite à la sous-section 2.1.6, permet d'étendre les conclusions précédentes dans le cas où le bruit chez Alice est unital et indépendant de celui de Bob. Pour les cas plus généraux (bruit non-unital local chez Alice et bruit potentiellement non-local Alice-Bob), on a recours à la technique de la wernerisation pour effectuer l'analyse et quantifier de manière pratique

la qualité des canaux de téléportation. On examine aussi l'effet du canal à effacement. Enfin, on fait un bref tour des effets de l'intrication brouillée lorsque l'on généralise la téléportation quantique standard à un plus grand nombre de dimensions.

Cette section est surtout une synthèse, et même si l'approche de modélisation utilisée est originale, tous les protocoles mentionnés, ainsi que la majorité des exemples et propositions que l'on présente, n'est pas nouvelle. La sous-section 3.1.4, ainsi que les propositions 21 et 22, sont originaux et font donc exception. On mentionne au fur et à mesure nos références pour les idées que l'on emprunte qui ne découlent pas naturellement du formalisme de l'informatique quantique, la paternité des résultats très directs étant ambiguë.

3.1.1 Qu'est-ce que la téléportation quantique

Le mot « téléportation », très populaire en science-fiction, peut évoquer plusieurs concepts différents. Il est donc important de préciser ce que l'on entend ici par téléportation, de même que ce que l'on n'entend pas ! La téléportation quantique [9] est un protocole de transfert d'information quantique qui respecte la loi de la conservation de l'énergie, demande le partage préalable d'intrication et ne contredit pas la théorie de la relativité restreinte. Elle ne dit rien sur l'état téléporté[1] et ne permet pas le clonage quantique.

Alors premièrement, lors de la téléportation quantique, ce qui est téléporté est l'information quantique d'un système. Ce n'est donc ni la matière, ni l'énergie. Le système d'arrivée peut même être de nature différente de celui de départ, en autant qu'il puisse contenir la même information quantique. Ainsi, on ne téléporte pas un photon, mais plutôt une certaine caractéristique de ce photon, comme sa polarisation ou l'information de son existence ou non-existence (dans ce cas une source d'énergie au point d'arrivée est nécessaire). Rien n'empêche cependant, du moins en théorie, de téléporter toutes les

[1] On verra des cas où la présence de bruit infirme cette propriété.

caractéristiques non-spatiales d'un photon vers un autre photon. On pourrait alors dire qu'on a téléporté un photon sans faire d'abus de langage.

Deuxièmement, la téléportation quantique nécessite une préparation : le partage d'une ressource commune. Alice doit au début du protocole avoir à sa disposition un état intriqué avec celui de Bob. Après le début de la procédure de téléportation, on peut resserrer les contraintes et n'autoriser que les opérations quantiques qui sont locales (sans restreindre la communication classique). Envoyer physiquement un état quantique n'est donc pas de la téléportation.

Troisièmement, lors du protocole, Alice doit envoyer de l'information classique à Bob. Avant de recevoir cette information classique cruciale, Bob n'a en ses mains rien de mieux qu'un état complètement mélangé. C'est cette condition qui empêche la communication supraluminique. En effet, l'information classique chemine à une vitesse au mieux égale à celle de la lumière et cela limite la vitesse de la téléportation. La téléportation quantique n'est donc pas instantanée.

Quatrièmement, dans le cas idéal, le résultat de la téléportation est le même peu importe l'état téléporté par Alice. Alice n'a pas à connaître ce qu'elle envoie et n'apprend rien après coup. En d'autres mots, Alice n'envoie pas par le canal classique la description de son état quantique. La téléportation quantique n'est pas une télécopie.

Cinquièmement, l'état téléporté n'est jamais à deux endroits en même temps. En effet, pour obtenir les bits classiques nécessaires à la réapparition de l'état quantique ρ chez Bob, Alice doit faire une mesure qui détruit l'état ρ. L'état est inexistant le temps que l'information classique chemine d'Alice à Bob.

Finalement pour résumer, voici la forme générale[2] d'un protocole de téléportation

[2]Cette forme n'est pas totalement générale, puisqu'elle se restreint aux protocoles sans communication de Bob vers Alice. On transcendera parfois ce modèle en permettant l'usage de communication de Bob vers

quantique. Il s'applique aussi bien à la téléportation quantique standard qu'à celle multi-ports.

Protocole (Téléportation quantique générale — description de haut-niveau)**.**

0. *Alice et Bob partagent un état intriqué sur le registre AB. Alice possède aussi dans le registre C un état ρ qu'elle veut téléporter à Bob.*

1. *Alice fait une mesure conjointe locale sur le système CA. Elle détruit ainsi son état quantique ρ et obtient de l'information classique qu'elle envoie à Bob.*

2. *Lors de la réception de cette information classique, Bob fait une opération quantique sur son état et récupère ρ.*

3.1.2 Protocole à un qubit sans bruit

On présente de manière formelle le protocole idéal de téléportation quantique standard pour un seul qubit [9], dans sa version utilisant $|\phi^+\rangle$ comme ressource[3]. Même si l'on ne traite qu'un seul qubit, le modèle est universel au niveau dimensionnel puisque l'on peut l'appliquer en parallèle pour envoyer tout état quantique de dimension supérieure. On se limite pour l'instant à des bruits qui ne changent pas la dimension de l'état envoyé. Le protocole suivant est illustré à la figure 3.1.

Protocole 1. *Alice désire envoyer le qubit quelconque $|\psi\rangle_C$ à Bob. Alice et Bob partagent une paire intriquée $|\phi^+\rangle_{AB}$.*

Alice, notamment pour combattre le bruit d'effacement à la sous-section 3.2.3 sur les relais quantiques.

[3]Les protocoles idéaux consommant un autre des quatre états de Bell s'obtiennent aisément à partir de celui-ci : il suffit d'appliquer une des matrices de Pauli à l'entrée du téléporteur, pré-téléportation ; ou bien à sa sortie, post-téléportation.

1. *Formellement (on fait parfois l'ellipse des symboles précisant les registres pour alléger la notation) :*

$$
\begin{aligned}
&|\psi\rangle_C |\phi^+\rangle_{AB} \\
&= (\alpha|0\rangle_C + \beta|1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \\
&= \frac{\alpha}{\sqrt{2}}|00\rangle_{CA}|0\rangle_B + \frac{\alpha}{\sqrt{2}}|01\rangle_{CA}|1\rangle_B + \frac{\beta}{\sqrt{2}}|10\rangle_{CA}|0\rangle_B + \frac{\beta}{\sqrt{2}}|11\rangle_{CA}|1\rangle_B \\
&= \alpha\left(\frac{|\phi^+\rangle + |\phi^-\rangle}{2}\right)|0\rangle + \alpha\left(\frac{|\psi^+\rangle + |\psi^-\rangle}{2}\right)|1\rangle + \beta\left(\frac{|\psi^+\rangle - |\psi^-\rangle}{2}\right)|0\rangle + \beta\left(\frac{|\phi^+\rangle - |\phi^-\rangle}{2}\right)|1\rangle \\
&= \big(|\phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) + |\psi^+\rangle(\beta|0\rangle + \alpha|1\rangle) + |\psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle)\big)/2 \\
&= \big(|\phi^+\rangle_{CA}|\psi\rangle_B + |\phi^-\rangle_{CA}(\mathsf{Z}|\psi\rangle_B) + |\psi^+\rangle_{CA}(\mathsf{X}|\psi\rangle_B) + |\psi^-\rangle_{CA}(\mathsf{XZ}|\psi\rangle_B)\big)/2
\end{aligned}
$$

2. *Alice effectue une mesure projective de ses 2 qubits dans la base de Bell et en communique le résultat à Bob, lequel effectue une correction y correspondant. Cela complète le protocole de téléportation. Le résultat final est donné dans le tableau 3.I suivant, où chaque ligne est équiprobable.*

Résultat classique d'Alice	État quantique « instantané » de Bob	Correction effectuée par Bob	État quantique final de Bob
ϕ_A^+	$\|\psi\rangle_B$	I	$\|\psi\rangle_B$
ϕ_A^-	$\mathsf{Z}\|\psi\rangle_B$	Z	$\|\psi\rangle_B$
ψ_A^+	$\mathsf{X}\|\psi\rangle_B$	X	$\|\psi\rangle_B$
ψ_A^-	$\mathsf{ZX}\|\psi\rangle_B$	XZ	$\|\psi\rangle_B$

Tableau 3.I – Résultat chez Bob, conditionné sur le résultat de la mesure d'Alice, de la téléportation quantique standard consommant $|\phi^+\rangle_{AB}$, en l'absence de bruit. Avant de recevoir l'information d'Alice, l'état de Bob est complètement mélangé. À la fin, l'état de Bob est toujours exactement l'état initial $|\psi\rangle$ d'Alice. Ce résultat est celui de la téléportation d'un état pur, mais il s'étend, par linéarité, à un mélange statistique.

Par linéarité on peut sans perdre de généralité utiliser le protocole pour téléporter un mélange statistique ρ plutôt qu'un état pur $|\psi\rangle$.

La téléportation est donc une opération qui permet de transférer un état quantique d'un registre à un autre en utilisant une paire intriquée (et l'envoi/réception de 2 bits d'information classique). On écrira ainsi :

$$\mathcal{C}^{CAB\to B}_{\text{téléportation}}(\cdot\otimes|\Phi^+_{AB}\rangle)\sim\mathcal{C}^{C\to B}_{\text{identité}}(\cdot)$$

tout en gardant en tête que les restrictions qui accompagnent la non-localité de la téléportation (pas de communication supraluminique) s'appliquent aussi au canal identité du deuxième cas.

L'extension du protocole à d>2 est directe, puisque l'on peut encoder tout qudit en $\lceil \log d \rceil$ qubits et téléporter ces qubits en parallèle à la place [9].

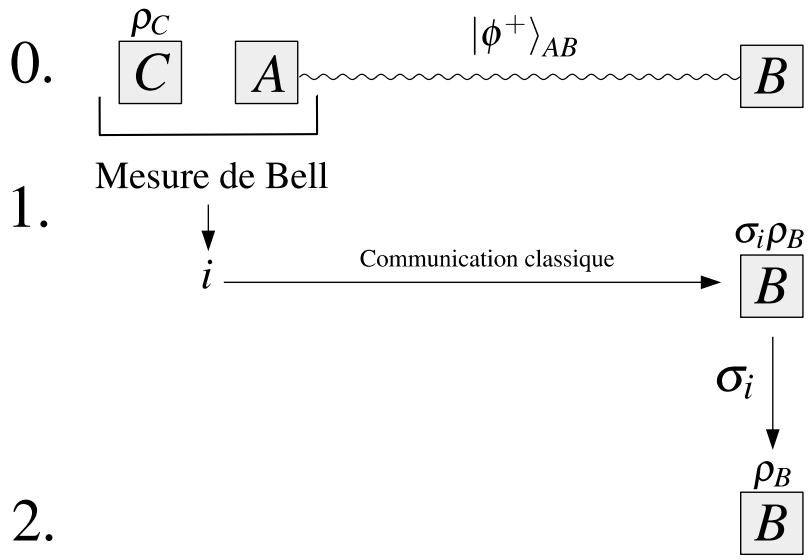

Figure 3.1 – Protocole de téléportation quantique standard du qubit ρ_C de Alice vers Bob. Alice et Bob partagent initialement un état intriqué $|\phi^+\rangle_{AB}$. Puis, Alice fait une mesure dans la base de Bell de ses qubits A et C. Elle en communique le résultat à Bob qui effectue l'opération de Pauli correspondante sur ce qui était sa moitié intriquée. Il retrouve alors ρ_B.

3.1.3 Effet du bruit chez Bob

On va commencer par étudier l'effet de l'intrication brouillée lorsque seule la moitié de Bob est brouillée. Cela peut survenir physiquement dans le cas où Alice se charge de générer l'intrication et qu'elle le fait de manière parfaite, mais que l'envoi de cette intrication à Bob est fautif. Un autre cas est celui où la mémoire quantique de Bob est de moins bonne qualité que celle d'Alice et où son intrication se dégrade alors beaucoup plus rapidement (peut-être qu'il fait significativement plus froid chez Alice). On modélise le canal de téléportation représentant ces scénarios d'intrication brouillée ainsi :

$$\mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ \left(\mathcal{C}^{A}_{\text{identité}} \otimes \mathcal{C}^{B}_{\text{brouillé}}\right)$$

En somme, on considère pour l'instant que l'intrication entre Alice et Bob est réalisée en premier lieu de manière parfaite, puis que la moitié de Bob passe dans un canal brouillé indépendant tandis que la moitié d'Alice est non-affectée. La téléportation est effectuée de manière standard par la suite. Cela se traduit par le nouveau protocole ci-dessous.

Protocole 2. *Alice désire toujours envoyer le qubit quelconque $|\psi\rangle_C$ à Bob. Cette fois, Alice et Bob partagent une paire intriquée qui est brouillée du côté de Bob par $\left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)(|\phi^+\rangle_{AB})$.*

1. *Formellement :*

$$\begin{aligned}
&(\mathcal{C}^{CA}_{identité} \otimes \mathcal{C}^{B}_{brouillé})(|\psi\rangle_C |\phi^+\rangle_{AB}) \\
&= (\mathcal{C}^{CA}_{identité} \otimes \mathcal{C}^{B}_{brouillé})(|\phi^+\rangle_{CA} |\psi\rangle_B + |\phi^-\rangle_{CA} (\mathsf{Z}|\psi\rangle_B) + |\psi^+\rangle_{CA} (\mathsf{X}|\psi\rangle_B) + |\psi^-\rangle_{CA} (\mathsf{XZ}|\psi\rangle_B))/2 \\
&= (|\phi^+\rangle_{CA} \mathcal{C}^{B}_{brouillé}(|\psi\rangle_B) + |\phi^-\rangle_{CA} \mathcal{C}^{B}_{brouillé}(\mathsf{Z}|\psi\rangle_B) \\
&\qquad\qquad + |\psi^+\rangle_{CA} \mathcal{C}^{B}_{brouillé}(\mathsf{X}|\psi\rangle_B) + |\psi^-\rangle_{CA} \mathcal{C}^{B}_{brouillé}(\mathsf{XZ}|\psi\rangle_B))/2
\end{aligned}$$

2. *Alice effectue une mesure projective de ses 2 qubits dans la base de Bell et en communique le résultat à Bob, lequel effectue la même correction qu'il aurait faite dans le cas sans bruit. L'état qu'obtient au final Bob est donné au tableau 3.II.*

Résultat classique d'Alice	État quantique « instantané » de Bob	Correction effectuée par Bob	État quantique final de Bob
ϕ_A^+	$\mathcal{C}^B_{\text{brouillé}}(\|\psi\rangle_B)$	I	$\mathcal{C}^B_{\text{brouillé}}(\|\psi\rangle_B)$
ϕ_A^-	$\mathcal{C}^B_{\text{brouillé}}(\mathsf{Z}\|\psi\rangle_B)$	Z	$\mathsf{Z}\circ\mathcal{C}^B_{\text{brouillé}}(\mathsf{Z}\|\psi\rangle_B)$
ψ_A^+	$\mathcal{C}^B_{\text{brouillé}}(\mathsf{X}\|\psi\rangle_B)$	X	$\mathsf{X}\circ\mathcal{C}^B_{\text{brouillé}}(\mathsf{X}\|\psi\rangle_B)$
ψ_A^-	$\mathcal{C}^B_{\text{brouillé}}(\mathsf{ZX}\|\psi\rangle_B)$	XZ	$\mathsf{XZ}\circ\mathcal{C}^B_{\text{brouillé}}(\mathsf{ZX}\|\psi\rangle_B)$

Tableau 3.II – Résultat, conditionné sur le résultat de la mesure d'Alice, de la téléportation quantique standard consommant $|\phi^+\rangle$, en présence d'un bruit uniquement chez Bob. Avant de recevoir l'information d'Alice, l'état de Bob est complètement mélangé peu importe le bruit. À la fin, l'état de Bob dépend du résultat d'Alice, contrairement au cas idéal. Ce résultat est celui de la téléportation d'un état pur, mais il est également valide, par linéarité, pour tout mélange statistique.

On peut l'expliciter à l'aide du formalisme de Kraus, où $\{\mathsf{A}_i\}$ représentent le canal brouillé. C'est fait au tableau 3.III.

Résultat classique d'Alice	État quantique final de Bob
ϕ_A^+	$\sum_i \mathsf{A}_i\|\psi\rangle\langle\psi\|\mathsf{A}_i^\dagger$
ϕ_A^-	$\sum_i \mathsf{ZA}_i\mathsf{Z}\|\psi\rangle\langle\psi\|\mathsf{ZA}_i^\dagger\mathsf{Z}$
ψ_A^+	$\sum_i \mathsf{XA}_i\mathsf{X}\|\psi\rangle\langle\psi\|\mathsf{XA}_i^\dagger\mathsf{X}$
ψ_A^-	$\sum_i \mathsf{XZA}_i\mathsf{ZX}\|\psi\rangle\langle\psi\|\mathsf{XZA}_i^\dagger\mathsf{ZX}$

Tableau 3.III – Expression dans le formalisme de Kraus du résultat de la téléportation quantique standard consommant $|\phi^+\rangle$, en présence d'un bruit uniquement chez Bob. Le résultat final varie selon le résultat de la mesure d'Alice.

Proposition 12. *Le canal résultant est donc dans la représentation de Kraus de la forme :*

$$\mathcal{C}^{CAB\to B}_{\textit{téléportation}}\circ\left(\mathcal{C}^A_{\textit{identité}}\otimes\mathcal{C}^B_{\textit{brouillé}}\right)(\cdot)=\sum_i(\sigma_j\mathsf{A}_i\sigma_j)(\cdot)(\sigma_j\mathsf{A}_i^\dagger\sigma_j)\ \textit{où}\ \sigma_j\in\{I,\mathsf{X},\mathsf{Z},\mathsf{XZ}\}$$

σ_j est connu a posteriori, mais uniformément aléatoire a priori.

Proposition 13. *On note que dans le cas général :*

$$\mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right) \nsim \mathcal{C}^{C\to B}_{brouillé}(\cdot)$$

Démonstration. Soit $\mathcal{C}^{B}_{\text{brouillé}}(\cdot) = \mathsf{H}(\cdot)\mathsf{H}$ et $|\psi\rangle = |0\rangle$, alors $\mathcal{C}^{B}_{\text{brouillé}}(|\psi\rangle) = \mathsf{H}|0\rangle = |+\rangle$, mais $\mathsf{Z}\cdot\mathcal{C}^{B}_{\text{brouillé}}(|\psi\rangle)\cdot\mathsf{Z} = \mathsf{ZHZ}|0\rangle = |-\rangle$. ■

Soit le scénario suivant : Alice veut envoyer un qubit à Bob, elle dispose d'un canal brouillé vers Bob et celui-ci n'affecte pas la dimension de l'état qui le traverse. On se demande si elle devrait téléporter son qubit en expédiant un qubit maximalement intriqué à travers le canal, ou plutôt envoyer directement son qubit. On s'intéresse ainsi à la fidélité de l'état quantique avant et après la traversée. On pourrait croire que celle-ci demeure la même dans les deux cas, mais c'est faux.

Proposition 14. *La fidélité d'un état quantique ρ peut varier selon si Alice l'envoie directement par le canal brouillé $\mathcal{C}^{B}_{brouillé}$ ou si elle l'envoie plutôt par le canal de téléportation brouillée $\mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)$.*

$$\forall \alpha \in [0,1],\ F\left(\rho, \mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)(\rho)\right) \geq \alpha \not\Rightarrow F\left(\rho, \mathcal{C}^{B}_{brouillé}(\rho)\right) \geq \alpha$$

La réciproque est également fausse :

$$\forall \alpha \in [0,1],\ F\left(\rho, \mathcal{C}^{B}_{brouillé}(\rho)\right) \geq \alpha \not\Rightarrow F\left(\rho, \mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)(\rho)\right) \geq \alpha$$

Démonstration. On exhibe un contre-exemple au premier énoncé. Soit $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{i\sqrt{3}}{2}|1\rangle$, $\mathcal{C}(\rho) = \mathsf{U}\rho\mathsf{U}^{\dagger}$ et $\mathcal{C}'(\rho) = \mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ \left(\mathcal{C}^{A}_{\text{identité}} \otimes \mathcal{C}^{B}\right)(\rho)$, avec $\mathsf{U} = \begin{pmatrix} \frac{1}{2} & \frac{i\sqrt{3}}{2} \\ \frac{-i\sqrt{3}}{2} & \frac{-1}{2} \end{pmatrix}$:

$$\mathcal{C}(|\psi\rangle) = \mathsf{U}|\psi\rangle = \frac{1}{2}|0\rangle + \frac{i\sqrt{3}}{2}|1\rangle = |\psi\rangle \quad \longrightarrow \quad F(|\psi\rangle, \mathcal{C}(|\psi\rangle)) = |\langle\psi|\psi\rangle|^2 = 1$$

$$\mathcal{C}'(|\psi\rangle)\Big|_{\substack{\text{résultat} \\ \text{d'Alice}=\phi^-}} = \mathsf{ZUZ}|\psi\rangle = |0\rangle \quad \longrightarrow \quad F(|\psi\rangle, \mathcal{C}(|\psi\rangle))\Big|_{\substack{\text{résultat} \\ \text{d'Alice}=\phi^-}} = |\langle 0|\psi\rangle|^2 = \frac{1}{4}$$

Si Alice obtient le résultat ϕ^- lors de sa mesure de Bell, le canal de téléportation ne transfère pas fidèlement l'état $|\psi\rangle$, alors que celui-ci est parfaitement transmis si Alice l'envoie directement (ou qu'elle mesure ϕ^+). Conditionner sur le résultat d'Alice n'est toutefois pas nécessaire pour démontrer la proposition, puisque les quatre résultats sont équiprobables et que la fidélité est bornée supérieurement par 1. Comme la fidélité conditionnée sur le résultat ϕ^- est plus petite que 1, alors la fidélité non-conditionnée l'est évidemment aussi. La réciproque se prouve de la même façon en prenant $|\psi'\rangle = \mathrm{Z}\,|\psi\rangle$. C'est alors le canal n'utilisant pas la téléportation qui est le moins bon. ■

On a donc montré que selon l'état, utiliser la téléportation est parfois pire, parfois mieux que de faire un envoi direct. Cette variabilité renforce l'idée exprimée à la sous-section 2.4.3 que la fidélité prise telle qu'elle n'est pas une bonne mesure de la qualité d'un canal de transmission. Le problème disparaît si l'on prend la fidélité espérée.

Proposition 15. *La fidélité espérée, lorsque l'on considère uniformément tous les états possibles à l'entrée, est la même pour l'envoi direct d'un qubit à travers $\mathcal{C}^{B}_{brouillé}$ que lors de sa téléportation brouillée $\mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)$.*

$$\bar{F}\left(\mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)\right) = \bar{F}\left(\mathcal{C}^{B}_{brouillé}\right)$$

Démonstration. La distribution est uniforme sur tous les états purs et on a ainsi :

$$\forall\,|\psi\rangle\,,\ \forall i,\ \exists\,|\psi'\rangle = \sigma_i\,|\psi\rangle\,,\ \text{où probabilité}(|\psi'\rangle) = \text{probabilité}(|\psi\rangle)$$

Les deux canaux ont alors une fidélité espérée égale sur tout sous-ensemble $\{|\psi\rangle\,, |\psi'\rangle\}$ de la distribution, et donc sur toute la distribution. ■

Il en suit que la fidélité d'intrication est de la même façon invariante :

Proposition 16. *L'opération de téléportation brouillée conserve la fidélité d'intrication.*

$$F_{intr}\left(\mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)\right) = F_{intr}\left(\mathcal{C}^{B}_{brouillé}\right)$$

Démonstration. Conséquence immédiate de la proposition précédente et de la propriété d'équivalence de la fidélité espérée avec la fidélité d'intrication, telle qu'énoncée à la proposition 8. ■

Cette dernière se calcule directement à l'aide de la formule 2.2 lorsque l'on connaît les opérateurs de Kraus du canal brouillé :

Proposition 17. *La fidélité d'intrication résultant du canal de téléportation brouillé uniquement chez Bob est donnée par l'équation suivante, où* $\{\mathsf{A}_i\}$ *sont les opérateurs de Kraus du bruit* $\mathcal{C}^B_{brouillé}$ *chez Bob.*

$$F_{intr}(\mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^A_{identité} \otimes \mathcal{C}^B_{brouillé}\right)) = \sum_i \frac{1}{4} |\operatorname{tr}(\mathsf{A}_i)|^2$$

3.1.4 Bruit invariant sous téléportation (cas qubit)

On peut se demander quelles conditions imposer sur un canal brouillant l'intrication pour qu'il commute avec l'opération de téléportation. Cette condition se traduit sous forme d'équation par :

$$\mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ \left(\mathcal{C}^A_{\text{identité}} \otimes \mathcal{C}^B_{\text{brouillé}}\right) \sim \mathcal{C}^B_{\text{brouillé}} \circ \mathcal{C}^{CAB\to B}_{\text{téléportation}}$$

L'invariance sous commutation signifie physiquement que la résultat du transfert d'information est exactement le même si le bruit apparaît chez Bob avant ou après la téléportation. Elle implique aussi qu'appliquer le bruit chez Bob est équivalent de l'appliquer directement sur l'état d'Alice à téléporter, pré-téléportation. Cette dernière équivalence se voit en simplifiant le terme de droite de la formule précédente :

$$\mathcal{C}^B_{\text{brouillé}} \circ \mathcal{C}^{CAB\to B}_{\text{téléportation}} \sim \mathcal{C}^B_{\text{brouillé}} \circ \mathcal{C}^{C\to B}_{\text{identité}} \sim \mathcal{C}^{C\to B}_{\text{identité}} \circ \mathcal{C}^C_{\text{brouillé}}$$

Précisément, on recherche la famille de canaux simultanément invariants sous les quatre opérations $\sigma_j(\cdot)\sigma_j$, où $\sigma_j \in \{I, \mathsf{X}, \mathsf{Z}, \mathsf{XZ}\}$. On dit que ces bruits commutent avec la téléportation. Pour trouver cette famille de bruits, on explicite les matrices de Pauli σ_j dans le formalisme de Choi-Jamiołkowski.

$$\mathsf{J}_I := I \otimes I^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathsf{J}_\mathsf{X} := \mathsf{X} \otimes \mathsf{X}^* = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathsf{J}_\mathsf{Y} := (i\mathsf{XZ}) \otimes (i\mathsf{XZ})^* = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathsf{J}_\mathsf{Z} := \mathsf{Z} \otimes \mathsf{Z}^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

On recherche toutes les matrices 4×4 qui commutent avec l'ensemble des canaux de Pauli J_{σ_i} et qui sont elles-mêmes des canaux quantiques dans la représentation de Choi-Jamiołkowski. En partant d'une matrice générale 4×4 et en appliquant les critères de commutativité, on trouve :

$$\text{Soit SPG, } \mathsf{J} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

$$\mathsf{J_Z J J_Z} = \mathsf{J} \Leftrightarrow \begin{pmatrix} a_{11} & -a_{12} & -a_{13} & a_{14} \\ -a_{21} & a_{22} & a_{23} & -a_{24} \\ -a_{31} & a_{32} & a_{33} & -a_{34} \\ a_{41} & -a_{42} & -a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

$$\Rightarrow \mathsf{J} = \begin{pmatrix} a_{11} & 0 & 0 & a_{14} \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ a_{41} & 0 & 0 & a_{44} \end{pmatrix}$$

$$\mathsf{J_X J J_X} = \mathsf{J} \Rightarrow \begin{pmatrix} a_{44} & 0 & 0 & a_{41} \\ 0 & a_{33} & a_{32} & 0 \\ 0 & a_{23} & a_{22} & 0 \\ a_{14} & 0 & 0 & a_{11} \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & 0 & a_{14} \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ a_{41} & 0 & 0 & a_{44} \end{pmatrix}$$

$$\Rightarrow \mathsf{J} = \begin{pmatrix} a_{11} & 0 & 0 & a_{14} \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{23} & a_{22} & 0 \\ a_{14} & 0 & 0 & a_{11} \end{pmatrix}$$

L'équation $\mathsf{J}_I\mathsf{J}\mathsf{J}_I = \mathsf{J}$ est trivialement vraie et la condition $\mathsf{J}_\mathsf{Y}\mathsf{J}\mathsf{J}_\mathsf{Y} = \mathsf{J}$ est respectée lorsque $\mathsf{J}_\mathsf{X}\mathsf{J}\mathsf{J}_\mathsf{X} = \mathsf{J}$ et $\mathsf{J}_\mathsf{Z}\mathsf{J}\mathsf{J}_\mathsf{Z}$ le sont. On trouve maintenant la matrice dynamique D_J afin d'expliciter les contraintes, soit l'hermicité, la positivité complète et la préservation de la trace, pour que J soit un canal quantique

$$\mathsf{D}_\mathsf{J} := \text{brass}^{(2,2)}[\mathsf{J}] = \begin{pmatrix} a_{11} & 0 & 0 & a_{14} \\ 0 & a_{14} & a_{23} & 0 \\ 0 & a_{23} & a_{14} & 0 \\ a_{22} & 0 & 0 & a_{11} \end{pmatrix}$$

On peut décomposer D_J en matrices de Pauli dans la représentation de Choi-Jamiołkowski.

$$\mathsf{D}_\mathsf{J} = \begin{pmatrix} p_I + p_\mathsf{Z} & 0 & 0 & p_I - p_z \\ 0 & p_\mathsf{X} + p_\mathsf{Y} & p_\mathsf{X} - p_\mathsf{Y} & 0 \\ 0 & p_\mathsf{X} - p_\mathsf{Y} & p_\mathsf{X} + p_\mathsf{Y} & 0 \\ p_I - p_z & 0 & 0 & p_I + p_\mathsf{Z} \end{pmatrix} = p_I I + p_\mathsf{X}\mathsf{X} + p_\mathsf{Y}\mathsf{Y} + p_\mathsf{Z}\mathsf{Z}$$

La condition d'hermicité de D_J implique celle de J et impose que $a_{11}, a_{14}, a_{22}, a_{23} \in \mathbb{R}$ et donc que $p_I, p_\mathsf{X}, p_\mathsf{Y}, p_\mathsf{Z} \in \mathbb{R}$ aussi. La préservation de la trace a pour condition $\underset{a,d}{\mathsf{D}_{a,b}} = \delta_{bd}$ et donne que $a_{11} + a_{44} = p_I + p_\mathsf{X} + p_\mathsf{Y} + p_\mathsf{Z} = 1$. Finalement, en manipulant les lignes et colonnes de D_J, on peut trouver ses valeurs propres :

$$\mathsf{D}_\mathsf{J} = \begin{pmatrix} p_I + p_\mathsf{Z} & 0 & 0 & p_I - p_z \\ 0 & p_\mathsf{X} + p_\mathsf{Y} & p_\mathsf{X} - p_\mathsf{Y} & 0 \\ 0 & p_\mathsf{X} - p_\mathsf{Y} & p_\mathsf{X} + p_\mathsf{Y} & 0 \\ p_I - p_z & 0 & 0 & p_I + p_\mathsf{Z} \end{pmatrix} \sim \begin{pmatrix} 2p_\mathsf{Z} & 0 & 0 & p_I - p_\mathsf{Z} \\ 0 & 2p_\mathsf{Y} & p_\mathsf{X} - p_\mathsf{Y} & 0 \\ 0 & 0 & 2p_\mathsf{X} & 0 \\ 0 & 0 & 0 & 2p_I \end{pmatrix}$$

Les valeurs propres de cette dernière matrice triangulaire supérieure sont les éléments de

sa diagonale, soit $\{2p_I, 2p_X, 2p_Y, 2p_Z\}$. Pour que J soit une application complètement positive, les valeurs propres de D doivent être positives ou nulles. On a au final que tout bruit qui commute avec la téléportation peut être décomposé en un mélange convexe des bruits de Pauli (incluant l'identité) dont les probabilités sont positives (ou nulles) et somment à 1. C'est donc exactement la famille des bruits de Pauli décrite à la sous-section 2.4.2.1. En somme, on a démontré ce résultat original :

Théorème 3. *Pour d=2 si l'on ne considère que du bruit local chez Bob*[4]*, seule la famille des bruits de Pauli commute avec la téléportation.*

3.1.5 Effet de bruits locaux chez Alice et chez Bob

Qu'en est-il si l'on rajoute à notre modèle précédent de téléportation pour un qubit du bruit du côté d'Alice avec la condition qu'il soit indépendant de celui chez Bob ? C'est-à-dire dans le cas où :

$$\mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ \left(\mathcal{C}^{A}_{\text{brouillé}} \otimes \mathcal{C}^{B}_{\text{brouillé}'} \right)$$

Physiquement, ce modèle peut représenter une génération correcte d'intrication par un tiers parti (serveur) et son envoi brouillé à Alice et Bob (clients). Il peut aussi représenter le bruit qu'introduit la mise en mémoire de cette intrication chez Alice et chez Bob lorsqu'ils sont distants spatialement dans l'approximation de Markov. On poursuit l'analyse précédente en examinant plusieurs sous-cas.

3.1.5.1 Bruit d'unitaires mélangés et bruit unital chez Alice

On commence par celui où les bruits chez Alice sont composés d'unitaires mélangés. On établit ensuite l'équivalence entre ceux-ci et les bruits unitaux. Puis on regarde l'impact sur la fidélité d'intrication.

[4] On utilise dans ce contexte-ci les termes *local* et *indépendant* de manière interchangeable pour dire que l'état d'Alice n'est pas affecté par le bruit chez Bob.

Si le bruit chez Alice est constitué d'unitaires mélangés, alors la situation peut se ramener au cas précédent où l'on avait du bruit simplement du côté de Bob. On a en effet :

Proposition 18. *Tout bruit local composé d'unitaires mélangés sur le qubit intriqué d'Alice peut être réduit à un bruit local sur le qubit intriqué de Bob. Par exemple, lorsque l'on prend l'état maximalement intriqué $|\phi^+\rangle_{AB}$, si les opérateurs de Kraus appliqués chez Alice sont $\{\sqrt{p_i}\mathsf{U}_i\}$, alors on peut réduire le bruit à celui des opérateurs de Kraus $\{\sqrt{p_i}\mathsf{U}_i^T\}$ appliqués chez Bob.*

Démonstration. En utilisant la propriété 1 vue à la sous-section 2.1.6, on trouve que :

$$\begin{aligned}\mathcal{C}^A_{\text{u.-m.}}\left(|\phi^+\rangle\langle\phi^+|_{AB}\right) &:= \sum_i (\mathsf{U}_i)_A(|\phi^+\rangle\langle\phi^+|_{AB})(\mathsf{U}_i^\dagger)_A \\ &= \sum_i (\mathsf{U}_i^T)_B(|\phi^+\rangle\langle\phi^+|_{AB})(\mathsf{U}_i^*)_B =: \mathcal{C}'^B_{\text{u.-m.}}\left(|\phi^+\rangle\langle\phi^+|_{AB}\right)\end{aligned}$$

On note que $\mathcal{C}'^B_{\text{u.-m.}}(\cdot)$ n'est pas nécessairement égal à $\mathcal{C}^A_{\text{u.-m.}}(\cdot)$, mais qu'il se calcule aisément. ■

L'intrication localement brouillée chez Alice peut donc toujours être vue comme de l'intrication brouillée strictement chez Bob dans le cas où le bruit est un mélange statistique d'opérateurs unitaires. Dans le cas d=2, on peut étendre cette équivalence à tous les canaux unitaux, dont les unitaires mélangés sont un sous-groupe, grâce à la proposition suivante tirée de l'ouvrage de référence de Bengtsson et Życzkowski [7] :

Proposition 19. *Pour d=2, tous les bruits unitaux sont des bruits composés d'unitaires mélangés.*[5]

La réduction précédente peut donc être étendue au cas où le bruit local chez Alice est unital.

Proposition 20. *Tout bruit unital local sur le qubit intriqué d'Alice peut être réduit à un bruit local sur le qubit intriqué de Bob. La réduction se fait de la même manière que*

[5] Cela ne tient plus pour d>2.

celle énoncée à la proposition 18. Il est bien sûr possible d'additionner le bruit local de la réduction à celui déjà présent chez Bob. Les opérateurs de Kraus suite à la réduction passent ainsi de $\{\mathsf{A}_i\}$ *chez Bob et* $\{\sqrt{p_j}\mathsf{U}_j\}$ *chez Alice à* $\{\sqrt{p_j}\mathsf{A}_i\mathsf{U}_j^T\}_{ij}$ *chez Bob (en utilisant* $|\phi^+\rangle_{AB}$ *comme ressource intriquée initiale).*

Cette simplification permet d'étendre l'effet sur la téléportation d'un bruit local chez Bob à celui de bruits indépendants chez Alice et chez Bob quand le bruit chez Alice est unital. Cette généralisation est donnée dans le tableau 3.IV ci-dessous, où $\{\mathsf{A}_i\}$ représente un bruit local (pas nécessairement unital) chez Bob et $\{\sqrt{p_j}\tilde{\mathsf{U}}_j\}$ un bruit local (le même ou un autre, mais il doit être unital) chez Alice.

Résultat classique d'Alice	État quantique final de Bob
ϕ_A^+	$\sum_{ij} p_j(\mathsf{A}_i\tilde{\mathsf{U}}_j^T)_B \,\|\psi\rangle\langle\psi\|_{AB} (\tilde{\mathsf{U}}_j^*\mathsf{A}_i^\dagger)_B$
ϕ_A^-	$\sum_{ij} p_j(\mathsf{Z}\mathsf{A}_i\tilde{\mathsf{U}}_j^T\mathsf{Z})_B \,\|\psi\rangle\langle\psi\|_{AB} (\mathsf{Z}\tilde{\mathsf{U}}_j^*\mathsf{A}_i^\dagger\mathsf{Z})_B$
ψ_A^+	$\sum_{ij} p_j(\mathsf{X}\mathsf{A}_i\tilde{\mathsf{U}}_j^T\mathsf{X})_B \,\|\psi\rangle\langle\psi\|_{AB} (\mathsf{X}\tilde{\mathsf{U}}_j^*\mathsf{A}_i^\dagger\mathsf{X})_B$
ψ_A^-	$\sum_{ij} p_j(\mathsf{X}\mathsf{Z}\mathsf{A}_i\tilde{\mathsf{U}}_j^T\mathsf{Z}\mathsf{X})_B \,\|\psi\rangle\langle\psi\|_{AB} (\mathsf{X}\mathsf{Z}\tilde{\mathsf{U}}_j^*\mathsf{A}_i^\dagger\mathsf{Z}\mathsf{X})_B$

Tableau 3.IV – Expression dans le formalisme de Kraus du résultat de la téléportation quantique standard consommant $|\phi^+\rangle$, en présence de bruits indépendants chez Alice et Bob. Le résultat final varie selon le résultat de la mesure d'Alice.

On peut établir un équivalent du théorème 3 pour les bruits unitaux locaux du côté de l'intrication d'Alice :

Proposition 21. *Pour d=2, de tous les bruits unitaux et locaux sur l'intrication d'Alice, seuls les bruits de la famille de Pauli peuvent se réduire à un bruit local chez Bob qui commute avec la téléportation si aucun bruit n'est présent chez Bob.*

Démonstration. Par la proposition 3, pour commuter avec la téléportation un bruit local chez Bob doit être un bruit de Pauli. Un bruit unital local agissant sur l'intrication d'Alice doit donc être équivalent à un bruit de Pauli local chez Bob. Aucun bruit n'est initialement chez Bob et la proposition 20 nous dit que le bruit réduit chez Bob est $\{\mathsf{A}_i^T\}$ et doit être

de Pauli. Les opérateurs de Pauli sont tous invariants sous transposition au moins à une phase globale près et ainsi parmi tous les bruits unitaux locaux chez Alice, seuls les bruits de Pauli se réduisent à des bruits qui commutent avec la téléportation. ■

On remarque que l'énoncé ne tient pas tout à fait si un bruit local est déjà présent chez Bob, en effet :

Proposition 22. *Pour d=2, il existe des bruits locaux et unitaux chez Alice* $\{\sqrt{p_j}\mathsf{U}_j\}$*, locaux chez Bob* $\{\mathsf{A}_i\}$*, qui ne sont pas de la famille des bruits de Pauli lorsque pris séparément, mais qui se réduisent ensemble à un bruit de Pauli uniquement chez Bob et commutent ainsi avec la téléportation. Cela arrive quand, les opérateurs de Kraus résultants,* $\{\sqrt{p_j}\mathsf{A}_i^T\mathsf{U}_j^T\}_{ij}$*, appartiennent à la famille des bruits de Pauli.*

Démonstration. Conséquence directe des propositions 20 et 3. ■

Ces bruits ont par contre peu d'importance physique, car leur construction est très artificielle.

Quant à la fidélité d'intrication de la téléportation sous ces conditions, on la trouve en modifiant légèrement la proposition 17 à la lueur de la réduction du bruit unital de Alice vers Bob.

Proposition 23. *La fidélité d'intrication résultante du canal de téléportation simultanément, mais indépendamment, brouillé de manière unitale chez Alice par* $\{\sqrt{p_j}\mathsf{U}_j\}$ *et de manière quelconque chez Bob par* $\{\mathsf{A}_i\}$ *est :*

$$F_{intr}(\mathcal{C}^{CAB\to B}_{téléportation}\circ\left(\mathcal{C}^{A}_{unital}\otimes\mathcal{C}^{B}_{brouillé}\right)) = \sum_{ij}\frac{1}{4}|\operatorname{tr}\left(\sqrt{p_j}\mathsf{A}_i^T\mathsf{U}_j^T\right)|^2$$

On pourrait vouloir exprimer la fidélité d'intrication résultante comme une fonction des fidélités individuelles des canaux brouillés d'Alice et Bob. Ce n'est cependant pas possible dans le cas général, comme le montre le contre-exemple simple suivant.

Proposition 24. *Soit le canal unital d'Alice, $\mathcal{C}^A_{unital}$, et celui brouillé de manière quelconque de Bob, $\mathcal{C}^B_{brouillé}$, alors*

$$F_{intr}(\mathcal{C}^{CAB\to B}_{téléportation} \circ \left(\mathcal{C}^A_{unital} \otimes \mathcal{C}^B_{brouillé}\right)) \neq \text{Fonction}\left(F_{intr}(\mathcal{C}^A_{unital}), F_{intr}(\mathcal{C}^B_{brouillé})\right)$$

Démonstration. On suppose l'existence de la fonction Fonction $\left(F_{\text{intr}}(\mathcal{C}^A_{\text{unital}}), F_{\text{intr}}(\mathcal{C}^B_{\text{brouillé}})\right)$. Soit le canal inversant toujours le bit $\mathcal{C}^A_{\text{unital}} = \mathcal{C}^A_{\text{inversion}}(p_{\mathsf{X}} = 1, \cdot)$ et celui inversant toujours la phase $\mathcal{C}^B_{\text{brouillé}} = \mathcal{C}_{\text{déphasant}}(p_{\mathsf{Z}} = 1, \cdot)$, alors :

$$F_{\text{intr}}(\mathcal{C}^A_{\text{unital}}) = F_{\text{intr}}(\mathcal{C}^B_{\text{brouillé}}) = \frac{1}{2}$$

et

$$F_{\text{intr}}(\mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ \left(\mathcal{C}^A_{\text{unital}} \otimes \mathcal{C}^B_{\text{brouillé}}\right)) = \frac{1}{4}$$

Cependant, si l'on prend le cas où le canal chez Bob inverse aussi le bit $\mathcal{C}'^B_{\text{brouillé}} = \mathcal{C}^B_{\text{inversion}}(p_{\mathsf{X}} = 1, \cdot)$, alors on a encore :

$$F_{\text{intr}}(\mathcal{C}^A_{\text{unital}}) = F_{\text{intr}}(\mathcal{C}'^B_{\text{brouillé}}) = \frac{1}{2}$$

mais pourtant :

$$F_{\text{intr}}(\mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ \left(\mathcal{C}^A_{\text{unital}} \otimes \mathcal{C}^B_{\text{brouillé}}\right)) = 1$$

On a à la fois Fonction $\left(\frac{1}{2}, \frac{1}{2}\right) = \frac{1}{4}$ et Fonction $\left(\frac{1}{2}, \frac{1}{2}\right) = 1$. La fonction n'existe donc pas dans le cas général. ■

Le contre-exemple ci-dessus illustre aussi le fait que même si dans la plupart des cas typiques de bruit, comme ceux de Pauli, l'ajout de bruit chez Alice n'aide en rien Bob, dans le cas général deux canaux ayant de basses fidélités d'intrication peuvent, une fois considérés simultanément, résulter en un canal ayant une grande fidélité d'intrication. On mentionne à la fin de la sous-section 3.1.7 qu'il existe des cas de ce phénomène qui sont moins triviaux que celui énoncé plus haut.

On clôt cette sous-section en faisant remarquer que dans les cas où l'intrication

peut être améliorée simplement en faisant une opération unitale locale chez Alice ou quelconque chez Bob, il n'y a pas pour les bruits considérés jusqu'ici d'avantage théorique à effectuer cette correction[6] avant ou après la téléportation. La différence pratique est qu'après la téléportation, l'opération la plus favorable peut être différente et sa réalisation technique plus aisée ou ardue selon le cas.

Proposition 25. *Si l'on peut améliorer la téléportation en effectuant préalablement l'opération unitale* $\{\sqrt{p_i}\mathsf{U}_i\}$ *chez Alice et l'opération quelconque* $\{\mathsf{A}_i\}$ *chez Bob* (PROPOSITION 1)*, alors on peut faire les améliorations* $\{\sqrt{p_i}\mathsf{U}'_i\}$ *et* $\{\mathsf{A}'_i\}$ *chez Bob après la téléportation et obtenir le même résultat* (PROPOSITION 2).

Démonstration. En effet, si σ_j est la rotation de Pauli que Bob applique sur son état suite à l'annonce d'Alice, alors

$$\forall j,\ \forall\{\sqrt{p_i}\mathsf{U}_i\},\forall\{\mathsf{A}_i\},\ \exists\{\sqrt{p_i}\mathsf{U}'_i\} = \{\sqrt{p_i}\sigma_j\mathsf{U}_i^T\sigma_j\},\ \exists\{\mathsf{A}'_i\} = \{\sigma_j\mathsf{A}_i\sigma_j\}$$
$$\text{t.q. PROPOSITION 1} \Rightarrow \text{PROPOSITION 2}$$

■

Ce ne sera plus le cas lorsque, plus tard, on utilisera les techniques d'oubli d'information classique et de wernerisation.

3.1.5.2 Bruit local non-unital chez Alice

On considère maintenant les bruits sur l'intrication d'Alice qui sont locaux, mais non-unitaux. On voit pourquoi l'approche par réduction qu'on a utilisée jusqu'ici n'est plus possible et en quoi ces bruits diffèrent des bruits unitaux au niveau du transfert d'information lors de la téléportation quantique. Cela ouvrira la voie à deux nouvelles techniques, l'oubli d'information classique et la wernerisation, que l'on verra aux sous-sections suivantes.

On a vu précédemment que lorsque l'intrication entre Alice et Bob est brouillée de manière unitale chez Alice, celle-ci peut toujours clamer que son état est intact et que le

[6] Cette optimisation naïve n'est pas à prendre au sens de *codes correcteurs*.

problème est plutôt chez Bob. On démontre maintenant que si le bruit est non-unital, alors Alice ne pourra pas faire porter le blâme à Bob et qu'il faudra donc changer d'approche.

Proposition 26. *Aucun bruit non-unital local chez Alice ne peut être réduit à un bruit uniquement chez Bob.*

Démonstration. Par définition, un bruit non-unital ne préserve pas l'identité, donc l'état complètement mélangé non plus, car celui-ci est proportionnel à l'identité. Une moitié d'une paire intriquée est localement complètement mélangée. Alice ne peut donc pas appliquer un bruit non-unital local chez elle et prétendre que son état demeure localement complètement mélangé. ■

Jusqu'à maintenant, tous les bruits considérés conservaient pour tout état téléporté ρ_C l'équiprobabilité des 2 bits classiques lors de la mesure d'Alice dans la base de Bell. Cette équiprobabilité assure qu'aucune information classique ne fuit lorsque l'on apprend le résultat de cette mesure conjointe sur CA (car la distribution restant uniforme, elle ne peut dépendre de l'état téléporté). Un bruit non-unital, tel le canal atténuant l'amplitude, agissant sur A brise cette règle.

Proposition 27. *Un bruit non-unital appliqué sur la moitié intriquée d'Alice causera une fuite d'information classique lors de la mesure de Bell du protocole de téléportation quantique.*

Démonstration. La moitié brouillée de la paire EPR dans le registre A est forcément localement biaisée puisqu'elle subit un bruit non-unital. On regarde localement l'état $\rho_A = a\pi_A + (1-a)\,|\psi\rangle\langle\psi|_A$, où π est l'état complètement mélangé et $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ est défini comme l'état pur vers lequel le qubit du registre A est biaisé (a est une constante qui dépend du « degré » de non-unitalité). Lorsque l'on téléporte l'état pur $|\psi'\rangle_C = \beta\,|0\rangle + \alpha\,|1\rangle$, la probabilité d'obtenir ϕ^-_{CA} comme résultat de la mesure de Bell sera toujours strictement plus faible que la moyenne des probabilités des autres résultats. En effet,

$$
\begin{aligned}
&\mathrm{tr}\left[\left(|\psi'\rangle\langle\psi'|_C \otimes \rho_A\right) \cdot |\phi^-\rangle\langle\phi^-|_{CA}\right] \\
&\quad = a\,\mathrm{tr}\left[\left(|\psi'\rangle\langle\psi'|_C \otimes \pi_A\right) \cdot |\phi^-\rangle\langle\phi^-|_{CA}\right] + (1-a)\,\mathrm{tr}\left[\left(|\psi'\rangle\langle\psi'|_C \otimes |\psi\rangle\langle\psi|_A\right) \cdot |\phi^-\rangle\langle\phi^-|_{AB}\right] \\
&\quad = \frac{a}{4} + (1-a)\,\mathrm{tr}\left[\left(\alpha\beta\,|00\rangle_{CA} + \alpha\beta\,|11\rangle_{CA} + \alpha\alpha\,|01\rangle_{CA} + \beta\beta\,|10\rangle_{CA}\right)\right. \\
&\quad \otimes \left.\left(\alpha^*\beta^*\,\langle 00|_{CA} + \alpha^*\beta^*\,\langle 11|_{CA} + \alpha^*\alpha^*\,\langle 01|_{CA} + \beta^*\beta^*\,\langle 10|_{CA}\right) \cdot |\phi^-\rangle\langle\phi^-|_{AB}\right] \\
&\quad = \frac{a}{4} + (1-a)\,\mathrm{tr}\left[\left(\sqrt{2}\alpha\beta\,|\phi^+\rangle_{CA} + \frac{\alpha\alpha}{\sqrt{2}}\left(|\psi^+\rangle_{CA} + |\psi^-\rangle_{CA}\right) + \frac{\beta\beta}{\sqrt{2}}\left(|\psi^+\rangle_{CA} - |\psi^-\rangle_{CA}\right)\right)\right. \\
&\quad \otimes \left.\left(\sqrt{2}\alpha^*\beta^*\,\langle\phi^+|_{CA} + \frac{\alpha^*\alpha^*}{\sqrt{2}}\left(\langle\psi^+|_{CA} + \langle\psi^-|_{CA}\right) + \frac{\beta^*\beta^*}{\sqrt{2}}\left(\langle\psi^+|_{CA} - \langle\psi^-|_{CA}\right)\right) \cdot |\phi^-\rangle\langle\phi^-|_{AB}\right] \\
&\quad = \frac{a}{4} + 0 < \mathrm{tr}\left[\left(|\psi'\rangle\langle\psi'|_C \otimes \rho_A\right) \cdot \left(I_{CA} - |\phi^-\rangle\langle\phi^-|_{CA}\right)\right] = \frac{\frac{3a}{4} + (1-a)}{3}
\end{aligned}
$$

Si Alice choisit plutôt d'envoyer $|\tilde{\psi}'\rangle_C = \beta\,|0\rangle_C - \alpha\,|1\rangle_C$, un calcul similaire nous permet de constater que c'est le résultat ϕ^+_{CA} qui a probabilité moindre. Et de même pour $|\psi\rangle_C$ et $|\tilde{\psi}\rangle_C = \alpha\,|0\rangle_C - \beta\,|1\rangle_C$ qui diminuent respectivement les chances d'obtenir ψ^-_{CA} et ψ^+_{CA}. Le résultat de la mesure est donc corrélé avec l'état envoyé : il y a fuite d'information classique. ■

Cette fuite classique appauvrit nécessairement l'information quantique transférée par la téléportation. Pour illustrer l'ampleur possible des dommages, on prend l'exemple radical du canal à atténuation d'amplitude de probabilité 1.

Exemple 4. *Soit $\mathcal{C}^A_{\text{atténuant-amplitude}}(p=1,\rho)$, ce canal remplace tout qubit le traversant par $|0\rangle$ et perd le qubit initial dans l'environnement. Si on l'applique sur $\rho_A = \mathrm{tr}_B\,|\phi^+\rangle\langle\phi^+|_{AB}$, la moitié intriquée ρ_B devient orpheline et restera à jamais un état complètement mélangé. La téléportation quantique est donc un échec total et aucune information quantique ne peut être transférée à l'aide de celle-ci. Par contre, la mesure de Bell faite par Alice est équivalente à une mesure dans la base orthogonale du qubit ρ_C (avec $\phi^\pm \to 0$ et $\psi^\pm \to 1$). Elle donne un peu d'information sur l'état. La conclusion est qu'en présence d'un tel bruit, si l'état envoyé par Alice est pur, Bob est mieux de partir de zéro et de recréer grâce à l'information classique l'état avec fidélité d'intrication $\frac{1}{2}$ (la borne classique) que d'appliquer verbatim le protocole de téléportation quantique qui ne lui permet même pas de dépasser une fidélité d'intrication de $\frac{1}{4}$ (le résultat aléatoire) !*

3.1.6 L'oubli post-téléportation de la mesure classique

L'information qui fuit à travers le canal classique est difficile à traiter. Pour continuer notre étude des effets de l'intrication brouillée, on va regarder ce qui arrive au canal de téléportation quantique quand on efface cette information. Pour modéliser la situation, on introduit un nouveau personnage, Damien, aux personnalités multiples. Damien-quantique[7] effectue uniformément aléatoirement une rotation de Pauli sur l'état à téléporter du côté d'Alice[8] juste avant la mesure de Bell, et il effectue la même rotation du côté de Bob à la toute fin du protocole. Par la suite, Damien-quantique se sauve : Alice et Bob n'apprennent jamais laquelle des quatre opérations de Pauli il a effectuée !

On constate maintenant que le comportement de Damien n'est pas vraiment quantique. En effet, du côté d'Alice son action revient strictement à intercepter l'information classique à la sortie de l'appareil de mesure d'Alice et d'y appliquer un masque jetable classique avant qu'Alice n'aie le temps de la lire. Du côté de Bob, l'action de Damien revient à venir se placer entre Bob et sa machine chargée de faire la rotation de Pauli en fonction de l'information classique. Une fois entre les deux, Damien-classique réapplique le masque jetable sur l'information classique (et ainsi restaure l'original). La téléportation se termine alors de manière normale et Damien-classique disparaît avec son masque jetable. L'information classique de la mesure d'Alice est, sans la connaissance de ce masque jetable, complètement arbitraire : le tour de Damien-classique a été d'effacer l'information classique pour Alice et Bob. Au final, Damien pourrait également n'être que dans l'imaginaire des autres personnages, du moment qu'ils s'entendent tous les deux pour ne pas tenir compte de l'information classique une fois le protocole de téléportation terminé. Faire semblant est beaucoup plus simple que d'effacer réellement de l'information classique et suffit pour la plupart des tâches (exception possible en

[7] Damien-quantique est équivalent au concept de « Pauli twirl » dans la littérature anglophone.

[8] Damien-quantique peut obtenir le même résultat en appliquant l'opération sur la moitié intriquée d'Alice plutôt que sur l'état à téléporter.

cryptographie). Au final, Damien-quantique, Damien-classique et Damien-imaginaire sont trois interprétations toutes aussi valides du même phénomène.

On explicite maintenant l'effet de Damien sur la téléportation quantique :

Proposition 28. *Soit un canal brouillé de téléportation (dont l'entrée et la sortie sont de dimension égale) qui résulte de l'application du protocole de téléportation quantique avec une intrication brouillée d'une manière quelconque. Soit* $\{\sigma_j \mathsf{A}_i \sigma_j\}_i$ *les opérateurs de Kraus du canal correspondant au résultat* j *de la mesure d'Alice, lequel n'est pas nécessairement uniformément distribué. Damien a l'impact suivant :*

$$\text{Damien}\left[\left\{\sigma_j \mathsf{A}_i \sigma_j\right\}_i\right] = \left\{\frac{1}{\sqrt{4}}\sigma_j \mathsf{A}_i \sigma_j\right\}_{ij}$$

Démonstration. On applique Damien-quantique sur le protocole standard de téléportation. On note que les opérateurs de Kraus obtenus ne sont pas simplifiés. ■

Et là coup de théâtre : ces opérateurs de Kraus correspondent à ceux d'un bruit de Pauli !

Théorème 4. *L'intervention de Damien (c'est-à-dire l'oubli de l'information classique), transforme tout bruit induit par la téléportation brouillée en bruit de Pauli.*[9]

$$\text{Damien}\left[\mathcal{C}^{CAB\to B}_{\textit{téléportation brouillée}}\right] \in \text{FAMILLE DES BRUITS DE PAULI}$$

Démonstration. On montre que le canal résultant de la téléportation brouillée avec action de Damien-quantique, $\text{Damien}\left[\mathcal{C}^{CAB\to B}_{\text{téléportation brouillée}}\right]$, commute avec la téléportation au sens de la section 3.1.4 et donc que c'est un bruit de Pauli par le théorème 3.

On utilise deux canaux de téléportation, $\text{Damien}\left[\mathcal{C}^{CAB\to B}_{\text{téléportation brouillée}}\right]$ et $\mathcal{C}^{CA'B'\to B'}_{\text{téléportation}}$.

[9] Cette propriété était déjà connue, voir [35] pour l'effet du « Pauli twirl » sur un canal quantique et [13] pour son application à la téléportation quantique. La preuve présentée ici reste celle de l'auteur de ce mémoire.

On désire prouver cette commutativité :

$$\mathcal{C}^{CA'B'\to B'}_{\text{téléportation}} \circ \text{Damien}\left[\mathcal{C}^{B'AB\to B'}_{\text{téléportation brouillée}}\right] \stackrel{?}{=} \text{Damien}\left[\mathcal{C}^{B'AB\to B'}_{\text{téléportation brouillée}}\right] \circ \mathcal{C}^{CA'B'\to B'}_{\text{téléportation}}$$

À droite la téléportation se fait de manière parfaite avant le bruit et donc les opérateurs de Kraus restent inchangés. À gauche, on utilise la proposition 12 et on constate que les opérateurs de Kraus finaux demeurent également inchangés. Damien $\left[\{\sigma_j \mathsf{A}_i \sigma_j\}_i\right] = \{\frac{1}{\sqrt{4}}\sigma_j \mathsf{A}_i \sigma_j\}_{ij}$ est un bruit qui commute toujours avec la téléportation et appartient ainsi à la famille des bruits de Pauli. ■

La téléportation quantique brouillée avec oubli d'information classique est ainsi dans le cas général équivalente à un canal brouillé de Pauli. Cela donne lieu à une nouvelle interprétation physique : au lieu de considérer le bruit comme provenant d'imperfections dans la ressource partagée d'intrication, on peut le considérer comme étant simplement un bruit classique sur le résultat de la mesure d'Alice. C'est-à-dire que selon cette version des faits, la téléportation se fait correctement, mais parfois Alice annonce à son insu la mauvaise information classique et Bob effectue alors une rotation de Pauli incorrecte, donnant lieu à un état final déformé.

Une autre interprétation de ce phénomène est qu'Alice et Bob effectuent le protocole de téléportation quantique normalement, mais avec un mélange statistique d'états de Bell. S'ils sont chanceux, le protocole aboutit au bon état final ; s'ils ne le sont pas, Bob reçoit un état modifié par une des trois matrices de Pauli. Cette interprétation démontre que la seule différence entre effectuer la téléportation avec comme ressource d'intrication l'état quelconque ρ_{AB}, et l'effectuer avec un mélange statistique de paires EPR (un bruit purement classique), est l'information classique de la mesure d'Alice ! On en déduit la fidélité d'intrication et les paramètres de Pauli du canal résultant.

Proposition 29. *Soit $\mathcal{C}^{CAB\to B}_{\text{téléportation brouillée avec oubli}}$ le canal résultant du protocole de téléportation quantique avec oubli de l'information classique et qui utilise l'état quelconque ρ_{AB} comme ressource d'intrication. Soit $\mathcal{C}^{CAB\to B}_{\text{téléportation brouillée}}$ le même canal sans oubli.*

Leur fidélité d'intrication est donnée par :

$$F_{intr}\left(\mathcal{C}^{CAB\to B}_{\text{téléportation brouillée}}\right) = F_{intr}\left(\mathcal{C}^{CAB\to B}_{\text{téléportation brouillée avec oubli}}\right) = \mathrm{tr}\left(\rho_{AB}\,|\phi^+\rangle\langle\phi^+|_{AB}\right)$$

tandis que les trois paramètres du bruit de Pauli résultant du canal avec oubli sont :

$$p_{\mathsf{X}} = \mathrm{tr}\left(\rho_{AB}\,|\psi^+\rangle\langle\psi^+|_{AB}\right), \quad p_{\mathsf{Y}} = \mathrm{tr}\left(\rho_{AB}\,|\psi^-\rangle\langle\psi^-|_{AB}\right), \quad p_{\mathsf{Z}} = \mathrm{tr}\left(\rho_{AB}\,|\phi^-\rangle\langle\phi^-|_{AB}\right)$$

Démonstration. L'équivalence entre les fidélités d'intrication des canaux quantiques avec et sans oubli vient du fait que l'information classique n'est pas prise en compte dans la mesure de la fidélité d'intrication et donc que son effacement est sans conséquence. Les formules impliquant la trace sont des résultats directs une fois ρ_{AB} dans la base de Bell. La preuve que Damien-quantique projette tout état ρ_{AB} dans la base de Bell est effectuée à la première partie de l'annexe sur la wernerisation à la section II. On substitue ici Damien-quantique par Damien-classique, soit l'oubli du résultat de la mesure. ■

La fidélité d'intrication n'est donc pas affectée par l'oubli d'information classique et utiliser cet outil est ainsi fort approprié lorsque l'on applique le protocole de téléportation tel quel. Par contre, pour l'analyse du meilleur protocole de téléportation possible, l'intervention hâtive de Damien peut être nuisible. Il faut donc faire attention. On l'illustre par un exemple.

Exemple 5. *Soit le canal de téléportation brouillée* $\mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ (I_A \otimes \mathsf{H}_B)$ *qui applique bêtement la porte d'Hadamard sur la moitié intriquée de Bob. Si la ressource initiale*

était $|\phi^+\rangle$*, alors*

$$
\begin{aligned}
F_{intr}\left(\mathcal{C}_{téléportation}^{CAB\to B}\circ(I_A\otimes \mathsf{H}_B)\right) &= \mathrm{tr}\left(\mathsf{H}_B\,|\phi^+\rangle\langle\phi^+|_{AB}\,\mathsf{H}_B\cdot|\phi^+\rangle\langle\phi^+|_{AB}\right)\\
&= \mathrm{tr}\left(\frac{1}{2}(|\psi^+\rangle_{AB}+|\phi^-\rangle_{AB})(\langle\psi^+|_{AB}+\langle\phi^-|_{AB})\cdot|\phi^+\rangle\langle\phi^+|_{AB}\right)=0\\
p_{\mathsf{X}} &= \mathrm{tr}\left(\mathsf{H}_B\,|\phi^+\rangle\langle\phi^+|_{AB}\,\mathsf{H}_B\cdot|\psi^+\rangle\langle\psi^+|_{AB}\right)=\frac{1}{2}\\
p_{\mathsf{Y}} &= \mathrm{tr}\left(\mathsf{H}_B\,|\phi^+\rangle\langle\phi^+|_{AB}\,\mathsf{H}_B\cdot|\psi^-\rangle\langle\psi^-|_{AB}\right)=0\\
p_{\mathsf{Z}} &= \mathrm{tr}\left(\mathsf{H}_B\,|\phi^+\rangle\langle\phi^+|_{AB}\,\mathsf{H}_B\cdot|\phi^-\rangle\langle\phi^-|_{AB}\right)=\frac{1}{2}
\end{aligned}
$$

L'utilisation du protocole tel quel de téléportation quantique standard dont l'intrication est ainsi brouillée se réduit donc à un canal dont la fidélité d'intrication est non seulement pire que la borne classique ($F_{intr}^{classique}=\frac{1}{2}$*), mais également pire que le protocole complètement aléatoire (*$F_{intr}^{aléatoire}=\frac{1}{4}$*). Sans oubli, cette affirmation est légèrement trompeuse, puisque l'état téléporté a simplement subi une rotation unitaire. Tant que l'on sait que l'intrication est ainsi brouillée, on peut modifier légèrement le protocole pour obtenir un canal résultant parfait. Il suffirait par exemple à Alice (ou Bob) d'appliquer* H *sur sa moitié intriquée avant de faire la téléportation, ou bien à Bob de faire la rotation unitaire* $\sigma_j\mathsf{H}\sigma_j$ *de son état à la fin du protocole de téléportation. Mais si l'on efface à la fin de la téléportation la valeur* j *de la mesure d'Alice, c'est-à-dire dans le cas de la téléportation avec oubli, alors la situation est bien plus désastreuse. La condition de l'état téléporté est aggravée et il subit maintenant un mélange statistique d'erreurs* X *et* Z *équiprobables. On pourrait effectuer une rotation* X *(ou* Z*) chez Bob a posteriori pour au moins égaler la borne classique, mais aucune rotation ne nous permet d'atteindre la fidélité d'intrication 1 comme avant. On va généraliser cette idée à la sous-section suivante sur la wernerisation.*

La simplification à l'aide de Damien rend aisée l'étude de l'effet de l'intrication brouillée de manière non-unitale chez Alice, mais son utilité ne s'arrête pas là. En pouvant réduire tout canal de téléportation quantique à un bruit de Pauli, on trouve une borne

inférieure sur la qualité du canal et on limite considérablement le nombre de paramètres à prendre en compte dans la quantification du bruit (3 paramètres, $\{p_X, p_Y, p_Z\}$, par qubit). Cela permet d'une part de mesurer de manière réaliste la propagation du bruit dans un réseau complexe (voir section 3.2) et d'autre part de choisir des bons codes correcteurs quantiques. Prétendre avoir oublié de l'information classique ne demande en pratique pas de manipulations supplémentaires et est ainsi trivial à réaliser expérimentalement. On pousse l'idée derrière Damien-quantique plus loin dans la section suivante en introduisant la wernerisation.

3.1.7 Wernerisation

À l'instar de Damien-quantique, la wernerisation [10] permet de transformer à l'aide de manipulations locales[10] tout bruit dans l'intrication chez Alice et/ou chez Bob en bruit de Pauli chez Bob, avec la condition d'oublier laquelle des manipulations on a aléatoirement choisie. Cette fois-ci, la manœuvre rend les trois types d'erreur (X, Y, Z) du bruit de Pauli équiprobables et celui-ci peut ainsi être décrit par un seul paramètre. Cela le rend très simple à analyser. De plus, son interprétation physique est intéressante puisqu'il coïncide avec un bruit dépolarisant de facteur $P = \frac{4-4\,\mathrm{tr}\left(\rho_{AB}|\phi^+\rangle\langle\phi^+|_{AB}\right)}{3}$ dans le régime $p_X = p_Y = p_Z \leq \frac{1}{4}$, c'est-à-dire dès que la ressource offre une qualité de téléportation égale ou supérieure à l'état complètement mélangé. On présente ici l'idée du protocole de wernerisation et les conséquences pour la téléportation. Les détails algébriques de la wernerisation sont donnés en annexe à la section II. On montre plus tard à la sous-section 3.2.2.2 comment combiner plusieurs bruits dépolarisants.

La wernerisation peut être décomposée en deux étapes[11], la première est Damien-quantique et ne nécessite ainsi pas dans le cadre de la téléportation standard de manipulations autres que l'oubli d'information. Par contre, la deuxième demande d'appliquer

[10] Elles sont explicitées en annexe à la section section II

[11] Cette vision, explicitée en annexe, est introduite par l'auteur, mais elle est strictement équivalente à la méthode en une étape présentée dans [12].

aléatoirement une de trois portes unitaires chez Alice et chez Bob et requiert donc des manœuvres expérimentales supplémentaires. On suppose naïvement ici que ce processus n'introduit pas de nouveau bruit dans la téléportation.

Proposition 30. *L'opération de wernerisation transforme toute intrication brouillée* ρ_{AB} *en état de werner de pureté* $p_W = \mathrm{tr}\left(\rho_{AB}\,|\phi^+\rangle\langle\phi^+|_{AB}\right)$*, et donc tout canal brouillant l'intrication chez Alice et Bob en bruit de Pauli* $p_X = p_Y = p_Z = \frac{1-\mathrm{tr}\left(\rho_{AB}|\phi^+\rangle\langle\phi^+|_{AB}\right)}{3}$ *local chez Bob. De manière plus spécifique, lorsque* $p_W \geq \frac{1}{4}$*, ce bruit chez Bob est dépolarisant :*

$$\text{wernerisation}\left[\mathcal{C}^{AB}_{\textit{brouillé}}(\cdot)\right] \sim \left(\mathcal{C}^{A}_{\textit{identité}} \otimes \mathcal{C}^{B}_{\textit{dépolarisant}}(P,\cdot)\right)$$

où $P = \frac{4-4\,\mathrm{tr}\left(\rho_{AB}|\phi^+\rangle\langle\phi^+|_{AB}\right)}{3}$.

Démonstration. L'effet de la wernerisation est démontré en annexe à la section II. La preuve y est faite pour $|\psi^-\rangle$, mais son adaptation à $|\phi^+\rangle$ est directe (on effectue l'opération XZ chez Alice ou chez Bob au début et à la fin du protocole de wernerisation). L'équivalence entre le bruit de Pauli wernerisé et le canal dépolarisant de paramètre P suit de leurs définitions. La fidélité d'intrication du canal dépolarisant chez Bob est donnée par :

$$F_{\text{intr}}\left(\mathcal{C}^{B}_{\text{dépolarisant}}(P,\cdot)\right) = \mathrm{tr}\left(\rho_{AB}\,|\phi^+\rangle\langle\phi^+|_{AB}\right) = (1-P) + \frac{P}{4} = \frac{1-3P}{4}$$

En inversant cette relation, on trouve la valeur de P ci-haut. ■

On remarque que dans le cas de la téléportation quantique, la wernerisation du côté d'Alice peut également être faite sur l'état à téléporter plutôt que sur l'état intriqué (du côté de Bob, les deux visions correspondent à la même opération). C'est le cas parce que pour toute opération unitaire U_A, l'opération $U_C^\dagger$ a exactement le même effet lors de la mesure conjointe AC (par invariance de la trace sous permutation cyclique).

Comme pour l'oubli d'information, laquelle est en fait équivalente à une wernerisation partielle, la wernerisation complète conserve la fidélité d'intrication du canal de téléportation quantique.

Proposition 31. *La fidélité d'intrication d'un canal wernerisé de pureté p_W est donnée par :*

$$F_{intr}\left(\text{wernerisation}\left[\mathcal{C}^{AB}_{brouillé}(\cdot)\right]\right) = F_{intr}\left(\mathcal{C}^{AB}_{brouillé}(\cdot)\right) = \text{tr}\left(\rho_{AB}\,|\phi^+\rangle\langle\phi^+|_{AB}\right) = p_W$$

On note que l'utilisation d'un état de Werner comme ressource intriquée dans le protocole de téléportation donne lieu à un canal dépolarisant dont la fidélité d'intrication dépend exclusivement de la pureté de l'état de Werner (les deux valeurs sont égales en fait). Optimiser l'un ou l'autre est donc strictement équivalent.

Une différence commune à Damien-quantique et à la wernerisation par rapport aux bruits unitaux considérés précédemment est que l'on peut parfois obtenir un meilleur canal si on le modifie à l'aide d'opérations locales chez Alice et chez Bob avant la téléportation, plutôt qu'après. Un canal brouillé qui applique trivialement chez Alice ou Bob une unitaire qui n'est pas l'identité et qui n'appartient pas à l'ensemble des douze opérations de la wernerisation en est l'exemple le plus simple, puisque ce canal ne peut être complètement réparé que si l'on agit avant la wernerisation (en faisant l'opération unitaire inverse). On choisit les opérations locales de manière à maximiser la pureté de l'état de Werner résultant. Cela amène la question suivante :

Question ouverte 1. *Sous quelles conditions est-ce que Alice peut optimiser son canal wernerisé de téléportation en se restreignant seulement à l'application préalable d'une rotation unitaire locale, qui serait alors donnée par :*

$$\arg\max_{\forall \mathsf{U}_A} \text{tr}\left(\mathsf{U}_A \cdot \mathcal{C}^{AB}_{brouillé}\left(|\phi^+\rangle\langle\phi^+|\right) \cdot \mathsf{U}_A^\dagger\,|\phi^+\rangle\langle\phi^+|_{AB}\right)$$

On s'est ici limité sans perdre de généralité au cas où seule Alice était chargée de la correction (voir la proposition 32).

Le canal complètement dépolarisant chez Alice (ou chez Bob) est un exemple évident de bruit unital pour lequel l'optimisation ci-dessus n'aide pas : il est invariant sous toute

transformation unitaire locale. Par contre, si l'on introduit artificiellement des bruits complètement atténuants chez Alice et chez Bob, alors on se retrouve avec le protocole de téléportation classique, où l'on reconstruit en partie l'état quantique à partir de sa description classique (nécessairement incomplète). Dans la même veine, si le bruit, maintenant non-unital, est complètement atténuant chez Alice ou chez Bob, on atteint la borne classique en appliquant le même bruit complètement atténuant chez l'autre personnage (donc d'un seul côté). Une opération unitaire n'aiderait pas. Un exemple moins trivial est donné par Badziag, Horodecki, Horodecki et Horodecki dans un article de 2000 [3], où un canal brouillé particulier arrive à dépasser la borne classique quand on rajoute un bruit non-unital (alors que la prouesse est impossible avec des opérations unitales locales).

On laisse donc la question ouverte, mais on rappelle tout de même qu'il n'est pas bénéfique qu'Alice et Bob appliquent chacun une transformation unitaire, puisqu'on peut considérer toute correction effectuée par Bob comme faite par Alice, et vice versa.

Proposition 32. *Effectuer préalablement une opération unitaire (potentiellement différente) de chaque côté n'offre rien de plus que d'effectuer une unitaire d'un seul côté quant à l'optimisation de la fidélité du canal résultant de la wernerisation.*

$$\begin{aligned}\max_{\forall \mathsf{U},\mathsf{U}'} \operatorname{tr}\Big(\big(\mathsf{U}_A \otimes \mathsf{U}'_B\big)\cdot \mathcal{C}^{AB}_{brouillé}\big(|\phi^+\rangle\langle\phi^+|\big)\cdot\big(\mathsf{U}_A^\dagger \otimes \mathsf{U}'^\dagger_B\big)\,|\phi^+\rangle\langle\phi^+|_{AB}\Big)\\ = \max_{\forall \mathsf{U}} \operatorname{tr}\Big(\mathsf{U}_A \cdot \mathcal{C}^{AB}_{brouillé}\big(|\phi^+\rangle\langle\phi^+|\big)\cdot \mathsf{U}_A^\dagger\,|\phi^+\rangle\langle\phi^+|_{AB}\Big)\end{aligned}$$

Démonstration. La preuve est classique : on se sert de l'invariance de la trace sous permu-

tation cyclique et on réutilise la propriété non-locale de $|\phi^+\rangle$ énoncée à la proposition 1.

$$\begin{aligned}
&\max_{\forall \mathsf{U},\mathsf{U}'} \operatorname{tr}\left((\mathsf{U}_A \otimes \mathsf{U}'_B)\cdot \mathcal{C}^{AB}_{\text{brouillé}}\left(|\phi^+\rangle\langle\phi^+|\right)\cdot(\mathsf{U}_A^\dagger \otimes \mathsf{U}'^\dagger_B)\,|\phi^+\rangle\langle\phi^+|_{AB}\right)\\
=&\max_{\forall \mathsf{U},\mathsf{U}'} \operatorname{tr}\left(\mathcal{C}^{AB}_{\text{brouillé}}\left(|\phi^+\rangle\langle\phi^+|\right)\cdot(\mathsf{U}_A^\dagger \otimes \mathsf{U}'^\dagger_B)\,|\phi^+\rangle\langle\phi^+|_{AB}\,(\mathsf{U}_A \otimes \mathsf{U}'_B)\right)\\
=&\max_{\forall \mathsf{U},\mathsf{U}'} \operatorname{tr}\left(\mathcal{C}^{AB}_{\text{brouillé}}\left(|\phi^+\rangle\langle\phi^+|\right)\cdot(\mathsf{U}_A^\dagger \mathsf{U}'^*_A \otimes I_B)\,|\phi^+\rangle\langle\phi^+|_{AB}\,(\mathsf{U}'_A \mathsf{U}_A^T \otimes I_B)\right)\\
=&\max_{\forall \mathsf{U}} \operatorname{tr}\left(\mathcal{C}^{AB}_{\text{brouillé}}\left(|\phi^+\rangle\langle\phi^+|\right)\cdot(\mathsf{U}_A^\dagger \otimes I_B)\,|\phi^+\rangle\langle\phi^+|_{AB}\,(\mathsf{U}_A \otimes I_B)\right)\\
=&\max_{\forall \mathsf{U}} \operatorname{tr}\left((\mathsf{U}_A \otimes I_B)\cdot \mathcal{C}^{AB}_{\text{brouillé}}\left(|\phi^+\rangle\langle\phi^+|\right)\cdot(\mathsf{U}_A^\dagger \otimes I_B)\cdot|\phi^+\rangle\langle\phi^+|_{AB}\right)
\end{aligned}$$

■

3.1.8 Effet d'un bruit potentiellement non-local

On aborde brièvement les bruits potentiellement non-locaux : on les définit et on en cerne une sous-catégorie pour laquelle on peut aisément généraliser les résultats de la sous-section 3.1.5 sur les bruits indépendants.

On entend par bruit potentiellement non-local un canal qui agit conjointement sur les registres intriqués d'Alice et de Bob. On définit alors un bruit potentiellement non-local comme une généralisation des cas précédents (un bruit local appartient ainsi à la famille des bruits potentiellement non-locaux). En fait, c'est le modèle le plus général de bruit dont l'entrée et la sortie sont 2 qubits. Ce qu'il peut faire de plus que les bruits précédemment traités, c'est induire des corrélations classiques ou quantiques entre les bruits chez Alice et Bob. On peut donner un sens physique à cette action en la voyant comme le bruit lors de la génération locale de la paire intriquée, avant la distribution. Il peut aussi être, dans un contexte adversoriel, le fruit de l'action de deux agents partageant des variables aléatoires classiques, ou même de l'intrication. S'ils peuvent communiquer, cette dernière leur permet en fait de simuler n'importe quelle opération quantique locale de manière non-locale.

Bien entendu, comme on inclut dans la catégorie des bruits potentiellement non-locaux les bruits non-unitaux locaux chez Alice, on ne peut les réduire dans le cas général

à des bruit locaux chez Bob. Mais même si l'on se restreint à des bruits unitaux mais non-locaux, la réduction n'est toujours pas possible. Pour le voir, on n'a qu'à prendre une transformation unitaire U_{AB} telle que $U_{AB}\left|\phi^{+}\right\rangle_{AB} = \left|00\right\rangle_{AB}$ et à réutiliser la preuve de la proposition 26. On peut toutefois toujours les simplifier en canaux brouillés de Pauli en oubliant l'information classique ou à l'aide de la wernerisation. Les deux techniques s'appliquent exactement de la même manière qu'à la sous-section précédente.

En se limitant seulement aux bruits potentiellement non-locaux dont les corrélations sont strictement classiques, on peut toutefois obtenir une simplification intéressante. On modélise l'intrication ainsi brouillée en effectuant un mélange statistique de canaux brouillés indépendamment chez Alice et chez Bob :

$$\mathcal{C}^{CAB\to B}_{\text{téléportation}} \circ \left(\sum_k p_k \left(\mathcal{C}^{A}_{\text{brouillé}_k} \otimes \mathcal{C}^{B}_{\text{brouillé'}_k} \right) \right)$$

Tous les résultats de la sous-section 3.1.5 utilisant la réduction d'un bruit chez Alice qui est local et unital se généralisent directement en remplaçant la réduction par celle qui suit.

Proposition 33. *L'effet de tout bruit agissant sur l'intrication d'Alice et Bob, de manière potentiellement non-locale, mais dont les corrélations sont strictement classiques, peut être réduit, si le bruit chez Alice conditionné sur celui de Bob est unital, à celui d'un bruit uniquement chez Bob. Lorsque ces conditions sont respectées, alors le bruit potentiellement non-local, dont les opérateurs de Kraus agissant sur $A \otimes B$ pourraient s'écrire de manière à former le terme de gauche de la formule ci-dessous, peut se réduire au bruit représenté par les opérateurs à droite, dans le cas où l'intrication est initialement $\left|\phi^{+}\right\rangle_{AB}$. On note que les opérateurs de Kraus ci-dessous ne sont pas donnés dans leur forme la plus compacte ou la plus simplifiée.*

$$\left\{ \sqrt{p_k} \{ \sqrt{p_{ik}} \mathsf{U}_{ik} \}_i \otimes \{A_{jk}\}_j \right\}_k \xrightarrow{\textit{se réduit à}} \left\{ \sqrt{p_k} \{ \sqrt{p_{ik}} \mathsf{U}_{ik}^{T} \}_i \otimes \{A_{jk}\}_j \right\}_k$$

Démonstration. Généralisation de la proposition 20 à un mélange statistique de bruits

indépendants, où le bruit chez Bob est quelconque et celui chez Alice est unital. ■

3.1.9 Effet d'un bruit changeant la dimension du registre

On a considéré rigide jusqu'à maintenant les dimensions des états intriqués subissant un bruit. En pratique, ce n'est pas toujours le cas. Par exemple, dans un système photonique à deux détecteurs, un polarisé verticalement et l'autre horizontalement, il arrive que l'on enregistre simultanément plus d'un clic. À l'inverse, parfois on perd le photon qui transporte l'information quantique. Dans les deux scénarios, le bruit présenté échappe aux modèles que l'on a jusqu'à maintenant regardés. On remédie partiellement à cette lacune en traitant le canal à effacement, car c'est un bruit très courant et la téléportation quantique s'y révèle particulièrement adaptée. On n'analysera pas les bruits menant à une sur-détection ou à un quelconque autre changement de dimension du registre.

En effet, au lieu d'envoyer directement un état quantique ρ et de le voir disparaître avec probabilité p_e dans un canal à effacement, on peut envoyer la moitié d'une paire intriquée (une ressource remplaçable) et s'en servir pour téléporter à coup sûr ρ en cas de succès si aucun autre bruit n'est présent [11].

Protocole 3 (Téléportation quantique standard robuste à l'effacement)**.**

1. *Alice tente d'envoyer la moitié d'une paire maximalement intriquée à Bob en utilisant le canal à effacement.*

$$\mathcal{C}^{A'\to B}_{effacement}(p_e, |\phi^+\rangle\langle\phi^+|_{AA'}) = p_e\,|1\rangle\langle 1|_E \otimes \pi_B + (1-p_e)\,|0\rangle\langle 0|_E \otimes |\phi^+\rangle\langle\phi^+|_{AB}$$

2. *Bob projette son état sur $\Pi_{EB} = |0\rangle\langle 0|_E \otimes I_B$. S'il obtient 1_E, alors la paire maximalement intriquée est perdue et Alice et Bob recommence à l'étape 1 (tant qu'une autre utilisation du canal à effacement est possible). Quand il obtient le résultat 0_E, alors il annonce à Alice le succès du transfert d'intrication et celle-ci peut lui téléporter son véritable état sans risque d'effacement. C'est-à-dire qu'il est possible grâce à la téléportation de transformer le canal à effacement en canal identité*

(conditionnel à la présence d'un canal classique d'Alice vers Bob pour téléporter, mais aussi d'un canal classique de Bob vers Alice pour que Bob puisse avertir de la réception[12]*) avec probabilité* $1-p_e$*, où* p_e *est la probabilité d'effacement.*

$$\left\{ \left(\mathcal{C}^{A\to B}_{effacement} + \mathcal{C}^{A\leftrightarrow B}_{classique} \right) \Big|_{\text{RÉUSSITE}} \sim \mathcal{C}^{AB}_{identité} \right\}$$

où l'événement RÉUSSITE *a probabilité* $1-p_e$

Si l'usage du canal à effacement de probabilité $p_e < 1$ est sans limite, alors le protocole réussit éventuellement et prend en moyenne $t = \frac{1}{1-p_e}$ utilisations.

Démonstration.

$$\begin{aligned} t &= \sum_{n=1}^{\infty} n p_e^{n-1}(1-p) \\ &= \sum_{n=0}^{\infty} p^n(1-p_e) + \sum_{n=0}^{\infty} n p_e^n (1-p_e) \\ &= \frac{1}{1-p_e}(1-p_e) + \frac{p_e}{(1-p_e)^2}(1-p_e) \\ &= \frac{1}{1-p_e} \end{aligned}$$

■

On revient au canal à effacement à la sous-section 3.2.3 lorsque l'on traite la téléportation avec relais quantiques.

Note. *Il est essentiel que Bob puisse avertir Alice de la réception ou de la non-réception de l'état intriqué. Sans ça, la réduction dans le cas général du canal à effacement à usages multiples au canal identité n'est pas valable. La preuve standard consiste à prendre le canal à effacement de probabilité* $p_e = \frac{1}{2}$ *et à personnifier l'environnement qu'on appelle Charlie. Charlie est alors entièrement responsable de l'effacement, c'est-à-dire que lorsque Bob constate un effacement de l'état envoyé, c'est parce que Charlie*

[12] Dans le cas où la communication classique de Alice vers Bob est interdite, on peut quand même réussir en simulant ce canal classique à l'aide du canal à effacement quantique de Alice vers Bob et du canal classique de Bob vers Alice.

l'a volé ! Si Bob est muet et ne peut envoyer de messages à Alice, alors il y a symétrie totale entre Bob et Charlie.[13] *Si Alice réussit à envoyer avec certitude tout état quantique à Bob (c'est-à-dire si* $\mathcal{C}^{A\to B}_{effacement}(\frac{1}{2},\cdot) \sim \mathcal{C}^{A\to B}_{identité}(\cdot)$*), alors Charlie reçoit également l'état non-modifié avec probabilité* 1 *(on dénomme ce canal de Alice vers Charlie (ou l'environnement) le canal complémentaire). L'existence d'une telle manœuvre implique celle du clonage quantique, lequel contrevient au principe d'incertitude. Elle est donc physiquement impossible.*

3.1.10 Téléportation d'un qudit

On s'est limité dans ce mémoire à l'étude de la téléportation brouillée d'un qubit, en se basant essentiellement sur l'argument que le protocole de téléportation d'un qubit peut être réalisé plusieurs fois en parallèle pour téléporter tout qudit. Mais on ne peut pas toujours garantir que tous ces qubits en parallèle soient suffisamment isolés les uns des autres pour justifier l'indépendance de leurs bruits. Aussi, il y a présentement beaucoup de recherche afin de trouver le meilleur support physique pour l'information quantique et il n'est pas impossible que, simplement pour des raisons de production de masse, l'unité de base du futur ne soit pas un qubit, mais un qutrit ou même un qudit de dimension 17. Dans ces deux situations (qubits parallèles et qudits farfelus), l'effet du bruit dans l'intrication vaut la peine d'être étudié et sans refaire intégralement l'analyse des sous-sections précédentes, on fait un bref tour d'horizon des résultats qui se généralisent aisément à d dimensions.

Au niveau de l'intrication, le qubit maximalement intriqué $|\phi^+\rangle$ se généralise directement en $|\phi_d^+\rangle$ lorsque l'on change la dimension. Les matrices de Pauli se généralisent également en d dimensions comme on l'a vu à la sous-section 2.2.2.1. La catégorie des bruits locaux chez Bob qui commutent avec la téléportation pour le qudit est ainsi la famille des bruits de Pauli généralisés. La preuve est esquissée en annexe à la section III.

[13] L'information classique dont Bob a besoin pour terminer la téléportation peut être copiée aisément et Charlie peut donc l'apprendre lui-aussi.

La propriété non-locale 1 qu'on a utilisée pour traiter tout bruit d'unitaires mélangés chez Alice comme du bruit chez Bob est encore vraie en d dimensions. Par contre, l'équivalence entre bruit unital et bruit d'unitaires mélangés donnée par la proposition 19 ne tient plus pour $d > 2$ et la réduction de tout bruit unital chez Alice vers un bruit chez Bob n'est pas valide dans le cas d-dimensionnel.

Quant à Damien-quantique et l'oubli d'information classique post-téléportation, le raisonnement reste valide en d dimensions en remplaçant les opérateurs de Pauli par leur généralisation. Le bruit résultant est un bruit de la famille de Pauli à $d^2 - 1$ paramètres et la fidélité d'intrication demeure invariante sous la simplification Damien-quantique.

Un piège concernant la wernerisation en d dimensions dans le cas d'un bruit brouillant conjointement l'intrication de plusieurs ports de téléportation en parallèle (la dimension du système est alors une puissance de 2 si ce sont des qubits) est de werneriser chaque qubit indépendamment et d'en conclure que le bruit résultat est un bruit globalement dépolarisant (ou du moins un bruit de Pauli dont toutes les erreurs sont équiprobables). Ainsi, même si un bruit est dépolarisant quand on considère séparément chaque canal de téléportation avec wernerisation, quand on considère le canal dans son ensemble, il peut exister des corrélations classiques entre les bruits brouillant chaque canal. Le bruit total n'est ainsi pas simplement le produit tensoriel de bruits dépolarisants. Pour l'illustrer, on n'a qu'à prendre le bruit qui dépolarise avec probabilité $0 < P < 1$ simultanément toute l'intrication de Bob. Le bruit individuellement wernerisé que la téléportation introduit sur chaque qubit téléporté est bel et bien un bruit dépolarisant, mais le bruit total ne l'est pas. Dès qu'un des qubits téléportés ne se comporte pas (lors d'une mesure de Bob par exemple) comme prévu, Bob sait que tous les autres sont complètement mélangés. Si on veut éliminer ces corrélations classiques, il faut vraiment généraliser la wernerisation sur l'ensemble des canaux parallèles de téléportation dont l'intrication est brouillée.

Pour ce faire, on doit procéder différemment de l'annexe II où on utilise l'invariance

de $|\psi^-\rangle$ sous toutes les opérations bi-latérales, puisqu'il n'existe pas d'état qui possède cette propriété dans le cas général en d dimensions. Une façon de contourner ce problème est de « werneriser l'état » plutôt que le canal. Par là, on veut dire qu'on effectue d'abord une opération choisie au hasard parmi un ensemble discret sur l'état pré-téléportation, puis on effectue l'opération inverse sur l'état post-téléportation. Pour former l'ensemble discret, on compose les opérateurs de Pauli généralisés (toujours équivalent à l'oubli post-téléportation de l'information classique) avec une autre famille de d^2-1 éléments qu'on n'explicite pas (il serait intéressant de le faire et ainsi prouver la manœuvre possible), mais dont le rôle est d'uniformiser les d^2-1 paramètres du bruit de Pauli en d dimensions. Le canal de téléportation résultant devrait alors être décrit par un paramètre unique, comme pour le qubit. Augmenter la dimension du canal de téléportation ne rendrait ainsi pas plus complexe la tâche d'en caractériser inférieurement la fidélité d'intrication.

Finalement, l'impact du canal à effacement sur la téléportation quantique est le même peu importe sa dimension. Si on utilise un canal à effacement de dimension d pour téléporter un qudit, alors c'est comme téléporter un qubit en ce qui concerne l'effacement. Si on utilise plusieurs canaux à effacement de dimension 2 en parallèle pour téléporter un qudit, alors c'est simplement comme téléporter plusieurs qubits dont l'effacement est indépendant.

3.2 Téléportation avec relais quantiques

Il est souvent difficile expérimentalement de distribuer l'intrication sur de grandes distances. Par exemple, les photons, fréquemment utilisés pour les tâches reliées aux communications autant classiques que quantiques, sont facile à perdre dans l'environnement. Il peut ainsi être intéressant de transporter l'intrication plusieurs fois sur de courtes distances plutôt que de s'entêter avec un improbable envoi longue-distance. C'est le raisonnement derrière les relais quantiques, lesquels sont basés sur le phénomène du transfert d'intrication. On décrit ce principe bien connu avant de s'attarder, dans une étude

originale, à l'effet de l'intrication brouillée sur la téléportation quantique avec relais dans les contextes de l'effacement de l'information classique et de la wernerisation. On finit avec une courte analyse, également nouvelle, des conséquences du facteur d'effacement sur le nombre idéal de relais dans un réseau de distribution d'intrication.

3.2.1 Transfert d'intrication

Le transfert d'intrication [43] est en fait le cas particulier de la téléportation quantique où l'état qu'on téléporte est lui-même déjà maximalement intriqué avec un tiers état. On donne le protocole qui permet à Alice de partager son intrication avec Charlie grâce à la coopération de l'intermédiaire Bob, et on l'illustre à la figure 3.2.

Protocole (Transfert d'intrication)**.**

0.
- *Alice crée la paire $|\phi^+\rangle_{AB}$ et envoie la moitié B à Bob.*
- *Pendant ce temps, Bob crée la paire $|\phi^+\rangle_{B'C}$ et envoie la moitié C à Charlie.*

1. *Bob mesure les deux qubits B et B' dans la base de Bell et annonce la réponse à Alice et/ou Charlie.*
2. *Alice ou Charlie effectue la rotation de Pauli correspondant au résultat de l'étape précédente.*

Bob transforme ainsi son intrication Alice-Bob et Bob-Charlie en intrication Alice-Charlie. On note que l'on peut ajouter autant de personnages à la chaîne que l'on désire : plus on est de fous, plus on rit ! Dans une situation à n participants, tous les nœuds intermédiaires peuvent s'abstenir de faire leur rotation de Pauli au fur et à mesure. Ils relèguent alors la charge à l'un des deux personnages finaux qui, une fois toutes les mesures de Bell effectuées, n'a plus qu'à faire qu'une seule opération : le produit de l'ensemble des rotations qu'il remplace $\prod_i \sigma_i$. On obtient le même résultat peu importe à qui sont attribuées les rotations de Pauli lorsque l'intrication et les manipulations sont parfaites.

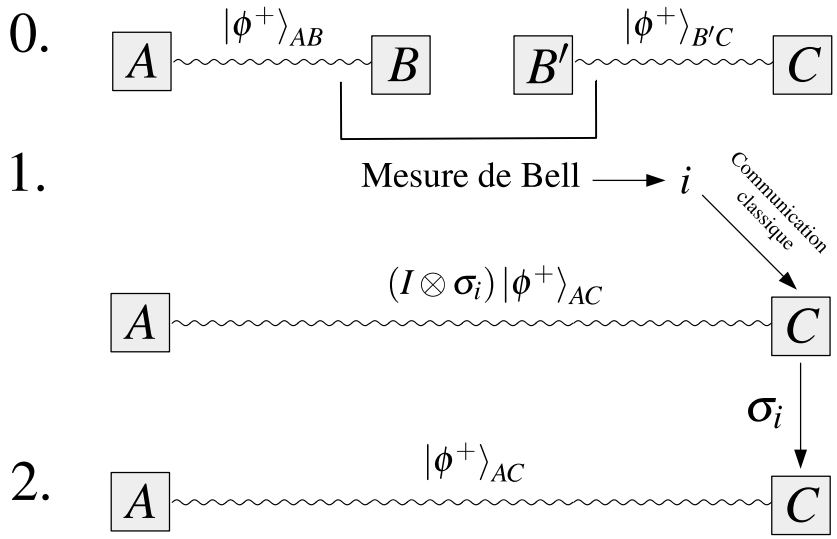

Figure 3.2 – Protocole de transfert d'intrication. L'intermédiaire Bob est intriqué avec Alice et Charlie. En effectuant une mesure de Bell sur ses deux états, Bob transfère son intrication à Alice et Charlie. Comme pour la téléportation standard, la communication classique du résultat de la mesure est nécessaire, puisque la paire EPR nouvellement créée n'est à ce moment plus nécessairement la même que les deux paires intriquées consommées par Bob. Alice ou Charlie doit donc rectifier leur état avec la rotation de Pauli appropriée.

3.2.2 Téléportation brouillée avec relais quantiques

On appelle, dans ce travail, la téléportation quantique avec relais le scénario où le transfert d'intrication, par mesure de Bell entre chaque noeud d'un réseau, permet d'établir un canal de téléportation entre les deux extrémités de la chaîne. On considère que c'est toujours le destinataire final de l'état téléporté qui exerce la rotation de Pauli correspondant à l'ensemble des résultats des mesures (du transfert d'intrication et de la téléportation). En l'absence totale de bruit, ce scénario mène au même résultat que si l'on effectue en série la téléportation complète (rotation de Pauli à chaque nœud). Dans la situation où l'intrication est brouillée, cette équivalence ne tient plus toujours. Toutefois, on retrouve cette correspondance si l'on oublie à la fin du protocole les résultats de toutes les mesures de Bell. La wernerisation permet également une simplification intéressante sous l'hypothèse que l'intrication n'est que légèrement brouillée.

3.2.2.1 L'oubli post-téléportation des mesures

On examine l'effet de l'intrication brouillée sur la téléportation quantique à l'aide de relais lorsque l'on oublie ultimement les résultats des mesures, en donnant d'abord le résultat du protocole complet de téléportation avec oubli quand on l'applique deux fois en chaîne, puis en le comparant avec la version avec relais.

Proposition 34. *Soit deux canaux de téléportation brouillée, le premier entre Alice et Bob et l'autre entre Bob et Charlie. Si* $\{\sigma_j \mathsf{A}_i \sigma_j\}_i$ *et* $\{\sigma_l \mathsf{A}'_k \sigma_l\}_k$ *sont les opérateurs de Kraus correspondant à l'effet de l'intrication brouillée conditionné sur les résultats* j *et* l *des mesures de Bell respectives d'Alice et Bob. Les probabilités des différents* j *et* l *ne sont pas nécessairement uniformes. Lorsque l'on effectue les deux téléportations, Alice vers Bob et Bob vers Charlie, en série, et qu'on efface les deux résultats classiques à la fin, l'effet de l'intrication brouillée sur le canal final entre Alice et Charlie s'exprime ainsi :*

$$\{\text{Damien}\left[\sigma_l \mathsf{A}'_k \sigma_l\right] \circ \text{Damien}\left[\sigma_j \mathsf{A}_i \sigma_j\right]\}_{ik} = \{\frac{1}{\sqrt{4}}\sigma_l \mathsf{A}'_k \sigma_l \circ \frac{1}{\sqrt{4}}\sigma_j \mathsf{A}_i \sigma_j\}_{ijkl}$$

Démonstration. On dédouble la proposition 28 et on compose ensemble chaque côté des deux équations résultantes. ■

On constate à présent que lorsque l'on utilise un relais, autrement dit quand Bob ne fait que mesurer dans la base de Bell et laisse la tâche d'effectuer la rotation de Pauli à Charlie, l'oubli après la téléportation de tous les résultats des mesures a le même effet que ci-dessus.

Proposition 35. *En présence de tout type d'intrication brouillée, la téléportation complète en chaîne sur plusieurs canaux et la téléportation avec relais qui utilise les mêmes canaux sont strictement équivalentes si l'on ne garde pas en mémoire les résultats des mesures de Bell.*

Démonstration. On reprend l'équation de la proposition précédente, mais Charlie applique σ_j au lieu de Bob. Les matrices de Pauli commutant à une phase globale près, on

retrouve le résultat de la proposition précédente.

$$\begin{aligned}\{\text{Damien}\left[\sigma_j \text{Damien}\left[\sigma_l \mathsf{A}'_k \sigma_l\right] \circ \mathsf{A}_i \sigma_j\right]\}_{ik} &= \{\text{Damien}\left[\sigma_j \frac{1}{\sqrt{4}} \sigma_l \mathsf{A}'_k \sigma_l \circ \mathsf{A}_i \sigma_j\right]\}_{ikl} \\ &= \{\frac{1}{\sqrt{4}} \sigma_j \frac{1}{\sqrt{4}} \sigma_l \mathsf{A}'_k \sigma_l \circ \mathsf{A}_i \sigma_j\}_{ijkl} \\ &= \{\frac{1}{\sqrt{4}} \sigma_l \mathsf{A}'_k \sigma_l \circ \frac{1}{\sqrt{4}} \sigma_j \mathsf{A}_i \sigma_j\}_{ijkl} \\ &= \{\text{Damien}\left[\sigma_l \mathsf{A}'_k \sigma_l\right] \circ \text{Damien}\left[\sigma_j \mathsf{A}_i \sigma_j\right]\}_{ik} \blacksquare\end{aligned}$$

Toujours dans le scénario où l'on oublie le résultat des mesures à la fin, on examine à présent le bruit de Pauli du canal résultant de l'utilisation de deux canaux reliés par un relais quantique et dont l'intrication est brouillée. On vient de voir que c'est équivalent à la réalisation de deux téléportations, l'une après l'autre. Le bruit résultant est donc simplement la composition des deux bruits de Pauli. On quantifie le résultat ainsi :

Proposition 36. *Le canal de téléportation avec oubli issu de la composition à l'aide d'un relais quantique de deux canaux en série consommant l'intrication brouillée* ρ_{AB} *et* $\rho'_{B'C'}$

est un canal brouillé de Pauli dont les valeurs $\{\tilde{p}_{\mathsf{X}}, \tilde{p}_{\mathsf{Y}}, \tilde{p}_{\mathsf{Z}}\}$ *sont données par :*

$$\begin{aligned}
\tilde{p}_{\mathsf{X}} &= p_{\mathsf{X}} p'_I + p_I p'_{\mathsf{X}} + p_{\mathsf{Y}} p'_{\mathsf{Z}} + p_{\mathsf{Z}} p'_{\mathsf{Y}} \\
\tilde{p}_{\mathsf{Y}} &= p_{\mathsf{Y}} p'_I + p_I p'_{\mathsf{Y}} + p_{\mathsf{X}} p'_{\mathsf{Z}} + p_{\mathsf{Z}} p'_{\mathsf{X}} \\
\tilde{p}_{\mathsf{Z}} &= p_{\mathsf{Z}} p'_I + p_I p'_{\mathsf{Z}} + p_{\mathsf{Y}} p'_{\mathsf{X}} + p_{\mathsf{X}} p'_{\mathsf{Y}}
\end{aligned}$$

$$\textit{avec} \begin{cases}
p_I = 1 - p_{\mathsf{X}} - p_{\mathsf{Y}} - p_{\mathsf{Z}} = \mathrm{tr}\left(\rho_{AB} |\phi^+\rangle\langle\phi^+|_{AB}\right) \\
p'_I = 1 - p'_{\mathsf{X}} - p'_{\mathsf{Y}} - p'_{\mathsf{Z}} = \mathrm{tr}\left(\rho'_{B'C'} |\phi^+\rangle\langle\phi^+|_{B'C'}\right) \\
p_{\mathsf{X}} = \mathrm{tr}\left(\rho_{AB} |\psi^+\rangle\langle\psi^+|_{AB}\right) \\
p'_{\mathsf{X}} = \mathrm{tr}\left(\rho'_{B'C'} |\psi^+\rangle\langle\psi^+|_{B'C'}\right) \\
p_{\mathsf{Y}} = \mathrm{tr}\left(\rho_{AB} |\psi^-\rangle\langle\psi^-|_{AB}\right) \\
p'_{\mathsf{Y}} = \mathrm{tr}\left(\rho'_{B'C'} |\psi^-\rangle\langle\psi^-|_{B'C'}\right) \\
p_{\mathsf{Z}} = \mathrm{tr}\left(\rho_{AB} |\phi^-\rangle\langle\phi^-|_{AB}\right) \\
p'_{\mathsf{Z}} = \mathrm{tr}\left(\rho'_{B'C'} |\phi^-\rangle\langle\phi^-|_{B'C'}\right)
\end{cases}$$

Démonstration. Pour toute intrication, les deux canaux sont réduits par Damien-quantique à des bruits de Pauli paramétrés selon la proposition 29. On compose ensuite les deux bruits de Pauli en utilisant notamment le fait que $\mathsf{Y} = i\mathsf{XZ}$, que les matrices de Pauli commutent et qu'elles sont auto-inverses. ■

On peut traiter un réseau avec plus de deux relais en appliquant simplement le résultant précédent en série. L'intrication entre chaque nœud peut être brouillée de manière variée. La fidélité d'intrication du canal de téléportation résultant est directement (voir proposition 29) donnée par $\tilde{p}_I = 1 - \tilde{p_{\mathsf{X}}} - \tilde{p_{\mathsf{Y}}} - \tilde{p_{\mathsf{Z}}}$, où les paramètres de droite sont donnés par la proposition ci-dessus. Ne pas enregistrer post-téléportation les résultats des mesures classiques est ainsi une bonne méthode pour borner inférieurement de manière quantitative la qualité d'un canal quantique.

3.2.2.2 Wernerisation

Le cas est un peu moins simple pour la wernerisation. En effet, effectuer la wernerisation entre chaque nœud est différent de l'appliquer seulement entre l'envoyeur et le destinataire de la téléportation, même si les deux canaux résultants sont des canaux de Pauli dont les erreurs sont équiprobables.

Proposition 37. *L'effet de l'intrication brouillée sur la téléportation entre Alice et Charlie avec Bob comme relais n'est pas le même si la wernerisation est faite uniquement entre Alice et Charlie que si elle est effectuée entre chaque participant adjacent.*

Démonstration. On exhibe un contre-exemple. Soit l'intrication brouillée dont l'effet est celui des deux canaux totalement déphasants $\mathcal{C}^{A\to B}_{\text{déphasant}}\left(p_{\mathsf{Z}}=\frac{1}{2},\rho\right)$ et $\mathcal{C}^{B\to C}_{\text{déphasant}}\left(p_{\mathsf{Z}}=\frac{1}{2},\rho\right)$, alors :

$$
\begin{aligned}
&\text{wernerisation}\left[\mathcal{C}^{A\to B}_{\text{déphasant}}\left(p_{\mathsf{Z}}=\frac{1}{2},\rho\right)\right]\circ\text{wernerisation}\left[\mathcal{C}^{B\to C}_{\text{déphasant}}\left(p_{\mathsf{Z}}=\frac{1}{2},\rho\right)\right]\\
&=\mathcal{C}^{A\to B}_{\text{dépolarisant}}\left(P=\frac{2}{3},\cdot\right)\circ\mathcal{C}^{B\to C}_{\text{dépolarisant}}\left(P=\frac{2}{3},\cdot\right)\\
&=\mathcal{C}^{A\to C}_{\text{dépolarisant}}\left(P=\frac{8}{9},\cdot\right)\\
&\neq\text{wernerisation}\left[\mathcal{C}^{A\to B}_{\text{déphasant}}\left(p_{\mathsf{Z}}=\frac{1}{2},\cdot\right)\circ\mathcal{C}^{B\to C}_{\text{déphasant}}\left(p_{\mathsf{Z}}=\frac{1}{2},\cdot\right)\right]\\
&=\text{wernerisation}\left[\mathcal{C}^{A\to C}_{\text{déphasant}}\left(p_{\mathsf{Z}}=\frac{1}{2},\cdot\right)\right]\\
&=\mathcal{C}^{A\to C}_{\text{dépolarisant}}\left(P=\frac{2}{3},\cdot\right)
\end{aligned}
$$

■

La wernerisation à répétition peut donc nuire. Mais ce n'est pas automatique : parfois elle aide. En effet, on peut trouver par un calcul similaire à celui ci-haut que la composition d'un canal inversant la phase avec probabilité $\frac{1}{2}$ et d'un canal inversant le bit avec la même probabilité n'est complètement dépolarisant que si l'on ne wernerise pas à chaque étape. Cependant, sous l'hypothèse la plus intéressante expérimentalement, c'est-à-dire en considérant que chaque canal subit un bruit de Pauli (toute intrication brouillée est équivalente à un bruit de Pauli dès que l'on néglige l'information classique) dont

les trois paramètres, $\{p_{\mathsf{X}}, p_{\mathsf{Y}}, p_{\mathsf{Z}}\}$, sont petits, on démontre que les deux méthodes de wernerisation sont équivalentes.

Proposition 38. *Soit deux canaux modélisant deux sections d'une chaîne de téléportation avec relais, $\mathcal{C}^{A\to B}$ et $\mathcal{C}'^{B\to C}$, et dont l'intrication est légèrement brouillée. On les compose ensemble afin d'appliquer la téléportation quantique avec relais quantique. Si $p_{\mathsf{X}}, p_{\mathsf{Y}}, p_{\mathsf{Z}}, p'_{\mathsf{X}}, p'_{\mathsf{Y}}, p'_{\mathsf{Z}} \ll 1$ sont les paramètres des bruits de Pauli des deux canaux initiaux sous l'effet de Damien-quantique, alors l'effet de l'intrication brouillée est le même si l'on wernerise à chaque nœud du réseau que simplement aux extrémités.*

Démonstration. D'une part on a :

$$\begin{aligned}
&\text{wernerisation}\left[\mathcal{C}^{A\to B}\right] \circ \text{wernerisation}\left[\mathcal{C}'^{B\to C}\right] \\
&= \mathcal{C}^{A\to B}_{\text{dépolarisant}}\left(P = \frac{4p_{\mathsf{X}}+4p_{\mathsf{Y}}+4p_{\mathsf{Z}}}{3}, \cdot\right) \circ \mathcal{C}'^{B\to C}_{\text{dépolarisant}}\left(P = \frac{4p'_{\mathsf{X}}+4p'_{\mathsf{Y}}+4p'_{\mathsf{Z}}}{3}, \cdot\right) \\
&= \mathcal{C}^{A\to C}_{\text{dépolarisant}}\left(P = 1 - \left(1 - \frac{4p_{\mathsf{X}}+4p_{\mathsf{Y}}+4p_{\mathsf{Z}}}{3}\right)\left(1 - \frac{4p'_{\mathsf{X}}+4p'_{\mathsf{Y}}+4p'_{\mathsf{Z}}}{3}\right), \cdot\right) \\
&\approx \mathcal{C}^{A\to C}_{\text{dépolarisant}}\left(P = \frac{4p_{\mathsf{X}}+4p_{\mathsf{Y}}+4p_{\mathsf{Z}}}{3} + \frac{4p'_{\mathsf{X}}+4p'_{\mathsf{Y}}+4p'_{\mathsf{Z}}}{3}, \cdot\right)
\end{aligned}$$

De l'autre, on compose d'abord les deux bruits comme à la proposition 36, mais avec l'approximation que leur addition est linéaire. Puis, on les wernerise et on retrouve le résultat ci-dessus.

$$\begin{aligned}
&\text{wernerisation}\left[\mathcal{C}^{A\to B} \circ \mathcal{C}'^{B\to C}\right] \\
&\approx \mathcal{C}^{A\to C}_{\text{dépolarisant}}\left(P = \frac{4p_{\mathsf{X}}+4p_{\mathsf{Y}}+4p_{\mathsf{Z}}}{3} + \frac{4p'_{\mathsf{X}}+4p'_{\mathsf{Y}}+4p'_{\mathsf{Z}}}{3}, \cdot\right) \\
&\approx \text{wernerisation}\left[\mathcal{C}^{A\to B}\right] \circ \text{wernerisation}\left[\mathcal{C}'^{B\to C}\right]
\end{aligned}$$

■

L'application unique du protocole de wernerisation dans un contexte de téléportation légèrement brouillée avec relais donne alors un canal résultant dépolarisant dont on peut approximer la fidélité par celle du canal issu de la composition des canaux individuellement wernerisés. C'est pratique, parce que la composition des bruits dépolarisants est

encore plus simple que celle des bruits de Pauli.

Proposition 39. *Soit un réseau de téléportation avec relais de n canaux en série dont l'intrication $\rho_{A_iB_i}$ est légèrement brouillée. Le canal résultant est, une fois wernernisé, un canal dépolarisant de paramètre P' avec*

$$P' = 1 - \prod_{i=1}^{n} \left(\frac{-1 + 4\,\mathrm{tr}\left(\rho_{AB}\,|\phi^+\rangle\langle\phi^+|_{A_iB_i}\right)}{3} \right)$$

Démonstration. Sous l'hypothèse que l'effet de l'intrication brouillée se réduit à des bruits de Pauli dont tous les paramètres de Pauli sont $\ll \frac{1}{n}$, le bruit est équivalent quand on wernerise aux extrémités, par la proposition précédente, à celui de n canaux dépolarisants. La composition de n canaux dépolarisants différents résulte simplement en un canal dépolarisant de paramètre P' donné par :

$$P' = 1 - \prod_{i=1}^{n} (1 - P_i)$$

Les paramètres P_i sont donnés par la proposition 30. ($P_i < 1$ car le bruit est léger.)

$$P_i = \frac{4 - 4\,\mathrm{tr}\,(\rho_{AB}\,|\phi^+\rangle\langle\phi^+|_{AB})}{3}$$

■

Par cette méthode, on transforme l'effet de toute intrication légèrement brouillée sur un système de téléportation quantique avec relais et oubli en bruit dépolarisant aisément calculable. La fidélité d'intrication se trouve alors par calcul direct $F_{\mathrm{intr}}\left(\mathcal{C}_{\text{dépolarisant}}(P,\cdot)\right) = \frac{4-3P}{4}$.

3.2.3 Relais quantiques et canaux à effacement

Un des plus grands avantages du protocole de téléportation sur l'envoi direct d'un registre physique est, comme mentionné précédemment, sa robustesse face au bruit d'un canal à effacement. En effet, si le qubit envoyé disparaît sans atteindre son destinataire, seule une paire intriquée est gaspillée et l'état quantique à envoyer demeure sain et sauf.

Lorsque chaque demi-paire EPR se rend intacte chez Alice et Bob, ils détiennent (à condition d'avoir aussi un canal classique bi-directionnel) un canal quantique virtuel parfait à usage unique. En présence de mémoires quantiques fiables, le taux de génération de ces canaux de téléportation à usage unique dépend de l'efficacité du canal classique (rarement le facteur limitant) et du taux de génération des paires EPR entre chaque nœud. Ce dernier est dans ce scénario directement relié au taux d'effacement du canal physique. Un trop grand pourcentage de pertes signifie un canal quantique lent. On voit que dans certains cas, quand le canal est très brouillé (par exemple lorsqu'il connecte deux participants fort éloignés), ce taux de rendement peut être augmenté de manière non-négligeable par l'utilisation de relais quantiques. On fait ici une courte analyse quantitative de l'impact du facteur d'effacement, en l'absence d'autres bruits, sur le nombre optimal de relais quantiques pour le partage d'intrication, en présence de mémoire quantique parfaite. Cette dernière condition signifie qu'une fois l'intrication partagée, elle ne se détériore pas avec le temps.

On considère un canal de longueur totale L dont l'effacement a probabilité p_e. On pose le canal homogène sur sa longueur et son effacement irréversible (l'irréversibilité suit de l'approximation de Markov). On peut calculer la probabilité d'effacement en fonction de la longueur l parcourue :

$$P_{\text{effacement}}(l) = 1 - e^{\frac{l}{L}\ln(1-p_e)}$$

Pour quantifier la rapidité du partage d'intrication, on pose que le partage d'intrication s'effectue par un processus de génération locale, puis de transmission[14]. Lors de l'utilisation du canal à effacement de pleine longueur, le taux de succès (de la transmission) par paire EPR générée est ainsi de $1 - p_e$. Par contre, en utilisant n relais quantiques (plus les deux participants aux extrémités) équidistants, le taux de succès du partage d'intrication

[14]Pour un canal à effacement avec un seul chemin d'Alice à Bob, la probabilité qu'Alice et Bob reçoivent tous les deux leur moitié de paire EPR reste la même peu importe le point où l'intrication est générée. On ne précise donc pas qui s'occupe de la génération.

entre les deux bouts par paire EPR générée devient :

$$\tau_{\text{succès}}(n) = \frac{e^{\frac{1}{n+1}\ln(1-p_e)}}{n+1}$$

Le taux de succès n'est donc pas nécessairement meilleur lorsque l'on utilise un plus grand nombre de relais. En dérivant $\tau_{\text{succès}}(n)$, on trouve les extrema :

$$\frac{d\tau_{\text{succ}}(n)}{dn} = -\frac{e^{\frac{1}{n+1}\ln(1-p_e)}}{(n+1)^2} - \frac{e^{\frac{1}{n+1}\ln(1-p_e)}\ln(1-p_e)}{(n+1)^3}$$

Cette fonction n'a ainsi qu'un seul extremum :

$$\frac{d\tau_{\text{succ}}(n)}{dn} = 0 \iff n+1 = -\ln(1-p_e)$$

Il est facile de voir que cet extremum est en fait un maximum global et donc dans le cas où l'on ne considère que du bruit par effacement, le nombre de relais quantiques optimal (vis-à-vis la minimisation de la consommation d'intrication) est :

$$n_{\text{opt}} = -\ln(1-p_e) - 1$$

Comme le nombre de relais quantique est nécessairement naturel, on discrétise le résultat ci-dessus en arrondissant vers le haut à partir du point :

$$\begin{aligned}
&\tau_{\text{succès}}(n) = \tau_{\text{succès}}(n+1) \\
\Leftrightarrow &\frac{e^{\frac{1}{n+1}\ln(1-p_e)}}{n+1} = \frac{e^{\frac{1}{n+2}\ln(1-p_e)}}{n+2} \\
\Leftrightarrow &p_e = 1 - e^{(n+1)(n+2)\log\frac{n+1}{n+2}} \\
\Leftrightarrow &p_e = 1 - \left(\frac{n+1}{n+2}\right)^{(n+1)(n+2)}
\end{aligned}$$

et en arrondissant vers le bas sinon.

Le tableau 3.V indique l'impact de différentes plages de taux d'effacement sur le nombre optimal de relais quantiques. À première vue, l'utilisation de nombreux relais ne semble pas souvent souhaitable et en-dessous d'un taux d'effacement de $p_e = \frac{3}{4}$, il vaut même mieux s'en passer complètement. Toutefois, l'ordre de grandeur des facteurs d'effacement commandant l'utilisation de plusieurs relais n'est en vérité pas déraisonnable. Dans le cas par exemple où les registres physiques des qubits sont des photons se propageant dans l'air, les pertes peuvent être énormes sur les grandes distances (il en est de même si le médium est la fibre optique). Par exemple, lors de l'expérience de téléportation sur 143 km aux Îles Canaries de 2012 [27], on a enregistré une atténuation dans le signal variant dans le temps entre 28,1 dB ($p_e \approx 1 - 10^{-3}$) et 39,0 dB ($p_e \approx 1 - 10^{-4}$). On extrapole un nouvel exemple pour illustrer le résultat.

Exemple 6. *Supposons qu'on établissait entre Montréal et Genève un canal à effacement homogène dans des conditions similaires à celles ayant régi l'expérience de 2012 aux Îles Canaries (nonobstant le fait que la Terre soit ronde), combien de relais quantiques devrait-on utiliser ?*

La distance Montréal-Genève est d'environ 40×143 *km. Le taux d'effacement pourrait ainsi varier entre* $p_e \approx 1 - 10^{-3\times 40}$ *et* $p_e \approx 1 - 10^{-4\times 40}$. *Il faudrait donc entre* 276 *et* 367 *relais quantiques. La grande différence entre les deux valeurs provient du fait que le taux d'effacement total est exponentiel par rapport au taux d'effacement par unité de longueur du canal. Composer plusieurs canaux à effacement résulte ainsi en un canal exponentiellement pire que ses parties.*

Il faut noter que le bruit engendré par la création locale de la paire intriquée et celui engendré par la mesure de Bell augmente avec le nombre n de relais. Les intermédiaires ne sont donc utiles que s'ils peuvent effectuer ces opérations de manière suffisamment fiable. Le bruit engendré par la rotation correctrice de Pauli est constant peu importe le nombre de relais si l'on remplace l'application de la rotation à chaque étape par l'exécution finale et unique de la composition des n rotations, et qu'on néglige le bruit dans la communication classique.

Taux d'effacement p_e	Nombre n optimal de relais quantiques
$p_e \leq \frac{3}{4}$	0
$\frac{3}{4} \leq p_e \lesssim 0.912$	1
$0.912 \lesssim p_e \lesssim 0,968$	2
...	...
$0,999972 \lesssim p_e \lesssim 0,999990$	10
...	...
$1-\left(\frac{n}{n+1}\right)^{(n)(n+1)} < p_e < 1-\left(\frac{n+1}{n+2}\right)^{(n+1)(n+2)}$	n

Tableau 3.V – Plus le taux d'effacement est élevé (plus le canal est long), et plus l'utilisation de relais quantique est bénéfique. Si le bruit d'effacement n'est pas très important et que d'autres facteurs ne commandent pas l'utilisation de relais quantiques, alors leur usage est déconseillé.

Au-delà du possible avantage pour la transmission d'intrication, l'utilisation de relais peut être nécessaire à cause de contraintes techniques et géométriques (où, par exemple, installer deux canaux plus courts est envisageable, mais pas un long). Ceux-ci permettent également d'alléger la structure d'un réseau cherchant à relier plusieurs nœuds.

3.3 Téléportation multi-ports quantique

La téléportation quantique multi-ports [24] diffère conceptuellement de la téléportation quantique standard. Voici un bref aperçu de la tâche idéalisée. Elle est aussi illustrée à la figure 3.3. Une description détaillée et nuancée du protocole suivra.

Protocole (Téléportation quantique multi-ports — description de haut-niveau)**.**

0. Alice et Bob partagent un état conjoint sur les registres $AB = A_1B_1A_2B_2\ldots A_iB_i\ldots A_nB_n$. Chaque registre A_i est appelé port d'entrée et chaque registre B_i port de sortie. On appelle simplement port le couple A_iB_i. Alice possède aussi dans le registre C un état ρ_C qu'elle veut téléporter à Bob. Tous les registres ont la même dimension.

1. *Alice effectue une mesure de type POVM sur l'ensemble conjoint des registres A_i et C. Elle obtient une valeur classique j qu'elle communique à Bob.*

2. *Bob retrouve l'état ρ_B dans le registre B_j. Il jette (ou ignore) tous les autres registres B_i, où $i \neq j$.*

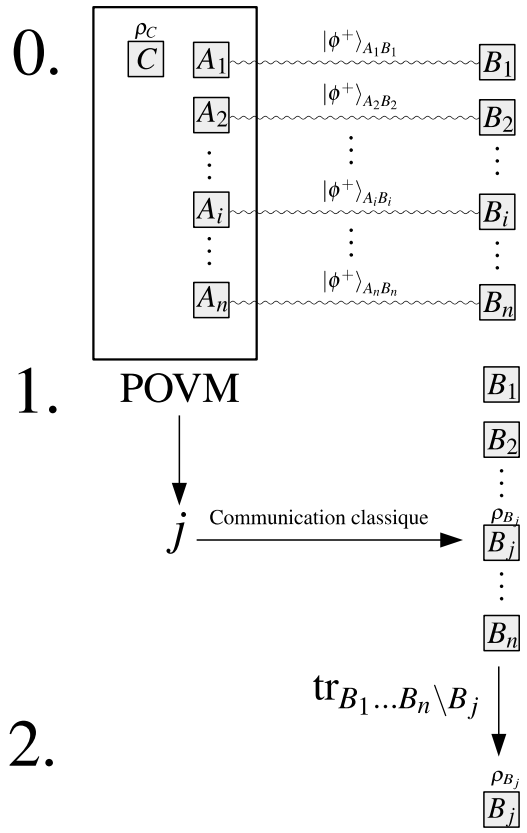

Figure 3.3 – Protocole de téléportation quantique multi-ports utilisant des paires EPR pour téléporter le qubit ρ_C de Alice vers Bob. Alice et Bob partagent initialement n paires $|\phi^+\rangle$. Puis, Alice fait une mesure de type POVM de ses n qubits A et de C. Elle en communique le résultat à Bob qui retrouve alors ρ_{B_j} dans le registre B_j et qui se débarrasse de tous les autres registres.

Tout l'intérêt et la puissance de la téléportation multi-ports proviennent de la caractéristique suivante : Bob n'a pas à appliquer de corrections sur son port de sortie pour

retrouver ρ. Tout ce qu'il doit faire c'est sélectionner le bon port ! Cela veut dire que Bob peut débuter et compléter un calcul quantique demandant un temps arbitraire sur chacun des ports de sortie avant même qu'Alice n'ait choisi quel état elle lui téléporterait. Lorsque Alice effectuera la mesure et lui annoncera le port, Bob aura instantanément la réponse ! Un exemple humoristique illustre ce phénomène à l'annexe IV.

Le désavantage le plus évident de la téléportation multi-ports est la nécessitée présagée par le paramètre n d'un grand nombre de ports de sortie (et d'entrée). En fait, la téléportation multi-ports est un protocole qui n'atteint la perfection qu'asymptotiquement. Donc en plus de demander beaucoup d'intrication, il n'est sans erreur que dans la limite $\lim_{n\to\infty}$. La forme que prend l'imperfection de la téléportation dans le cas où le nombre n de ports de sortie est fini dépend du protocole utilisé. Il en va de même pour la structure de l'intrication consommée qui peut prendre plusieurs formes. On s'appuie donc sur les travaux de S. Ishizaka et T. Hiroshima [24, 25, 23] pour clarifier ces deux aspects de la téléportation multi-ports et se pencher sur la mesure de type POVM au cœur du protocole. On analyse ensuite l'effet de l'intrication brouillée selon différents modèles à la manière de la section 3.1 sur la téléportation standard.

La preuve de la téléportation multi-ports figurant dans ce travail (et complétée à l'annexe V) est nouvelle dans ses détails, mais elle s'appuie fortement sur l'originale [25, 23]. L'analyse de l'effet du bruit est quant à elle complètement originale, sauf mentions contraires au début de la sous-section 3.3.4 et à la proposition 54..

3.3.1 Protocole déterministe vs probabiliste

Plusieurs versions du protocole de téléportation multi-ports existent. La première division concerne le POVM effectué par Alice à l'étape 1 (se référer au protocole ci-haut). La version *déterministe* fut introduite par S. Ishizaka et T. Hiroshima dans un article de 2008 [24], tandis que la version *probabiliste* l'a été dans un article de 2009 des mêmes auteurs [25]. Bien que les deux protocoles soient asymptotiquement équivalents, ce choix

affecte le type d'imperfection dans le cas réaliste où le nombre de ports d'entrée n est fini.

La téléportation multi-ports dans sa version *déterministe* est un protocole dont le résultat $j \in \{1,\ldots,n\}$ de la mesure assure toujours une téléportation (brouillée) de l'état ρ_C vers le port B_j. Toutefois, la fidélité d'intrication de l'état post-téléportation ρ'_B par rapport à l'état pré-téléportation ρ_C est < 1 lorsque n est fini. Plus n est grand, plus l'état ρ'_B à la sortie est près de l'état ρ_C à l'entrée. Asymptotiquement, la fidélité atteint 1 et la téléportation est parfaite.

Il existe une autre façon d'effectuer la mesure de type POVM. C'est la version *probabiliste*. Dans ce cas, $j \in \{0,\ldots,n\}$ peut aussi prendre la valeur 0. Lorsque ce résultat est obtenu, l'état téléporté n'arrive pas dans un des ports de sortie et on le considère perdu[15]. Cependant, lorsque $j \neq 0$, alors l'état ρ'_B post-téléportation est exactement identique à l'état ρ_C à l'entrée. En augmentant n, on diminue la probabilité d'obtenir $j = 0$. Asymptotiquement, cette probabilité est 0 et la téléportation réussit toujours.

On s'intéresse dans ce qui suit uniquement au protocole probabiliste. Les résultats obtenus seront tout de même asymptotiquement valides pour le protocole déterministe.

3.3.2 Intrication

Une autre distinction à prendre en compte lorsque l'on considère le protocole de téléportation multi-ports est la ressource utilisée, c'est-à-dire la forme de l'intrication partagée.

On se limite dans ce travail au cas où l'intrication partagée est n paires EPR. On

[15] Bob pourrait quand même le récupérer avec probabilité et fidélité 1, mais cela lui demanderait de faire, avec la collaboration d'Alice, une opération quantique conjointe sur tous ses ports de sortie (voir [23]). Cette correction complexe qui ne commute pas avec toute opération indépendante sur chaque port de sortie dénature complètement l'avantage initial de la téléportation multi-ports. C'est pourquoi on ne s'y intéresse pas.

utilise cette fois $|\psi^-\rangle$ plutôt que $|\phi^+\rangle$ afin de rendre plus directe la démonstration. L'intrication a ainsi la forme $\rho_{AB} = \bigotimes_{i=1}^{n} |\psi^-\rangle\langle\psi^-|_{A_iB_i}$. Pour n fini, ce n'est pas optimal[16]. Par contre, la manipulation autant algébrique qu'expérimentale de n états EPR de dimension $d = 4$ est plus simple que celle d'un état de dimension $d = 4^n$ et comme le résultat est asymptotiquement aussi valable, on préfère cette version.

3.3.3 Protocole probabiliste pour un qubit avec paires EPR

On commence par expliquer le fonctionnement derrière le protocole pour téléporter un qubit. On a établi dans la sous-section précédente que l'on utiliserait l'intrication $\rho_{AB} = \bigotimes_{i=1}^{n} |\psi^-\rangle\langle\psi^-|_{A_iB_i}$ pour téléporter le qubit ρ_C. La prochaine étape consiste donc à expliciter le POVM que doit utiliser Alice lors de sa mesure et à montrer que la probabilité que cette mesure téléporte, avec pleine fidélité, ρ_C vers Bob tend vers 1 lorsque n tend vers l'infini. On ne se penche dans ce mémoire que sur la téléportation multi-ports du qubit, même si contrairement à la téléportation standard, effectuer la téléportation multi-ports d'un qubit plusieurs fois en parallèle n'est pas équivalent à la réalisation de la téléportation multi-ports d'un qudit.

3.3.3.1 Allure du POVM

Pour avoir une bonne intuition du genre de mesure qui donne lieu à la téléportation avec des paires EPR, on considère le cas de la téléportation multi-ports avec comme seule ressource $|\psi^-\rangle_{A_1B_1}$, autrement dit $n = 1$.

Dans ce cas, on peut utiliser naïvement le protocole de la téléportation standard. Si Alice effectue une mesure et obtient le résultat $|\psi^-\rangle_{CA_1}$, la téléportation multi-ports est réussie. Si Alice obtient comme résultat n'importe lequel des trois autres états de Bell,

[16] En effet, en gardant le nombre n de ports de sortie fixe, on peut faire mieux en prenant un certain état partagé dont l'intrication des n ports est inter-reliée. Ce résultat est exposé dans les premiers articles introduisant les téléportations multi-ports déterministe [24] et probabiliste [25].

alors on considère la téléportation comme échouée. Les quatre résultats sont équiprobables et ce protocole naïf nous permet de minorer la probabilité maximale de réussite que peut atteindre la téléportation multi-ports par celle que peut atteindre la téléportation standard : $\mathsf{P}_{\text{succès}}(n=1) \geq \frac{1}{4}$.

On pourrait aussi montrer que $\mathsf{P}_{\text{succès}}(n=1) \leq \frac{1}{4}$, car le contraire implique la possibilité pour Alice et Bob de communiquer de manière supraluminique (on n'en fait pas la démonstration). Réaliser le protocole de téléportation multi-ports à $n=1$ port de sortie en utilisant la téléportation quantique standard (et donc en espérant mesurer $|\psi^-\rangle$) est ainsi optimal.

Ce qu'il est important de constater, c'est qu'en utilisant l'ensemble $\bigotimes_{i=1}^{n} |\psi^-\rangle\langle\psi^-|_{A_iB_i}$ comme ressource intriquée, l'état ρ_C d'Alice est téléporté vers Bob lorsque Alice réussit une projection de la forme suivante (où $\rho^{\text{déchet}}$ est un état résiduel sans importance) :

$$\rho_C \otimes \left(\bigotimes_{i=1}^{n} |\psi^-\rangle\langle\psi^-|_{A_iB_i} \right) \xrightarrow{\text{projection}} |\psi^-\rangle\langle\psi^-|_{CA_j} \otimes \rho^{\text{déchet}}_{A_1\ldots A_n \setminus A_j} \tag{3.1}$$

Ce qu'on cherche donc est un POVM qui offre asymptotiquement à Alice une probabilité 1 d'obtenir $\psi^-_{CA_j}$ comme résultat de mesure, où le j peut être n'importe lequel des n ports. Cette projection est le principe derrière la téléportation multi-ports quantique.

On présente informellement[17] le POVM qu'Alice effectue sur ses n demi-paires EPR et son qubit à téléporter. En premier, pour obtenir un résultat de la forme de l'équation 3.1, elle doit poser un POVM équivalant de manière intuitive à la question suivante :

[17] La notation pour expliciter rigoureusement le POVM (la partie « déchet » surtout) est très lourde et n'est pas nécessaire pour le reste de ce travail. Le POVM pour le protocole probabiliste utilisant des paires EPR est donné dans l'article de 2009 [25].

Question 1

Est-ce que le qubit du registre C forme une paire $|\psi^-\rangle_{CA_i}$ avec l'un des ports d'entrée A_i ? Lequel ?

Comme on a voulu l'expliquer ci-dessus avec l'exemple à $n = 1$ port, une réponse affirmative à cette question assure le succès de la téléportation. Alice n'a alors qu'à envoyer le numéro du port j par message classique à Bob. On va montrer qu'asymptotiquement cette mesure est toujours concluante.

Pour bâtir cette mesure, on considère la mesure correspondant à la question intermédiaire[18] :

Question 2

Combien de paires $|\psi^-\rangle$ peut-on simultanément former avec les $n+1$ qubits des registres A et C ?

On appelle cette quantité r.

Pour résumer, voici comment Alice s'y prend pour réaliser le POVM de la téléportation multi-ports. En premier, elle effectue la projection correspondant à la question 2 et forme ainsi r couples $|\psi^-\rangle$ entre ses $n+1$ qubits. Ensuite, elle projette son résultat selon la question 1 et apprend si ρ_C a été pairé (et avec qui). Si oui, c'est avec un des n ports d'entrée chez Alice. ρ_C est donc téléporté vers le port de sortie correspondant chez Bob, qui bien sûr ne le sait pas tant qu'Alice ne le lui a pas annoncé par communication classique.

[18] Cette mesure est conceptuellement importante, mais on verra qu'il n'est pas nécessaire de la réaliser concrètement (ou plutôt, que l'on peut en oublier le résultat dès que toutes les mesures du côté d'Alice ont été effectuées).

3.3.3.2 Calcul de la probabilité de succès

Pour établir la validité du protocole, on doit démontrer que sa probabilité de succès tend vers 1 quand $\lim_{n\to\infty}$. On fait un bref détour en conditionnant sur r.

Comme tous les qubits des registres A sont localement complètement mélangés et que le POVM derrière la question 2 telle qu'énoncée ne fait pas de distinction entre le qubit C à téléporter et chacun des ports d'entrées A_i, on a par symétrie que la probabilité que le qubit à téléporter appartienne à une paire $|\psi^-\rangle$ est la même que celle de n'importe quel port d'entrée. La probabilité de succès sachant r paires parmi $n+1$ qubits est ainsi simplement le rapport du nombre de qubits en couple sur le nombre total de qubits $n+1$.

Proposition 40. *La probabilité, conditionnée sur r, de succès du protocole probabiliste de téléportation multi-ports utilisant des paires EPR,* $\mathsf{P}_{succès|r}(n)$*, est donnée par :*

$$\mathsf{P}_{succès|r}(n) = \frac{2r}{n+1}$$

On note que l'on pourra calculer directement la probabilité de succès $\mathsf{P}_{\text{succès}}(n)$ lorsque l'on connaîtra la probabilité $\mathsf{P}_r(n)$ de former exactement r paires $|\psi^-\rangle$ avec les $n+1$ qubits des registres A et C :

$$\mathsf{P}_{\text{succès}}(n) = \sum_r \mathsf{P}_{\text{succès}|r}(n) \cdot \mathsf{P}_r(n)$$

On se penche donc sur ce calcul.

3.3.3.3 Calcul de $\mathsf{P}_r(n)$

En physique, on fait souvent référence au spin : une propriété physiquement mesurable (elle a les mêmes unités que $\hbar$, soit des *joule·secondes*) de certaines particules. Derrière cette caractéristique physique se cache une abstraction mathématique qui permet de classer les états en fonction de leur symétrie. Cette abstraction sans unité, qu'on appelle les *nombres quantiques*, permet de classifier toute forme d'information quantique, même

si celle-ci n'est pas encodée dans des particules ayant concrètement un spin physique. Ici, on va s'en servir pour subdiviser l'espace de tous les états quantiques composés de $n+1$ qubits.

Autrement dit, on va diviser cet espace, dont la base est de 2^{n+1} états, en sous-espaces dont tous les états sont paramétrés par un S de même valeur. Le nombre quantique S associé à un qubit est $S = \frac{1}{2}$. Par abus de langage, on va appeler S le spin total d'un état quantique plutôt que le *nombre quantique associé au spin total*[19].

On pose sans le démontrer[20] que le POVM correspondant à la question 2 effectue en fait une projection dans le sous-espace de spin total $S = \frac{n+1}{2} - r$.

Proposition 41. *Répondre à la question 2 projette les $n+1$ qubits d'Alice vers le sous-espace de spin total S. Le spin total S et le paramètre r sont directement reliés par*

$$S(r) = \frac{n+1}{2} - r$$

$\mathsf{P}_r(n)$ est ainsi le ratio du nombre d'états orthogonaux de spin total $S = \frac{n+1}{2} - r$ sur le nombre total d'états composant la base de l'espace à $n+1$ qubits.

$$\mathsf{P}_r(n) = \mathsf{P}_{\frac{n+1}{2}-S}(n) = \frac{\#\text{ états orthogonaux de spin total } S}{2^{n+1}}$$

La classification selon le spin des états formés par la composition de qubits (cette composition forme ici le groupe $SU(2)^{\otimes n+1}$) est un problème classique en mécanique quantique. Dans le cas qui nous intéresse, il y a deux paramètres de dégénérescence[21]

[19] Le véritable spin total $\tilde{S}$ est relié à son nombre quantique S par la formule $\tilde{S} = \sqrt{\frac{3\hbar^2}{4}}$. De plus, il n'a un sens que lorsque l'on parle de particules qui, contrairement à l'abstraction mathématique qu'est le qubit, ont concrètement un spin physique. On peut toutefois attribuer des nombres quantiques à des états quantiques sans commettre de faute formelle.

[20] L'intuition est que la paire $|\psi^-\rangle$ a un spin total $S = 0$, tandis que toutes les autres paires EPR ont une symétrie reliée à un spin total $S = 1$.

[21] Un état $|\psi\rangle$ est dit dégénéré s'il correspond à plus d'un état du système. On lève la dégénérescence en prenant en compte un ou plusieurs paramètres supplémentaires. Par exemple, $\mathrm{tr}_B(|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B) = \mathrm{tr}_B(|0\rangle\langle 0|_A \otimes |1\rangle\langle 1|_B)$ est un état dégénéré (dégénérescence de degré 2), mais en considérant le registre B, les deux états $|00\rangle_{AB}$ et $|01\rangle_{AB}$ deviennent orthogonaux et la dégénérescence est levée.

correspondant aux états de spin total S. Le premier concerne la multiplicité $\mathrm{c}^{[n+1,S]}$ du spin total. Celle-ci est levée lorsque l'on discrimine les états selon leur spin S_z. S_z est la projection du spin de l'état sur un axe $\hat{z}$ donné [22], par exemple $|000\ldots0\rangle\langle000\ldots0|$. La seconde dégénérescence, $\mathrm{g}^{[n+1,S]}$, correspond à la multiplicité de permutation des $n+1$ qubits, c'est-à-dire qu'on peut obtenir des états linéairement indépendants en changeant l'ordre des qubits.

Le cas de la multiplicité $\mathrm{c}^{[n+1,S]}$ est simple. S_z peut prendre des valeurs entières ou demi-entières et est borné par $\pm S_z$. Le nombre quantique $S_z \in \{-S, -S+1, \ldots, S\}$ peut donc prendre $2S+1$ valeurs.

Proposition 42. *Le degré de dégénérescence* $\mathrm{c}^{[n+1,S]}$ *dû à* S_z *est donné par :*

$$\begin{aligned}\mathrm{c}^{[n+1,S]} &= 2S+1 \\ &= n+2-2r\end{aligned}$$

Le degré de dégénérescence $\mathrm{g}^{[n+1,S]}$ est moins direct. Dans beaucoup de problèmes courants de composition de spins, on procède de manière itérative en ayant recours aux coefficients de Clebsch-Gordan. C'est d'ailleurs ce qui est fait dans les articles originaux sur la téléportation multi-ports [24, 25]. Toutefois on peut procéder autrement parce que la symétrie de ce problème est propice à l'utilisation des tableaux de Young. On retrouve ainsi plus facilement la formule analytique. On la donne ici telle quelle, mais le calcul est fait à l'annexe V.

Proposition 43. *Le degré de dégénérescence* $\mathrm{g}^{[n+1,S]}$ *dû aux permutations possibles des* $n+1$ *qubits est donné par :*

$$\begin{aligned}\mathrm{g}^{[n+1,S]} &= \frac{(n+1)!}{\left(\frac{n+1}{2}-S\right)!\left(\frac{n+3}{2}+S\right)!}\cdot(2S+1) \\ &= \frac{(n+1)!}{r!\,(n-r+2)!}\cdot(n-2r+2)\end{aligned}$$

[22] Ici encore, on devrait parler du *nombre quantique associé à la projection du spin sur l'axe* $\hat{z}$ pour être plus rigoureux. La différence est d'un facteur $\hbar$.

On a maintenant toute l'information nécessaire pour expliciter $\mathsf{P}_r(n)$ et $\mathsf{P}_{\text{succès}}(n)$.

Proposition 44. *La probabilité conditionnelle de succès* $\mathsf{P}_r(n)$ *est donnée par :*

$$\begin{aligned}\mathsf{P}_r(n) &= \frac{\#\ \textit{états orthogonaux de spin total } S}{2^{n+1}} \\ &= \mathrm{c}^{[n+1,S]} \cdot \mathrm{g}^{[n+1,S]} \cdot \frac{1}{2^{n+1}} \\ &= (2S+1)^2 \cdot \frac{(n+1)!}{\left(\frac{n+1}{2}-S\right)!\left(\frac{n+3}{2}+S\right)!} \cdot \frac{1}{2^{n+1}} \\ &= (n+2-2r)^2 \cdot \frac{(n+1)!}{r!\,(n-r+2)!} \cdot \frac{1}{2^{n+1}}\end{aligned}$$

Proposition 45. *La probabilité totale de succès* $\mathsf{P}_{succès}(n)$ *est égale à :*

$$\begin{aligned}\mathsf{P}_{succès}(n) &= \sum_r \mathsf{P}_{succès|r}(n) \cdot \mathsf{P}_r(n) \\ &= \sum_{r=0}^{\lfloor \frac{n+1}{2} \rfloor} \left(\frac{2r}{n+1} \cdot (n+2-2r)^2 \cdot \frac{(n+1)!}{r!\,(n-r+2)!} \cdot \frac{1}{2^{n+1}} \right) \\ &= \sum_{r=1}^{\lfloor \frac{n+1}{2} \rfloor} \left(\frac{2r}{2^{n+1}} \cdot (n+2-2r)^2 \cdot \frac{n!}{r!\,(n-r+2)!} \right)\end{aligned}$$

On précise que n est toujours le nombre de ports d'entrée et que $n+1$ est le nombre total de qubits chez Alice.

On peut aussi donner la probabilité en fonction de S afin de comparer le résultat à la littérature.

$$\begin{aligned}\mathsf{P}_{\text{succès}}(n) &= \sum_{r=1}^{\lfloor \frac{n+1}{2} \rfloor} \left(\frac{2r}{2^{n+1}} \cdot (n+2-2r)^2 \cdot \frac{n!}{r!\,(n-r+2)!} \right) \\ &= \sum_{S=\frac{n-1}{2}-\lfloor \frac{n-1}{2} \rfloor}^{\frac{n-1}{2}} \frac{n+1-2S}{2^{n+1}} \cdot (2S+1)^2 \cdot \frac{n!}{\left(\frac{n+1}{2}-S\right)!\left(\frac{n+3}{2}+S\right)!} \\ &= \sum_{S=\frac{n-1}{2}-\lfloor \frac{n-1}{2} \rfloor}^{\frac{n-1}{2}} \frac{(2S+1)^2 \cdot n!}{2^n \cdot \left(\frac{n-1}{2}-S\right)!\left(\frac{n+3}{2}+S\right)!}\end{aligned}$$

On retrouve bel et bien la formule telle que donnée à l'équation 50 de l'article original de 2009 [25].

On donne deux précisions sur ce résultat en se référant au même article de S. Ishizaka et T. Hiroshima [25]. La première concerne l'optimalité de $\mathsf{P}_{\text{succès}}(n)$. Il n'existe pas de mesure qu'Alice peut faire lorsqu'elle partage des paires EPR avec Bob qui va donner une meilleure probabilité de succès que celle énoncée aux propositions 44 et 45 ci-dessus. Ensuite en deuxième, on mentionne que le comportement asymptotique de $\mathsf{P}_{\text{succès}}(n)$ est donné par :

$$\mathsf{P}_{\text{succès}}(n) \xrightarrow[n\to\infty]{} \sqrt{\frac{8}{\pi n}}$$

On note que bien qu'il y ait effectivement convergence vers 1, celle-ci est très lente : il faut quadrupler le nombre de ports pour diminuer la probabilité d'échec de moitié !

On termine en clarifiant le rôle de l'information générée à l'étape intermédiaire (question 2) correspondant au conditionnement sur r. En effet, une fois la téléportation terminée, toute l'information classique autre que le port de sortie est inutile et peut même être nuisible. Effectivement, si l'on se débarrasse de tous les ports, la fuite d'information est sans conséquence. Par contre, en pratique, il pourrait être intéressant de recycler l'intrication des ports non-utilisés une fois la téléportation réussie (cette possibilité est étudiée pour le cas déterministe dans un article de 2013 [36]). Dans ce cas, plus on génère d'information classique à propos de ces ports durant notre mesure, plus on dégrade leur intrication (parce qu'un état intriqué est localement complètement mélangé). On a notamment intérêt à effectuer la mesure de manière à minimiser l'information qu'on apprend sur le spin total des $n+1$ qubits d'Alice. Comme la probabilité de succès varie avec le spin total S, l'indication du succès de la téléportation est une fuite nécessairement inévitable lorsque le nombre de ports est supérieur à 2. Cette dernière vient brouiller légèrement[23] l'intrication restante. Avec un nombre de ports $n > 2$ fini, on peut donc limiter la fuite d'intrication, mais pas l'éliminer complètement.

[23] Plus le nombre de ports utilisés est élevé, moindre est le bruit. Il est d'ailleurs asymptotiquement nul. L'article de 2013 mentionné ci-dessus [36] le quantifie pour la téléportation multi-ports déterministe.

Finalement, on a présenté le protocole en utilisant la paire EPR $|\psi^-\rangle_{A_iB_i}$. C'est parce que cet état, qu'on appelle aussi l'état singulet, est particulier : il est le seul des quatre états de Bell à posséder un spin 0 (les autres ont un spin 1). La relation entre r et S n'est valide que si r représente la quantité de $|\psi^-\rangle$. Pour effectuer le protocole avec un autre état de Bell, on fait plutôt d'abord l'opération de Pauli appropriée sur l'état qu'on veut téléporter (par exemple XZ si l'on utilise $|\phi^+\rangle$ comme ressource). Ensuite, on effectue *verbatim* le protocole donné plus haut pour $|\psi^-\rangle$.

3.3.4 Effet du bruit chez Bob

On est maintenant en mesure de s'attaquer à l'effet de l'intrication brouillée sur la téléportation multi-ports (probabiliste et avec des paires EPR). On procède comme à la section 3.1 avec la téléportation quantique standard et on commence ainsi par le scénario où l'intrication est brouillée uniquement du côté de Bob. On suppose donc que toute l'intrication a été générée parfaitement et que les n ports d'Alice sont intacts. On considère d'abord que le bruit est indépendant d'un port de sortie à l'autre, mais qu'il peut être différent. On ne prend pas nécessairement pour acquis que le nombre de ports n est assez grand pour que soit négligeable la probabilité que la téléportation échoue, mais on rappelle que lorsque c'est le cas, tous les résultats s'appliquent également à la version déterministe de la téléportation multi-ports avec des paires EPR. Le contenu de cette sous-section devient original après la proposition 47.

Le principe même de la téléportation multi-ports est que toute opération (le brouillage d'intrication est une opération) sur l'état en sortie commute avec l'opération de téléportation. Ainsi, tous les bruits commutent et l'effet de l'intrication brouillée chez Bob sur la téléportation multi-ports est trivial [24, 25].

Proposition 46. *Soit $\{\{\mathsf{A}_{ij}\}_j\}_i$ les ensembles d'opérateurs de Kraus définissant les bruits sur chacun des ports de l'ensemble $\{B_i\}_i$ de Bob. Alors le résultat de la téléportation*

sachant k, où k est le résultat de la mesure d'Alice, est exactement le même que si l'on avait appliqué préalablement le bruit $\{\mathsf{A}_{kj}\}_j$ sur l'état à téléporter.

$$\left[\mathcal{C}^{CAB\to B_k}_{\text{TQMP}|i=k} \circ \left(\bigotimes_{i=1}^{n}\left(\mathcal{C}^{A_i}_{identité}\otimes\mathcal{C}^{B_i}_{brouillé_i}\right)\right)(\cdot) \sim \mathcal{C}^{C\to B_k}_{brouillé_k}\right](\cdot) = \mathsf{A}_{kj}(\cdot)\mathsf{A}^{\dagger}_{kj}$$

Comme il n'y a pas de bruit chez Alice, les n ports demeurent équiprobables et la probabilité de succès de la mesure ne varie pas. Tous les bruits sur l'intrication des ports autres que B_k n'ont aucune incidence sur l'état téléporté et le processus de téléportation.

Démonstration. Comme Bob n'a pas à effectuer d'opérations sur son port de sortie pour le retrouver, une fois le résultat d'Alice connu, la situation est identique à celle où l'état téléporté avait toujours été dans le port B_k à la place de l'intrication et qu'il avait subit l'opération ayant brouillé celle-ci. Tous les autres bruits aboutissent à la poubelle en même temps que les ports $i \neq k$ qu'ils brouillent. ■

Une autre façon de le voir est que la téléportation multi-ports probabiliste, quand elle réussit, a un effet identique à celui du protocole où Alice effectue la téléportation quantique standard avec un port au hasard parmi les n ports d'entrée et que, par chance divine, elle obtient toujours le résultat de Bell pour lequel Bob n'a pas à faire de corrections sur son état. Dans ce cas, brouiller l'intrication ou brouiller l'état est équivalent. Cela illustre une première différence notable par rapport à la téléportation quantique standard dont seuls les bruits de Pauli chez Bob détenaient cette propriété de commutation.

Il s'en suit évidemment que toutes les mesures de distance conditionnées sur le port de sortie k restent invariantes que l'on applique le bruit sur l'état téléporté ou sur son port de sortie k, puisque l'état résultant est le même.

Proposition 47. *La fidélité, la fidélité d'intrication et la fidélité espérée conditionnées sur le résultat k de la mesure d'Alice ne sont pas affectées par l'utilisation de la téléportation*

multi-ports par rapport à l'emploi direct du canal $\mathcal{C}^{B}_{brouillé_k}$.

$$F\left(\rho, \mathcal{C}^{CAB\to B_k}_{\text{TQMP}|i=k} \circ \bigotimes_{i=1}^{n} \left(\mathcal{C}^{A_i}_{identité} \otimes \mathcal{C}^{B_i}_{brouillé_i}\right)(\rho)\right) = F\left(\rho, \mathcal{C}^{B_k}_{brouillé_k}(\rho)\right)$$

$$\bar{F}\left(\mathcal{C}^{CAB\to B_k}_{\text{TQMP}|i=k} \circ \bigotimes_{i=1}^{n} \left(\mathcal{C}^{A_i}_{identité} \otimes \mathcal{C}^{B_i}_{brouillé_i}\right)\right) = \bar{F}\left(\mathcal{C}^{B_k}_{brouillé_k}\right)$$

$$F_{intr}\left(\mathcal{C}^{CAB\to B_k}_{\text{TQMP}|i=k} \circ \bigotimes_{i=1}^{n} \left(\mathcal{C}^{A_i}_{identité} \otimes \mathcal{C}^{B_i}_{brouillé_i}\right)\right) = F_{intr}\left(\mathcal{C}^{B_k}_{brouillé_k}\right)$$

Démonstration. Conséquence immédiate de la proposition 46. ■

Par contre, si l'on ne conditionne pas, c'est-à-dire si l'on oublie l'information classique k après avoir sélectionné le bon port, le résultat de la téléportation va changer si les canaux brouillant l'intrication de chacun des ports ne sont pas tous identiques. On a là une deuxième différence importante par rapport à la téléportation quantique standard avec oubli (Damien). Au lieu d'introduire un « Pauli twirl », oublier post-téléportation le résultat de la mesure transforme simplement le canal de téléportation multi-ports avec oubli en une moyenne sur les n ports de tous les canaux ayant indépendamment brouillé l'intrication chez Bob. On ne pourra donc pas utiliser dans les sous-sections suivantes l'oubli d'information pour borner inférieurement la qualité d'un canal dont les bruits sont plus complexes (comme les bruits non-unitaux et potentiellement non-locaux). Par contre, calculer les espérances plutôt que de conditionner sur chaque port simplifie quand même l'analyse du bruit dans des grands réseaux et l'argument qu'on a utilisé pour justifier l'oubli d'information et la wernerisation à la sous-section 3.2 tient toujours : oublier de l'information classique permet de réduire (énormément dans ce cas-ci, car le nombre de ports n se doit d'être très grand) la quantité de paramètres à prendre en compte lorsque l'on veut borner inférieurement la fidélité d'un réseau. On remarque qu'oublier quel port on a gardé et quels ports on a jetés n'a absolument aucun impact si le bruit est pareil d'un port à l'autre.

Proposition 48. *Soit $\{\{\mathsf{A}_{ij}\}_j\}_i$ les ensembles d'opérateurs de Kraus définissant les bruits sur chacun des ports de l'ensemble $\{B_i\}_i$ de Bob. Alors, le résultat de la téléportation avec oubli post-téléportation du résultat k de la mesure d'Alice est le même que si l'on avait appliqué préalablement la moyenne des bruits $\{\{\mathsf{A}_{ij}\}_j\}_i$ sur l'état à téléporter (et qu'on l'avait ensuite envoyé à Bob par un canal de transmission parfait).*

$$\mathcal{C}_{\mathrm{TQMP}}^{CAB\to B}\circ\left(\bigotimes_{i=1}^{n}\left(\mathcal{C}_{identité}^{A_i}\otimes\mathcal{C}_{brouillé_i}^{B_i}\right)\right)(\cdot)\sim\sum_{i=1}^{n}\frac{1}{n}\mathcal{C}_{brouillé_i}^{C\to B}(\cdot)\sim\sum_{ij}\frac{1}{n}\mathsf{A}_{ij}(\cdot)\mathsf{A}_{ij}^{\dagger}$$

Démonstration. En oubliant k, Bob obtient le mélange probabiliste des n résultats $k\neq 0$ possibles de la mesure d'Alice. Il n'y a pas de bruit chez Alice et ils sont donc tous équiprobables. ■

Les différentes mesures non-conditionnées de fidélité sont évidemment elles-aussi simplement l'espérance des fidélités conditionnées sur chaque port. Si n est grand et que les ports de sortie sont construits de manière identique (et donc que les bruits sont de prime abord très similaires), alors cette fidélité est proche de la fidélité conditionnée et en est donc une bonne approximation.

Proposition 49. *La fidélité, la fidélité d'intrication et la fidélité espérée non-conditionnées sur le résultat k de la mesure d'Alice sont les moyennes des fidélités correspondantes sur l'ensemble des n ports.*

$$F\left(\rho,\mathcal{C}_{\mathrm{TQMP}}^{CAB\to B}\circ\bigotimes_{i=1}^{n}\left(\mathcal{C}_{identité}^{A_i}\otimes\mathcal{C}_{brouillé_i}^{B_i}\right)(\rho)\right)=\sum_{i=1}^{n}\frac{1}{n}F\left(\rho,\mathcal{C}_{brouillé_i}^{B}(\rho)\right)$$

$$\bar{F}\left(\mathcal{C}_{\mathrm{TQMP}}^{CAB\to B}\circ\bigotimes_{i=1}^{n}\left(\mathcal{C}_{identité}^{A_i}\otimes\mathcal{C}_{brouillé_i}^{B_i}\right)\right)=\sum_{i=1}^{n}\frac{1}{n}\bar{F}\left(\mathcal{C}_{brouillé_i}^{B}\right)$$

$$F_{intr}\left(\mathcal{C}_{\mathrm{TQMP}}^{CAB\to B}\circ\bigotimes_{i=1}^{n}\left(\mathcal{C}_{identité}^{A_i}\otimes\mathcal{C}_{brouillé_i}^{B_i}\right)\right)=\sum_{i=1}^{n}\frac{1}{n}F_{intr}\left(\mathcal{C}_{brouillé_i}^{B}\right)$$

Démonstration. Conséquence immédiate de la proposition 48. ■

3.3.4.1 Effet de bruits inter-ports chez Bob

On lève la contrainte d'indépendance entre les bruits dans l'intrication des différents ports de sortie chez Bob. On obtient un type de bruit qui n'a pas d'équivalent dans la version standard de la téléportation quantique. On en examine les conséquences pour le protocole multi-ports asymptotique.

Proposition 50. *Soit $\{\mathsf{A}_j\}_j$ les opérateurs de Kraus définissant le bruit global sur l'ensemble B des n ports de Bob. Alors, le résultat de la téléportation sachant k, où k est le résultat de la mesure d'Alice, est donné ci-dessous. On considère n suffisamment grand pour que l'information du succès de la téléportation n'affecte pas les ports différents de k.*

$$\mathcal{C}^{CAB\to B}_{\mathrm{TQMP}|i=k} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)(\cdot) \sim \mathcal{C}^{C\to B_k}_{brouillé_k}(\cdot) \sim \mathrm{tr}_{B_1\ldots B_n\setminus B_k}\left(\mathsf{A}_j(\cdot\otimes \pi_{B_1\ldots B_n\setminus B_k})\mathsf{A}_j^\dagger\right)$$

La présence de l'état complètement mélangé $\pi_{B_1\ldots B_n\setminus B_k}$ dans l'équation ci-dessus est légèrement trompeuse, puisqu'en fait tous ces ports $i \neq k$ sont encore parfaitement intriqués avec les ports du côté d'Alice. Alice pourrait par exemple mesurer tous ses qubits restant dans une base quelconque et en communiquer le résultat à Bob. On donne le résultat quand Alice mesure individuellement chacun de ses qubits.

Proposition 51. *Si à la fin de la situation précédente, Alice mesure ses qubits dans une base quelconque $\otimes_{i\neq k}|b_i\rangle\langle b_i|$ et en donne les résultats a_i (et la base y correspondant) à Bob, l'état chez Bob devient :*

$$\mathcal{C}^{CAB\to B}_{\mathrm{TQMP}|i=k} \circ \left(\mathcal{C}^{A}_{identité} \otimes \mathcal{C}^{B}_{brouillé}\right)(\cdot) \sim \mathrm{tr}_{B_1\ldots B_n\setminus B_k}\left(\mathsf{A}_j\left(\cdot\otimes\left(\bigotimes_{i\neq k}|a_i\rangle\langle a_i|\right)_{B_1\ldots B_n\setminus B_k}\right)\mathsf{A}_j^\dagger\right)$$

Cette technique ne peut pas être combinée avec l'oubli du résultat de k, car Bob doit associer chaque mesure au port correspondant. Si Bob oublie toute l'information classique qu'Alice lui communique, on retrouve exactement le résultat de la proposition 50. C'est normal, puisque Bob n'a pas fait d'opérations concrètes sur son état. On ne voit pas d'intérêt pratique à la méthode de caractérisation du bruit avec mesure chez Alice,

puisque l'espérance de la fidélité d'intrication demeure la même peu importe la base qu'Alice choisit pour faire sa mesure. Bob y gagne ainsi peu et est forcé à conditionner son état sur n paramètres, ce qui devient vite impensable dans un grand réseau quantique.

3.3.5 Effet de bruits locaux chez Alice et chez Bob

On rajoute au bruit chez Bob du bruit indépendant chez Alice en suivant le même modèle que pour la téléportation quantique standard. On étudie d'abord l'impact des bruits unitaux chez Alice, puis celui des bruits non-unitaux. On prend pour le moment le bruit indépendant d'un port à l'autre.

3.3.5.1 Bruit d'unitaires mélangés et bruit unital chez Alice

Comme on a vu en traitant la téléportation standard à la sous-section 3.1.5.1, on peut considérer tous les bruits composés d'unitaires mélangés sur l'intrication d'Alice comme de l'intrication brouillée chez Bob. De plus, comme on téléporte un qubit, cette affirmation s'étend toujours à toute la classe des bruits unitaux puisque ceux-ci peuvent encore s'écrire comme des bruits composés d'unitaires mélangés. On obtient ainsi directement le résultat de la téléportation quand l'intrication est brouillée unitalement chez Alice et de manière quelconque chez Bob :

Proposition 52. *Soit $\{\{\mathsf{A}_{ij}\}_j\}_i$ l'ensemble des opérateurs de Kraus définissant le bruit sur chaque port de l'ensemble $\{B_i\}_i$ de Bob et soit $\{\{\sqrt{p_l}\mathsf{U}_{il}\}_l\}_i$ ceux désignant le bruit unital sur les moitiés intriquées $\{A_i\}_i$ d'Alice. Alors, le résultat de la téléportation sachant k, où k est le résultat de la mesure d'Alice, est exactement le même que si l'on avait appliqué préalablement le bruit $\{\sqrt{p_l}\mathsf{A}_{kj}\mathsf{U}_{kl}^\dagger\}_{jl}$ sur l'état à téléporter et qu'on l'avait envoyé directement par le canal identité.*

$$\mathcal{C}^{CAB\to B}_{\mathrm{TQMP}|i=k} \circ \bigotimes_{i=1}^{n} \left(\mathcal{C}^{A_i}_{unital_i} \otimes \mathcal{C}^{B_i}_{brouillé_i}\right)(\cdot) \sim \mathcal{C}^{C\to B_k}_{brouillé_k} \circ \left(\mathcal{C}^{C\to C}_{unital_k}\right)^{\dagger}(\cdot) \sim p_l \mathsf{A}_{kj}\mathsf{U}_{kl}^\dagger(\cdot)\mathsf{U}_{kl}\mathsf{A}_{kj}^\dagger$$

Les n ports sont équiprobables. Les bruits sur l'intrication $B_{i\neq k}$ n'ont pas d'effet sur le résultat de la téléportation. La probabilité que la mesure d'Alice annonce un échec est ainsi inchangée.

Démonstration. On écrit le bruit unital comme un mélange probabiliste d'opérateurs unitaires à l'aide de la proposition 18. Puis, on utilise la propriété 2, concernant la non-localité de l'état de Bell $|\psi^-\rangle$, pour transformer toute unitaire U_l chez Alice en son inverse $\mathsf{U}_l^\dagger$ chez Bob. Après cette réduction, il n'y a plus de bruit chez Alice et le processus de mesure d'Alice est identique à celui du cas précédent, c'est-à-dire celui de la proposition 46, où son intrication n'était pas brouillée. ■

On ne reformule pas le résultat de la proposition 47 concernant les mesures de fidélité du canal résultant, car son adaptation est évidente. Il en va de même pour le nouveau résultat quand on oublie l'information k après la téléportation, où, à la manière de la proposition 48, on fait simplement la moyenne du bruit sur tous les ports. On donne toutefois celui correspondant à l'espérance de la fidélité d'intrication quand on oublie ultimement k, car cette mesure caractérise concrètement la qualité du canal. On s'intéresse à l'espérance de la fidélité d'intrication pour deux raisons. En premier lieu, elle est unique et donc plus évocatrice que la horde des fidélités d'intrication conditionnées. Ensuite, on préfère en général pouvoir prédire si un état sera téléporté de manière fiable plutôt que de pouvoir quantifier après coup si l'état s'est bien téléporté.

Proposition 53. *La fidélité d'intrication (non-conditionnée) du canal de téléportation multi-ports avec intrication brouillée unitalement par $\{\{\sqrt{p_l}\mathsf{U}_{il}\}_l\}_i$ chez Alice et de manière quelconque, par $\{\{\mathsf{A}_{ij}\}_j\}_i$, chez Bob est donnée par :*

$$F_{intr}\left(\mathcal{C}_{\text{TQMP}}^{CAB\to B}\circ\bigotimes_{i=1}^{n}\left(\mathcal{C}_{unital_i}^{A_i}\otimes\mathcal{C}_{brouillé_i}^{B_i}\right)\right)=\sum_{ijl}\frac{1}{4n}|\operatorname{tr}\left(\sqrt{p_l}\mathsf{A}_{ij}\mathsf{U}_{il}^\dagger\right)|^2$$

Démonstration. On utilise la proposition 52 et la définition 52. ■

On relaxe maintenant la condition d'indépendance dans le bruit brouillant l'intrication de chaque port chez Alice. Comme on traite alors l'intrication chez Alice comme un qudit

de dimension $d = 2^n$, on ne peut plus considérer tout bruit unital chez Alice comme un bruit d'unitaires mélangés (c'était seulement vrai pour $d = 2$). On laisse alors tomber les bruits unitaux et on se concentre sur les bruits d'unitaires mélangés. On voit qu'on peut encore assigner à Bob la faute du brouillage dans l'intrication d'Alice.

Proposition 54. *Le bruit d'unitaires mélangés sur tous les ports d'Alice peut être vu comme du bruit uniquement chez Bob. Soit* $d = 2^n$.

$$(\mathsf{U}_d \otimes I_d)\,|\psi^-\rangle^{\otimes n} = \left(I_d \otimes (\mathsf{XZ})^{\otimes n} \cdot \mathsf{U}_d^T \cdot (\mathsf{ZX})^{\otimes n}\right)|\psi^-\rangle^{\otimes n}$$

Démonstration. Cette proposition est une conséquence de la proposition 1 et elle n'est donc pas inédite. En effet :

$$\begin{aligned}(\mathsf{U}_d \otimes I_d)\,|\psi^-\rangle^{\otimes n} &= (\mathsf{U}_d \otimes I_d) \circ \left((\mathsf{ZX})^{\otimes n} \otimes I_d\right)|\phi^+\rangle^{\otimes n} \\ &= \left(I_d \otimes (\mathsf{XZ})^{\otimes n} \cdot \mathsf{U}_d^T\right)|\phi^+\rangle^{\otimes n} \\ &= \left(I_d \otimes (\mathsf{XZ})^{\otimes n} \cdot \mathsf{U}_d^T \cdot (\mathsf{ZX})^{\otimes n}\right)|\psi^-\rangle^{\otimes n}\end{aligned}$$ ■

La réduction a une forme légèrement différente, mais peut quand même se faire et on peut donc traiter le cas de l'intrication brouillée chez Alice comme on a fait pour les bruits inter-ports chez Bob à la sous-section 3.3.4.1. On énonce ce principe global, mais on ne réécrit pas individuellement tous les résultats.

Proposition 55. *On peut considérer tout bruit agissant conjointement sur toute l'intrication d'Alice et étant composé d'unitaires mélangés* $\{\sqrt{p_l}\mathsf{U}_l\}_l$ *comme un bruit d'unitaires mélangés chez Bob dont les opérateurs de Kraus sont de la forme :*

$$\{\sqrt{p_l}\,(\mathsf{XZ})^{\otimes n} \cdot \mathsf{U}_l^T \cdot (\mathsf{ZX})^{\otimes n}\}_l$$

Démonstration. Conséquence de la réduction à la proposition 54. ■

On remarque qu'un tel bruit, même s'il est assez complexe, n'affecte toujours pas la distribution de probabilité de la mesure d'Alice. Il ne change donc pas la probabilité de succès de la mesure de la téléportation multi-ports, laquelle dépend exclusivement du

nombre n de ports.

3.3.6 Wernerisation

Finalement, on applique la wernerisation et l'oubli post-téléportation du numéro du port de sortie pour transformer tout canal de téléportation multi-ports avec intrication brouillée en canal de Pauli chez Bob dont les trois types d'erreur de Pauli sont équiprobables. Comme on l'a vu aux sections sur la téléportation quantique standard et sur les relais quantiques, ce canal est caractérisé par le paramètre unique p_W. Ce dernier est égal à sa fidélité d'intrication et permet de juger à l'avance de la capacité du canal de téléportation multi-ports à envoyer de l'information quantique. Lorsque $p_W \geq \frac{1}{4}$, ce canal a une interprétation physique très intéressante : il peut être vu comme un canal dépolarisant de facteur $P = \frac{4-4p_W}{3}$. Cette analyse est une extension naturelle, mais inédite, de celle effectuée à la section 3.1.7.

Proposition 56. *Soit un canal de téléportation multi-ports dont l'intrication totale $\rho_{A_1A_2\ldots A_nB_1B_2\ldots B_n}$ entre Alice et Bob est brouillée de manière quelconque (tant que la dimension de chaque registre reste fixe). Alors en appliquant la wernerisation individuellement sur chaque port et en oubliant le résultat classique d'Alice post-téléportation, Alice et Bob obtiennent un canal de Pauli dont les trois types d'erreur de Pauli sont équiprobables. Dans le régime $\sum_{i=1}^{n} \frac{1}{n} \operatorname{tr}\left(\rho_{A_iB_i} |\psi^-\rangle\langle\psi^-|_{A_iB_i} \geq \frac{1}{4}\right)$, ce canal est un canal dépolarisant dont le facteur de dépolarisation P est donné par :*

$$P = \sum_{i=1}^{n} \frac{4 - 4\operatorname{tr}\left(\rho_{A_iB_i} |\psi^-\rangle\langle\psi^-|_{A_iB_i}\right)}{3n}$$

La mesure d'Alice se fait normalement : tous les ports sont équiprobables et la probabilité d'échec de la mesure, associée au nombre de ports n, reste la même.

Démonstration. Une fois wernerisé, chaque port d'entrée forme avec son port de sortie correspondant un canal de Pauli dont les trois types d'erreur de Pauli sont équiprobables. Du côtés d'Alice, la wernerisation individuelle sur chaque port rend le bruit globalement

unital. En effet, même un simple « Pauli twirl » aurait suffit à cette tâche, puisque ce dernier rend chaque état intriqué-mais-brouillé localement complètement mélangé. Sans consultation avec Bob, l'intrication d'Alice est alors indistinguable du cas non-brouillé (lui aussi localement complètement mélangé). La distribution de probabilité du POVM d'Alice, incluant la probabilité d'échec, est donc strictement identique. Enfin, comme l'état a probabilité égale d'aboutir dans chacun des ports, le bruit moyen est caractérisé par la moyenne sur tous les ports des facteurs individuels d'erreur. Si la fidélité d'intrication du canal de téléportation est meilleure que celle du canal complètement dépolarisant, celui-ci peut alors être réécrit comme un canal dépolarisant. Toute corrélation restante avec l'intrication brouillée des autres ports disparaît dans la poubelle lors de la trace partielle. ■

Contrairement à la téléportation quantique standard de n qubits en parallèle, il n'est pas nécessaire de généraliser la wernerisation à 2^n dimensions, puisqu'à la fin de la téléportation multi-ports, Bob trace sur tous les ports sauf un. Pour obtenir un canal de Pauli dont les trois types d'erreur sont équiprobables (ou un canal dépolarisant lorsque applicable), il est ainsi suffisant pour Alice et Bob d'appliquer indépendamment sur chaque port[24] d'intrication la wernerisation discrète telle que donnée à l'annexe II. On note que contrairement à la téléportation standard, l'oubli post-téléportation de l'information de la mesure de Bell ne permet pas de réduire la wernerisation à un choix d'une parmi trois opérations unitaires bilatérales. Douze options sont strictement nécessaires.

Autre remarque sur l'utilisation de la wernerisation : on a vu que l'avantage principal de la téléportation multi-ports est que Bob peut commencer tout calcul quantique sur son état avant qu'Alice n'ait songé à l'état qu'elle téléporterait. La wernerisation n'inhibe pas cette propriété : Bob n'a qu'à commencer son calcul quantique par la transformation unitaire choisie aléatoirement parmi les douze choix qu'offre la wernerisation discrète. Au

[24]Pour la téléportation quantique standard, Alice peut faire sa part de la wernerisation en effectuant une opération ou bien sur son qubit à téléporter, ou bien sur sa moitié EPR intriquée. Ce n'est plus le cas pour la wernerisation de la téléportation multi-ports, puisque le choix aléatoire doit être répété indépendamment pour chaque port. Alice doit donc appliquer ses transformations directement sur au moins $n-1$ de ses n paires intriquées.

moment de la mesure, Bob appliquera la sienne (la même) et le canal sera correctement wernerisé si le choix est éventuellement oublié.

En bref, la wernerisation permet pour la téléportation multi-ports comme pour la quantique standard de simplifier et de borner inférieurement le canal de téléportation utilisant tout type d'intrication brouillée. Le canal de Pauli résultant peut être décrit par un paramètre unique. Lorsque sa fidélité d'intrication n'est pas pire que celle d'un canal dont la sortie est complètement aléatoire, on peut aussi l'interpréter comme un canal dépolarisant et ainsi le combiner facilement avec d'autres canaux dépolarisants, comme on l'a vu à la section 3.2. La wernerisation en parallèle assure également que la mesure d'Alice se comporte comme dans le cas où l'intrication est non-brouillée, avec notamment dans le cas multi-ports probabiliste, la même probabilité d'échec.

On arrête là notre analyse et on ne donne pas plus de détails sur l'effet des bruits non-unitaux ou potentiellement non-locaux. On ne reparle pas non-plus des bruits d'effacement, dont l'effet sur la téléportation multi-ports est pratiquement le même que celui-de la téléportation quantique standard. Enfin, on ne traite pas l'effet de l'intrication brouillée sur la téléportation multi-ports d'un qudit. On note d'ailleurs que, comme le fait remarquer S. Ishizaka dans un article de 2015 sur arXiv [23], la téléportation multi-ports dans le cas général du qudit recèle beaucoup de problèmes ouverts, dont le calcul des probabilités de réussite de la téléportation d'un qudit en fonction du nombre de ports n dans la version probabiliste avec des paires EPR (c'est-à-dire la généralisation à d dimensions de la variante qu'on a étudiée).

CHAPITRE 4

CONCLUSION

La téléportation quantique, de par son utilité pour transporter l'information quantique, sera certainement omniprésente dans le monde quantique de demain. Toutefois, ce monde quantique sera nécessairement brouillé, puisqu'en pratique aucune expérience physique n'est parfaite. On s'est donc penché sur la question de la téléportation quantique d'Alice à Bob en présence de ressources quantiques brouillées. Pour y arriver, on a introduit au chapitre 2 le formalisme quantique nécessaire à la modélisation de ce phénomène, lequel on a ensuite étudié au chapitre 3. On a comparé trois types de téléportation quantique, la téléportation standard, la téléportation avec relais quantiques et la téléportation multi-ports, en présence de plusieurs modèles, plus et moins généraux, d'intrication brouillée.

Cette modélisation de l'intrication brouillée à l'aide des canaux de transmission a demandé la catégorisation d'une grande variété de bruits et a illustré le contraste de leurs propriétés. On a aussi vu concrètement quand le formalisme de Kraus suffisait, et quand on devait plutôt faire appel à celui de Choi-Jamiołkowski. De la même manière, on a comparé de manière pratique l'utilisation des différentes notions de fidélité.

On a exploré la question « Quand utiliser la téléportation quantique ? » : en premier, en montrant qu'un canal brouillé a la même fidélité d'intrication qu'on l'utilise pour la téléportation quantique standard ou pour la transmission directe d'information quantique, et que les deux canaux sont même strictement équivalents lorsque l'on se restreint aux bruits de Pauli ; en deuxième, en étudiant l'avantage que procure la téléportation quantique en présence d'un canal à effacement et en minimisant le coût de cet avantage dans un réseau d'intrication quantique ; en troisième, en expliquant le principe de la téléportation multi-ports et des calculs qu'elle permet de réaliser.

On a aussi répondu à la question « Où est le bruit ? » en déterminant quels modèles

d'intrication brouillée peuvent, et ne peuvent pas, être ramenés à un modèle où l'intrication est brouillée seulement chez Bob (ou seulement chez Alice), et en explicitant ces réductions. Une conséquence pratique est que pour tout protocole où Alice et Bob corrigent leur intrication brouillée avant la téléportation, il existe un protocole similaire aboutissant au même résultat, mais où leurs deux rôles de correction sont inter-changés (Alice agit à la place de Bob, et vice versa). Cette pseudo-symétrie peut avoir de l'importance lorsqu'il y a disparité entre les moyens techniques des deux participants : le joueur le plus fort peut se charger des manœuvres les plus difficiles. À un niveau plus fondamental, cette étude nous a globalement permis de mieux comprendre l'aspect non-local de l'intrication.

Quant à la question « De quelle force est le bruit ? » : on a calculé directement la fidélité d'intrication pour les cas simples, et utilisé la wernerisation pour les cas généraux. On s'est également servi de l'effacement post-téléportation du résultat de la mesure classique, lequel avait un impact différent pour la téléportation standard et pour la téléportation multi-ports, pour simplifier les expressions du bruit. Au final, on a pu établir des protocoles permettant toujours de réduire le bruit de la téléportation brouillée à celui d'un canal de Pauli dont les trois types d'erreur sont équiprobables et qui, dans un certain régime, peut être interprété comme un canal dépolarisant. Cela indique que pour réaliser une téléportation quantique fidèle, il est particulièrement utile de pouvoir corriger le canal dépolarisant. On a également quantifié comment ce bruit dépolarisant s'additionnait dans la section sur la téléportation avec relais quantiques. On note que la simplification par oubli d'information quantique est utile pour bâtir un protocole robuste au bruit (borne inférieure), mais insuffisante dans un contexte cryptographique où l'on veut restreindre le canal complémentaire (borne supérieure).

En cours de route, on s'est éloigné légèrement du sujet principal pour expliquer comment fonctionne la téléportation quantique multi-ports dans sa version probabiliste à 2 dimensions. On ne sait pas si la méthode qu'on a utilisée (en partie en annexe V) pour retrouver le résultat de 2009 [25], lequel est uniquement valide pour $d = 2$, peut

se généraliser à d dimensions. Cette question, comme plusieurs autres concernant la téléportation multi-ports, reste ouverte.

BIBLIOGRAPHIE

[1] Adams, Douglas. *The Hitchhiker's Guide to the Galaxy*. Hitchhiker's Guide to the Galaxy. Random House Publishing Group, 2007. ISBN 9780307417138.

[2] Aspect, Alain, Jean Dalibard et Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25):1804, 1982.

[3] Badziag, Piotr, Michał Horodecki, Paweł Horodecki et Ryszard Horodecki. Local environment can enhance fidelity of quantum teleportation. *Physical Review A*, 62 (1):012311, 2000.

[4] Barut, Asim et Ryszard Raczka. *Theory of group representations and applications*. World Scientific Publishing Co Inc, 1986.

[5] Beigi, Salman et Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[6] Bell, John S. On the einstein podolsky rosen paradox, 1964.

[7] Bengtsson, Ingemar et Karol Życzkowski. *Geometry of Quantum States*. Cambridge University Press, 2006. ISBN 9780511535048. Cambridge Books Online.

[8] Bennett, Charles H et Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. Dans *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.

[9] Bennett, Charles H, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres et William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895, 1993.

[10] Bennett, Charles H., Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin et William K. Wootters. Purification of noisy entanglement and faithful

teleportation via noisy channels[phys. rev. lett. 76, 722 (1996)]. *Phys. Rev. Lett.*, 78: 2031–2031, Mar 1997.

[11] Bennett, Charles H, David P DiVincenzo et John A Smolin. Capacities of quantum erasure channels. *Physical Review Letters*, 78(16):3217, 1997.

[12] Bennett, Charles H, David P DiVincenzo, John A Smolin et William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5): 3824, 1996.

[13] Bowen, Garry et Sougato Bose. Teleportation as a depolarizing quantum channel, relative entropy, and classical capacity. *Phys. Rev. Lett.*, 87(26):267901, 2001.

[14] Buhrman, Harry, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky et Christian Schaffner. Position-based quantum cryptography : Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014.

[15] Diósi, Lajos. *A short course in quantum information theory : an approach from theoretical physics*, volume 827. Springer, 2011.

[16] Dowling, Jonathan P. *Schrödinger's killer app : race to build the world's first quantum computer*. CRC Press, 2013.

[17] Einstein, A., B. Podolsky et N. Rosen. Can quantum-mechanical description of physical reality be considered complete ? *Phys. Rev.*, 47:777–780, May 1935.

[18] Frame, James Sutherland, G de B Robinson, Robert M Thrall et al. The hook graphs of the symmetric group. *Canad. J. Math*, 6(316):C324, 1954.

[19] Hahn, Erwin L. Spin echoes. *Physical review*, 80(4):580, 1950.

[20] Harter, W.G. QM for AMOP — chapter 24, Avril 2016.

[21] Hensen, Bas, H Bernien, AE Dréau, A Reiserer, N Kalb, MS Blok, J Ruitenberg, RFL Vermeulen, RN Schouten, C Abellán et al. Loophole-free bell inequality

violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575): 682–686, 2015.

[22] Huttner, Bruno, Antoine Muller, Jean-Daniel Gautier, Hugo Zbinden et Nicolas Gisin. Unambiguous quantum measurement of nonorthogonal states. *Physical Review A*, 54(5):3783, 1996.

[23] Ishizaka, Satoshi. Some remarks on port-based teleportation. *arXiv preprint arXiv :1506.01555*, 2015.

[24] Ishizaka, Satoshi et Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.*, 101(24):240501, 2008.

[25] Ishizaka, Satoshi et Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Physical Review A*, 79(4):042306, 2009.

[26] Lloyd, Seth. Universal quantum simulators. *Science*, 273(5278):1073, 1996.

[27] Ma, Xiao-Song, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Bernhard Wittmann, Alexetra Mech, Johannes Kofler, Elena Anisimova, Vadim Makarov, Thomas Jennewein, Rupert Ursin et Anton Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489 (7415):269–273, septembre 2012. ISSN 0028-0836.

[28] Nielsen, Michael A. et Isaac L. Chuang. *Quantum Computation and Quantum Information : 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th édition, 2011. ISBN 1107002176, 9781107002173.

[29] Pfaff, Wolfgang, BJ Hensen, Hannes Bernien, Suzanne B van Dam, Machiel S Blok, Tim H Taminiau, Marijn J Tiggelman, Raymond N Schouten, Matthew Markham, Daniel J Twitchen et al. Unconditional quantum teleportation between distant solid-state quantum bits. *Science*, 345(6196):532–535, 2014.

[30] Porter, Frank. The permutation group and young diagrams, Mars 2009.

[31] Roddenberry, Gene, Harold Livingston et Alan Dean Foster. *Star Trek : The Motion Picture.* Dirigé par Robert Wize. *Paramount Pictures,* 1979.

[32] Salvail, Louis. Notes du cours sujets en informatique quantique (ift6195), Avril 2016.

[33] Shor, Peter W. Algorithms for quantum computation : Discrete logarithms and factoring. Dans *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[34] Shor, Peter W. Scheme for reducing decoherence in quantum computer memory. *Physical review A*, 52(4):R2493, 1995.

[35] Silva, Marcus, Easwar Magesan, David W Kribs et Joseph Emerson. Scalable protocol for identification of correctable codes. *Physical Review A*, 78(1):012347, 2008.

[36] Strelchuk, Sergii, Michał Horodecki et Jonathan Oppenheim. Generalized teleportation and entanglement recycling. *Phys. Rev. Lett.*, 110(1):010505, 2013.

[37] Tannoudji, Cohen Claude, Diu Bernard et Laloë Franck. Mécanique quantique. tome i. 1973.

[38] Tittel, Wolfgang, Jürgen Brendel, Hugo Zbinden et Nicolas Gisin. Violation of bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.*, 81(17):3563, 1998.

[39] Ursin, Rupert, Thomas Jennewein, Markus Aspelmeyer, Rainer Kaltenbaek, Michael Lindenthal, Philip Walther et Anton Zeilinger. Communications : Quantum teleportation across the danube. *Nature*, 430(7002):849–849, 2004.

[40] Watrous, John. Lecture notes in theory of quantum information, Fall 2011.

[41] Werner, Reinhard F. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277, 1989.

[42] Wilde, Mark M. *Quantum Information Theory*. Cambridge University Press, 2013. ISBN 9781107067844.

[43] Zukowski, Marek, Anton Zeilinger, Michael A Horne et Aarthur K Ekert. Event-ready-detectors bell experiment via entanglement swapping. *Physical Review Letters*, 71(26):4287–4290, 1993.

Annexe I

Équation de Schrödinger et déphasage expérimental

Pour comprendre une source importante en pratique de déphasage, il est utile de revenir à la formulation physique de la mécanique quantique. On se base sur l'ouvrage de référence par Cohen et Tannoudji [37]. En physique, un état quantique pur (l'extension à un mélange statistique est directe) évolue selon l'équation de Schrödinger :

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

Dans le cas où le système est fermé, l'énergie est conservée. Le hamiltonien ne dépend pas du temps et l'équation de Schrödinger peut se réécrire dans sa version indépendante du temps :

$$H\,|\psi_n(t)\rangle = E_n\,|\psi_n(t)\rangle$$

Les états $|\psi_n(t)\rangle$ sont les états propres du hamiltonien indépendant du temps et les énergies associées E_n leurs valeurs propres. Ces états stationnaires forment la base orthogonale du système quantique et s'explicitent :

$$|\psi_n(t)\rangle = e^{\frac{-iE_nt}{\hbar}}\,|\psi_n(t=0)\rangle$$

On peut voir que contrairement au hamiltonien, chaque état n'est pas lui-même indépendant du temps. Sa phase complexe tourne à une vitesse constante qui dépend directement de son énergie. Comme chaque état n'a pas nécessairement la même énergie, il est fréquent que les phases des états évoluent à des vitesses différentes.

Dans une expérience concrète d'informatique quantique, lorsque l'état est dans une superposition d'états stationnaires d'énergies différentes, il y aura création d'une différence de phase $e^{\frac{-i(E_N-E'_n)t}{\hbar}}$. Sur papier, il est facile de rectifier cette différence de phase lors des opérations subséquentes ou bien d'en prendre compte lors des mesures. En pratique

cependant, des imperfections dans l'environnement peuvent agir sur l'hamiltonien et faire varier légèrement ses niveaux d'énergie. Ces perturbations peuvent changer au cours d'une expérience de telle façon qu'il devient difficile de les corriger par simple calibrage des instruments. C'est donc une source de bruit déphasant.

Dans l'approximation où le hamiltonien est constant lors d'une même ronde de l'expérience, mais variable d'une ronde à l'autre, une technique existe pour lutter activement contre ce déphasage. Le truc consiste à symétriser les niveaux d'énergie à l'aide de l'opérateur de Pauli généralisé $\mathsf{X}(0)$ (voir la définition 21 de la section 2.2.2.1). Si le déphasage se fait sur un temps t, on applique d fois l'opérateur de décalage cyclique $\mathsf{X}(0)$: une fois à chaque temps $t_i = \frac{i \cdot t}{2d}$ pour $i = 1, 2, \ldots, d$, où d est la dimension du système[1].

Par exemple, on prend le cas d'un qubit dans l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ subissant sur un temps t' une différence de phase de $e^{\frac{-i(E_0-E_1)t'}{\hbar}}$ entre ses états $|0\rangle$ et $|1\rangle$ de niveaux d'énergie respectifs E_0 et E_1. Si on le laisse évoluer librement, on obtient l'état :

$$|\psi(t')\rangle = \alpha|0\rangle + e^{\frac{-i(-E_0+E_1)t'}{\hbar}}\beta|1\rangle$$

En effectuant une inversion-de-bit quantique X aux temps $t_1 = t'/2$ et $t_2 = t'$. On retrouve $|\psi\rangle$ au temps t'.

[1] Le phénomène dans le domaine de la résonance magnétique a été découvert en 1950 par E. L. Hahn[19]. La technique est donc souvent appelée écho de Hahn ou « spin echo » en anglais.

Démonstration.

$$
\begin{aligned}
|\psi(t=0)\rangle &= \alpha|0\rangle + \beta|1\rangle \\
|\psi(t<\tfrac{t'}{2})\rangle &= \alpha e^{\frac{-iE_0 t}{\hbar}}|0\rangle + e^{\frac{-iE_1 t}{\hbar}}\beta|1\rangle \\
&= \alpha|0\rangle + e^{\frac{-i(-E_0+E_1)t}{\hbar}}\beta|1\rangle \\
|\psi(\tfrac{t'}{2}<t<t')\rangle &= \alpha e^{\frac{-i(-E_0+E_1)(t-\frac{t'}{2})}{\hbar}}|1\rangle + e^{\frac{-i(-E_0+E_1)\frac{t'}{2}}{\hbar}}\beta|0\rangle \\
|\psi(t=t')\rangle &= \alpha e^{\frac{-i(-E_0+E_1)\frac{t'}{2}}{\hbar}}|0\rangle + e^{\frac{-i(-E_0+E_1)\frac{t'}{2}}{\hbar}}\beta|1\rangle \\
&= \alpha|0\rangle + \beta|1\rangle \\
&= |\psi(t=0)\rangle
\end{aligned}
$$

■

Le généralisation au qudit de l'écho de Hahn ainsi formulé est directe, mais n'est à la connaissance de l'auteur jamais explicitée dans la littérature.

Annexe II

Wernerisation discrète

La wernerisation (« twirl » en anglais) est utilisée pour transformer toute paire de qubits ρ_{AB} en état de Werner de pureté $p_W = \mathrm{tr}(\rho_{AB}|\psi^-\rangle\langle\psi^-|_{AB})$ [10], ou bien de manière équivalente, tout canal $\mathcal{C}^{AB}_{\text{brouillé}}$ en canal $\left(\mathcal{C}^{A}_{\text{identité}} \otimes \mathcal{C}^{B}_{\text{Pauli}}\right)$ de probabilités $p_{\mathsf{X_B}} = p_{\mathsf{Y_B}} = p_{\mathsf{Z_B}} = \frac{1-p_W}{3}$. Lorsque $p_W \geq \frac{1}{4}$, on peut aller plus loin et réécrire le canal de Bob comme un canal dépolarisant $\mathcal{C}^{B}_{\text{dépolarisant}}\left(P = \frac{4-4p_W}{3}, \cdot\right)$. La wernerisation peut se faire de manière discrète ou continue [10, 12]. On dérive ici une preuve pour un protocole où l'on applique une opération unitaire discrète bilatérale choisie uniformément aléatoirement parmi douze opérations possibles. On sépare l'opération unitaire unitaire en deux étapes séquentielles (l'ordre n'a pas d'importance) pour illustrer que la wernerisation est une extension du processus qu'on a appelé Damien-quantique (« Pauli twirl » dans la littérature anglophone). La preuve, qu'on a dérivée ici pour l'état EPR $|\psi^-\rangle$, s'appliquerait avec peu de modifications à $|\phi^+\rangle$.

Soit la matrice densité quelconque de 2 qubits, on peut invoquer le théorème de décomposition spectrale pour la décomposer en un mélange probabiliste d'états purs :

$$\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Chacun de ces états purs peut s'écrire dans la base de Bell :

$$|\psi_i\rangle_{AB} = a_i|\psi^-\rangle + b_i|\phi^-\rangle + c_i|\phi^+\rangle + d_i|\psi^+\rangle = (a_i + b_i\mathsf{X}_B + ic_i\mathsf{X}\mathsf{Z}_B + d_i\mathsf{Z}_B)|\psi^-\rangle_{AB} \tag{II.1}$$

En exploitant la propriété 2 vue à la section 2.1.6, on écrit l'effet d'une transformation unitaire bilatérale sur $|\psi_i\rangle_{AB}$ comme :

$$\mathsf{U}_A \otimes \mathsf{U}_B|\psi_i\rangle_{AB} = a_i|\psi^-\rangle + \mathsf{U}_B(b_i\mathsf{X}_B + ic_i\mathsf{X}\mathsf{Z}_B + d_i\mathsf{Z}_B)\mathsf{U}^\dagger{}_B|\psi^-\rangle_{AB} \tag{II.2}$$

On définit notre opération de wernerisation discrète comme l'application séquentielle de deux transformations unitaires $\mathsf{U}_1, \mathsf{U}_2$ choisies uniformément au hasard parmi deux groupes. Le premier est l'ensemble des matrices de Pauli et $\mathsf{U}_1 \in_R \{I, \mathsf{X}, i\mathsf{XZ}, \mathsf{Z}\}$, tandis que le deuxième choix est $\mathsf{U}_2 \in_R \{\frac{\mathsf{X}+i\mathsf{XZ}}{\sqrt{2}}, \frac{\mathsf{X}+\mathsf{Z}}{\sqrt{2}}, \frac{i\mathsf{XZ}+\mathsf{Z}}{\sqrt{2}}\}$. En oubliant le choix qu'on a fait après avoir effectué l'opération correspondante, on obtient le mélange statistique suivant (toujours pour chaque état pur $|\psi_i\rangle$) :

$$\begin{aligned}
\tilde{\rho}_{iAB} &= \frac{1}{\#\{\mathsf{U}_1\}\#\{\mathsf{U}_2\}} \sum_{\mathsf{U}_1,\mathsf{U}_2} \mathsf{U}_{2A}\mathsf{U}_{1A}\mathsf{U}_{2B}\mathsf{U}_{1B}\,|\psi_i\rangle\langle\psi_i|\,\mathsf{U}_{1A}^{\dagger}\mathsf{U}_{2A}^{\dagger}\mathsf{U}_{1B}^{\dagger}\mathsf{U}_{2B}^{\dagger} \\
&= \frac{1}{12} \sum_{\mathsf{U}_1,\mathsf{U}_2} \mathsf{U}_{2A}\mathsf{U}_{1A}\mathsf{U}_{2B}\mathsf{U}_{1B}\,(a_i + b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\,\langle\psi^-|\ldots \\
&\qquad\qquad \ldots|\psi^-\rangle\,(a_i^* + b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\,\mathsf{U}_{1A}^{\dagger}\mathsf{U}_{2A}^{\dagger}\mathsf{U}_{1B}^{\dagger}\mathsf{U}_{2B}^{\dagger} \\
&= \frac{1}{12} \sum_{\mathsf{U}_1,\mathsf{U}_2} \mathsf{U}_{2B}\mathsf{U}_{1B}\,(a_i + b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\,\mathsf{U}_{1B}^{\dagger}\mathsf{U}_{2B}^{\dagger}\,\langle\psi^-|\ldots \\
&\qquad\qquad \ldots|\psi^-\rangle\,\mathsf{U}_{2B}\mathsf{U}_{1B}\,(a_i^* + b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\,\mathsf{U}_{1B}^{\dagger}\mathsf{U}_{2B}^{\dagger} \\
&= |a_i|^2\,|\psi^-\rangle\langle\psi^-| + \frac{1}{12} \sum_{\mathsf{U}_1,\mathsf{U}_2} \mathsf{U}_{2B}\mathsf{U}_{1B}\,(b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\,\mathsf{U}_{1B}^{\dagger}\mathsf{U}_{2B}^{\dagger}\,\langle\psi^-|\ldots \\
&\qquad\qquad \ldots|\psi^-\rangle\,\mathsf{U}_{2B}\mathsf{U}_{1B}\,(b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\,\mathsf{U}_{1B}^{\dagger}\mathsf{U}_{2B}^{\dagger}
\end{aligned}$$

La deuxième égalité utilise l'équation II.1 et la troisième l'équation II.2. La dernière égalité vient du fait que $\mathsf{U}(\cdot)\mathsf{U}^{\dagger}$ préserve toujours la trace. $a_i I$ de trace $2a_i$ fait partie d'un sous-espace orthogonal à celui de $(b_i\mathsf{X}_B + c_i\mathsf{Z}_B + d_i\mathsf{XZ}_B)$ qui est de trace 0. Tout terme croisé entre ces deux sous-espaces est donc nul.

Ensuite, on explicite la somme sur U_1 et on simplifie.

$$
\begin{aligned}
&= |a_i|^2 |\psi^-\rangle\langle\psi^-| + \frac{1}{12}\sum_{\mathsf{U}_2}(\mathsf{U}_{2B}(b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}(b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger \\
&\quad + \mathsf{U}_{2B}\mathsf{X}_B(b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\mathsf{X}_B\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}\mathsf{X}_B(b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\mathsf{X}_B\mathsf{U}_{2B}^\dagger \\
&\quad + \mathsf{U}_{2B}\mathsf{XZ}_B(-b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\mathsf{ZX}_B\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}\mathsf{XZ}_B(b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\mathsf{ZX}_B\mathsf{U}_{2B}^\dagger \\
&\quad + \mathsf{U}_{2B}\mathsf{Z}_B(b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\mathsf{Z}_B\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}\mathsf{Z}_B(b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\mathsf{Z}_B\mathsf{U}_{2B}^\dagger) \\
&= |a_i|^2 |\psi^-\rangle\langle\psi^-| + \frac{1}{12}\sum_{\mathsf{U}_2}(\mathsf{U}_{2B}(b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}(b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger \\
&\quad + \mathsf{U}_{2B}(b_i\mathsf{X}_B - ic_i\mathsf{XZ}_B - d_i\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}(b_i^*\mathsf{X}_B - ic_i^*\mathsf{XZ}_B - d_i^*\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger \\
&\quad + \mathsf{U}_{2B}(-b_i\mathsf{X}_B + ic_i\mathsf{XZ}_B - d_i\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}(-b_i^*\mathsf{X}_B + ic_i^*\mathsf{XZ}_B - d_i^*\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger \\
&\quad + \mathsf{U}_{2B}(-b_i\mathsf{X}_B - ic_i\mathsf{XZ}_B + d_i\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_{2B}(-b_i^*\mathsf{X}_B - ic_i^*\mathsf{XZ}_B + d_i^*\mathsf{Z}_B)\mathsf{U}_{2B}^\dagger) \\
&= |a_i|^2 |\psi^-\rangle\langle\psi^-| + \frac{1}{3}\sum_{\mathsf{U}_2}(|b_i|^2\mathsf{U}_2\mathsf{XU}_2^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_2\mathsf{XU}_2^\dagger + |c_i|^2\mathsf{U}_2\mathsf{XZU}_2^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_2\mathsf{ZXU}_2^\dagger \\
&\qquad\qquad + |d_i|^2\mathsf{U}_2\mathsf{ZU}_2^\dagger|\psi^-\rangle\langle\psi^-|\mathsf{U}_2\mathsf{ZU}_2^\dagger)
\end{aligned}
$$

On remarque que si l'on arrête la wernerisation ici sans appliquer U_2 (on poserait $\mathsf{U}_2 = I$ dans l'équation ci-dessus), on retrouve exactement Damien-quantique et les deux qubits sont un mélange statistique des quatre états de Bell. Damien-quantique projette ainsi tout état ρ_{AB} dans la base de Bell. Cela signifie que lorsque l'on applique la wernerisation complète à la téléportation quantique, on peut remplacer la première étape, celle qui implique U_1, par l'effacement post-téléportation de l'information classique de la mesure d'Alice et passer tout de suite à l'application de U_2. Cette seconde porte sert à uniformiser les probabilités d'obtenir les trois mauvais états de Bell dans le mélange et transforme donc un bruit de Pauli quelconque en un bruit de Pauli dont $p_\mathsf{X} = p_\mathsf{Y} = p_\mathsf{Z}$.

On poursuit le développement. L'effet des trois opérations $\{\mathsf{U}_2(\cdot)\mathsf{U}_2{}^\dagger\}$ sur les portes $\{\mathsf{X}, \mathsf{iXZ}, \mathsf{Z}\}$ est, à une phase globale près, de les permuter entres-elles. On peut donc développer la somme en U_2 et réécrire :

$$
\begin{aligned}
&= |a_i|^2 |\psi^-\rangle\langle\psi^-| + \frac{1}{3}(|b_i|^2 \mathsf{X}_B |\psi^-\rangle\langle\psi^-| \mathsf{X}_B + |b_i|^2 \mathsf{X}\mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}\mathsf{X}_B + |b_i|^2 \mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}_B \\
&\qquad + |c_i|^2 \mathsf{X}_B |\psi^-\rangle\langle\psi^-| \mathsf{X}_B + |c_i|^2 \mathsf{X}\mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}\mathsf{X}_B + |c_i|^2 \mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}_B \\
&\qquad + |d_i|^2 \mathsf{X}_B |\psi^-\rangle\langle\psi^-| \mathsf{X}_B + |d_i|^2 \mathsf{X}\mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}\mathsf{X}_B + |d_i|^2 \mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}_B) \\
&= |a_i|^2 |\psi^-\rangle\langle\psi^-| + \frac{1}{3}(|b_i|^2 + |c_i|^2 + |d_i|^2)(\mathsf{X}_B |\psi^-\rangle\langle\psi^-| \mathsf{X}_B + \mathsf{X}\mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}\mathsf{X}_B + \mathsf{Z}_B |\psi^-\rangle\langle\psi^-| \mathsf{Z}_B) \\
&= |a_i|^2 |\psi^-\rangle\langle\psi^-| + (|b_i|^2 + |c_i|^2 + |d_i|^2) \frac{|\phi^-\rangle\langle\phi^-| + |\phi^+\rangle\langle\phi^+| + |\psi^+\rangle\langle\psi^+|}{3}
\end{aligned}
$$

Finalement, par linéarité on peut recombiner de manière probabiliste les matrices densité de chaque état pur composant le mélange statistique :

$$
\tilde{\rho}_{AB} = \sum_i p_i \left(|a_i|^2 |\psi^-\rangle\langle\psi^-| + \left(|b_i|^2 + |c_i|^2 + |d_i|^2\right) \frac{|\phi^-\rangle\langle\phi^-| + |\phi^+\rangle\langle\phi^+| + |\psi^+\rangle\langle\psi^+|}{3} \right)
$$

L'opération de wernerisation discrète pour deux qubits transforme donc tout état ρ_{AB} en état de Werner de pureté $p_W = \sum_i |a_i|^2$, où $|a_i|^2 = p_i \operatorname{tr}\left(|\psi^i\rangle\langle\psi^i|_{AB} |\psi^-\rangle\langle\psi^-|_{AB}\right)$. ■

Annexe III

Bruit indépendant chez Bob commutant avec la téléportation (cas général qudit)

On a vu à la section 3.1.4 que dans le cas du qubit, seuls les bruits chez Bob qui appartiennent à la famille des bruits de Pauli commutent avec la téléportation quantique standard. On ébauche ici la preuve (inédite) démontrant l'extension de ce résultat au cas général en D dimensions. On utilise la notation à doubles-indices et la représentation de Choi-Jamiołkowski telles qu'elles sont définies à la sous-section 2.2.3.3. Toutes les additions sont entendues cycliques (modulo D).

On trouve les conditions qu'imposent sur une matrice quelconque de dimension appropriée la commutation avec tous les opérateurs de Pauli généralisés. On commence par $\mathsf{X}(x)$. Les opérateurs de Pauli généralisés $\mathsf{X}(x)$ sont dans la représentation de Choi-Jamiołkowski donnés par $\underset{c,d}{\mathsf{X}(x)_{a,b}}$ tel que :

$$\underset{c,d}{\mathsf{X}(x)_{a,b}} := \underset{c,d}{(\mathsf{X}(x) \otimes \mathsf{X}^*(x))_{a,b}} = \mathsf{X}(x)_{ac} \cdot \mathsf{X}^*(x)_{bd} = \delta_{a,(c+x)} \cdot \delta_{b,(d+x)}$$

On impose la commutation.

$$\begin{aligned}
\mathsf{JX} = \mathsf{XJ} &\Leftrightarrow \sum_{cd} \underset{c,d}{\mathsf{J}_{a,b}} \cdot \underset{g,h}{\mathsf{X}_{c,d}} = \sum_{cd} \underset{c,d}{\mathsf{X}_{a,b}} \cdot \underset{g,h}{\mathsf{J}_{c,d}} \\
&\Leftrightarrow \sum_{cd} \underset{c,d}{\mathsf{J}_{a,b}} \cdot \delta_{(c,g+x)} \cdot \delta_{(d,h+x)} = \sum_{cd} \underset{g,h}{\mathsf{J}_{c,d}} \cdot \delta_{(a,c+x)} \cdot \delta_{(b,d+x)} \\
&\Leftrightarrow \underset{c+x,d+x}{\mathsf{J}_{a+0,b+0}} = \underset{c+0,d+0}{\mathsf{J}_{a-x,b-x}} \\
&\Leftrightarrow \underset{c+x,d+x}{\mathsf{J}_{a+x,b+x}} = \underset{c,d}{\mathsf{J}_{a,b}}
\end{aligned}$$

On fait la même chose pour les opérateurs de Pauli généralisés $\mathsf{Z}(z)$, lesquels sont

donnés par $\underset{c,d}{\mathsf{Z}(z)_{a,b}}$ tel que :

$$\underset{c,d}{\mathsf{Z}(z)_{a,b}} := \underset{c,d}{(\mathsf{Z}(z)\otimes\mathsf{Z}^*(z))_{a,b}} = \mathsf{Z}(z)_{ac}\cdot\mathsf{Z}^*(z)_{bd} = e^{\frac{2\pi i\cdot zb}{D}}\delta_{ac}\cdot e^{\frac{-2\pi i\cdot zd}{D}}\delta_{bd}$$

On impose la commutation.

$$\begin{aligned}
\mathsf{JZ}=\mathsf{ZJ} &\Leftrightarrow \sum_{cd}\underset{c,d}{\mathsf{J}_{a,b}}\cdot\underset{g,h}{\mathsf{Z}_{c,d}} = \sum_{cd}\underset{c,d}{\mathsf{Z}_{a,b}}\cdot\underset{g,h}{\mathsf{J}_{c,d}}\\
&\Leftrightarrow \sum_{cd}\underset{c,d}{\mathsf{J}_{a,b}}\cdot e^{(c-d)\frac{2\pi iz}{d}}\cdot\delta_{c,g}\cdot\delta_{d,h} = \sum_{cd}\underset{g,h}{\mathsf{J}_{c,d}}\cdot e^{(a-b)\frac{2\pi iz}{d}}\cdot\delta_{a,c}\cdot\delta_{b,d}\\
&\Leftrightarrow \underset{c,d}{\mathsf{J}_{a,b}}\cdot e^{(c-d)\frac{2\pi iz}{d}} = \underset{c,d}{\mathsf{J}_{a,b}}\cdot e^{(a-b)\frac{2\pi iz}{d}}\\
&\Leftrightarrow \left\{\underset{c,d}{\mathsf{J}_{a,b}}\neq 0 \Rightarrow a+d=b+c\right\}
\end{aligned}$$

Comme tous les opérateurs de Pauli peuvent être obtenus (à une phase globale près) en faisant le produit d'un opérateur $\mathsf{X}(x)$ avec un opérateur $\mathsf{Z}(z)$, les deux conditions précédentes sont suffisantes pour assurer la commutativité du bruit J avec tous les opérateurs de Pauli.

La condition $\{a+d=b+c \mod D\}$ est vérifiée pour D^3 valeurs du quadruplet $\{a,b,c,d\}$. Et la condition $\{\underset{c+x,d+x}{\mathsf{J}_{a+x,b+x}} = \underset{c,d}{\mathsf{J}_{a,b}}\}$ assure que la quantité de chaque élément de $\underset{c,d}{\mathsf{J}_{a,b}}$ soit un multiple de D. Il y a donc au plus $D^{3-1}=D^2$ variables indépendantes dans la représentation de Choi-Jamiołkowski d'un canal invariant sous téléportation. Comme il existe exactement D^2 matrices de Pauli généralisées en D dimensions, qu'elles commutent (à une phase globale près), sont extrémales et sont linéairement indépendantes, on en conclut que seules les combinaisons convexes de matrices de Pauli généralisées sont invariantes sous téléportation. On appelle cette famille les bruits de Pauli généralisés.

Annexe IV

Impact de la téléportation multi-ports sur la poésie vogonne

Arthur vient d'apprendre qu'un vaisseau vogon est en route pour faire sauter sa planète afin de permettre le passage d'une grande voie express hyperspatiale ! Les Vogons sont ignobles et têtus, mais Arthur connaît leur point faible : la mauvaise poésie [1]. Il décide ainsi d'écrire quelques vers pour amadouer le capitaine vogon chargé d'anéantir sa chère planète. Arthur sait d'ailleurs que celui-ci sera soit Jeltz, qui aime particulièrement les *vers de terre*, ou bien son frère Geltz, qui lui ne jure que par les *vers blancs*. Mais le temps lui manque et Arthur ne peut rédiger deux poèmes. Il doit obligatoirement faire un choix : *vers de terre* ou *vers blancs* ? On voit comment la téléportation quantique multi-ports permet (asymptotiquement) à Arthur de sauver sa planète en choisissant les bon vers à tout coup.

Arthur prépare donc deux immenses[1] téléporteurs quantiques multi-ports dont chaque registre est assez grand pour contenir un aspirant-poète. À chacun des ports d'arrivée, il attache un livre pour y puiser son inspiration. Les livres du premier téléporteur font tous l'étude des *vers de terre*, tandis que ceux du deuxième portent tous sur les *vers blancs*. Arthur programme ensuite sur sa planète un ordinateur doté d'un système de reconnaissance faciale de manière à ce que s'il identifie Jeltz, Arthur soit téléporté à travers le premier téléporteur, et que si au contraire il aperçoit plutôt Geltz, il soit téléporté à travers le second. L'ordinateur est également chargé, une fois la téléportation effectuée, d'ouvrir le bon port de sortie afin d'en libérer Arthur, qui aura alors composé le poème le mieux adapté à son auditoire difficile. En attendant le vaisseau vogon, Arthur rentre dans une cellule d'isolation[2] pour se reposer, puisqu'à ce moment tout le travail est déjà

[1] On omet le fait que l'univers d'Arthur n'est probablement pas assez vaste pour héberger la quantité déraisonnable de matière nécessaire à cette entreprise. On suppose aussi qu'écrire un bon (mauvais) poème vogon est une tâche plus longue et complexe que celle de construire ces deux téléporteurs.

[2] On veut dire par là qu'elle subit la même évolution unitaire (ou absence d'évolution) que chaque port d'entrée des deux téléporteurs.

accompli : son foyer sera épargné.

La morale est que la téléportation quantique multi-ports permet en théorie de réaliser tout calcul quantique sur un état avant même de l'avoir choisi. Ici, on a fait en parallèle deux calculs, $\mathsf{U}_{\text{poésie}}\left(|?\rangle_A \otimes |\text{vers de terre}\rangle_B\right)$ et $\mathsf{U}_{\text{poésie}}\left(|?\rangle_A \otimes |\text{vers blancs}\rangle_B\right)$, mais on a décidé seulement à la fin lequel de ces deux calculs compléter avec l'entrée $|?\rangle_A = |\text{Arthur}\rangle_A$. La construction du téléporteur est une tâche ardue, mais elle prend toujours un temps constant. On note que dans ce scénario, la téléportation multi-ports est utile parce qu'on ne dispose pas de plusieurs copies de l'état $|\text{Arthur}\rangle_A$. Sinon, on ferait simplement en parallèle les deux calculs avec $|\text{Arthur}\rangle_A$ et on obtiendrait les deux poèmes.

L'utilité de la téléportation multi-ports ne s'arrête pas là et on pourrait pousser l'idée plus loin. En fait, la téléportation multi-ports permet de compléter tout calcul quantique non-local en un seul tour de communication classique[3]. Cela permet de briser tous les protocoles cryptographiques de validation de position si l'on ne restreint pas la quantité disponible d'intrication [5][14].

[3]Ce protocole nécessite une quantité exponentielle d'intrication, ce qui peut paraître peu encourageant, mais le meilleur protocole connu qui n'utilise pas la téléportation multi-ports en demande lui une quantité doublement-exponentielle [5].

Annexe V

Calcul du degré de dégénérescence de permutation lors de la composition de qubits

On quantifie ici la dégénérescence $g^{[n+1,S]}$ du système à $n+1$ qubits dont le spin total est S. On utilise pour cela les tableaux de Young, dont on ne donne que les notions nécessaires au calcul qui nous intéresse. Les définitions sont tirées d'un document de Frank Porter [30]. Les tableaux de Young sont plus faciles à visualiser que les coefficients de Clebsch-Gordan employés, pour obtenir le même résultant, dans l'article original de la téléportation multi-ports probabiliste [25].

La composition de $n+1$ qubits peut être illustrée à l'aide des diagrammes et tableaux de Young. Un diagramme de Young est un arrangement de cases sur plusieurs rangées. Les cases sont justifiées à gauche et les rangées disposées, dans la notation francophone[1], de manière à ce que la taille des rangées ne diminue pas lorsqu'on monte d'étage. Les diagrammes représentant des états composés de $n+1$ qubits ont exactement $n+1$ cases et au plus deux rangées. La longueur de la rangée supérieure détermine S (référence : figure 23.3.2, page 45 de l'ouvrage [20]). La figure V.1 illustre ces principes.

Un tableau de Young est un diagramme de Young dont chaque case est remplie par un nombre entier. Si le tableau a $n+1$ cases, alors ces entiers vont de 1 à $n+1$. Le tableau de Young est standard si les nombres habitant ses cases sont toujours croissants à même une rangée de gauche à droite et à même une colonne de bas en haut. On s'intéresse aux tableaux de Young standard, car le nombre de tableaux différents pour $n+1$ et S fixés est égal au degré de dégénérescence $g^{[n+1,S]}$. On peut dénombrer les tableaux de Young standard d'une certaine forme à l'aide du théorème dont le nom anglais est « hook-length formula » [18].

[1] Dans le monde anglophone, les diagrammes et tableaux de Young sont notés avec l'axe vertical inversé par rapport à leurs homologues francophones : les rangées inférieure sont ainsi plus courtes ou égales aux rangées supérieures.

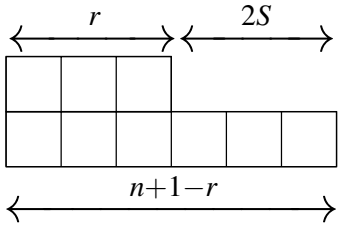

Figure V.1 – Diagramme de Young représentant les états composés de $n+1$ qubits et ayant comme spin total S. Les paramètres $n+1$ et $\{S$ ou $r\}$ déterminent totalement la forme du diagramme (ou vice versa). On voit bien la relation entre S et le paramètre r défini à la section 3.3.3.1. Ce dernier correspond au nombre de colonnes à deux étages.

Théorème 5. *Soit N le nombre total de cases composant un diagramme de Young d'une forme T fixée et soit γ_i la longueur de crochet (on la définit tout de suite après) de la i-ème case de ce diagramme, alors :*

$$\#\textit{ tableaux standard de Young de forme } T = \frac{N!}{\prod_i^N \gamma_i}$$

La longueur de crochet γ_i d'une case i d'un diagramme de Young est 1 plus la somme du nombre de cases au-dessus et à droite de cette case. La figure V.2 le montre graphiquement.

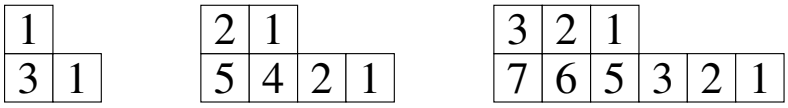

Figure V.2 – Trois diagrammes de Young dont chaque case contient sa longueur de crochet. Ces formes correspondent à des diagrammes de Young de tailles respectives $N_1 = 3$, $N_2 = 6$ et $N_3 = 9$ et de spins totaux respectifs $S_1 = \frac{1}{2}$, $S_2 = 1$ et $S_3 = \frac{3}{2}$.

On remarque par la même occasion à la figure V.2 que pour tout diagramme de Young à deux colonnes, de taille $N = n+1$ et de spin total S, les longueurs de crochet sur la rangée du haut sont égales aux entiers de 1 à r, tandis que celles du bas sont égales aux entiers de 1 à $n+2-r$, en sautant $2S+1$. On peut donc écrire une formule analytique pour quantifier la dégénérescence $g^{[n+1,S]}$.

Proposition 57. *Le degré de dégénérescence de permutation de l'état de spin total S quand on compose ensemble $n+1$ qubits est donné par :*

$$\begin{aligned} \mathrm{g}^{[n+1,S]} &= \#\ \textit{tableaux standard de Young de forme}\ \{N = n+1,\ \mathrm{Spin} = S\} \\ &= \frac{(n+1)!}{(r)!(n+2-r)!} \cdot (n+2-2r) \\ &= \frac{(n+1)!}{(\frac{n+1}{2}-S)!(\frac{n+3}{2}+S)!} \cdot (2S+1) \end{aligned}$$

■