Université de Montréal

Sur l'identification des états produits par une source quantique maximalement décorrélée.

par
Serge-Olivier Paquette

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

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

Août, 2016

RÉSUMÉ

Nous définissons une source uniforme maximalement décorrélée comme un ensemble d'états quantiques qui sont pris chacun dans une base différente d'un ensemble de bases mutuellement non-biaisées et dont le nombre d'états est égal à la dimension de l'espace considéré. Nous tentons d'obtenir une borne supérieure sur la probabilité d'identifier les états émis par une telle source grâce à des techniques numériques et analytiques. Nous proposons aussi un protocole cryptographique de preuve de connaissance non-interactif novateur qui utilise une telle source comme élément principal de sa preuve de sécurité.

Mots clés : informatique quantique, théorie de l'information, optimisation semi-définie, cryptographie, identification, mesure, preuve de connaissance.

ABSTRACT

Distinguishability of states produced by a maximally uncorrelated quantum source

We define a maximally uncorrelated quantum source as an ensemble of quantum states, each taken in a different base from a set of mutually unbiased basis and such that the number of states equals the dimension of the space they live in. We explore upper bounds on the probability of distinguishing such states using numerical and analytical techniques. We also propose a novel cryptographic protocol for a non interactive proof of knowledge in which such a source is used as the main technical tool for the security proof.

Keywords: Quantum computing, Cryptography, Information Theory, Semidefinite optimization, Distinguishability, measure, proof of knowledge.

TABLE DES MATIÈRES

0.1 Notation

$\mathbb{C}$	Le corps des complexes
$\mathcal{A}, \mathcal{B}, \ldots$	Espace de Hilbert
$\alpha, \beta, \ldots$	Sous-espace
$A, B, \ldots$	Opérateur
$\mathcal{H}_n$	Espace de Hilbert sur n qubits
$\mathbb{1}_{\mathcal{A}}$	Identité sur $\mathcal{A}$
$\mathbb{1}_n$	Identité sur $\mathcal{H}_n$
$\|\psi\rangle$	Vecteur (ket)
ρ	Opérateur de densité
$\mathcal{L}(\mathcal{X}, \mathcal{Y})$	$\{\mathbf{A} \mid \mathbf{A}$ est une application linéaire de $\mathcal{X}$ vers $\mathcal{Y}\}$
$\mathcal{L}(\mathcal{X})$	$\mathcal{L}(\mathcal{X}, \mathcal{X})$
$\mathcal{L}_{n,m}$	$\mathcal{L}(\mathcal{H}_m, \mathcal{H}_n)$
$\mathcal{L}_n$	$\mathcal{L}(\mathcal{H}_n)$
$\mathrm{U}(\mathcal{X})$	$\{U \in \mathcal{L}(\mathcal{X}) \mid U^*U = \mathbb{1}\}$
$\mathrm{Her}(\mathcal{X})$	$\{A \in \mathcal{L}(\mathcal{X}) \mid A = A^*\}$
$\mathrm{Pos}(\mathcal{X})$	$\{P \in \mathcal{L}(\mathcal{X}) \mid \forall \|\phi\rangle \in \mathcal{X}, \quad \langle\phi\|P\|\phi\rangle \geq 0\}$.
$\mathrm{D}(\mathcal{X})$	$\{A \in \mathrm{Pos}(\mathcal{X}) \mid \mathrm{tr}\, A = 1\}$
σ_i	Opérateurs de Pauli
$\mathbb{P}_n$	Ensemble des matrices de Pauli sur n qubits
$\hat{\mathbb{P}}_n$	Groupe de Pauli sur n qubits
$\langle X, Y \rangle$	Produit scalaire de X et Y
$\mathrm{tr}\, X$	Trace de X
$X \otimes Y$	Produit de Kronecker de X et Y
$X^{\otimes n}$	Produit tensoriel n fois
X^*	Le transposé conjugué de X (adjoint)

REMERCIEMENTS

Je remercie premièrement Louis Salvail, Rébecca Lapointe et le reste du LITQ. Une mention spéciale à François pour sa lecture attentive.

Je remercie ultimement l'Ineffable et la Droititude.

CHAPITRE 1

INTRODUCTION

La mécanique quantique est le modèle mathématique qui permet une description du monde physique au niveau atomique et subatomique. Les prédictions qu'elle fait sont souvent, il va sans dire, totalement contre-intuitives, voire étranges. En effet, certains objets décrits par cette théorie possèdent un ensemble de caractéristiques n'ayant aucune contrepartie classique et dont la nature est impossible à connaître en totalité. S'il est possible de déterminer parfaitement l'une des propriétés, la connaissance parfaite des autres est physiquement impossible. L'exemple canonique de ce phénomène est le fameux principe d'incertitude d'Heisenberg [17], assurant en quelque sorte qu'il n'est pas possible de déterminer à la fois la position et l'impulsion d'un objet quantique avec une précision arbitraire. Nous disons donc d'une part que ces observables sont incompatibles et que leur connaissance mutuelle est complémentaire, et d'autre part que les sources qui les produisent sont décorrélées. L'impossibilité d'identifier parfaitement un état quantique de manière générale est à la base de la réputation ésotérique de la mécanique quantique. Depuis les travaux d'Heisenberg, beaucoup de recherches ont été faites afin de comprendre les mécanismes sous-jacents à la complémentarité d'états et à ses conséquences. L'étude des mesures d'identification d'états est un pilier de la théorie quantique et plus récemment de la théorie de l'information quantique. Plusieurs approches sont étudiées dans la littérature afin de caractériser la capacité à identifier un état aussi fidèlement que possible, et ce, avec diverses stratégies. C'est toutefois un problème ouvert que de trouver une forme analytique pour la mesure d'identification optimale pour un ensemble d'états général.

Le but de ce mémoire est d'étudier la capacité d'un dispositif à discriminer des états

quantiques qui sont obtenus d'une source maximalement décorrélée au sens où elle produit un état par base d'un ensemble maximal de bases mutuellement non biaisées. Une instance importante de ce problème que nous verrons est l'identification d'une source qui produit avec probabilité uniforme un photon polarisé dans la base diagonale ou un photon polarisé dans la base rectilinéaire. Nous commençons l'exposé avec un ensemble de préliminaires mathématiques, puis nous présentons le problème d'identification d'une source quantique ainsi que la définition formelle d'une source maximalement décorrélée. Nous présentons ensuite une application cryptographique d'une telle source qui en justifie la définition. Le reste du travail présente les diverses pistes de solutions afin de borner supérieurement la probabilité d'identification ainsi que les problèmes qui leur sont associés. Nous donnons ainsi une borne inférieure sur l'entropie de l'état créé par la source, une expression de la mesure optimale pour obtenir des résultats numériques ainsi que la construction d'une mesure qui minimise l'erreur en moindre carré. Nous comparons ensuite les résultats obtenus numériquement avec ce que nous connaissons théoriquement ainsi que les prochaines directions de recherche.

CHAPITRE 2

PRÉLIMINAIRES MATHÉMATIQUES

Dans cette section, nous présentons premièrement le formalisme mathématique de la mécanique quantique utile pour la théorie de l'information quantique, tout en étant conscients que ce formalisme ne fait qu'effleurer la profondeur du bagage théorique général et sans trop se soucier de la justification physique des modèles décrits ci-dessous. Nous montrons ensuite une construction des bases mutuellement non biaisés, qui fait office de preuve d'existence et qui utilise l'ensemble des matrices de Pauli. La présentation faite ici est standard dans la littérature de la théorie de l'information quantique et se retrouve dans des ouvrages tels [33] et [45] avec certains passages plus spécifiques pris dans les notes du cours de John Watrous [43] et de Louis Salvail [38].

La théorie quantique est directement caractérisée par sa nature fondamentalement probabiliste et donne lieu à des conséquences étonnantes. Son développement est intimement lié à l'évolution des mathématiques du 20e siècle, plus particulièrement en algèbre linéaire, en analyse fonctionnelle et en algèbre abstraite par les travaux de géants tels que Von Neumann, Heisenberg, Dirac, Schrödinger, Pauli et Feynmann, pour n'en nommer que quelques-uns.

2.1 Espaces de Hilbert

Le contexte général dans lequel nous travaillons est l'espace de Hilbert. Le corps dans lequel nous faisons les calculs est $\mathbb{C}$, le corps des nombres complexes. Pour $z \in \mathbb{C}$, nous notons $\overline{z}$ le conjugué complexe de z, c'est-à-dire que si $z = x + iy$, alors $\overline{z} = x - iy$. Nous tenons pour acquises les propriétés des espaces vectoriels.

Définition 2.1.1. (Espace de Hilbert)

Nous appelons *espace de Hilbert*, noté généralement $\mathcal{H}$ ou bien $\mathcal{A}, \mathcal{B}, \ldots$ un espace vectoriel sur le corps des complexes muni d'un produit scalaire. Les éléments de $\mathcal{H}$ sont appelés vecteurs. Nous ne considérons généralement que des espaces de dimensions finis.

Nous noterons les éléments φ de $\mathcal{H}$ avec la notation de Dirac. Un *ket* $|\varphi\rangle$ est un vecteur colonne et un *bra* $\langle\varphi|$ est une fonctionnelle linéaire sur $\mathcal{H}$, que nous prendrons comme le transposé conjugué complexe du ket $\langle\varphi| = |\varphi\rangle^*$, donc un vecteur ligne. Cette notation est très utile. On exprime ainsi par exemple le produit scalaire euclidien de façon naturelle :

$$\langle\psi|\phi\rangle = \begin{pmatrix} \overline{\alpha_1} & \ldots & \overline{\alpha_n} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \sum_{i=1}^{n} \overline{\alpha_i}\beta_i$$

On dit qu'une base ou plus généralement un ensemble k de vecteurs $\{|x_1\rangle, \ldots, |x_k\rangle\}$ est *orthonormée* si $\forall i, j$

$$|\langle x_i|x_j\rangle| = \delta_{i,j}$$

où $\delta_{i,j}$ est le delta de Kronecker.

Nous notons les ensembles d'opérateurs importants suivants :

- $\mathcal{L}(\mathcal{X}, \mathcal{Y}) = \{\mathbf{A} \mid \mathbf{A}$ est une application linéaire de $\mathcal{X}$ vers $\mathcal{Y}\}$
- $\mathcal{L}(\mathcal{X}) = \mathcal{L}(\mathcal{X}, \mathcal{X})$,

- $\mathcal{L}_{n,m} = \mathcal{L}(\mathcal{H}_m, \mathcal{H}_n)$,
- $\mathcal{L}_n = \mathcal{L}(\mathcal{H}_n)$.
- $\mathrm{U}(\mathcal{X}) = \{U \in \mathcal{L}(\mathcal{X}) \,|\, U^*U = \mathbb{1}\}$. On dit que U est *unitaire*.
- $\mathrm{Her}(\mathcal{X}) = \{A \in \mathcal{L}(\mathcal{X}) \,|\, A = A^*\}$. On dit que A est *hermitien*.
- $\mathrm{Pos}(\mathcal{X}) = \{P \in \mathcal{L}(\mathcal{X}) \,|\, \forall |\phi\rangle \in \mathcal{X}, \quad \langle\phi|P|\phi\rangle \geq 0\}$. On dit alors que P est *positif* ou *semi-défini positif*. Si $\langle\phi|P|\phi\rangle > 0$, alors P est dit *défini positif*.
- $\mathrm{D}(\mathcal{X}) = \{A \in \mathrm{Pos}(\mathcal{X}) \,|\, \mathrm{tr}\, A = 1\}$. A est un *opérateur* de densité.
- On dit que $P \in \mathcal{L}(\mathcal{X})$ est un *projecteur* si $P^2 = P$.
- On dit que A est *normal* si $AA^* = A^*A$.

On peut voir que les opérateurs hermitiens, unitaires et positifs sont tous normaux. Ces opérateurs sont omniprésents en mécanique quantique et possèdent des propriétés importantes que nous verrons.

Définition 2.1.2. (Équivalence unitaire) Soit $A, B \in \mathcal{L}_n$, on dit que A et B sont des opérateurs *unitairement équivalents* s'il existe $U \in \mathrm{U}(\mathcal{L}_n)$ tel que

$$A = UBU^*$$

C'est une relation d'équivalence car elle est symétrique, réflexive et transitive.

Si A est unitairement équivalent à une matrice diagonale D dont les seules entrées non nulles sont sur la diagonale, alors on dit que A est unitairement diagonalisable.

Définition 2.1.3. (Valeur et vecteur propre) Soit $A \in \mathcal{L}_n$, s'il existe un nombre $\lambda \in \mathbb{C}$ et un vecteur $|\psi\rangle \in \mathcal{H}_n$ tel que $A|\psi\rangle = \lambda|\psi\rangle$, alors on dit que λ est une *valeur propre* de A et que $|\psi\rangle$ est un vecteur propre de A associé à λ.

Théorème 2.1.1. *(Théorème spectral) A est un opérateur normal si et seulement si A est unitairement diagonalisable. Alors $A = UDU^*$ et les éléments de D sont les valeurs propres de A, les vecteurs colonnes de U sont les vecteurs propres de A et ils sont orthonormés.*

Définition 2.1.4. (Commutateur) Soient $A, B \in \mathcal{L}_n$, nous appelons respectivement *commutateur* et *anticommutateur* les opérations

$$[A, B] = AB - BA \quad \text{et} \quad \{A, B\} = AB + BA \ .$$

Nous disons aussi que A, B *commutent* si $[A, B] = 0$ et *anticommutent* si $\{A, B\} = 0$.

Théorème 2.1.2. *Soit $\{A_i\}_i \in \mathcal{L}_n$ une famille de matrices diagonalisables, alors ces matrices sont diagonalisables dans la même base (partagent les mêmes sous-espaces propres) si et seulement si elles commutent 2 à 2.*

2.2 États quantiques

Un état quantique vit dans un espace de Hilbert. L'état quantique est fait une représentation mathématique de l'état d'un objet dont le comportement est régi par les lois de la mécanique quantique. On associe à un objet ou système quantique S un espace de Hilbert $\mathcal{S}$ de même dimension n que le nombre de degrés de liberté de S.

Définition 2.2.1. On appelle *état pur* du système (traditionnellement nommé fonction d'onde) un vecteur $|\psi\rangle \in \mathcal{S}$ normalisé, c.-à-d. tel que $\langle\psi|\psi\rangle = 1$. Soit $B = \{|x_1\rangle, \ldots, |x_n\rangle\}$ une base de $\mathcal{S}$, on représente $|\psi\rangle$ dans la base B de la manière suivante :

$$|\psi\rangle = \sum_{i=1}^{n} \gamma_i |x_i\rangle \ ,$$

où $\gamma_i \in \mathbb{C}$ sont les amplitudes en i et $\sum_{i=1}^{n} |\gamma_i|^2 = 1$. On dit que $|\psi\rangle$, exprimé dans la base b, est en *superposition* des états (vecteurs) de cette base.

Par exemple,

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ et} \\ |-\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

sont des états quantiques en superposition des états de la *base calculatoire* :

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{et} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad .$$

Tout vecteur qui s'écrit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ et tel que $|\alpha|^2 + |\beta|^2 = 1$ est appelé *qubit* et est le pendant quantique d'un bit $b \in \{0, 1\}$ classique avec la propriété supplémentaire de superposition. Si l'on mesure l'état dans la base calculatoire, on obtient le résultat $|0\rangle$ avec probabilité $|\alpha|^2$ et le résultat $|1\rangle$ avec probabilité $|\beta|^2$.

Plus généralement, soient $|\phi\rangle$ et $|\gamma\rangle$ des états arbitraires, alors on appelle *fidélité* la quantité : $|\langle\phi|\gamma\rangle| \in [0, 1]$, parfois aussi dite *chevauchement*, car $|\langle\phi|\gamma\rangle|^2$ représente la probabilité que l'état $|\gamma\rangle$ se fasse passer pour l'état $|\phi\rangle$.

Une manière plus générale de représenter un état est de considérer un opérateur de densité :

$$\rho \in \mathrm{D}(\mathcal{S}) \ ,$$

où comme on l'a déjà vu

$$\mathrm{D}(\mathcal{S}) = \{A \in \mathrm{Pos}(\mathcal{S}) \,|\, \mathrm{tr}\, A = 1\} \ .$$

Ce type d'opérateur capture l'idée d'un mélange statistique. On dit que $\rho \in \mathrm{D}(\mathcal{S})$ est *pur* si $\rho^2 = \rho$, c'est-à-dire qu'il s'écrit comme produit externe $|\psi\rangle\langle\psi|$ pour un état pur $|\psi\rangle$. Nous disons d'un état qui n'est pas pur, ou dont la nature n'est pas spécifiée, qu'il est *mixte*.

Soit $P = (p_i, \rho_i)_{i=1}^n$ une distribution de probabilité sur les états ρ_i, c'est-à-dire que $p_i \in [0,1]$, $\sum_i p_i = 1$ et $P : \mathrm{D}(\mathcal{X}) \to [0,1]$ est une fonction qui associe à un état ρ_i une probabilité p_i, alors l'opérateur de densité suivant est un état mixte :

$$\sigma = \sum_{i=1}^{n} p_i \rho_i \in \mathrm{D}(\mathcal{S}) \ .$$

C'est la forme la plus générale d'un état quantique. On peut en principe associer à tout opérateur de densité un système quantique correspondant et vice-versa. Il y a donc une équivalence entre le formalisme mathématique et le monde physique.

Soit $\mathrm{U}(\mathcal{S}) = \{U \in \mathcal{L}(\mathcal{S}) \,|\, U^*U = \mathbb{1}\}$ l'ensemble des opérateurs unitaires. Les transformations valides pour un système quantique sont représentées mathématiquement par des opérateurs de $\mathrm{U}(\mathcal{S})$. On appelle *transformation unitaire* toute transformation linéaire $T : \mathcal{S} \to \mathcal{S}$ telle qu'il existe $U \in \mathrm{U}(\mathcal{S})$ de sorte que $T(|\psi\rangle) = U|\psi\rangle$. Toute transformation unitaire est aussi une évolution valide d'un système quantique. L'ensemble de ces transformations forme un groupe sous la composition (multiplication matricielle) ;

elles sont toutes composables et inversibles : L'inverse d'un opérateur unitaire U est évidemment U^* et pour tout U et $V \in \mathrm{U}(\mathcal{S})$, on vérifie facilement que $UV \in \mathrm{U}(\mathcal{S})$.

L'équivalent d'une transformation unitaire sur un opérateur de densité $\rho \in \mathrm{D}(\mathcal{X})$ est la conjugaison $T(\rho) = U\rho U^*$.

En termes mathématiques, un opérateur de densité ρ peut être interprété comme un objet auquel on peut appliquer un autre objet M_x afin d'en extraire une distribution de probabilité pour un ensemble X de valeurs x. Nous appelons ce processus une *mesure* sur ρ.

Soit $\rho \in \mathrm{D}(\mathcal{S})$, une mesure sur ρ est l'interaction entre un appareil de mesure et le système considéré. On appelle *observable* un opérateur hermitien O qui agit d'une telle manière sur le système observé. Par hermicité, un observable possède une décomposition spectrale :

$$O = \sum_i \lambda_i P_i \ ,$$

avec les P_i des projecteurs sur l'espace propre associé à la valeur propre λ_i de O. On dit que le résultat de la mesure est la valeur «classique» i qui est obtenue avec probabilité

$$p(i) = \mathrm{tr}\{P_i\rho\} \ .$$

On appelle l'ensemble $\{P_i\}_i$ une *mesure projective* ou *mesure de Von Neumann* et la règle qui associe les probabilités aux valeurs propres de l'observable est la *règle de Born*. Par les propriétés de la décomposition spectrale, les P_i obtenus ainsi sont nécessairement orthogonaux (ou peuvent facilement le devenir par le procédé de Gram-Schmidt si la multiplicité des valeurs propres est plus grande que 1), et donc le nombre de résultats

possibles pour une mesure projective est inférieur ou égal à la dimension de l'espace considéré.

On considère une forme de mesure plus générale et très utile car elle caractérise l'ensemble des mesures physiquement réalisables, appelée POVM («Positive Operator Valued Measure»). Tout ensemble $\{M_m\}$ tel que $M_m \in \mathrm{Pos}(\mathcal{S})$ (c.-à-d. $M_m \geq 0$) et

$$\sum_m M_m = \mathbb{1}_{\mathcal{S}}$$

est un POVM et constitue une mesure valide du système. On peut montrer que ces mesures sont équivalentes aux mesures projectives en joignant des systèmes auxiliaires et en faisant une mesure projective sur les systèmes combinés, mais nous tenons subséquemment pour acquis le formalisme de POVM. Voir [33] pour une introduction.

Comme un état quantique est confiné dans son espace de Hilbert, il est naturel de considérer la description mathématique de systèmes conjoints dans un produit de chacun de leur espace respectif, qu'on appelle *produit tensoriel*.

Exemple 2.2.1. (Espace $\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}$ de n qubits.)

On considère l'espace qui contient n qubits distincts. Soit $x \in \{0,1\}^n$, on note $|x\rangle \in \mathcal{H}_n$ le produit tensoriel de n qubits. Par exemple, $|0\rangle \otimes |1\rangle$ est noté $|01\rangle$. On voit naturellement que $\dim(\mathcal{H}_n) = 2^n$.

De la même manière qu'on puisse joindre deux espaces pour décrire le comportement conjoint de deux systèmes, on peut obtenir le comportement isolé d'un sous système.

Définition 2.2.2. Soit A et B deux systèmes quantiques, avec espace de Hilbert respectifs $\mathcal{A}$ et $\mathcal{B}$. Alors l'unique opérateur

$$\mathrm{tr}_A : \mathcal{L}(\mathcal{A} \otimes \mathcal{B}) \to \mathcal{L}(\mathcal{B})$$

tel que pour tout opérateur $\rho^{AB} = \rho^A \otimes \rho^B \in \mathcal{L}(\mathcal{A} \otimes \mathcal{B})$,

$$\mathrm{tr}_A \, \rho^{AB} = \rho^B \, \mathrm{tr} \, \rho^A$$

est appelé *trace partielle sur* A.

Exemple 2.2.2. Les états suivants sont appelés *états de Bell* ou *paires EPR* :

$$\begin{aligned}
\left|\psi^+\right\rangle &= \frac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle\right) \\
\left|\psi^-\right\rangle &= \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right) \\
\left|\phi^+\right\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \\
\left|\phi^-\right\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right)
\end{aligned}$$

et possèdent les propriétés suivantes :

- Ils sont intriqués, c'est-à-dire qu'ils ne peuvent pas s'écrire comme le produit tensoriel de deux états purs.
- Les deux premiers sont parfaitement anti-corrélés. La mesure dans la même base des deux qubits donne toujours des résultats opposés.
- Les deux derniers sont parfaitement corrélés. La mesure dans la même base des deux qubits donne toujours des résultats identiques.

2.3 Bases mutuellement non biaisées

Nous présentons ici la construction des bases mutuellement non biaisées (BMNB) pour n qubits qui fait également office de preuve constructive. Nous donnons d'abord une présentation générale sur les propriétés des BMNB, puis après avoir introduit les matrices de Pauli, nous les utiliserons pour construire explicitement les BMNB de $\mathcal{H}_n$.

Définition 2.3.1. Soit $\mathcal{H}$ un espace de Hilbert. Un ensemble de bases orthonormées $\{\mathcal{B}_i\}$ de $\mathcal{H}$, avec $|x_i\rangle \in \mathcal{B}_i$ et $|y_{i'}\rangle \in \mathcal{B}_{i'}$, est un ensemble de *bases mutuellement non biaisées* si

$$\begin{aligned} i \neq i', \quad &\Rightarrow \quad |\langle x_i|y_{i'}\rangle|^2 = \frac{1}{d} \text{ et} \\ i = i', \quad &\Rightarrow \quad |\langle x_i|y_{i'}\rangle|^2 = \delta_{x,y} \end{aligned}$$

avec d la dimension de $\mathcal{H}$.

L'interprétation opérationnelle de ces ensembles est que si un état est parfaitement déterminé dans l'une des bases, le résultat d'une mesure dans n'importe quelle autre des bases de l'ensemble est parfaitement aléatoire. Un exemple d'ensemble de BMNB en dimension 2 est l'ensemble des vecteurs propres des matrices de Pauli.

Pour un espace de Hilbert de dimension d, un opérateur de densité ρ est déterminé par $d^2 - 1$ nombres réels, alors que la mesure dans une base donnée fournit $d - 1$ probabilités indépendantes. On a donc besoin de mesurer dans $d + 1$ bases différentes afin de spécifier entièrement ρ. Il a été montré que l'ensemble des bases qui maximise l'inférence, par la tomographie, d'un opérateur de densité quelconque est un ensemble de bases mutuellement non-biaisées [22], [23] et [46].

Les ensembles de BMNB sont aussi, paradoxalement peut-être, maximalement incompatibles au sens où ils maximisent les relations d'incertitude ; si on prépare un état dans l'une des bases, la mesure dans une autre base nous donnera un résultat parfaitement aléatoire. C'est une manifestation plus générale du principe d'incertitude d'Heisenberg pour la position et l'impulsion. Un compte rendu éclairant des propriétés des relations d'incertitude en théorie de l'information sur les bases mutuellement non-biaisées est donné dans [44]. L'une des utilisations les plus célèbres est sans doute dans le protocole de distribution de clé *BB84* [6].

On utilise, sans le montrer, le fait qu'il existe un ensemble de $d+1$ BMNB pour tout espace de Hilbert de dimension $d = p^m$ où p est un nombre premier. Ivanović à montré que ce nombre est atteint pour une dimension première [22] et le cas pour une puissance d'un nombre premier est donné par Wootters et Fields [46]. Ce nombre $d+1$ est aussi maximal ; il ne peut y en avoir plus. Il existe en fait une construction explicite simple d'un ensemble de bases mutuellement non biaisées pour l'espace $\mathcal{H}_n$ sur n qubits que nous présentons et qui est donnée entre autres dans [29],[37] et [25] avec un partitionnement adéquat des matrices de Pauli $\mathbb{P}_n$. La preuve de correspondance entre les ensembles de bases unitaires maximalement commutantes et les bases mutuellement non biaisées indiquées est inspirée de [29] et est un cas particulier de la preuve plus générale du théorème ci-dessous pris dans [2]. Une construction plus générale pour p^m arbitraire est donnée par [27] avec l'application de la transformée de Fourier finie ou via la théorie de Galois dans [26].

Définition 2.3.2. Une *base unitaire maximalement commutante* pour un espace de Hilbert $\mathcal{X}$ de dimension d est un ensemble $M = \{u_1, \ldots, u_{d^2}\}$ de matrices unitaires contenant l'identité, qui est une base de $\mathcal{L}(\mathcal{X})$ et qui peut être partitionné en $M = \mathbb{1}_{\mathcal{X}} \cup C_1 \cup \ldots C_{d+1}$ de $d+1$ sous-ensembles disjoints C_j contenant chacun $d-1$ opérateurs commutants.

Théorème 2.3.1. *Une base unitaire orthogonale maximalement commutante définit un*

ensemble complet de $d+1$ BMNB. Ces bases sont constituées des vecteurs propres qui diagonalisent chaque sous-ensemble commutant C_i de la partition M.

Nous n'incluons pas la preuve de ce théorème, mais nous allons l'utiliser pour montrer la construction des bases pour l'espace $\mathcal{H}_n$ sur n qubits.

2.3.1 Matrices de Pauli sur n qubits

Un ensemble d'opérateurs particulièrement important et omniprésent dans la théorie quantique est appelé *groupe de Pauli* et est construit à partir d'un ensemble particulier de matrices. Pour plus de détails, voir le livre de *Nielsen et Chuang* [33].

Définition 2.3.3. Les trois matrices suivantes sont appelées *matrices de spin de Pauli*.

$$\left\{ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \right\} .$$

Ces opérateurs sont hermitiens, unitaires et normaux, mais il est facile de voir qu'ils ne sont pas positifs.

On a que la base de calcul $\mathcal{B}_+ = \{|0\rangle, |1\rangle\}$ est constituée des vecteurs propres de σ_z dont $|0\rangle$ à valeurs propres 1 et $|1\rangle$ à valeur propre -1, et la base diagonale $\mathcal{B}_\times = \{|+\rangle, |-\rangle\}$ est constituée des vecteurs propres de σ_x avec valeurs propres respectives 1 et -1 de la même manière. Les vecteurs propres de σ_y sont :

$$|\circlearrowright\rangle = \frac{1}{\sqrt{2}} = (|0\rangle + i|1\rangle)$$
$$|\circlearrowleft\rangle = \frac{1}{\sqrt{2}} = (|0\rangle - i|1\rangle) \ .$$

et forment une autre base de l'espace $\mathcal{H}_1 = \mathbb{C}^2$, appelée la *base circulaire*.

Une propriété remarquable de cet ensemble est qu'il forme une base de l'espace des matrices unitaires sur un qubit. C'est-à-dire que n'importe quel opérateur $X \in \mathrm{U}(\mathbb{C}^2)$ s'écrit comme combinaire linéaire unique des matrices de Pauli avec coefficient dans $\mathbb{C}$. Nous allons maintenant généraliser ces propriétés pour n qubits.

Définition 2.3.4. Nous pouvons renommer les matrices avec indices $\sigma_1 = \sigma_x, \sigma_2 = \sigma_y, \sigma_3 = \sigma_z,$. Si l'on ajoute l'identité $\sigma_0 = \mathbb{1}_2$ à l'ensemble des matrices de Pauli, alors on appelle *groupe de Pauli* l'ensemble :

$$\mathbb{P} = \{i^j \sigma_k\}_{j,k} \ ,$$

avec $j = 0, 1, 2, 3$ et $k = 0, 1, 2, 3$ muni de la multiplication matricielle.

Il est simple de voir que cet ensemble est fermé sous la multiplication, que chaque matrice est auto-inverse (à un multiple de i^k près) et que l'ordre du groupe des 16. On remarque de plus les relations de commutation suivantes qui caractérisent les éléments de cet ensemble :

$$\begin{aligned} &[\sigma_1, \sigma_2] = 2i\sigma_3 \quad [\sigma_1, \sigma_3] = 2i\sigma_2 \quad [\sigma_2, \sigma_3] = 2i\sigma_1 \\ &\{\sigma_1, \sigma_2\} = 0_2 \quad \{\sigma_1, \sigma_3\} = 0_2 \quad \{\sigma_2, \sigma_3\} = 0_2 \ , \end{aligned}$$

On a de plus l'importante relation :

$$\sigma_i^2 = \sigma_0 \ .$$

Définition 2.3.5. On nomme *groupe de Pauli sur n qubits* l'ensemble

$$\hat{\mathbb{P}}_n = \left\{ i^j \bigotimes_{l=1}^{n} \sigma_{k,l} \right\}_{i,j} \ .$$

Si l'on ne considère pas la phase, c'est-à-dire le nombre complexe i^j de norme 1 devant l'opérateur, nous retrouvons l'ensemble connu sous le nom de *matrices de Pauli sur* n *qubits* qu'on note $\mathbb{P}_n$. Cet ensemble constitue une base orthogonale de l'espace des matrices unitaires agissantes sur n qubits et est unique à une transformation unitaire près. Les matrices de Pauli possèdent toutes $\{-1, 1\}$ comme valeurs propres, chacune de multiplicité $\frac{2^n}{2}$ et elles ont une trace nulle, sauf la matrice identité.

2.3.2 Construction des BMNB pour $\mathcal{H}_n$

La construction se fait en 2 parties. On montre premièrement que l'ensemble des $4^n - 1$ matrices de Pauli sur n qubits, c'est-à-dire $\mathbb{P}_n \setminus \{\mathbb{1}_n\}$, peut bien être partitionné en $2^n + 1$ ensembles de $2^n - 1$ matrices commutantes, puis on utilise une telle partition pour obtenir un unique choix de BMNB.

Pour la première partie, on utilise l'existence, prouvée par Wootters [46], d'un ensemble de $2^n + 1$ BMNB noté $\{B_A\}_{A=0,\dots,2^n}$. Soit

$$P_\alpha^A = |\alpha_A\rangle\langle\alpha_A|$$

le projecteur sur l'élément $|\alpha\rangle$ de la base B_A. Alors on définit un ensemble d'opérateurs O_a^A par leur décomposition spectrale :

$$O_a^A = \sum_{\alpha=0}^{2^n-1} \lambda_{a,\alpha} P_\alpha^A \ ,$$

où $\{\lambda_{a,\alpha}\}_{a,\alpha}$ est le spectre de O_a^A que l'on peut voir comme les éléments dans une matrice $\Lambda = (\lambda_{a,\alpha})$ de dimension $2^n \times 2^n$, où toutes les lignes sont orthogonales et constituées d'un nombre égal de 1 et -1, sauf une rangée entièrement constituée de 1. Un exemple d'une telle matrice est la famille des matrices d'Hadamard :

$$H_n = H^{\otimes n} \quad \text{où} \quad H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \ .$$

Mais le choix ne s'y limite pas. Toute permutation des colonnes pourrait satisfaire. On choisit de plus pour tout A, $O_0^A = \mathbb{1}_n$, ce qui sera utile plus tard. De cette manière on obtient l'identité suivante :

$$\Lambda P_A = O_A \ ,$$

où

$$P_A = \begin{pmatrix} P_0^A \\ P_1^A \\ \vdots \\ P_{2^n-1}^A \end{pmatrix} \quad \text{et} \quad O_A = \begin{pmatrix} O_0^A \\ O_1^A \\ \vdots \\ O_{2^n-1}^A \end{pmatrix} \ .$$

Remarquons que l'équation est inversible car Λ est construite inversible. De cette ma-

nière, on obtient $2^n + 1$ ensembles de $2^n - 1$ opérateurs O_a^A (si l'on ne compte pas l'identité O_0^A) indicés par A et où chaque ensemble d'opérateurs possède une base de vecteurs propres commune (donc tous les opérateurs y commutent) avec valeurs propres 1 et -1. Ces sous-ensembles sont orthogonaux :

$$\begin{aligned} \mathrm{tr}\{O_a^A O_b^B\} &= \sum_{\alpha,\beta} \lambda_{a,\alpha}\lambda_{b,\beta}\,\mathrm{tr}\{P_\alpha^A P_\beta^B\} \ , \\ \mathrm{tr}\{O_a^A O_b^A\} &= \sum_{\alpha} \lambda_{a,\alpha}\lambda_{b,\alpha} = 2^n\delta_{ab} \ . \end{aligned}$$

et tous les opérateurs sont de trace nulle sauf O_0^A. Ils sont donc unitairement équivalents à l'ensemble des matrices de Pauli.

Nous venons de montrer que l'existence de $2^n + 1$ bases mutuellement non biaisées est équivalente à l'existence de $2^n + 1$ sous-ensembles commutant de matrices de Pauli. La deuxième partie de la preuve nous montre qu'on obtient, de n'importe quel partitionnement des matrices de Pauli en $2^n + 1$ sous-ensembles de $2^n - 1$ matrices commutantes, un ensemble maximal de BMNB, complétant la correspondance.

Soit $A = \{O_1^A, \ldots O_{2^n-1}^A\}$ une telle partition. Tous les opérateurs de A possèdent une base de vecteurs propres conjoints. Notons $\{|\alpha_A\rangle\}_\alpha$ cette base et $\lambda_{a,\alpha}$ leurs valeurs propres associées. Par les propriétés connues des matrices de Pauli, on sait que le spectre de chaque O_a^A est constitué d'un nombre égal de 1 et -1 et que ces matrices sont orthogonales. En ajoutant l'opérateur O_0^A, on peut construire une matrice de la même forme que Λ plus haut.

Soit $\varepsilon = \frac{\Lambda}{\sqrt{2^n}}$, on voit facilement que cette matrice est orthogonale. On peut donc inverser l'équation $\Lambda P_A = O_A$ et en reprenant la notation de projecteurs, toutes les matrices de

A peuvent être représentées de la manière suivante :

$$P_\alpha^A = 2^{-n} \sum_{\alpha=0}^{2^n-1} O_a^A \ ,$$

où $O_0^A = \mathbb{1}_n$. On obtient ainsi $2^n + 1$ bases mutuellement non biaisées car si $A \neq B$,

$$\begin{aligned} \mathrm{tr}\{P_\alpha^A P_\beta^B\} &= 2^{-2n} \,\mathrm{tr}\left\{ \left(\mathbb{1}_n + \sum_{a\neq 0} \lambda_{\alpha,a} O_a^A \right) \left(\mathbb{1}_n + \sum_{b\neq 0} \lambda_{\beta,b} O_b^B \right) \right\} \\ &= 2^{-n} + 2^{-2n} \sum_{a\neq 0} \sum_{b\neq 0} \lambda_{\alpha,a} \lambda_{\beta,b} \,\mathrm{tr}\left\{ O_a^A O_b^B \right\} \end{aligned}$$

et la partie de droite s'annule. Si $A = B$, l'équation devient

$$\begin{aligned} \mathrm{tr}\{P_\alpha^A P_\beta^A\} &= 2^{-n} \sum_a \lambda_{\alpha,a} \lambda_{\beta,a} \\ &= \delta_{\alpha\beta} \ , \end{aligned}$$

ce qui définit bien un ensemble de bases mutuellement non biaisées. Le défi qui reste ici est de trouver un ordre adéquat des colonnes de la matrice Λ pour chaque sous-ensemble de matrices de Pauli qui donne les bonnes combinaisons linéaires de vecteurs propres. Ceci n'est pas évident bien que ce soit toujours possible.

On donne un exemple pour 2 qubits. On trouve premièrement une partition adéquate des matrices de Pauli, puis on trouve une base de l'espace propre pour un des sous-ensembles obtenus. Afin de simplifier la notation, nous allons écrire (ab) pour représenter $\sigma_a \otimes \sigma_b$

avec $\sigma_i = \mathbb{1}$. Voici une partition valide, c'est-à-dire que pour chaque $M_i \subset \mathbb{P}_2$, les éléments de M_i commutent.

$$\begin{aligned} M_0 &= \{(zi), (iz), (zz)\} \\ M_1 &= \{(xi), (iy), (xy)\} \\ M_2 &= \{(yi), (ix), (yx)\} \\ M_3 &= \{(yy), (zx), (xz)\} \\ M_4 &= \{(xx), (yz), (zy)\} \ . \end{aligned}$$

En utilisant la matrice

$$\Lambda = H \otimes H = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \ ,$$

on obtient par exemple la base d'indice 0 qui correspond à la base de calcul.

$$\frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} \mathbb{1} \otimes \mathbb{1} \\ \sigma_z \otimes \mathbb{1} \\ \mathbb{1} \otimes \sigma_z \\ \sigma_z \otimes \sigma_z \end{pmatrix} = \begin{pmatrix} P_0^0 \\ P_1^0 \\ P_2^0 \\ P_3^0 \end{pmatrix} \ .$$

En prenant un élément arbitraire :

$$\begin{aligned} P_3^0 &= \frac{1}{4}\left(\mathbb{1}\otimes\mathbb{1} - \sigma_z\otimes\mathbb{1} - \mathbb{1}\otimes\sigma_z + \sigma_z\otimes\sigma_z\right) \\ &= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ &= |11\rangle\langle 11| \ . \end{aligned}$$

On peut ainsi de suite obtenir un ensemble de bases mutuellement non biaisées pour n qubits.

2.4 Théorie de l'information

La théorie de l'information s'intéresse à quantifier des limites précises pour des tâches opérationnelles. Les outils développés répondent donc à des besoins spécifiques et sont définis en fonction de ces besoins.

La nature opérationnelle des quantités définies par la théorie de l'information implique que celles-ci sont beaucoup plus compréhensibles lorsque mises en situation. Nous introduisons donc deux personnages, Alice et Bob, qui veulent communiquer d'une certaine manière. Supposons par exemple qu'Alice détienne une information sous la forme d'une variable aléatoire X qui prend valeur dans un ensemble fini $i = 1, \ldots, n$ et qu'elle souhaite transmettre cette information à Bob. Les tâches typiques de la théorie de l'information sont donc, par exemple, la compression de cette information et la transmission sur un canal bruité ou l'encodage-décodage de manière à éviter les erreurs ou l'obfuscation

de l'information. Nous nous intéressons dans ce mémoire à la capacité de Bob à décoder l'information qu'Alice lui envoie dans un encodage quantique donné. Définissons quelques quantités utiles.

En pratique, on peut définir un message comme étant une suite de symboles pris d'un alphabet $X = \{x_1, \dots x_n\}$. On peut supposer sans perte de généralité que chaque symbole du message a une probabilité indépendante $p(x_i) \in [0, 1]$ d'apparaître, telle que $\sum_i p(x_i) = 1$.

2.4.1 Entropie de Shannon

Définition 2.4.1 (Entropie de Shannon [39])**.** Soit $X = \{(x_i, p_i)\}_{i=1}^n$ une variable aléatoire, alors la quantité suivante est appelée *Entropie de Shannon* de X.

$$\begin{aligned} H(X) &:= H(p_1, \dots, p_n) = -\sum_i p_i \lg p_i \\ &= \mathbb{E}[-\log p(x)] \end{aligned}$$

Le logarithme est pris en base 2 et l'entropie d'une variable quantifie ainsi en bits (binary digits) l'information que l'on obtient lorsqu'on apprend le résultat d'une expérience de la variable aléatoire X (un symbole de l'alphabet). De manière équivalente, c'est la quantité d'incertitude en moyenne qu'on a sur la valeur de X avant la réception ou encore la quantité de bits nécessaire pour communiquer parfaitement la nature de la variable aléatoire. C'est cette idée sur l'équivalence incertitude-information qu'a eue Shannon et qui fut le point de départ de toute la théorie de l'information. La deuxième égalité est interprétée comme étant l'espérance de la *surprise*, $s(x_i) = -\log p(x_i)$, associé à la

réalisation de x_i. On remarque que l'entropie est indépendante des événements. Elle ne prend en compte que leurs probabilités associées.

Deux cas particuliers de variable aléatoire sont à considérer pour l'interprétation de mesures entropiques. Le cas où $H(X) = 0$ et où $H(X) = \log n$. Si $H(X) = 0$, alors la variable aléatoire X ne possède qu'un seul événement x_1 qui arrive avec probabilité $p_1 = 1$. Il n'existe aucune surprise et on n'a besoin d'aucune information pour décrire la variable ;

$$H(1, 0, \ldots, 0) = 0$$

Si $H(X) = \log n$, alors chaque symbole a probabilité égale et il faut $\log n$ bits pour en spécifier une occurrence. On a

$$H(X) = H(\frac{1}{n}, \ldots, \frac{1}{n})$$

On peut facilement généraliser cette quantité pour les variables aléatoires conjointes ; soient X et Y deux variables aléatoires, $H(X, Y)$ est l'entropie de la distribution conjointe de X et Y définie de la même manière :

$$H(X, Y) = \mathbb{E}[s(x, y)]$$

On définie aussi naturellement l'entropie conditionnelle qui quantifie l'incertitude sur X conditionnellement à la connaissance de Y ou le nombre de bits additionels par symbole nécessaire pour spécifier X et Y lorsque seulement Y est connu.

$$\begin{aligned} H(X|Y) &:= H(X,Y) - H(Y) \\ &= \mathbb{E}[s(x|y)] \end{aligned}$$

Pour plus d'informations et les justifications de ces définitions, voir le livre de Cover et Thomas [8].

2.4.2 Entropie de Rényi

L'entropie de Shannon n'est utile que lorsque nous avons accès à un grand nombre de copies d'un message car elle calcul l'incertitude en moyenne, de là la caractérisation asymptotique mentionnée plus haut. Une mesure plus générale d'information est donnée par Rényi [36] sous la forme suivante :

Définition 2.4.2. Soit $X = \{(x_i, p_i)\}_{i=1}^n$ une variable aléatoire et $\alpha \in [0,1) \cup (1,\infty)$, alors la quantité suivante est appelée *entropie de Rényi d'orde* α de X.

$$H_\alpha(X) = \frac{1}{1-\alpha} \log \left(\sum_{i=1}^n p_i^\alpha \right) \quad .$$

Comme pour l'entropie de Shannon, le logarithme est en base 2 car la quantité mesure des bits. Cette mesure, paramétrée par $\alpha \in [0,1) \cup (1,\infty)$, est une fonction décroissante en α. On remarque 3 cas particuliers qui sont intéressant, soit lorsque $\alpha \to 1$, $\alpha = 2$ et $\alpha \to \infty$.

On peut montrer grâce à la rêgle de l'Hôpital que $\lim_{\alpha \to 1} H_\alpha(X) = H(X)$, l'entropie de Shannon. L'entropie de Rényi d'ordre 2 est appelée *entropie de collision* :

$$H_2(X) = -\log\left(\sum_{i=1}^{n} p_i^2\right) = -\log p(X = Y) \ ,$$

où X et Y sont deux variables aléatoires indépendantes et identiquement distribuées.

Le cas où $\alpha \to \infty$ est appelé *min-entropie* :

$$H_\infty(X) = \min_i[-\log p_i] = -\log \max_i p_i \ .$$

Cette quantité caractérise la meilleure chance de deviner la valeur de X. On peut aussi facilement montrer que

$$\log n \geq H_1(X) \geq H_2(X) \geq H_\infty(X) \ .$$

CHAPITRE 3

LE PROBLÈME D'IDENTIFICATION D'ÉTATS QUANTIQUES

Étant donné que des états non orthogonaux ne peuvent être distingués parfaitement, le problème qui consiste à trouver une mesure pour discriminer un état parmi un ensemble fini d'états non orthogonaux est fondamental pour plusieurs applications de la mécanique quantique [20][18] et a récemment pris de l'importance avec l'arrivée des technologies de la cryptographie quantique [13]. A cette fin, plusieurs stratégies existent dans le but de minimiser l'erreur d'estimation qui dépendent de la façon dont on formule le problème d'identification et de l'information connue a priori [3].

3.1 Identification des états produits par une source quantique

Dans cette section, nous définissons en premier lieu ce qu'est une source quantique puis nous voyons la formulation formelle du problème d'identification générale dans un contexte d'optimisation et nous montrons ensuite un exemple instructif d'une telle source qui nous servira à des fins d'analyse. Nous présentons ensuite la source maximalement décorrélée, laquelle constitue le cœur du problème de ce mémoire, puis nous voyons un exemple d'application cryptographique qui en motive l'étude.

Définition 3.1.1. Une source quantique dans le contexte de la théorie de l'information est n'importe quel processus qui produit un état quantique $|\psi_i\rangle$ parmi un ensemble fini d'états $\{|\psi_x\rangle\}_{x\in X}$ selon une variable aléatoire $x \in X := \{0,1\}^n$ afin de transmettre cet état sur un canal pour qu'il soit détecté par un appareil de mesure qui en extrait une valeur classique $y \in Y := \{0,1\}^n$. À une source S est donc associée une description mathématique sous forme d'un ensemble $E_X = \{(p_x, |\psi_x\rangle)\}_{x\in X}$.

Une source ayant une interprétation opérationnelle, on utilisera de manière équivalente la description opérationnelle de la source S et sa description mathématique E_X, cette dernière étant utilisée plus couramment dans la littérature de la mécanique quantique.

Le problème d'identification est traditionnellement énoncé sous forme d'un jeu entre Alice et Bob : soit $\{|\varphi_1\rangle, \ldots, |\varphi_n\rangle\}$ un ensemble d'états quantiques. La source (Alice) choisit un indice $i \in I = \{1, \ldots, n\}$ avec probabilité p_i, puis elle envoie l'état $|\varphi_i\rangle$ à Bob à l'aide d'un canal quantique. La tâche de ce dernier est de déterminer la valeur de la variable aléatoire, c'est-à-dire de retrouver i en mesurant l'état de la meilleure manière possible, ce que nous définissons ci-dessous.

Définition 3.1.2. Soit $x \in X$ une variable aléatoire prenant valeur dans un ensemble fini X et soit $\{|\psi_x\rangle\}_{x\in X}$ une collection d'états purs d'un espace de Hilbert $\mathcal{X}$. On construit alors l'opérateur de densité associé à l'ensemble $E_X = \{(p_x, |\psi_x\rangle)\}_{x\in X}$:

$$\rho = \sum_{x\in X} p_x |\psi_x\rangle\langle\psi_x| \ .$$

Le problème d'identification que nous considérons consiste à minimiser l'erreur d'identification, c'est-à-dire de maximiser la probabilité de retrouver la valeur classique $x \in X$ à partir d'une certaine mesure, définie par un ensemble d'opérateurs de mesure $\mathcal{M}_x = \{M_x\}_{x\in X}$, appliquée sur $\rho \in \mathrm{D}(\mathcal{X})$. Si on appelle *probabilité de succès* la probabilité d'identifier x, noté $p_{succ}^{\mathcal{M}_X}(S)$ pour une mesure $\mathcal{M}_X$ et une source S, alors on peut écrire le problème sous forme d'optimisation de la manière suivante :

$$p_{succ}^{opt}(S) = \max_{\mathcal{M}_X \in \mathrm{POVM}(\mathcal{X})} \left\{ p_{succ}^{\mathcal{M}_X}(S) \right\} \ ,$$

où

$$
\begin{aligned}
p_{succ}^{\mathcal{M}_X}(S) &= \sum_{x \in X} p_x \Pr\big(\text{ obtenir le résultat } x \,|\, \text{l'état est } |\psi_x\rangle\,\big) \\
&= \sum_{x \in X} p_x \,\mathrm{tr}\{M_x |\psi_x\rangle\langle\psi_x|\} \quad .
\end{aligned}
$$

Le problème d'identification est donc celui de trouver une mesure satisfaisant $p_{succ}^{opt}(S)$, mais nous nous intéressons aussi à trouver une borne supérieure aussi petite que possible sur cette quantité.

Il n'existe pas de méthode analytique connue pour résoudre le problème et plusieurs stratégies ont été utilisées de manière ingénieuse dans la littérature afin d'obtenir des bornes inférieures et supérieures intéressantes sur cette probabilité [42] [30]. Nous connaissons des conditions suffisantes pour qu'une telle mesure soit satisfaite, mais nous ignorons comment la trouver excepté dans certains cas particuliers [19] [47]. Il existe aussi d'autres stratégies, par exemple si l'on permet à Bob de s'abstenir de répondre lorsqu'il est incertain ou bien de minimiser l'erreur au sens des moindres carrés [15], [34]. Nous verrons cette dernière plus en profondeur ainsi que son lien avec la formulation donné ci-haut.

Définition 3.1.3. On dit d'une source S quelle est τ-décorrélée si, pour toute paire d'états produits par la source, le produit scalaire au carré des états est constant et égal à τ.

Plus précisément, une source S qui produit l'ensemble $E_X = \{(p_x, |\psi_x\rangle)\}_{x \in X}$ est τ-décorrélée si $\forall\, x \neq x'$,

$$
|\langle\psi_x|\psi_{x'}\rangle|^2 = \tau \quad .
$$

Un cas particulièrement intéressant que nous verrons plus en détail est lorsque $\tau = \frac{1}{d}$ et $\#X = d$ où d est la dimension de l'espace.

3.2 Source uniforme maximalement décorrélée

La source que nous définissons ici est un cas particulier d'une source $\frac{1}{d}$-décorrélée où les états produits sont pris dans un ensemble de bases mutuellement non biaisées.

Définition 3.2.1. Soit $A = \{1, \ldots, 2^n\}$ et $c : A \to \{0,1\}^n$ une fonction arbitraire qui à a, associe $c(a)$. Alors une *source maximalement décorrélée* $\mathcal{S}_c$ déterminée par c est définie comme un *ensemble* $\mathcal{E}_c = \{(2^{-n}, |c(a)\rangle\}_{a\in A}$ qui produit des états quantiques $|c(a)\rangle$ de n qubits pris chacun dans une base d'indice a d'un ensemble $\mathcal{B} = \{B_a\}_{a\in A}$ de 2^n bases mutuellement non biaisés avec probabilité uniforme.

Cette source définit donc un opérateur de densité :

$$\rho_c \;=\; \frac{1}{2^n}\sum_{a\in A} |c(a)\rangle\langle c(a)| \;\; .$$

La fonction c qui à une base $B_a \in \mathcal{B}$ associe l'élément $|c(a)\rangle \in B_a$ est appelée *fonction défi*, est sous le contrôle de la source et connue de Bob. De cette manière, chaque base est représentée par un seul élément et nous disons de cette source qu'elle est maximalement décorrélée premièrement parce qu'une mesure qui détermine parfaitement un état dans l'une de ces bases est parfaitement décorrélée avec toute mesure effectuée dans n'importe quelle autre base de $\mathcal{B}$, puis deuxièmement parce qu'elle choisit les bases parmi l'ensemble avec probabilité uniforme.

Dans ce mémoire, on s'intéresse à une distribution de probabilité uniforme sur les bases, mais les résultats pour des probabilités $p(a)$ se généralisent à une distribution quelconque. On laisse de plus la fonction c complètement arbitraire, mais connue publiquement, sous le contrôle de la source, afin de trouver des résultats aussi généraux que possible.

Exemple 3.2.1. Un exemple classique d'une telle source est le suivant. Soit une source S_0 qui produit avec probabilité $\frac{1}{2}$ l'état $|0\rangle$ ou bien l'état $|+\rangle$. Il est facile de montrer que la meilleure mesure pour distinguer ces états donne $p_{succ}^{opt}(S) = \cos^2(\frac{\pi}{8})$.

Nous voyons dans la section suivante en quoi une telle source est utile. Nous présentons un protocole de preuve de connaissance à témoins dont la preuve de sécurité en dépend.

CHAPITRE 4

APPLICATION CRYPTOGRAPHIQUE D'UNE SOURCE QUANTIQUE MAXIMALEMENT DÉCORRÉLÉE

Les sources maximalement décorrélées étant intimement liées aux bases mutuellement non biaisées peuvent servir dans plusieurs applications. Un exemple bien connu est la capacité à distinguer les états $|0\rangle$ et $|+\rangle$ ou encore $|1\rangle$ et $|-\rangle$ dans le protocole de distribution de clé BB84 [6].

Nous montrons ici une application nouvelle d'une telle source comme élément principal de la sécurité d'un protocole qui permet d'instancier l'heuristique de Fiat-Shamir pour un Σ-protocole arbitraire. Nous présentons d'abord de manière informelle la notion de protocole de preuve de connaissance à divulgation nulle, puis nous donnons la définition d'un Σ-protocole qui en est une famille. Nous montrons ensuite les grandes lignes de l'argument ainsi que l'idée de la preuve.

Définition 4.0.1. Soient Peggy (P) et Victor (V) deux entitées, on dira que Peggy est le prouveur et Victor le vérificateur. L'objectif de Peggy est de prouver mathématiquement à Victor qu'elle connaît un secret en ne révélant aucune autre information que la connaissance de ce secret. Nous appellons de tels protocoles preuves de connaissance à divulgation nulles.

4.1 Σ-Protocoles

Définition 4.1.1. Un Σ-protocole est un protocole de preuve de connaissance en 3 messages. Plus spécifiquement, soit R une relation binaire, c.-à-d. $R \subset \{0,1\}^* \times \{0,1\}^*$ tel que si $(x, w) \in R$, alors $|x|$ est borné supérieurement par un polynôme en $|w|$. On a

traditionnellement que si $(x, w) \in R$, alors x est une instance d'un problème calculatoire et w est une solution à x. On dit que w est un *témoin* de x, c'est le secret que connaît P.

Les Σ-protocoles doivent posséder les propriétés suivantes :

Complétude : si P et V suivent le protocole correctement et que P connaît w, V accepte toujours.

Intégrité : Si P ne connaît pas w, alors V accepte avec probabilité $p < \frac{1}{2}$.

Intégrité spéciale : pour tout x et toute paire de conversations acceptantes (a, c, z) et (a, c', z') où $c \neq c'$, on peut calculer efficacement w tel que $(x, w) \in R$.

De la propriété d'intégrité spéciale, nous pouvons aisément déduire la propriété suivante :

Définition 4.1.2 (intégrité spéciale faible)**.** Pour tout x qui n'est pas une instance valide et tout premier message a, il existe au plus un défi c tel que V accepte la conversation.

Nous prendrons cette version affaiblie de l'intégrité spéciale pour la suite.

Alors un Σ protocole est de la forme suivante :

Protocole 1 : Σ-protocole

1. Soit $(x, w) \in R$, Peggy connaît (x, w) et Victor ne connaît que x.
2. P envoie un message a ;
3. V envoie une chaîne aléatoire $c \in \{0, 1\}^n$;
4. P répond $z(a, c)$ et V accepte ou refuse étant donné (x, a, c, z) ;

L'heuristique de Fiat-Shamir se donne comme objectif de transformer n'importe quel Σ-protocole en un protocole non interactif où un seul message de P à V suffit [12]. La

sécurité de cette heuristique a été montrée par Pointcheval et Stern [35] et ne fonctionne que dans le modèle de l'oracle aléatoire. Un oracle aléatoire est une fonction boîte noire H qui, lorsqu'on lui donne pour la première fois en entrée x, répond de manière parfaitement aléatoire $H(x) \in_R \{0,1\}^n$. La fonction redonne exactement la même réponse pour toute requête subséquente identique.

Définition 4.1.3. L'Heuristique de Fiat-Shamir pour un Σ-protocole fonctionne comme suit :

Protocole 2 : Fiat-Shamir pour un Σ-protocole

1 Soit $(x, w) \in R$, Peggy connaît (x, w) et Victor ne connaît que x.
2 P choisi a et demande à l'oracle $c = H(a)$;
3 P envoie $(a, c, z(a, c))$;
4 V vérifie que $c = H(a)$ et accepte ou refuse étant donné (x, a, c, z) ;

Cette heuristique dépend de l'existence d'un oracle aléatoire, mais Goldwasser et Kalai ont montré que n'importe quelle instanciation de l'oracle aléatoire par une fonction de hachage cryptographique ne satisfait à aucune des preuves de sécurité acceptées [14]. Il n'existe aucune preuve de sécurité, même calculatoire, d'un protocole de connaissance non interactif. Nous donnons dans ce mémoire des indications qui laissent croire qu'il est possible de réaliser cette tâche grâce à des ressources quantiques.

4.2 Instanciation de l'heuristique avec ressources quantiques

Notre objectif est de réaliser une version pratiquement non-intéractive de n'importe quel Σ-protocole avec l'intégrité spéciale faible. La seule intéraction supposée est l'échange préalable d'intrication quantique. Soit $\mathcal{B}$ un ensemble de 2^n bases mutuellement non biaisées

Protocole 3 : Fiat-Shamir pour un Σ-protocole

1 Soit $(x, w) \in R$, Peggy connaît (x, w) et Victor ne connaît que x. P et V partagent n paires EPR, c'est-à-dire un état biparti $\rho^{PV} = |\Psi^-\rangle\langle\Psi^-|^{\otimes n}$;

2 P choisit de manière aléatoire un indice $a \in \{0,1\}^n$ auquel est associé une base $B_a \in \mathcal{B}$;

3 Elle mesure sa partie des paires EPR dans la base B_a, obtient le résultat $|c_a\rangle$, $a \in \{0,1\}^n$ avec probabilité uniforme ;

4 Elle envoie $(a, c_a, z(a, c_a))$ à V sur un canal classique ;

5 V vérifie que P dit vrai en mesurant sa partie des états dans la même base B_a et devrait obtenir $|\overline{c}_a\rangle$ avec probabilité 1 ;

Ici les paires EPR font office d'oracle aléatoire, premièrement parce que les résultats sont parfaitement corrélés entre P et V s'ils mesurent dans la même base, et deuxièmement parce que le résultat est parfaitement aléatoire pour une base donnée. P ne peut pas prédire c_a étant donné un choix de a. Pour tricher, un $\hat{P}$ malhonnête devrait être capable de choisir une fonction $c : A \to \{0,1\}^n$ qui associe à chaque a un élément $c(a)$ de son choix de manière à ce que V accepte la chaîne $(a, c(a), z(a, c(a)))$ avec une probabilité non négligeable. Nous montrons maintenant que cette tâche est équivalente à distinguer une source maximalement décorrélée.

Théorème 4.2.1. *La meilleure stratégie de $\hat{P}$ est de trouver un POVM Λ_a pour distinguer un ensemble $\mathcal{E} = \left\{(|c(a)\rangle\langle c(a)|, 2^{-n})\right\}_{a\in A}$ d'états dans des bases mutuellement non biaisées, c'est-à-dire une source maximalement décorrélée.*

Démonstration. Soient $n \in \mathbb{N}$ et $\rho^{PV} = |\Psi^-\rangle\langle\Psi^-|^{\otimes n}$, $\{B_a\}_{a\in A}$ un ensemble de bases mutuellement non biaisées de $\mathcal{H}_n$ indicé par $a \in A$ et tel que $\forall\, a$, $B_a = \{|x_a\rangle\}_{x\in\{0,1\}^n}$. On note Λ_a le POVM utilisé par le prouveur malhonnête $\hat{P}$ pour mesurer ρ^P. La tâche de $\hat{P}$ est de faire mesurer $|c(a)\rangle\langle c(a)|$ pour un a quelconque selon une fonction c de son

choix. On peut donc assumer que si $\hat{P}$ réussi, c'est que V a bien mesuré un tel état.

$$
\begin{aligned}
p_{succ} &= \Pr(\text{ P trouve } (a, c(a)) \text{ tel que V accepte }) \\
&= \sum_a \mathrm{tr}\left\{(\Lambda_a^P \otimes |c(a)\rangle\langle c(a)|^V)\rho^{PV}\right\} \\
&= \sum_a \mathrm{tr}\left\{(\Lambda_a^P \otimes \mathbb{1}^V)(\mathbb{1}^P \otimes |c(a)\rangle\langle c(a)|^V)\rho^{PV}\right\} \\
&= \sum_a \mathrm{tr}\left\{(\sqrt{\Lambda_a}^P \otimes \mathbb{1}^V)(\mathbb{1}^P \otimes |c(a)\rangle\langle c(a)|^V)(\sqrt{\Lambda_a}^P \otimes \mathbb{1}^V)(\mathbb{1}^P \otimes |c(a)\rangle\langle c(a)|^V)\rho^{PV}\right\} \\
&= \sum_a \mathrm{tr}\left\{(\sqrt{\Lambda_a}^P \otimes \mathbb{1}^V)(\mathbb{1}^P \otimes |c(a)\rangle\langle c(a)|^V)\rho^{PV}(\sqrt{\Lambda_a}^P \otimes \mathbb{1}^V)(\mathbb{1}^P \otimes |c(a)\rangle\langle c(a)|^V)\right\} \\
&= 2^{-n}\sum_a \mathrm{tr}_P\left\{\sqrt{\Lambda_a}^P |c(a)\rangle\langle c(a)|_a^P \sqrt{\Lambda_{a,c}}^P\right\} \\
&= 2^{-n}\sum_a \mathrm{tr}_P\left\{\Lambda_a^P |c(a)\rangle\langle c(a)|^P\right\}
\end{aligned}
$$

La deuxième égalité est obtenue car on suppose que $\forall a$, V obtient $|c(a)\rangle\langle c(a)|$. La quatrième égalité est vraie car Λ_a^P est un opérateur positif, donc sa racine carrée positive existe. La cinquième égalité est vrai par cyclicité de la trace, l'égalité suivante s'obtient en prenant la trace partielle sur V car l'état ρ^{PV} est un état de Bell et la dernière avec la cyclicité de la trace encore une fois.

Ainsi, on voit que la tâche de $\hat{P}$ malhonnête se réduit à distinguer un ensemble d'états $\{|c(a)\rangle\langle c(a)|\}_{a\in\{0,1\}^n}$ pris avec probabilité uniforme selon une fonction c de son choix.

□

Une borne supérieure sur cette probabilité peut donc nous donner une preuve de sécurité pour cette variante de l'heuristique de Fiat-Shamir quantique. L'idéal serait de montrer que la probabilité est bornée supérieurement par une constante strictement inférieure à 1, car nous pourrions répéter le protocole afin d'amplifier cette probabilité. Nous avons

trouvé des indications qu'il existe une telle borne, mais nous n'avons pas réussi à prouver le résultat. Ce sont ces indications qui constituent le reste du travail.

CHAPITRE 5

IDENTIFICATION D'UNE SOURCE MAXIMALEMENT DÉCORRÉLÉE

Dans ce chapitre, nous prenons tout d'abord les lunettes de la théorie de l'information en regardant ρ comme un substrat d'information. Cette approche assez subtile peut nous en apprendre beaucoup sur la capacité à distinguer l'état. Le résultat, bien que surprenant, nous donne des indices sur la non-trivialité du problème. La deuxième partie, traitant d'optimisation convexe, nous donne une méthode *ad hoc* afin d'obtenir la mesure optimale pour une source en particulier (c.-à-d. un choix particulier de fonction défi $\mathcal{C}$). Cette méthode est malheureusement inefficace calculatoirement pour de grandes dimensions. Nous l'utilisons pour obtenir des résultats numériques pour $2, 4$ et 8 qubits puis nous obtenons une condition générale d'optimalité utile théoriquement. La troisième partie nous invite à considérer une stratégie différente qui consiste en la construction d'une mesure, généralement sub optimale, mais minimisant l'erreur d'identification au sens des moindres carrés. Nous comparons finalement les résultats numériques obtenus pour l'entropie, la mesure optimale et la mesure des moindres carrés.

5.1 Caractérisation d'une source en termes d'information

L'*entropie de Von Neumann* [32] caractérise la capacité d'un ensemble d'états à contenir de l'information classique et cette capacité est elle-même une manifestation de la distinguabilité de la source qui le produit [24]. Pour plus de détails sur la théorie de l'information quantique, voir [33] et [45].

5.1.1 Entropie de Von Neumann et information quantique

Si une source produit un état mixte dans une base orthogonale connue, on peut l'identifier parfaitement ; on est dans un régime classique et l'information de la source est directement proportionnelle à la distribution de probabilité de la préparation de l'état mixte. Si par contre la base n'est pas orthogonale, il existe un chevauchement des états en superposition au sens du produit scalaire et un état peut se faire passer pour un autre. En perdant la capacité à distinguer, on perd la capacité à retrouver l'information encodée dans l'état.

Définition 5.1.1. Soit $\rho \in \mathcal{H}$ un état quantique, on appelle *entropie de Von Neumann* la quantité

$$S(\rho) := -\operatorname{tr}(\rho \lg \rho) \ .$$

On peut voir que si $\{\lambda_i\}$ est l'ensemble des valeurs propres de ρ, alors

$$S(\rho) = -\sum_i \lambda_i \lg \lambda_i$$

est équivalent à l'entropie de Shannon.

On interprète cette quantité comme étant le minimum sur l'incertitude quant au résultat d'une mesure projective de l'état ρ [45].

Deux cas particuliers d'entropie de Von Neumann pour un état quantique sont les extrêmes du spectre entropique, c'est-à-dire lorsque $S(\rho) = 0$ ou $S(\rho) = n$. Premièrement, $S(\rho) = 0$ implique que l'état est parfaitement déterminé, sans aucune incertitude sur la source ; sans perte de généralité, on a que $S(\rho) = H(1, 0, \ldots, 0)$. L'état est pur et parfaitement distinguable. À l'autre extrême, si $S(\rho) = n$, alors en examinant la décomposition spectrale (donc orthogonale), cela implique une distribution uniforme des valeurs propres $S(\rho) = H(\frac{1}{n}, \ldots, \frac{1}{n})$. L'état peut être distingué parfaitement en mesu-

rant dans la base des vecteurs propres et est donc considéré classique et uniformément distribué. Les phénomènes quantiques intéressants apparaissent donc lorsque les états ne sont pas orthogonaux et ainsi $0 < S(\rho) < n$.

5.1.2 Entropie de Rényi quantique

Ici nous formalisons une relation importante entre l'entropie et la distinguabilité d'un état grâce à la caractérisation opérationnelle de la min-entropie. Nous utilisons à cette fin l'entropie de Rényi quantique.

L'entropie de Von Neumann, à l'instar de l'entropie de Shannon, n'est qu'un cas particulier de ce qu'on appelle l'*entropie de Rényi d'ordre* α [36] dans sa version quantique :

$$S_\alpha(\rho) = \frac{1}{1-\alpha} \log \mathrm{tr}(\rho^\alpha) \ .$$

Cette mesure, comme sa version classique, est paramétrée par $\alpha \in [0, 1) \cup (1, \infty)$ et est une fonction décroissante en α.

Bien qu'on ne puisse pas connaître l'entropie de Von Neumann pour toute source maximalement décorrélée, il se trouve qu'on peut la borner par l'entropie de Rényi d'ordre 2 qui elle est facile à calculer car elle n'utilise que les produits scalaires au carré entre les états produits par la source.

$$
\begin{aligned}
\rho^2 &= 2^{-2n}\left(\sum_a |c(a)\rangle\langle c(a)|\right)\left(\sum_{a'} |c(a')\rangle\langle c(a')|\right) \\
&= \left(\sum_{a=a'} |c(a)\rangle\langle c(a)| + \sum_{a\neq a'} |c(a)\rangle\langle c(a)||c(a')\rangle\langle c(a')|\right) \\
\operatorname{tr}\rho^2 &= 2^{-2n}(2^n + 2^n(2^n-1)2^{-n}) \\
&= 2^{1-n} - 2^{-2n} \ .
\end{aligned}
$$

Donc

$$
\begin{aligned}
S_2(\rho) &= -\log(\operatorname{tr}(\rho^2)) \\
&= -\log(2^{1-n} - 2^{-2n}) \\
&= -\log(2^{1-n}(1 - 2^{-n-1})) \\
&= n - 1 - \log(1 - 2^{-n-1})
\end{aligned}
$$

On peut ainsi en déduire que

$$
S(\rho) \geq n - 1 - \log(1 - 2^{-n-1})
$$

avec $\log(1 - 2^{-n-1})$ qui tend vers 0 lorsque $n \to \infty$.

De cette borne inférieure sur l'entropie de Von Neumann, on peut directement déduire une borne inférieure sur la capacité d'identification de la source grâce au théorème suivant :

Théorème 5.1.1. *Soit $S(\rho) = n - \varepsilon(n)$ pour un opérateur de densité $\rho = \frac{1}{2^n}\sum_{i=1}^{2^n} |\psi_i\rangle\langle\psi_i|$*

représentant une source S. Alors

$$p_{succ}^{opt}(S) \geq 2^{-\varepsilon(n)} \ .$$

Démonstration. Une manière équivalente de représenter la source S avec ensemble $E_X = \{(p_x, |\psi_x\rangle)\}_{x \in X}$ est en utilisant un état biparti

$$\rho_{XB} = \frac{1}{2^n} \sum_{i=1}^{2^n} |i\rangle\langle i|_X \otimes |\psi_i\rangle\langle\psi_i|_B \ ,$$

avec $\{|i\rangle\}$ une base orthogonale de $\mathcal{H}_n$. De cette manière, on peut écrire l'entropie conditionnelle de la variable classique X étant donné l'accès au système quantique B par l'opérateur de densité $\rho_B = \frac{1}{2^n} \sum_{i=1}^{2^n} |\psi_i\rangle\langle\psi_i|$:

$$S(X|B) = S(XB) - S(B) \ .$$

Dans [28], les auteurs montrent que l'entropie de Rényie conditionnelle d'ordre $\alpha \to \infty$, la min-entropie conditionnelle, est directement reliée à la mesure optimale :

$$p_{succ}^{opt}(S) = 2^{-S_\infty(X|B)} \ .$$

Il a aussi été montré [41] que

$$S_\infty(X|B) \leq S(X|B) \ .$$

En combinant les deux résultats, on a que

$$p_{succ}^{opt}(S) \geq 2^{-S(X|B)} \ ,$$

dont la partie de droite est facile à calculer, l'état ρ_{XB} étant un état classique-quantique.

$$\begin{aligned} S(X|B) &= S(XB) - S(B) \\ &= S(X) + 2^{-n} \sum_i S(|\psi_i\rangle\langle\psi_i|) - S(B) \\ &= n - (n - \varepsilon(n)) \\ &= \varepsilon(n) \ . \end{aligned}$$

Ce qui complète la preuve.

□

On peut ainsi en déduire que toute source $\frac{1}{2^n}$-décorrélée peut être distinguée avec probabilité au moins aussi grande que $\frac{1}{2^{1+\log(1-2^{-n-1})}}$. C'est une quantité monotone croissante et bornée supérieurement par $\frac{1}{2}$. On a donc que

$$\lim_{n\to\infty} \frac{1}{2^{1+\log(1-2^{-n-1})}} = \frac{1}{2} \ .$$

5.1.3 Identification d'une source $\frac{1}{2^n}$-décorrélée avec phases relatives constantes

Le but de cette section est de montrer les limites du lien entre le chevauchement deux à deux des états et la distinguabilité globale de la source. *Jozsa* et *Schlienz* [24] ont

précisément étudié ce problème pour montrer que l'entropie de Von Neumann est en fait une propriété globale des états (ou de l'opérateur de densité) et non pas une fonction des chevauchements individuels des paires d'états de la source. On peut effectivement voir grâce à un exemple simple que si l'on ne considère que le produit scalaire constant entre les états, alors il est possible de trouver une mesure projective qui distingue la source avec probabilité exponentiellement près de 1.

Exemple 5.1.1. Soit une base orthonormale $\{|v_i\rangle\}_{i=1,\ldots,2^n}$ et soit $|\hat{v}\rangle = |v_{2^n}\rangle$. Alors nous construisons un ensemble de $2^n - 1$ états $|\gamma_j\rangle = \alpha|\hat{v}\rangle + \beta|v_j\rangle$ de manière à ce que $\langle\gamma_j|\gamma_k\rangle = 2^{-\frac{n}{2}}$. Un calcul direct montre que $\alpha = 2^{-\frac{n}{4}}$ et $\beta = \sqrt{1 - 2^{-\frac{n}{2}}}$ donnent un tel état. Cette source, bien qu'elle possède la propriété d'être $\frac{1}{2^n}$-décorrélée, n'est pas maximalement décorrélée car les états ne sont pas pris dans un ensemble de bases mutuellement non-biaisées.

En choisissant la mesure projective $\Pi_i = |v_i\rangle\langle v_i|$, on obtient que

$$\begin{aligned} p_{succ}^{\Pi} &= \frac{1}{2^n - 1} \sum_{i=1}^{2^n-1} \mathrm{tr}\{|\gamma_i\rangle\langle\gamma_i||v_i\rangle\langle v_i|\} \\ &= \frac{1}{2^n - 1} \sum_{i=1}^{2^n-1} |\beta|^2 |\langle v_i|v_i\rangle|^2 \\ &= \frac{1}{2^n - 1} \sum_{i=1}^{2^n-1} (1 - 2^{-\frac{n}{2}}) \\ &= \left(1 - 2^{-\frac{n}{2}}\right) \quad . \end{aligned}$$

Ceci indique qu'un tel état est asymptotiquement distinguable. Bien sûr, cette source produit un état de moins qu'une source maximalement décorrélée, ce qui est négligeable lorsque n augmente. Nous pourrions tout aussi bien considérer une dimension supplé-

mentaire pour la mesure afin d'avoir $|\hat{v}\rangle$ orthogonal avec 2^n autres états et construire ainsi une source produisant 2^n états purs. Cet exemple montre que le produit scalaire constant entre les états n'est pas une caractéristique suffisante pour trouver une borne supérieure assez petite sur la probabilité de succès. Nous verrons plus bas que les observations numériques sur des sources maximalement décorrélées indiquent que cette probabilité ne tend non seulement pas vers 1, mais en plus qu'elle décroît lorsque n augmente.

Nous avons beaucoup de difficulté à obtenir des résultats analytiques satisfaisants sur la probabilité optimale de distinguer bien que les simulations numériques nous aident beaucoup. Il semble, comme nous l'avons vu plus haut, qu'une des raisons soit que les phases jouent un rôle très important dans la détermination des états et qu'on ne puisse pas les ignorer. Ceci indique que l'analyse se complexifie lorsqu'on considère la construction explicite, car lorsque l'on prend un ensemble de bases complet, il y a nécessairement une forme d'interférence entre les phases relatives des différents états choisis.

5.2 Optimisation convexe et mesure optimale

L'objectif de cette section est double ; on présente d'une part la théorie de l'optimisation semi-définie qui ammène à trouver numériquement la mesure optimisant la probabilité d'identification de manière itérative pour un ensemble d'états donné en temps polynomial, puis ensuite un volet théorique où l'on montre une condition nécessaire et suffisante qu'une mesure particulière doit remplir afin qu'elle soit optimale pour un ensemble donné. La présentation est inspirée des notes de cours de John Watrous [43] ainsi que [11]. Les preuves des résultats peuvent être retrouvées dans ces références.

5.2.1 Trouver la mesure optimale

Nous restreignons la formulation de programmation semi-définie (PSD) à la théorie de l'information quantique. Une bonne source pour la compréhension générale de l'optimisation convexe dont la PSD est le livre de Boyd et Vanderberghe [7].

Définition 5.2.1. Un *programme semi-défini* est un triplet $PSD = (\Phi, A, B)$ où :

- Φ est un super-opérateur de $\mathcal{X}$ vers $\mathcal{Y}$ qui préserve l'hermicité, et
- $A \in \mathrm{Her}\,\mathcal{X}$ et $B \in \mathrm{Her}\,\mathcal{Y}$

On associe à PSD deux problèmes d'optimisation qu'on appelle *primal/dual*.

Primal

Maximiser $\langle A, X\rangle$

Sujet à : $\Phi(X) = B$

$X \in \mathrm{Pos}\,\mathcal{X}$

Dual

Minimiser $\langle B, Y\rangle$

Sujet à : $\Phi^*(Y) \geq A$

$Y \in \mathrm{Her}\,\mathcal{Y}$

Où Φ^* est l'opérateur adjoint au sens du produit scalaire de Hilbert-Schmidt. C'est-à-dire que $\forall\, X \in \mathcal{X},\ Y \in \mathcal{Y}$,

$$\langle \Phi(X), Y \rangle = \langle X, \Phi^*(Y) \rangle \ .$$

On esquisse quelques résultats, sans preuve, sur l'optimalité et la dualité. Soit les ensembles suivants :

$$\begin{aligned} \mathcal{A} &= \{X \in \mathrm{Pos}\,\mathcal{X} | \Phi(X) \leq B\} \ , \\ \mathcal{B} &= \{Y \in \mathrm{Her}\,Y | \Phi^*(Y) \geq A\} \ . \end{aligned}$$

Si $X \in \mathcal{A}$ on dit que X est primal-atteignable, si $Y \in \mathcal{B}$, alors Y est dual-atteignable. Soit aussi les deux optima suivants :

$$\begin{aligned} a &= \sup_{X \in \mathcal{A}} \langle A, X \rangle \ , \text{ et} \\ b &= \inf_{Y \in \mathcal{B}} \langle B, Y \rangle \ . \end{aligned}$$

On nomme la relation $a \leq b$ dualité faible. Le résultat suivant est facile à prouver avec les propriétés du produit scalaire.

Théorème 5.2.1 (Dualité faible)**.** *Pour tout PSD, on a que* $a \leq b$

De plus, la relation $a = b$ est appelée dualité forte. Le résultat suivant nous permettra de prouver l'optimalité du POVM.

Théorème 5.2.2. *(Slater)[40] Pour tout programme semi-défini, nous avons les résultats suivants :*

1. *Si $\mathcal{A} \neq \emptyset$ et s'il existe un opérateur Hermitien Y tel que $\Phi^*(Y) \geq a$, alors $a = b$ et il existe un opérateur $X \in \mathcal{A}$ pour lequel $\langle A, X \rangle = a$.*

2. *Si $\mathcal{B} \neq \emptyset$ et s'il existe un opérateur positif semi-défini X tel que $\Phi(X) = B$ et $X > 0$, alors $a = b$ et il existe un opérateur $Y \in \mathcal{B}$ pour lequel $\langle B, Y \rangle = b$.*

L'intérêt majeur de ce formalisme est qu'il nous donne une méthode ad hoc pour obtenir une mesure optimale. Comme les conditions du théorème de dualité de Slater sont essentiellement toujours satisfaites pour des états quantiques [11], on sait qu'une mesure optimale unique peut être trouvée. Nous connaissons des algorithmes itératifs de points intérieurs qui nous donnent avec grande précision cette mesure en temps polynomial pour un ensemble donné d'états [1] [31]. Nous présentons plus bas un ensemble de résultats de simulations numériques de sources maximalement décorrélées et les probabilités de succès optimales obtenues grâce à ce formalisme.

5.2.2 Montrer qu'une mesure est optimale

Le théorème suivant, montré d'abord par [21] puis par [47] et [18], est maintenant devenu un exemple introductif classique d'application des PSD lorsqu'ils sont présentés en théorie de l'information quantique et donne une condition nécessaire et suffisante pour qu'une mesure donnée soit une mesure optimale pour ensemble d'états. La présentation ici est inspirée de [11].

On utilise l'optimisation en PSD pour formuler un couple primal/dual. Soit $\mathcal{H} = \mathcal{A} \otimes \mathcal{X}$ où $\mathcal{A}$ est l'espace de Hilbert $\mathcal{H}_n$ et $\mathcal{X}$ est un espace euclidien de dimension 2^n.

Primal

Maximiser $\langle A, X \rangle$

Sujet à : $\Phi(X) = B$

$$X \in \mathrm{Pos}\,\mathcal{H} \ .$$

Avec

$$A = 2^{-n} \begin{pmatrix} |c(1)\rangle\langle c(1)| & 0 & \dots & 0 \\ 0 & |c(2)\rangle\langle c(2)| & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & |c(2^n)\rangle\langle c(2^n)| \end{pmatrix} ,$$

$$X = \begin{pmatrix} \Lambda_1 & 0 & \dots & 0 \\ 0 & \Lambda_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & \Lambda_{2^n} \end{pmatrix} .$$

On choisit :

$$\Phi(X) = \mathrm{tr}_{\mathcal{X}}\, X = \sum_a \Lambda_a = \mathbb{1}_n \ .$$

Donc $B = \mathbb{1}_n$ et $X \in \mathrm{Pos}\,\mathcal{H}$ définissent une mesure.

On a donc tout ce qu'il faut pour définir le dual :

Dual

Minimiser $\langle B, Y \rangle$

Sujet à : $\Phi^*(Y) \geq A$

$$Y \in \mathrm{Her}\,\mathcal{A} \ .$$

On peut montrer que

$$\Phi^*(Y) = \mathbb{1}_n \otimes Y \geq A \iff \forall a, Y \geq 2^{-n}|c(a)\rangle\langle c(a)| \ .$$

De là, le théorème d'Holevo sur l'optimalité d'une mesure sur ρ :

Théorème 5.2.3. *la mesure $\mathcal{M}$ est optimale pour l'ensemble $\varepsilon = \{(2^{-n}, |c(a)\rangle\langle c(a)|)\}_a$ si et seulement si*

$$\sum_{i=1}^{2^n} |c(i)\rangle\langle c(i)| M_i \geq |c(j)\rangle\langle c(j)|, \ \ \forall j \in \{0,1\}^n \ .$$

Bien qu'il soit très difficile de trouver une telle mesure et de montrer son optimalité de manière analytique, on peut utiliser ces techniques pour trouver numériquement la mesure optimale pour des cas particuliers. Nous avons obtenu les résultats suivants pour la mesure optimale grâce à une librairie d'optimisation convexe et un logiciel de calcul numérique. Une recherche exhaustive a été faite pour 2 qubits, et une génération d'états aléatoires a été faite avec plusieurs milliers d'itérations pour 4 qubits. Nous affichons la moyenne de la probabilité d'identification ainsi que la variance. Nous reprenons ces résultats à la section 4.4 afin de les comparer à ceux obtenus grâce à la méthode de la section suivante.

Nombre de qubits	2	4
p_{succ}^{opt}	$0,7784$	$0,7334$
Variance	$0,92377 \times 10^{-5}$	$0,11408 \times 10^{-6}$

5.2.3 Piste de solution incomplète

La démarche de la section précédente nous donne en fait une méthode alternative de borner supérieurement la probabilité optimale d'identification. En effet, par la dualité

faible, nous avons que

$$p_{succ}^{opt} = \max_X \langle A, X \rangle \leq \langle B, Y \rangle = \operatorname{tr} Y$$

pour n'importe quel Y dual-atteignable. C'est-à-dire que si l'on pouvait trouver un Y tel que $\forall\, a$,

$$Y \geq |c(a)\rangle\langle c(a)|$$

et que $\operatorname{tr} Y \leq 1 - \frac{1}{p(n)}$ pour un polynôme en n, alors ça suffirait pour prouver la sécurité du protocole. Nous n'avons pas réussi à trouver un tel Y. Une technique classique consiste à considérer la racine carré d'un opérateur car les états états purs, on a que $|c(a)\rangle\langle c(a)|^2 = |c(a)\rangle\langle c(a)|$. Dans le raisonnement qui suit nous avons tout multiplié par 2^n afin de simplifier les calculs.

Soit

$$Y = \sum_a |c(a)\rangle\langle c(a)| \ ,$$

alors clairement, $\forall a,\ Y \geq |c(a)\rangle\langle c(a)|$. Nous avons aussi que

$$\sqrt{Y} \geq \sqrt{|c(a)\rangle\langle c(a)|} = |c(a)\rangle\langle c(a)| \ .$$

On peut donc en déduire que

$$\operatorname{tr} \sqrt{\sum_a |c(a)\rangle\langle c(a)|} \geq 2^n p_{succ}^{opt} \ ,$$

Une borne supérieure non triviale sur $\mathrm{tr}\,\sqrt{Y}$ et indépendante du choix de fonction c nous donnerait ainsi une solution. Nous n'avons pas réussi à trouver une telle borne.

5.3 La mesure des moindres carrés

S'il ne nous est pas possible de trouver une forme explicite de la mesure d'identification optimale aussi facilement, tout n'est pas perdu. Il existe en effet d'autres critères pour une bonne mesure afin d'établir une stratégie et de contourner le problème. C'est ainsi qu'on considère une mesure projective astucieuse qui, à défaut de maximiser la probabilité de détection, minimisera la probabilité d'erreur au sens des moindres carrés. On appellera donc naturellement ce POVM *mesure des moindres carrés* (MMC).

Cette mesure fut originalement appelée «Pretty good measurement» dans [16] en 1994 puis «Square Root Measurement» dans [15] en 1996, [10] démontre en 2001 que les deux mesures concordent en fait avec une mesure plus générale, appelée la mesure des moindres carrés. Cette construction est devenue un résultat fondamental dans une foule d'applications.

Considérons un ensemble d'états purs linéairement indépendants $\{|\varphi_i\rangle\}_{i=1}^m$ de $\mathcal{H}$ tel que $m = \dim(\mathcal{H})$. On cherche une mesure $\{M_j\}_j = \{|\mu_j\rangle\langle\mu_j|\}_j$ qui minimise la somme des normes au carré des vecteurs d'erreurs $|e_i\rangle = |\varphi_i\rangle - |\mu_i\rangle$:

$$E = \sum_{i=1}^{m} \||e_i\rangle\|^2$$

avec $\||e_i\rangle\|^2 = \langle e_i|e_i\rangle$.

Nous montrons comment obtenir une telle mesure et présentons les conditions dans lesquelles elle est optimale. Nous considérons le cas où les états $|\varphi_i\rangle$ sont linéairement indépendants. Bien que ce ne soit pas le cas en général, nous n'avons trouvé aucune

combinaison de $|c(a)\rangle$ pour laquelle ce ne soit pas le cas pour $n = 2, 3, 4$ et 8 qubits. Ceci simplifiera beaucoup l'analyse. Nous formulons l'hypothèse suivante :

Hypothèse 5.3.1. *Les états produits par une source maximalement décorrélée sont toujours linéairement indépendants, peu importe la fonction défi $\mathcal{C}$.*

Théorème 5.3.2. *(Mesure des moindres carrés)[10] Soit $\Phi = \big(|\varphi_1\rangle \dots |\varphi_m\rangle\big)$ une matrice de plein rang dont les vecteurs colonnes sont les états $|\varphi_i\rangle$, alors les vecteurs $|\mu_i\rangle$ de la mesure qui minimisent le carré de l'erreur sont donnés par les colonnes de la matrice*

$$\hat{M} = (\Phi\Phi^*)^{-\frac{1}{2}}\Phi \ ,$$

qu'on peut réécrire de manière explicite $\hat{M} = (|\mu_1\rangle \dots |\mu_n\rangle)$ où :

$$|\mu_i\rangle\langle\mu_i| = \left(\sum_{j=1}^{m} |\varphi_j\rangle\langle\varphi_j|\right)^{-\frac{1}{2}} |\varphi_i\rangle\langle\varphi_i| \left(\sum_{j=1}^{m} |\varphi_k\rangle\langle\varphi_k|\right)^{-\frac{1}{2}} \ .$$

Ce théorème important est une conséquence de la décomposition en valeurs singulières, qui est une factorisation matricielle fondamentale :

Théorème 5.3.3. *(Décomposition en valeurs singulière) Soit $\Phi \in \mathcal{L}_{m,n}$, alors il existe $U \in \mathrm{U}(\mathcal{L}_n)$, $V \in \mathrm{U}(\mathcal{L}_m)$ et $\Sigma \in \mathcal{L}_{m,n}$ une matrice diagonale avec des éléments réels non nuls tels que*

$$\Phi = U\Sigma V^* \ .$$

Notons $\{|u_i\rangle\}_i$ les vecteurs colonnes de U et $\{|v_j\rangle\}_j$ les vecteurs colonnes de V. De plus, les éléments non nuls σ_i, $i \in \{1, \dots min(m, n)\}$, de la diagonale de Σ sont appelés valeurs singulières *de A.*

La *décomposition en valeurs singulières* (DVS) est plus générale que la décomposition spectrale car elle s'applique aussi aux opérateurs qui ne sont pas carrés. Elle y est toutefois intimement liée car :

$$\Phi\Phi^* = (U\Sigma V)(V^*\Sigma U^*) = U\Sigma^2 U^*$$

et

$$\Phi^*\Phi = (V^*\Sigma U^*)(U\Sigma V) = V^*\Sigma^2 V \ \ ,$$

qui sont respectivement les décompositions spectrales de $\Phi\Phi^*$ et $\Phi^*\Phi$.

Construisons donc la MMC à partir des colonnes de Φ.

On considère l'erreur E à minimiser qu'on peut réécrire de la manière suivante :

$$\begin{aligned} E &= \sum_{i=1}^{m} \langle e_i | e_i \rangle \\ &= \sum_{i=1}^{m} (\langle \varphi_i | - \langle \mu_i |)(|\varphi_i\rangle - |\mu_i\rangle) \\ &= \mathrm{tr}\{(\Phi - M)(\Phi - M)^*\} \\ &= \mathrm{tr}\{U^*(\Phi - M)(\Phi - M)^* U\} \ \ . \end{aligned}$$

Alors on peut réécrire

$$|\psi_i\rangle = (\Phi - M)^* |u_i\rangle \ \ .$$

Comme $\Phi^*|u_i\rangle = \sigma_i |v_i\rangle$ par la DVS de $\Phi^* = V\Sigma^* U^*$, on a que

$$|\psi_i\rangle = \sigma_i|v_i\rangle - M^*|u_i\rangle \ .$$

Puisqu'on veut toujours minimiser E, nous obtenons la forme suivante :

$$\begin{aligned} E &= \sum_{i=1}^{m} \langle\psi_i|\psi_i\rangle \\ &= \sum_{i=1}^{m} \left(\sigma_i^2 + 1 - \sigma_i \left(\langle v_i|M^*|u_i\rangle + \langle u_i|M|v_i\rangle\right)\right) \ , \end{aligned}$$

qui sera minimal lorsque la partie de droite sera maximisée, ce qui peut être atteint si

$$\begin{aligned} M^*|u_i\rangle &= |v_i\rangle \text{ et} \\ M|v_i\rangle &= |u_i\rangle \ , \end{aligned}$$

car $\sigma_i \geq 0$. Ainsi on obtient le M optimal, noté $\hat{M}$ construit comme

$$\begin{aligned} \hat{M} &= \sum_{i=1}^{m} |u_i\rangle\langle v_i| \\ &= UV^* \ . \end{aligned}$$

Notons qu'on peut écrire la matrice de mesure $\hat{M}$ à partir des états $|\varphi\rangle$:

$$\begin{aligned}\hat{M} &= ((\Phi\Phi^*))^{-\frac{1}{2}}\,\Phi \\ &= (U\Sigma^2U^*)^{-\frac{1}{2}}(U\Sigma V^*) \\ &= U\Sigma^{-1}U^*U\Sigma V^* \\ &= UV^*\end{aligned}$$

Dont les vecteurs colonnes de $\hat{M}$ sont

$$|\mu_i\rangle = \left(\sum_{j=1}^{m} |\varphi_j\rangle\langle\varphi_j|\right)^{-\frac{1}{2}} |\varphi_i\rangle \ .$$

Remarquons que Φ est inversible car nous avons fait l'hypothèse que les vecteurs sont linéairement indépendants et de nombre égal à la dimension. Si ce n'est pas le cas, le résultat tient encore en considérant une matrice *pseudo-inverse de Penrose* [10].

On obtient ainsi une forme fermée pour l'erreur qu'on a minimisée :

$$\begin{aligned}E_{\min} &= \sum_{i=1}^{m}(1-\sigma_i)^2 \\ &= 2n - 2\sum_{i=1}^{m}\sigma_i \ .\end{aligned}$$

Voyons maintenant quelques propriétés de cette mesure. Il importe de comprendre comment cette mesure se comporte par rapport à une mesure optimale. Nous avons des résultats numériques qui montrent que la MMC correspond à la mesure optimale pour tous

les cas que nous avons pu tester pour 2 et 4 qubits. Bien que nous n'ayons pas réussi à montrer l'optimalité de la MMC, nous avons le théorème suivant qui borne la probabilité d'identification maximale par rapport au résultat de la MMC et qui satisfait aux applications cryptographiques.

Théorème 5.3.4. *(Barnum-Knill)[4] Soit $E = \{(|\psi_i\rangle, p_i)\}_{i=1}^n$ un ensemble de n états, et soit $p_{succ}^{MMC}(\mathcal{E})$ et $p_{succ}^{opt}(E)$ la probabilité de distinguer E pour une mesure optimale et pour la MMC respectivement, alors*

$$\sqrt{p_{succ}^{MMC}(E)} \geq p_{succ}^{opt}(E) \ .$$

Démonstration. Soit $\mathcal{M} = \{|m_i\rangle\langle m_i|\}$ un ensemble d'opérateurs de mesure optimale. Alors on a :

$$\begin{aligned}
p_{succ}^{opt}(E) &= 2^{-n} \sum_i |\langle\psi_i|m_i\rangle|^2 \\
&= 2^{-n} \sum_i |\langle\psi_i|\rho^{-\frac{1}{4}}\rho^{\frac{1}{4}}|m_i\rangle|^2 \\
&\leq 2^{-n} \sum_i \left(\langle\psi_i|\rho^{-\frac{1}{2}}|\psi_i\rangle\right)\left(\langle m_i|\rho^{\frac{1}{2}}|m_i\rangle\right) \\
&\leq \sqrt{2^{-n}\left(\sum_i \left(\langle\psi_i|\rho^{-\frac{1}{2}}|\psi_i\rangle\right)\right)\underbrace{\left(\sum_j \left(\langle m_j|\rho^{\frac{1}{2}}|m_j\rangle\right)\right)}_{\leq 1}} \\
&\leq \sqrt{2^{-n}\left(\sum_i \langle\psi_i|\rho^{-\frac{1}{2}}|\psi_i\rangle\right)} \\
&= \sqrt{p_{succ}^{MMC}(E)}
\end{aligned}$$

□

On obtient aussi une borne inférieure intéressante sur la probabilité de distinguer de la MMC. Nous utilisons le lemme suivant, prouvé par Beigi et König [5], et que nous ne prouvons pas, mais qui nous permet d'obtenir la borne inférieure :

Lemme 5.3.5. *[5]*

Pour distinguer un ensemble $\{(\frac{1}{N}, \eta_i\}$ *d'états, la probabilité moyenne de succès de la* MMC *est :*

$$p_{succ}^{MMC} \geq \frac{1}{N\overline{r}\,\mathrm{tr}\{\overline{\eta}^2\}} \ ,$$

avec

$$\overline{r} = \frac{1}{N}\sum_{i=1}^{N} \mathrm{rang}(\eta_i) \textit{ et } \overline{\eta} = \frac{1}{N}\sum_{i=1}^{N} \eta_i \ .$$

Théorème 5.3.6. *On peut toujours distinguer les états produits par une source maximalement décorrélée avec probabilité plus grande que* $\frac{1}{2} + \varepsilon(n)$.

Démonstration. Soient

$$E_i = \left(\sum_a \sigma_a\right)^{-\frac{1}{2}} \sigma_i \left(\sum_{a'} \sigma_{a'}\right)^{-\frac{1}{2}} \ .$$

On considère la probabilité moyenne de succès :

$$p_{succ}^{MMC} = \frac{1}{2^n}\sum_a \mathrm{tr}\{E_i\sigma_i\} \ .$$

On peut donc appliquer directement le lemme énoncé précédemment ;

Soit $N = 2^n$, $\bar{\eta} = \frac{1}{2^n}\sum_a |c(a)\rangle\langle c(a)|$, $\bar{r} = 1$.

$$\bar{\eta}^2 = \frac{1}{2^{2n}} \left(\sum_{a=a'} |c(a)\rangle\langle c(a')| + \frac{1}{2^{n/2}} \sum_{a \neq a'} |c(a)\rangle\langle c(a')| \right) \quad ,$$

$$\begin{aligned} \mathrm{tr}\{\bar{\eta}^2\} &= \frac{1}{2^{2n}} \left(\sum_{a=a'} \mathrm{tr}\{\left|c(a)\rangle\langle c_(a')\right|\} + \frac{1}{2^{n/2}} \sum_{a \neq a'} \mathrm{tr}\{|c(a)\rangle\langle c(a')|\} \right) \\ &= \frac{1}{2^n} + \frac{2^n - 1}{2^{2n}} \\ &= \frac{2}{2^n} - \frac{1}{2^{2n}} \quad . \end{aligned}$$

Ainsi, on obtient

$$p_{succ}^{MMC} \geq \frac{1}{2^n \left(\frac{2}{2^n} - \frac{1}{2^{2n}} \right)} = \frac{1}{2 - \frac{1}{2^n}} \quad .$$

□

5.4 Simulation numérique d'une source maximalement décorrélée

Nous présentons ici la méthode que nous avons utilisée afin de construire numériquement des états qui sont produits par une source maximalement décorrélée ainsi que les limites de cette méthode. Nous présentons ensuite les résultats obtenus ainsi qu'une courte analyse de leur signification.

5.4.1 Génération des états

La méthode de construction des BMNB pour n qubits donnée dans le chapitre 2 est simple à comprendre, mais nous n'avons pas trouvé de méthode efficace pour générer les états de manière numérique. La méthode présentée ici est calculatoirement beaucoup

plus simple que cette dernière, bien que la preuve de correctitude soit plus complexe. L'idée est d'obtenir l'ensemble des états pour toutes les bases à partir d'une seule matrice unitaire en effectuant des opérations simples sur celle-ci. Nous disons d'un tel ensemble de bases qu'il est complet et cyclique. Bien que la méthode que nous décrivons ne fonctionne que pour un nombre de qubits qui est une puissance de 2, elle offre des avantages calculatoires qui ne sont pas négligeables. Pour plus détails voir [25].

L'objectif est de trouver une matrice unitaire U_n^1, pour n qubits, dont les colonnes sont tous les vecteurs d'une base B_1 prise dans un ensemble de BMNB $\mathcal{B} = \{B_i\}_{i=1}^{2^n+1}$ et telle que U_n^j donne de la même manière les vecteurs de la base j et $U_n^{2^n+1} = \mathbb{1}_n$. La construction de la matrice U_{2m}^1 se fait itérativement avec celle de U_m^1. Nous nommons cette matrice U_n^1 *matrice génératrice pour* n *qubits.*

Soit

$$V_1 = H \cdot \mathsf{diag}(1, -i) = \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix} \ ,$$

avec $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ ainsi que l'opérateur de vectorisation suivant :

$$\mathcal{M} : \mathcal{L}(\mathbb{C}^d) \to \mathbb{C}^{d^2} \ ,$$

qui, à une matrice $V = (v_{i,j})$ de dimension $d \times d$, associe un vecteur à d^2 composantes de la manière suivante :

$$\mathcal{M}(V) = \begin{pmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,d} & v_{2,1} & \dots & v_{d,d} \end{pmatrix} \ .$$

De cette manière, les auteurs de [25] montrent qu'on peut obtenir la matrice génératrice des bases :

$$U_m = -\frac{V_m}{\operatorname{tr} V_m} \quad \text{et} \quad V_{2m} = H^{\otimes 2m} \cdot \mathsf{diag}(\mathcal{M}(V_m)) \ .$$

Les vecteurs colonnes de cette matrice U_m forment une base orthonormée, et si $U_m = U_m^1$, en prennant les puissances successives de U_m^1 on obtient les autres bases. On peut ainsi facilement obtenir n'importe quel vecteur i de la base j pour k qubits en prenant la i-ème colonne de la matrice U_k^j.

5.4.2 Résultats numériques d'une mesure optimale, MMC et entropie

Nous donnons ici les résultats numériques obtenus pour le problème d'identification d'une source maximalement décorrélée. En utilisant la construction explicite des bases donnée ci-haut, on simule successivement une source pour $n = 1, 2, 4$ et 8 qubits et on obtient des valeurs pour la probabilité de succès de la MMC et la probabilité de détection optimale. Nous verrons que ces deux mesures semblent se confondre. Pour l'optimisation convexe, nous avons utilisé la librairie d'optimisation semi-définie CVX [9].

Pour 1 qubit, le résultat de la mesure optimale ($\cos^2(\frac{\pi}{8})$) est un exercice classique de théorie de l'information quantique et la MMC est toujours optimale. Pour 2 qubits, nous avons généré l'ensemble des 16 états possibles qui correspondent à une source maximalement décorrélée. Pour 4 qubits, comme l'ensemble de tous les états possibles à une cardinalité de 16^{16}, il est irréaliste de faire une recherche exhaustive. Nous avons donc pris un échantillon aléatoire de 10000 états et avons comparé la mesure optimale et la MMC sur ces états. Pour 8 qubits, nous avons considéré la MMC sur 10000 états également, mais l'optimisation devient trop intensive en calcul. Voici les résultats :

Nombre de qubits	2	4	8
p_{succ}^{opt}	0,7784	0,7334	n/a
Variance	0,92377 $\times 10^{-5}$	0,11408 $\times 10^{-6}$	n/a
p_{succ}^{MMC}	0,7783	0,73391	0,72140
Variance	0,92519 $\times 10^{-5}$	0,14614 $\times 10^{-5}$	0,35308$\times 10^{-8}$

Plusieurs choses sont à remarquer. Premièrement, il semble que la probabilité de succès de la mesure optimale soit extrêmement près de celle de la MMC. Il serait très possible que l'inégalité soit due à la précision machine. Encore plus remarquable est que la probabilité de succès semble décroître avec le nombre de qubits et que la variance soit très petite. Ce fait est en contradiction avec le résultat obtenu pour une source $\frac{1}{d}$-décorrélée montré au début du chapitre et avec le fait que le choix de fonction défi ne change pas beaucoup la probabilité de succès. Il semble donc que pour toute source maximalement décorrélée, la probabilité de succès est bornée supérieurement par une constante, au moins $\cos^2(\frac{\pi}{8})$, qui est la borne pour 1 qubit.

Nous mettons aussi les résultats de simulation pour l'entropie de Von Neumann, en moyenne, pour 2, 4 et 8 qubits ainsi que la borne inférieure induite. On observe une tendance de l'entropie vers $n-1$, ce qui donne aussi des indications sur la possibilité de discriminer les états avec une probabilité qui ne tend pas vers 1.

Nombre de qubits	2	4	8
Entropie	1,4178	3,3123	7,2808
Variance	0,0105	0,23487$\times 10^{-5}$	0,82759$\times 10^{-8}$
Borne induite	0,6679	0,62084	0,6074

CHAPITRE 6

CONCLUSION

En utilisant l'optimisation semi-définie, nous avons obtenu pour 2 et 4 qubits que la MMC est très près de la mesure optimale, la différence étant possiblement dû à la précision machine. Bien qu'il serait intéressant de montrer que la mesure optimale est égale à la MMC, il nous est simplement utile d'utiliser le théorème de Barnum-Knill qui borne la probabilité optimale de succès par celle de la MMC. On observe aussi que la probabilité de distinguer ces états diminue lorsque le nombre de qubits augmente. C'est une question ouverte de savoir si les bornes inférieures et supérieures inférées plus haut sont atteintes dans la limite du nombre de qubits. Un résultat remarquable de nos simulations est la tendance de la probabilité de succès vers 0.72. Ceci faisant écho aux résultats de théorie des matrices aléatoires donné par Montanaro [30], où l'auteur montre que pour «presque tous» les ensembles de n états aléatoires de dimension n, la probabilité d'identification est bornée inférieurement par 0.72. Le niveau du cadre de l'analyse de ce résultat dépassant le niveau de l'auteur de ce mémoire, il serait intéressant pour de futurs travaux d'investiguer d'une part si la probabilité est réellement décroissante, et d'autre part si elle atteint cette borne. Le potentiel théorique d'une borne supérieure constante est aussi très grand, étant donné l'importance du protocole d'instanciation de Fiat-Shamir donné ci-haut.

BIBLIOGRAPHIE

[1] Farid Alizadeh. Interior point methods in semidefinite programming with applications to combinatorial optimization. *SIAM Journal on Optimization*, 5(1):13–51, 1995.

[2] Somshubhro Bandyopadhyay, P Oscar Boykin, Vwani Roychowdhury et Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34 (4):512–528, 2002.

[3] Stephen M Barnett et Sarah Croke. Quantum state discrimination. *Advances in Optics and Photonics*, 1(2):238–278, 2009.

[4] Howard Barnum et Emanuel Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *Journal of Mathematical Physics*, 43(5): 2097–2106, 2002.

[5] Salman Beigi et Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011. URL `http://stacks.iop.org/1367-2630/13/i=9/a=093036`.

[6] Charles H Bennett et Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. Dans *1984 International Conference on Computers, Systems & Signal Processing, Bangalore, India*, pages 175–179, 1984.

[7] Stephen Boyd et Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[8] Thomas M Cover et Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[9] Inc. CVX Research. CVX : Matlab software for disciplined convex programming, version 2.0. `http://cvxr.com/cvx`, août 2012.

[10] Yonina C Eldar et G David Forney Jr. On quantum detection and the square-root measurement. *Information Theory, IEEE Transactions on*, 47(3):858–872, 2001.

[11] Yonina C Eldar, Alexandre Megretski et George C Verghese. Designing optimal quantum detectors via semidefinite programming. *Information Theory, IEEE Transactions on*, 49(4):1007–1012, 2003.

[12] Amos Fiat et Adi Shamir. How to prove yourself : Practical solutions to identification and signature problems. Dans *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.

[13] Christopher A Fuchs et Jeroen Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

[14] Shafi Goldwasser et Yael Tauman Kalai. On the (in) security of the fiat-shamir paradigm. Dans *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*, pages 102–113. IEEE, 2003.

[15] Paul Hausladen, Richard Jozsa, Benjamin Schumacher, Michael Westmoreland et William K Wootters. Classical information capacity of a quantum channel. *Physical Review A*, 54(3):1869, 1996.

[16] Paul Hausladen et William K Wootters. A 'pretty good'measurement for distinguishing quantum states. *Journal of Modern Optics*, 41(12):2385–2390, 1994.

[17] Werner Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3-4):172–198, 1927.

[18] Carl W Helstrom. *Quantum detection and estimation theory*. Academic press, 1976.

[19] Alexander S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973.

[20] Alexander S Holevo. *Statistical structure of quantum theory*, volume 67. Springer Science & Business Media, 2003.

[21] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[22] ID Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A : Mathematical and General*, 14(12):3241, 1981.

[23] ID Ivanovic. Unbiased projector basis over c 3. *Physics Letters A*, 228(6):329–334, 1997.

[24] Richard Jozsa et Jürgen Schlienz. Distinguishability of states and von neumann entropy. *Physical Review A*, 62(1):012301, 2000.

[25] Oliver Kern, Kedar S Ranade et Ulrich Seyfarth. Complete sets of cyclic mutually unbiased bases in even prime-power dimensions. *Journal of Physics A : Mathematical and Theoretical*, 43(27):275305, 2010. URL `http://stacks.iop.org/1751-8121/43/i=27/a=275305`.

[26] Andreas Klappenecker et Martin Rötteler. Constructions of mutually unbiased bases. Dans *Finite fields and applications*, pages 137–144. Springer, 2004.

[27] Andrei B Klimov, Luis L Sánchez-Soto et Hubert de Guise. Multicomplementary operators via finite fourier transform. *Journal of Physics A : Mathematical and General*, 38(12):2747, 2005.

[28] R. Konig, R. Renner et C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, Sept 2009. ISSN 0018-9448.

[29] Jay Lawrence, Časlav Brukner et Anton Zeilinger. Mutually unbiased binary observable sets on n qubits. *Physical Review A*, 65(3):032320, 2002.

[30] Ashley Montanaro. On the distinguishability of random quantum states. *Communications in mathematical physics*, 273(3):619–636, 2007.

[31] Yurii Nesterov et Arkadii Nemirovskii. *Interior-point polynomial algorithms in convex programming*, volume 13. Siam, 1994.

[32] Johann v Neumann. *Mathematische grundlagen der quantenmechanik*, volume 38. Springer-Verlag, 2013.

[33] Michael A Nielsen et Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[34] Asher Peres et William K Wootters. Optimal detection of quantum information. *Physical Review Letters*, 66(9):1119, 1991.

[35] David Pointcheval et Jacques Stern. Security proofs for signature schemes. Dans *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 387–398. Springer, 1996.

[36] Alfred Renyi. On measures of entropy and information. Dans *Fourth Berkeley symposium on mathematical statistics and probability*, volume 1, pages 547–561, 1961.

[37] JL Romero, Gunnar Björk, AB Klimov et LL Sánchez-Soto. Structure of the sets of mutually unbiased bases for n qubits. *Physical Review A*, 72(6):062310, 2005.

[38] Louis Salvail. Sujets en informatique quantique. Notes de cour.

[39] C.E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, page p.623, July 1948.

[40] Morton Slater. Lagrange multipliers revisited. Dans *Traces and Emergence of Nonlinear Programming*, pages 293–306. Springer, 2014.

[41] Marco Tomamichel, Roger Colbeck et Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55(12):5840–5847, 2009.

[42] Jon Tyson. Two-sided estimates of minimum-error distinguishability of mixed quantum states via generalized holevo–curlander bounds. *Journal of Mathematical Physics*, 50(3):032106, 2009.

[43] John Watrous. Theory of quantum information. Lecture Notes.

[44] Stephanie Wehner et Andreas Winter. Entropic uncertainty relations—a survey. *New Journal of Physics*, 12(2):025009, 2010. URL `http://stacks.iop.org/1367-2630/12/i=2/a=025009`.

[45] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[46] William K Wootters et Brian D Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.

[47] Horace P Yuen, Robert S Kennedy et Melvin Lax. Optimum testing of multiple hypotheses in quantum detection theory. *Information Theory, IEEE Transactions on*, 21(2):125–134, 1975.