UNIVERSITÉ DE LIMOGES

ÉCOLE DOCTORALE SISMI
SCIENCES ET INGÉNIERIE DES SYSTÈMES, MATHÉMATIQUES, INFORMATIQUE

T H È S E

pour obtenir le titre de

Docteur de l'Université de Limoges
Mention : Mathématiques et applications

Présentée et soutenue par

Don Jean Baptiste ANOMAN

Contributions relatives à la génération quantique d'aléa

Thèse dirigée par François ARNAULT

préparée au laboratoire Xlim, Université de Limoges

soutenue le 02 Décembre 2021

Jury :

Rapporteurs :	Victor Magron	-	Chargé de recherche CNRS (HDR)
	Ayoub Otmani	-	Professeur à l'Université de Rouen-Normandie
Examinateurs :	François Arnault	-	Maître de Conférences HDR à l'Université de Limoges
	Eleni Diamanti	-	Directrice de recherche Laboratoire d'Informatique, Sorbonne université, PCQC
	Philippe Gaborit	-	Professeur à l'Université de Limoges
	Simone Naldi	-	Maître de Conférences à l'Université de Limoges
Invités :	Alastair Abbott	-	Chargé de Recherche à INRIA Grenoble
	Cyril Branciard	-	Chargé de Recherche à Institut Néel Grenoble

Remerciements

Je remercie tous ceux et celles qui m' ont aidé, à commencer par mes parents, monsieur et madame ANOMAN Don, ma famille, mes amis et tous nos bienfaiteurs. Je remercie mon encadrant, monsieur François Arnault pour son aide inestimable pour me former au domaine du quantique et pour l'encadrement la thèse. Je remercie monsieur Simone Naldi pour son aide dans l'avancement de nos travaux. Je remercie enfin tous mes collègues les doctorants, ainsi que les chercheurs du laboratoire avec qui j'ai passé d'agréables moments. Comme on le dit chez nous :

"Yékin Nancè"

Résumé

La physique classique, par son caractère fondamentalement déterministe, ne permet pas la production d'aléa vrai. La physique quantique, quant à elle, fait des prévisions probabilistes, sur des processus qui paraissent donc fondamentalement aléatoires. De plus, les réponses apportées aux paradoxes de type EPR, comme la réponse formulée par les inégalités de Bell [17] et leurs expérimentations par Alain Aspect, montrent que la physique quantique ne peut être complétée en une théorie entièrement prédictive. Une question émane alors : Quelles sont les expériences quantiques fondamentalement aléatoires et, quelle quantité d'aléa est ainsi produite ?
Stephano Pironio et Al [62] donnent une borne inférieure sur la quantité d'aléa (ou l'entropie) des suites aléatoires produites au travers du jeu de Bell. Et, cette quantité est fonction des violations de l'inégalité CHSH. Mais, de manière plus directe, Cristian S. Calude et Al [4] montrent que presque toutes les mesures quantiques produisent de l'aléa : c'est le caractère indéfini du résultat de presque toutes les mesures quantiques. Ainsi, sur la base de ce résultat, ils présentent des schémas de génération d'aléa utilisant des observables incompatibles implémentées l'une à la suite de l'autre (voir [6]). Dans le cadre de cette thèse, notre but est ainsi de proposer de nouveaux schémas de génération quantique d'aléa basés sur ce caractère aléatoire intrinsèque aux expériences quantiques. Nous le faisons, dans le chapitre 5, au travers de protocoles que l'on a présentés en poster respectivement à TQC 2020 [14] et QCRYPT 2020 [10]. Ces protocoles explorent l'utilisation de produits d'observables incompatibles implémentées l'une à la suite de l'autre comme le font les auteurs de [37]. Le premier protocole (TQC 2020) est un générateur d'entropie maximale basé sur un unique qutrit n'utilisant que des opérations sur SU(2), donc facilement implémentables. Pour un apport en sécurité à ces protocoles, nous dérivons, à partir d'inégalités de Bell déjà existantes notamment CHSH et CHSH-3 (initialement CGLMP pour qutrits [30]), de nouvelles inégalités. Cette fois-ci, l'on considère une configuration constituée d'un unique Qutrit où la contrainte de commutativité des observables n'est pas imposée. La borne classique est cette fois-ci obtenue sous l'hypothèse du Réalisme macroscopique [52], comme celles des inégalités temporelles [37]. Ces bornes classiques sont égales à celles obtenues dans le cadre du réalisme locale. Cependant, les bornes quantiques peuvent être plus grandes que celles des expressions originelles permettant ainsi une meilleure résistance au bruit et donc à de potentielles attaques. Ces violations par rapport au cadre classique ne sont plus dues à la non localité mais plutôt au caractère indéfini des résultats de presque toutes les mesures quantiques. De plus, dans le cadre du deuxième poster [10] la borne quantique de la nouvelle expression est obtenue par une SDP qui nous donne des états et mesures permettant d'atteindre cette borne. Ils sont à l'œuvre dans le protocole de génération d'aléa avec des propriétés d'auto test.

Cette thèse a aussi été l'occasion de revisiter certains aspects de la cryptographie quantique comme la distribution quantique de clé.

Abstract

The deterministic nature of classical physics does not allow true randomness production. Quantum physics, on the other side, makes probabilistic forecasts about processes that seem to be intrinsically random. Moreover, answers to EPR type paradoxes, like the answer formulated through Bell inequality [17], show that quantum physics can not be completed in a full deterministic theory. We may wonder what are the quantum experiments allowing true randomness production and what is the quantity of randomness produced.

Stephano Pironio and Al [62] give a lower bound on the quantity of randomness (entropy) produced by Bell's game.

In a more direct way, Cristian S. Calude and Al [4] show that almost all quantum measurements produce genuine randomness (Strong Kochen Specker theorem and its consequences).

Hence, using this latter result, they show a quantum random number generator using non compatible measurements implemented one after the other (see [6]).

In our work during this PhD thesis, we aim to produce randomness using this latter result of Cristian S. Calude. Thus we show in chapter 5, the protocols we presented at TQC 2020 [14] and Qcrypt 2020 [10]. This works explore the use of product of compatible measurements implemented one after the other as in [37]. The first protocol is a maximal entropy generator using only one qutrit with operation on SU(2), thus, easily implementable. To improve the security of this protocols, we deduce, new quantum inequalities from existing inequalities namely CHSH [29] and CHSH-3 (initially CGLMP for qutrits [30]). Here, we consider configuration using only one qutrit, where the constrain of commuting observables is released. The classical bounds are then obtained under the hypothesis of macroscopic reality defined in [52] (and also used for classical bounds of temporal inequalities [37]). This classical bounds are the same as in the frame of local realism. However, the quantum bounds can be greater than those of the original expressions, allowing thus a better resistance to noise and attacks. This violations with respect to classical bound are no more due to non locality but, they are due to indefiniteness of outcomes of quantum measurements. Moreover, for our second work [10], the quantum bound of the new expression is obtained using an SDP that gives us also the state and measurements allowing to reach this bound. We use them to show a random number generator with self testing arguments.

During this PhD, we also give an analysis of some aspects of quantum cryptography as QKD.

Table des matières

Liste des tableaux

Table des figures

Introduction

La découverte des lois de la nature et leur application au quotidien a guidé l'évolution de l'humanité, permettant une amélioration des conditions de vie, voire la survie du genre humain. À contrario, le manque de connaissance de ces lois naturelles a souvent été cause de désastres parmi lesquels on peut citer les mauvaises récoltes et famines, ou encore le manque d'anticipation de catastrophes naturelles et leurs nombreuses victimes. Cependant, le manque de connaissance, propre à tout point de vue partiel, n'est pas seulement un état d'ignorance à déplorer. Mais, il peut s'avérer être un atout pour celui qui en connaît davantage. C'est en effet sur le manque de connaissance de certains hommes que d'autres hommes fondent leur stratégie en temps de conflit, et plus précisément dans la dissimulation des données importantes. C'est sur ce principe que repose la cryptographie (étymologiquement la science du secret). Comme le révèle l'histoire de cette discipline, les outils de ce savoir ont, pour la plupart, connu leur essor au travers des conflits. Et ce, depuis le chiffrement de César, la machine Enigma, jusqu'aux outils mathématiques complexes de notre époque.
La sécurité des outils originels reposait sur le fait que la méthode de chiffrement n'était connue que des personnes échangeant les messages : une partie de la sécurité pouvait ainsi reposer sur le manque de connaissance du mécanisme de chiffrement. Ce mode de fonctionnement apparait comme la ligne directrice du chiffre de César où la méthode, le décalage de trois (3) lettres, n'était connue que de l'empereur et de ses généraux. Dès 1883, en revanche, ce mode de fonctionnement a été officiellement désavoué par Auguste KERCKHOFFS dans sa publication intitulée « La cryptographie militaire » au *Journal des sciences militaires* [44]. Il y énonce les six "desiderata de la cryptographie militaire" qui sont les règles essentielles pour un cryptosystème robuste. Parmi celles-ci, le principe de KERCKHOFFS stipule que la sécurité d'un système ne doit résider que dans le secret de la clé et non dans la méconnaissance du mécanisme de fonctionnement.

Ainsi, pour parvenir à bout d'un cryptosystème, on pourrait en faire une cryptanalyse consistant à déterminer les clés à partir des failles du système. C'est à ce problème difficile que s'attaque une bonne partie des cryptologues. Ainsi, en s'attaquant uniquement à la cryptanalyse, on suggère que les clés utilisées sont générées de manière satisfaisante.

Est-ce vraiment le cas ?

Dans le chapitre 1 de cette thèse, nous analysons les principes de production de nombres aléatoires, (appelé l'ALÉA et qui constitue les clés), basés sur des procédés de la physique classique. Ces autres principes utilisent des expériences dont les résultats sont prédéterminés d'avance. Mais cependant, ces résultats nous paraissent aléatoires du

fait d'un manque d'informations sur ces expériences. Or, par certaines attaques telles que celles par canaux cachés, un attaquant peut retrouver les informations ayant servi à initialiser les expériences. Ce dernier aura ainsi un certain avantage pour deviner l'aléa précédemment produit. De ce fait nous déduisons la nécessité de l'utilisation de générateurs d'aléa basés sur des expériences intrinsèquement aléatoires. C'est cette propriété que nous offre la physique quantique.

Dans les chapitres 2 et 3, nous donnons les pré-requis de la physique quantique qui est une science qui décrit de manière formelle les interactions entre particules à l'échelle atomique et subatomique. Nous donnons ensuite les fondements logiques du caractère indéterminé des résultats des mesures quantiques. Ce caractère selon lequel les résultats des mesures ne sont pas déterminés d'avance quelque soit la connaissance qu'on a des conditions initiales. Ces pré-requis et fondements s'avèrent nécessaires à la compréhension et à la justification des schémas de génération quantique d'aléa.

Dans le chapitre 4, nous rappelons les différents schémas de production quantique d'aléa déjà existants. Ceux-ci s'articulent autour de deux groupes :

1. Les générateurs dont la fiabilité est basée sur la description détaillée des appareils utilisés (voir [48]).
2. Les générateurs dont la fiabilité est basée sur des inégalités quantiques (voir par exemple [62]).

Dans la mesure où ce deuxième type de générateur permet la détection d'éventuelles erreurs et intrusions d'attaquant, nous nous attarderons un peu plus sur ce sujet. En effet, l'idée générale est résumée par le fait que plus la violation des inégalités est grande, moins il y a de chance qu'un attaquant puisse intervenir. Ici, le terme violation désigne le rapport, plus grand que 1, entre la valeur quantique et la borne classique. De plus, les générateurs de ce type font pour la plupart intervenir des produits d'observables commutatives.

Dans le chapitre 5, en exposant **nos contributions** à la recherche, nous souhaitons améliorer la sécurité des protocoles, au travers d'inégalités quantiques permettant une plus grande violation. Nous dérivons alors des inégalités quantiques faisant intervenir des produits d'observables cette fois-ci **potentiellement non-commutatives**. De plus, nous décrivons nos différents protocoles basés sur ces inégalités. Ces protocoles ont été présentés comme poster aux conférences TQC2020 et QCRYPT 2020.

Dans le chapitre 6, du fait des limites de nos précédents travaux, nous étudions le cadre formel des inégalités temporelles utilisant des produits d'observables potentiellement non commutatives. Ce cadre nous décrit alors les propriétés fondamentales de la physique quantique démontrées aux travers de la violation d'inégalités portant sur des observables potentiellement non commutatives. Nous déduisons de plus, dans ce cadre, la borne d'une inégalité de Bell bien connue (CGLMP d=3).

Le **chapitre 7** quant à lui reprend les différents aspects de la cryptographie quantique revisités au travers de cette thèse. Nous y présentons notamment une version intriquée du protocole "six states". Nous proposons de plus une généralisation des polynômes de Mermin (indicateurs d'intrication multipartite) au travers d'un lien entre ces polynômes et les polynômes homogènes de Bell introduits par François ARNAULT [12].

Chapitre 1

Limites des méthodes de la physique classique pour la production d'aléa

Mots clés : *aléatoire, imprédictible, indéterminé, chaos*

Contents

1.1 Objectif et résumé du chapitre

Au vu de l'engouement suscité par la physique quantique, et, au vu du titre de cette thèse *Contributions relatives à la génération quantique d'aléa*, une question légitime émane :

Pourquoi ne plus produire de l'aléa avec la physique classique et se tourner vers la physique quantique ?

Dans ce chapitre, nous y apporterons des éléments de réponse. Pour ce faire, nous décrirons les principes généraux des différentes méthodes de la physique classique pour la production d'aléa. Nous étayerons nos propos de divers exemples. Cela nous conduira à mettre en lumière les limites de ces méthodes classiques. De par leurs limites enfin, ces méthodes ne peuvent guère être considérées comme des candidates idéales pour la production d'aléa.

NB : Ce chapitre est sciemment dénué de tout le formalisme mathématique décrivant avec précision les notions de physique classique qui y sont abordées. Nous nous focalisons plutôt sur les idées générales permettant de se soustraire de la physique classique pour se tourner vers la physique quantique. Ce choix est fait dans le souci de faciliter la compréhension mais aussi, du fait que ces notions de physique classique ne sont point le coeur de nos travaux. Ces derniers sont plutôt tournés vers la physique quantique.

1.2 Méthodes prédictibles de production d'aléa

Dès le développement des outils numériques de traitement de l'information, le besoin d'aléa s'est considérablement accru. Les premières méthodes pour le produire ont essentiellement consisté en des méthodes numériques, basées sur des fonctions mathématiques.

1.2.1 Méthodes numériques

Les premières méthodes de production d'aléa sont basées sur l'implémentation machine de fonctions mathématiques. Parmi ces implémentations, les plus populaires sont les LFSR (Linear Feedback Shift Register = Registre à décalage à rétroaction linéaire) [39] auxquels divers améliorations ont été apportées notamment dans [13]. Bien d'autres fonctions sont aussi utilisées. La validation des sorties générées par ces fonctions est effectuée au travers d'une liste de tests statistiques standardisés par le NIST [16]. Ces tests, évaluant les propriétés statistiques d'une suite de nombres transmise, ne garantissent pas

le caractère aléatoire des sorties des algorithmes. Cela vient du fait que, tous ces algorithmes proposés, avec la même entrée, produisent la même sortie. De ce fait, la suite de nombres produite n'est point aléatoire pour un attaquant possédant déjà l'entrée de l'algorithme. De plus, cette suite de nombres n'est point aléatoire pour un attaquant ayant déjà collecté les résultats d'une précédente exécution de l'algorithme. En ce sens que la suite produite à l'exécution précédente sera la même que celle produite à l'exécution courante. Ainsi, il nous faut régulièrement changer l'initialisation, **appelée graine**, des algorithmes.

1.2.2 Graines prédictibles

Au vu du paragraphe précédent, notre conscience est éclairée sur le besoin d'une graine (initialisation) différente à chaque utilisation des algorithmes de génération d'aléa. Pour cela nous avons recours à de l'aléa émanant d'expériences physiques (sources d'entropie), comme par exemple le mouvement de la souris, les lettres entrées au clavier, les différentes communications entre applications [40]. Néanmoins, ces graines ainsi générées, sont prédictibles. Cela signifie que tout attaquant qui a accès à l'environnement de l'ordinateur au moment de la production de la graine (par attaque par canaux cachés), peut collecter les informations d'entrée et prédire la graine. Ainsi, l'aléa produit ne lui sera pas aussi aléatoire qu'il le faut.
Certains constructeurs [33] ont recours à des composants utilisant des expériences chaotiques, qualifiées d'imprédictibles, pour la génération des graines des algorithmes. La suite de ce chapitre est donc consacrée à la description des idées à l'oeuvre dans ces mécanismes de la physique classique dits imprédictibles.

1.3 Méthodes basées sur des expériences dites imprédictibles (chaos)

La section précédente nous a permis d'exposer les limites des méthodes de génération de graines aléatoires basées sur des phénomènes prédictibles. Le terme prédictible signifiant qu'il nous est possible d'avoir assez d'informations sur les états initiaux pour prédire tous les états futurs du système.

Pour pallier à ce défaut de prédictibilité de l'aléa, nous nous tournons vers des phénomènes de la **physique classique dits imprédictibles**.

Définition 1.1. *Il nous faut ici faire la distinction entre les termes suivants :* ***aléatoire, imprédictible et indéterminé****.*

Les résultats d'une expérience peuvent nous apparaitre ***Aléatoires*** *(c'est à dire, d'après le Larousse, soumis au hasard, dont le résultat est incertain) si :*

- *Les résultats de mesure sont* ***Indéterminés*** *c'est à dire qu'ils ne préexistent pas avant d'avoir effectué la mesure. Il va donc de soi que les résultats soient* ***intrinsèquement aléatoires****. C'est le cas des expériences en physique quantique.*

- *Ou, les résultats sont* ***Imprédictibles*** *c'est à dire : Bien que* ***connaissant la loi d'évolution du système****, nous n'avons pas assez de connaissances sur les états initiaux pour prédire tous les résultats de l'expérience. Ce sont des* ***dynamiques chaotiques*** *[72, 64], où, nous ne pouvons avoir que des approximations des conditions initiales. De plus, ces dynamiques (ensemble d'états ou de points) chaotiques s'avèrent sensibles aux variations plus petites que la précision des approximations.*

Les définitions précédentes nous indiquent que, dans le cas des dynamiques chaotiques, dont on connait les lois régissant l'évolution, les états de ces dynamiques sont imprédictibles. Cette imprédictibilité émane d'une limite épistémique (d'un manque d'information) sur les conditions initiales. C'est ce que nous explique le mathématicien français Henri Poincaré au chapitre IV de la référence [64] :

"Mais lors même que les lois naturelles (Lois d'évolution des systèmes) n'auraient plus de secret pour nous, nous ne pourrons connaitre la situation initiale qu'approximativement. (Or) il peut arriver que de ***petites différences*** *dans les conditions initiales en engendrent de* ***très grandes*** *dans les phénomènes finaux ; une petite erreur sur les premières produirait une erreur énorme sur les derniers. La* ***prédiction devient impossible*** *et nous avons le phénomène fortuit (ou aléatoire) ".*

À cette étape de notre raisonnement, nous pourrions légitimement nous demander pourquoi ne pas se contenter des phénomènes chaotiques pour produire de l'aléa, du fait de leur imprédictibilité.
L'exemple suivant nous présente deux cas qui étayent les limites de ces dynamiques pour une production idéale d'aléa :

Exemple 1.1.
Nous souhaitons donner une idée des limites des dynamiques chaotiques pour une production idéale d'aléa. Pour cela regardons ensemble les deux cas suivants :

1. *Cas d'école : Fonction Logistique [74]*
   Considérons une expérience physique (E), utilisée dans la production d'aléa, dont la dynamique (suite de points) est donnée par :

$$D_{0.20000001243} : \quad x_0 := 0.20000001243;\ x_n := 4x_{n-1}(1 - x_{n-1})$$

   Considérons de plus, une prédiction des résultats de cette expérience décrite par la dynamique :

$$D_{0.2} : y_0 := 0.2;\ y_n := 4y_{n-1}(1 - y_{n-1})$$

   La dynamique $D_{0.2}$, est une approximation intuitive de l'expérience physique (E) dont la dynamique est $D_{0.20000001243}$. Cela vient du fait qu'elles suivent la même loi d'évolution et ont des points de départs assez proches. De plus la prédiction $D_{0.2}$ semble plus facile à atteindre car le point de départ a moins de précision.
   Le graphique suivant nous montre les deux dynamiques en fonction du nombre $'n'$ d'étapes (d'itérations des dynamiques).

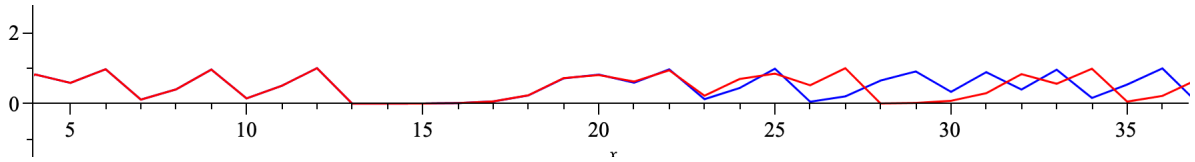

FIGURE 1.1 – Dynamiques $D_{0.20000001243}$(bleue) et $D_{0.2}$(rouge) en fonction du nombre d'itérations

Au vu du graphique, on constate qu'avant la 22-ième itération, les dynamiques $D_{0.20000001243}$(bleue) et $D_{0.2}$(rouge) sont quasiment indistinguables. Cependant, à partir de cette 22-ième itération les deux dynamiques sont clairement distinctes (sans aucune propriété de convergence de l'une vers l'autre).

Ainsi, les résultats de l'expérience (E), peuvent nous paraitre aléatoires, après un nombre d'étapes assez grand, si on ne s'en tient qu'à l'approximation $D_{0.2}$.

***Cependant**, les premiers résultats de la prédiction $D_{0.2}$ semblent assez proches de ceux de l'expérience (E). Cela signifie que tout **attaquant**, ayant une approximation $D_{0.2}$ des conditions initiales de l'expérience (E), détient un **certain avantage** pour prédire les premiers résultats de cette expérience (pour chacun des premiers résultats de (E), il peut expliciter un intervalle assez petit qui le contient).*

L'exemple suivant permet d'étayer le fait que l'attaquant, qui a une approximation des conditions initiales a tout de même un avantage dans la prédiction des premiers états de la dynamique du système.

2. *Météo et effet papillon*

   *Les phénomènes météorologiques suivent une dynamique chaotique qu'on émule grâce aux mesures effectuées par une multitude de capteurs [69]. Cette dynamique chaotique, fortement sensible aux conditions initiales, explique le célèbre **effet papillon** formulé par Edward N. Lorenz en ces termes : "Un battement d'ailes de papillon au Brésil peut-il déclencher une tornade au Texas ?" [54].*

   Cette forte sensibilité aux conditions initiales est la raison pour laquelle la météo effective peut nous sembler décorrélée de celle prédite de nombreuses semaines avant. Le phénomène météorologique observé nous paraissant ainsi aléatoire. Cependant, les prévisions météorologiques, que nous donnent Météo France par exemple, sont "quasiment" exactes sur une voire deux semaines.

Aux termes de cet exemple et comme nous confirme la théorie rigoureuse écrite dans [74, 72], **les propriétés d'imprédictibilité du chaos sont des propriétés aux limites**. Cela signifie qu'elles sont obtenues après un nombre relativement grand d'itérations des dynamiques chaotiques. Pourtant, dans une production idéale d'aléa, tout attaquant possédant des informations d'une précision infinie sur une itération n, ne doit avoir aucun avantage pour deviner la sortie de l'itération $n+1$. Cette propriété, manquante dans le cas des dynamiques chaotiques, nous est offerte par la théorie quantique.

Dans le cadre de la physique quantique en effet, l'aléa n'est point dû à une quelconque ignorance. Mais, il découle du caractère indéterminé (non défini d'avance) des résultats des mesures quantiques. Cela signifie simplement que, tout attaquant qui connaitrait exactement l'état d'une particule quantique (itération n), n'aurait aucun avantage pour deviner le résultat de la mesure de la particule (sortie de l'itération $n+1$).

Enquérons-nous donc, avec plus de précisions du formalisme quantique et de ses avantages pour la production d'aléa.

Première partie

Production quantique actuelle d'aléa

Chapitre 2

Pré-requis

Mots clés : *Postulats de physique quantique, qubits, qutrits, observables, projecteurs, produit scalaire*

Contents

Ce chapitre a pour but de présenter les outils de base du formalisme quantique pour la compréhension des travaux abordés au cours de cette thèse. Il est en grande partie tiré du chapitre 2 de [59]

2.1 Les états quantiques

Les éléments de base de la physique quantique sont les très petites particules (les photons, les atomes, les électrons). Leurs états, ainsi que bien d'autres notions essentielles de ce champs d'études, sont décrits à l'aide de postulats (des lois tenues pour vraies).

2.1.1 Cas d'une particule

Le premier postulat de la physique quantique stipule qu'à un système physique isolé, on associe un espace vectoriel sur $\mathbb{C}$ qu'on peut noter $\mathbb{H}$. Cet espace $\mathbb{H}$, alors muni d'un produit scalaire hermitien, est un espace de Hilbert. Il est appelé *espace des états du système*. Le système est entièrement défini par un vecteur d'état qui est un vecteur unitaire de l'espace. Son état est alors un **état pur** (nous n'aborderons pas le cas des états mixtes dans le cadre de ces travaux). Ce vecteur unitaire s'écrit alors, par la notation de Dirac *ket* : $|\Psi\rangle$.

Exemple 2.1. *Considérons le cas des qubits (bits quantiques) : Ces éléments sont décrits dans un espace vectoriel de dimension 2 . Soient* $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ *et* $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ *une base orthonormale de l'espace. Alors tout état du système représenté par le vecteur* $|\Psi\rangle$ *s'écrit*

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

avec α *et* β *des complexes vérifiant* $|\alpha|^2 + |\beta|^2 = 1$.

Dans le cadre de cette thèse, nos recherches sont effectuées à l'aide de qutrits qui sont des particules pouvant être dans 3 états possibles et donc représentées dans un espace de Hilbert de dimension $d = 3$. Ce formalisme permet de simplifier l'écriture de certaines notions très utiles pour la suite.

Produits scalaires et extérieurs

Considérons l'espace dual de H qui est l'espace des applications linéaires de H dans $\mathbb{C}$ et que nous notons H^*. Alors, le dual d'un vecteur $|\Psi\rangle = \begin{pmatrix}a_1\\a_2\\...\\a_n\end{pmatrix}$ est le vecteur noté "bra" : $\langle\Psi| = \begin{pmatrix}a_1^* & a_2^* & ... & a_n^*\end{pmatrix}$ où a_i^* est le conjugué de a_i. Ce vecteur dual est un élément de H^*. Ainsi donc, le produit scalaire entre $|\Psi\rangle = \begin{pmatrix}a_1\\a_2\\...\\a_n\end{pmatrix}$ et $|\Phi\rangle = \begin{pmatrix}b_1\\b_2\\...\\b_n\end{pmatrix}$ est

donné par

$$(|\Psi\rangle, |\Phi\rangle) = \begin{pmatrix} a_1^* & a_2^* & ... & a_n^* \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ ... \\ b_n \end{pmatrix} = a_1^* b_1 + a_2^* b_2 + ... + a_n^* b_n$$

$$= \langle\Psi| \, |\Phi\rangle$$

On le note $\langle\Psi|\Phi\rangle$.
Ce produit scalaire est sesquilinéaire (linéaire par rapport à la deuxième composante et pseudo-linéaire par conjugué par rapport à la première).
Soit U une matrice carrée telle que le vecteur $U|\Psi\rangle \in H$ alors le produit scalaire de $|\Psi\rangle$ *et* $U|\Phi\rangle$ s'écrit

$$(|\Psi\rangle, U|\Phi\rangle) = \langle\Psi|U|\Phi\rangle = (U^\dagger|\Psi\rangle, |\Phi\rangle)$$

où $U^\dagger$ est la transconjuguée (transposée de la conjuguée complexe) de U. On peut aussi voir que

$$|\Psi\rangle^\dagger = \langle\Psi|$$

Nous définissons aussi le **produit extérieur** qui permet d'avoir une bonne vision du formalisme et des calculs effectués en physique quantique.
Soient V et W des espaces de Hilbert de dimensions finies. Soient $|w\rangle \in W$ *et* $|v\rangle \in V$. Le produit extérieur de $|w\rangle$ *et* $|v\rangle$ est l'application linéaire :

$$\begin{aligned} |w\rangle\langle v| : & V \to W \\ & |v'\rangle \mapsto (|w\rangle\langle v|)|v'\rangle = |w\rangle.\langle v|v'\rangle \end{aligned}$$

Un exemple d'utilisation de ces notions pour les calculs est donné en annexe. Nous avons ainsi défini les états purs d'une seule particule. Or, dans la pratique, on utilise des systèmes constitués de plusieurs particules. C'est le cas de la distribution de clés quantiques (QKD), et aussi de la production quantique d'aléa. La prochaine sous partie de cette thèse s'attachera à décrire certaines particularités des systèmes composés de plusieurs particules.

2.1.2 Les états de plusieurs particules

La description des états de plusieurs particules se base sur le quatrième postulat de la mécanique quantique. Selon celui-ci l'espace des états d'un système composé de plusieurs particules est le **produit tensoriel** des espaces des états (nous définirons cette

notion dans la partie suivante). C'est-à-dire que si l'espace H_1 est associé à la première particule, H_2 à la deuxième particule ... H_n à la n-ième particule, alors les n particules, considérées comme un même système sont associées à l'espace $H_1 \otimes H_2 \otimes \ ... \ \otimes H_n$. De plus , si la première particule a été préparée d'avance dans l'état $|\phi_1\rangle$, la deuxième dans l'état $|\phi_2\rangle$ ... la n-ième particule dans l'état $|\phi_n\rangle$ alors , l'état du système est décrit par $|\phi_1\rangle \otimes |\phi_2\rangle \otimes \ ... \ \otimes |\phi_n\rangle$.
Attention cela ne signifie pas que l'état de plusieurs particules est forcément un produit tensoriel d'états. C'est cette distinction qui est à l'origine de la notion d'intrication quantique :

Définition 2.1. *Un état de plusieurs particules est dit* ***séparable (non intriqué)*** *si l'état de l'ensemble est le produit tensoriel de l'état de chaque particule. Dans le cas contraire, cet état est dit* ***intriqué***

Dans le cas d'un état de plusieurs particules intriquées, la mesure sur une partie permet de connaitre l'état des autres parties sans agir directement sur elles. Ce phénomène qualifié par Albert Einstein de "spooky action at distance" est la base de bien d'expériences remarquables comme celles d'Alain Aspect [15].
Il nous faut donc donner du sens à cette notion de produit tensoriel.

2.1.3 Produit tensoriel

Considérons deux espaces de Hilbert $\mathbb{H}_1$ et $\mathbb{H}_2$ de dimensions respectives n et k :
$\mathbb{H}_1$ de base orthonormale $\{|v_i\rangle \ , \ i = 1 \, ... \, n\}$
$\mathbb{H}_2$ de base orthonormale $W = \{|w_j\rangle \ , \ j = 1 \, ... \, k\}$.
Alors le produit tensoriel de $\mathbb{H}_1$ et $\mathbb{H}_2$ noté $\mathbb{H}_1 \otimes \mathbb{H}_2$ est un espace vectoriel de dimension $n \times k$ (sur le même espace que les précédents) et de base

$$\{|v_i\rangle \otimes |w_j\rangle \ ; \ i = 1 \, ... \, n, \ j = 1 \, ... \, k\}$$

On peut avoir la vision pratique suivante :
si $|u\rangle = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \in \mathbb{H}_1$ *et* $|r\rangle = \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} \in \mathbb{H}_2$ alors

$$|u\rangle \otimes |r\rangle = \begin{pmatrix} u_1 \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} \\ \\ u_2 \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} u_1 \, r_1 \\ u_1 \, r_2 \\ u_1 \, r_3 \\ u_2 \, r_1 \\ u_2 \, r_2 \\ u_2 \, r_3 \end{pmatrix}$$

On le note $|u\rangle \otimes |r\rangle = |u\rangle|r\rangle = |u \, r\rangle$

En règle générale, étant données deux matrices A et B , on a

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & ... & a_{1n}B \\ a_{21}B & a_{22}B & ... & a_{2n}B \\ ... & & & \\ a_{n1}B & a_{n2}B & ... & a_{nn}B \end{pmatrix}$$

Les propriétés fondamentales du produit tensoriel sont exposées en annexe.
Intéressons-nous maintenant à l'application de cette notion au cas de deux particules.

2.1.3.1 Cas de deux particules

Représentation des états purs
Supposons que nous ayons deux particules : la première particule, A, à laquelle on associe l'espace $\mathbb{H}_A$ et la deuxième particule B, à laquelle on associe l'espace $\mathbb{H}_B$.
Soit $\{|a_i\rangle \ , \ i = 1 ... n\}$ une base orthonormale de $\mathbb{H}_A$ et $\{|b_j\rangle \ , \ j = 1 ... k\}$ une base orthonormale de $\mathbb{H}_B$.
On a ainsi $\{|a_i b_j\rangle \ , \ i = 1 ... n \ ; \ j = 1 ... k\}$, une base de $\mathbb{H}_A \otimes \mathbb{H}_B$ qui est ordonnée en

$$(|a_1 b_1\rangle \, , \, |a_1 b_2\rangle \, ... \, |a_1 b_k\rangle \, , \, |a_2 b_1\rangle \, ... \, |a_n b_k\rangle)$$

Alors l'état du système composé des deux particules s'exprime dans la base ci-dessus : $|AB\rangle = \sum_{ij} c_{ij} |a_i b_j\rangle$. On le représente par le vecteur

$$|AB\rangle = \begin{pmatrix} c_{11} \\ ... \\ c_{1k} \\ c_{21} \\ ... \\ c_{n\,k} \end{pmatrix}$$

2.2 Mesures et observables

La mesure :
Le troisième postulat de la mécanique quantique stipule que les mesures quantiques sont décrites par une collection $\{M_m\}$ d'opérateurs de mesure (à chaque mesure on associe une collection d'opérateurs de mesure). Ce sont des matrices agissantes sur l'espace des états du système mesuré (endomorphismes). L'indice m ici fait référence aux résultats possibles de mesures.
En d'autres termes, étant donné un système physique (un simple électron par exemple) on

s'attend, après mesure d'une certaine quantité, à obtenir des résultats réels ou complexes : $\{m\}$. C'est le cas de la mesure de spin sur une particule de spin $\frac{1}{2}$. On espère obtenir $m = -\frac{1}{2}$ *ou* $m = \frac{1}{2}$. Pour ce faire, sur l'espace de Hilbert $\mathbb{H}$ dans lequel notre système est décrit, on définit un ensemble d'opérateurs $\{M_m\}$ où les indices m représentent les différents résultats possibles après mesure. Ainsi, d'après ce même postulat, si l'état quantique du système était, juste avant la mesure, $|\Psi\rangle$, alors la probabilité qu'on obtienne le résultat m après mesure est donné par

$$p(m) = \langle\Psi|M_m^\dagger M_m|\Psi\rangle$$

qui doit être un nombre positif inférieur ou égal à 1. De plus, l'état du système juste après mesure (à condition d'avoir obtenu m) est donné par le vecteur

$$\frac{M_m|\Psi\rangle}{\sqrt{\langle\Psi|M_m^\dagger M_m|\Psi\rangle}}$$

Les opérateurs de mesure (les matrices donc) d'une même collection vérifient la relation d'états complets :

$$\sum_n M_m^\dagger M_m = I \tag{2.2}$$

qui provient du fait que la somme des probabilités donne 1

$$1 = \sum_m p(m) = \sum_m \langle\Psi|M_m^\dagger M_m|\Psi\rangle = \langle\Psi|(\sum_m M_m^\dagger M_m)|\Psi\rangle \text{ et cela pour tout } |\Psi\rangle \in \mathbb{H}$$

Les mesures utilisées en pratique sont appelées **mesures projectives**. Pour les définir, introduisons la notion d'observable.

Observables

Un observable M est un opérateur agissant sur l'espace $\mathbb{H}$ des états d'un système. Traditionnellement nous utilisons des opérateurs hermitiens ($M = M^\dagger$) mais il est aussi possible d'utiliser des opérateurs unitaires [12] : ($MM^\dagger = M^\dagger M = Id$). Considérant un espace vectoriel $\mathbb{H}$ de dimension n, il existe une base orthonormale $\{|i\rangle\,,\, i = 1 \ldots n\}$ de H telle que

$$\begin{aligned} M &= \sum_{i=1}^{n} m_i |i\rangle\langle i| \\ &= \sum_{i=1}^{n} m_i P_i \end{aligned}$$

où les m_i sont les valeurs propres de M relatifs aux vecteurs propres $|i\rangle$

Si une valeur propre m a un espace propre de dimension multiple engendré par $\{|i\rangle, i = 1 \dots 3\}$ par exemple, on aura

$$P_m = P_1 + P_2 + P_3 = |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|$$

c'est pourquoi on trouvera plus souvent écrit [59]

$$M = \sum_m m P_m$$

Les P_m sont des **Projecteurs** ($P_m^2 = P_m$) d'où le nom de mesure projective.
Il faut noter que les m_i sont aussi les résultats possibles des mesures.
On en déduit le lemme suivant

lemme 2.1. *Étant donné une particule dans l'état $|\Psi\rangle \in \mathbb{H}$ la probabilité que la mesure sur ce vecteur donne m est : $p(m) = \langle\Psi|P_m|\Psi\rangle$*

En effet

Démonstration.

$p(m) = \langle\Psi|P_m^\dagger P_m|\Psi\rangle$

vu que la transconjuguée d'une somme est la somme des transconjuguées (on transpose puis on conjugue) et que $(|i\rangle\langle i|)^\dagger = |i\rangle\langle i|$

on a bien $P_m^\dagger = P_m$

$p(m) = \langle\Psi|P_m P_m|\Psi\rangle$

$p(m) = \langle\Psi|P_m|\Psi\rangle$

□

Nous pourrons aussi trouver dans la littérature la notion de **POVM** (positive operator - valued measure), ce qui signifie que la mesure est entièrement décrite par $\{E_m\}$ tels que E_m est un opérateur positif (c'est à dire $\forall\, |\Psi\rangle \in \mathbb{H}, \langle\Psi|E_m|\Psi\rangle \geq 0$). C'est le cas, par exemple, lorsqu'on pose $E_m = M_m^\dagger M_m$.
Dans le contexte des POVM, étant donné un état $|\Psi\rangle$ la probabilité d'obtenir le résultat m après mesures est $p(m) = \langle\Psi|E_m|\Psi\rangle$.

Les outils décrits ci-dessus permettent de s'approprier les notions élémentaires dont nous aurons besoin pour la suite de ce travail. Il nous faut de plus comprendre l'importance de l'entropie pour quantifier l'aléa.

2.3 L'entropie

Étant donné un processus qui génère un résultat dans l'ensemble $\{m\}$, la quantité d'informations contenue dans ce processus est le $[-log_2]$ de la distribution de probabilité. La quantité d'information contenue dans m est $[-log_2(p(m))]$. L'espérance de la quantité d'information est alors appelée **l'entropie** de l'expérience et est donnée par la formule :

$$H(X) = \sum_m -p(m)\, log_2(p(m))$$

Dans le cas de la génération d'aléa décrite dans [62], nous avons besoin de l'entropie d'une variable aléatoire X conditionnée par le fait qu'une autre variable Y ait un résultat particulier $(Y = y)$. Dans ce cas on aura :

$$H(X|Y = y) = \sum_i -p(X = x_i|Y = y) log_2(p(x_i|Y = y))$$

De là on définit $H(X|Y)$ comme la moyenne sur tous les y_j de $H(X|Y = y_j)$.
On a donc

$$\begin{aligned} H(X|Y) &= -\sum_j p(Y = y_j)\, H(X|Y = y_j) \\ &= -\sum_j p(Y = y_j) \sum_i p(X = x_i|Y = y_j) log_2(p(x_i|y_j)) \\ &= -\sum_{i,j} p(x_i \cap y_j) log_2(p(x_i|y_j)) \end{aligned}$$

Il faut donc retenir la formule

$$H(X|Y) = -\sum_{i,j} p(x_i \cap y_j)\ log_2(p(x_i|y_j)) \tag{2.3}$$

Ainsi, si on souhaite avoir une borne inférieure sur la quantité d'aléa produite dans nos expériences, il faut minorer $H(X|Y)$.

Or, $\forall i, j \quad p(x_i|y_j) \leq max(p(x_i|y_j)) =: p_{max}$

$$p(x_i|y_j) \leq p_{max} \text{ et donc}$$
$$log_2(p(x_i|y_j)) \leq log_2(p_{max})$$
$$\text{D'où } \sum_{i,j} p(x_i \cap y_j)\ log_2(p(x_i|y_j)) \leq \sum_{i,j} p(x_i \cap y_j)\ log_2(p_{max})$$

Étant donné que $\{(x_i \cap y_j)\}$ constitue l'ensemble des événements possibles, nous avons

$$\sum_{i,j} p(x_i \cap y_j)\ log_2(p(x_i|y_j)) \leq (\sum_{i,j} p(x_i \cap y_j))\ log_2(p_{max}) = log_2(p_{max})$$

ceci induit que

$$H(X|Y) \geq -log_2(p_{max})$$

d'où on pose

$$H_\infty(X|Y) := -log_2(p_{max}) \tag{2.4}$$

et on a la relation

$$H(X|Y) \geq H_\infty(X|Y)$$

Si on a un processus qui donne en sortie les variables A et B et dont les entrées sont X et Y on a aussi la même formule :

$$H(AB|XY) \geq H_\infty(AB|XY)$$

Ayant établi les outils de base de cette thèse, tournons nous maintenant vers les justifications du caractère indéterministe de la physique quantique et son utilisation dans la génération de nombres aléatoires.

Chapitre 3

Inégalité de Bell CHSH-2, Théorèmes Kochen Specker et Strong Kochen Specker

Mots clés : *paradoxe EPR, réalisme local, Inégalités de Bell, KS, Strong KS*

Contents

3.1 Objectif et résumé du chapitre

Dans ce chapitre, nous proposons des outils justifiant l'utilisation de la physique quantique pour la production d'aléa. Ces outils ont été conçus pour répondre aux critiques contre le formalisme quantique, parmi lesquels le paradoxe EPR [34], soutenant que l'aléa quantique proviendrait d'un manque d'information sur les états initiaux des systèmes quantiques. Cela impliquait pour eux, la possible présence de variables cachées, complétant la description des systèmes, rendant ainsi déterministes les résultats de mesures (conclusion du paradoxe EPR [34]).

Pour répondre à ces critiques, le premier outil consiste en les inégalités de Bell [17] dont la plus connue est l'inégalité CHSH [29]. Elles permettent de déduire que la physique quantique n'admet pas d'interprétation déterministe locale avec des variables cachées et, n'est donc pas réaliste locale (voir les définitions à la section 3.2 et les explications à la section 3.3). Ainsi, toute théorie déterministe à variable cachée en accord avec la physique quantique, doit-être non locale. Par les violations de ces inégalités (rapport, plus grand que 1, entre la valeur quantique et la borne classique), on conclut donc que les résultats de mesures quantiques ne sont pas, prédéterminés, fixés d'avance, par l'environnement immédiat de la mesure.
Cependant, ces précédents résultats n'impliquent pas nécessairement le caractère indéterminé des issues des mesures quantiques. En effet, il existe des interprétations déterministes mais Non-Locales en accord avec les prédictions de la physique quantique (voir les travaux de Bohm [19]).

Pour aborder directement l'indéterminisme, nous étudions dans un Second temps le théorème de Kochen-Specker [47]. Il montre qu'il est légitime d'affirmer que la physique quantique est effectivement indéterministe. Cela sous l'hypothèse que les résultats des mesures ne soient pas prédéterminés en fonction du contexte (voir la section 3.4).

Enfin, on déduit le caractère indéterministe de presque toutes les mesures quantiques grâce au théorème *Strong Kochen-Specker* (voir Théorème 3.1). Ses implications sont la base théorique de la production d'aléa que nous proposons dans le chapitre 5.

3.2 Définitions

Avant d'entamer le cœur de ce chapitre, nous proposons de s'accorder sur les définitions suivantes. Ces définitions sont données dans [28] par J.F Clauser et A Shimony, auteurs de l'inégalité CHSH. Ces notions sont utilisées comme hypothèses de base dans la déduction des bornes, dans le cadre de la physique classique, des inégalités décrites plus bas.
Nous appelons :

- **Réalisme** (Introduction [28]) : Point de vue philosophique selon lequel les réalités externes sont supposées être existantes et avoir des propriétés définies, indépendamment de l'observation de ces propriétés.

- **Théorie à variables cachées déterministes** (Page 1889 de la référence [28]) : Toute théorie qui postule l'existence d'états pour un système, états pour lesquels les observables quantiques ont toujours une valeur définie.

- **Locale** (Théories locales à variables cachées déterministes) Page 1888 [28]
  Le résultat de mesure d'une particule n'est influencé que par son environnement immédiat.
  Plus précisément :
  Soient deux particules.
  Soient, A la mesure à effectuer sur la première particule, et B celle à effectuer sur la deuxième particule.
  Le résultat de la mesure A de la première particule est noté a, et, le résultat de la mesure B de la deuxième particule est noté b.
  Soit λ un paramètre.
  Ainsi, une fois λ fixé, et les particules séparées, le résultat a ne peut dépendre que de la mesure A sur la première particule et de λ, le paramètre préétabli. Ce résultat ne dépend pas de la mesure B. Et vice versa

- Toute interprétation (ou théorie) déterministe locale en terme de variables cachées de la physique quantique, la ferait rentrer dans le cadre du réalisme local. (Introduction [28])

3.3 Les inégalités de Bell et les tests d'Alain Aspect

3.3.1 Idée

Les écrits de John Bell [17] en 1966 constituent la première avancée majeure permettant de rejeter toute interprétation déterministe Locale (voir section 3.2) en terme de Variables Cachées pour la physique quantique. Nous en déduisons le fait que toute théorie en accord avec les prédictions de la physique quantique doit nécessairement être Non-Locale (voir la discussion Partie 3 [28]).

Pour effectuer sa démonstration, John Bell formalise au travers d'inégalités, les contraintes respectées par toute théorie locale à variables cachées. Les prédictions de la physique quantique, quant à elles, violent ces inégalités.

Pour la vérification pratique, il faut attendre les expériences d'Alain Aspect [15] basée sur l'inégalité CHSH, une simplification des inégalités originelles de Bell.

3.3.2 Cas d'école : CHSH en dimension d=2 ou CHSH-2 [29]

3.3.2.1 Cas Classique (réaliste local)

Considérons le jeu schématisé comme suit

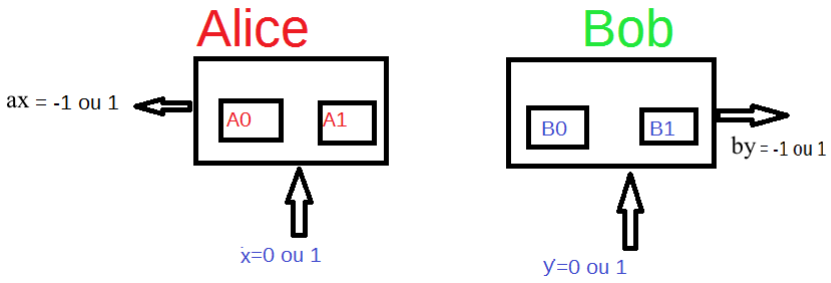

FIGURE 3.1 – Jeu de Bell

Alice choisit aléatoirement (de manière uniforme) $x \in \{0\,,\,1\}$, appuie sur le bouton A_x qui donne à son tour un résultat $a_x \in \{-1\,,\,1\}$. De même chez Bob.

Ils gagnent à ce jeu si $a_x\, b_y = (-1)^{xy}$ dans ce cas ils ont un gain de 1. Dans le cas contraire ils perdent (gain de -1).

On considère ainsi l'entité

$$I = a_0b_0 + a_0b_1 + a_1b_0 - a_1b_1$$

et en particulier à l'espérance :

$$E(I) = E(A_0B_0) \,+\, E(A_0B_1) \,+\, E(A_1B_0) \,-\, E(A_1B_1)$$

Dans le cas de la physique classique (du réalisme local) on obtient l'inégalité suivante :

Inégalité CHSH (Clauser Horne Shimony Holt) 1.
Dans le cadre du réalisme local on a

$$|E(I)| = |E(A_0B_0) + E(A_0B_1) + E(A_1B_0) - E(A_1B_1)| \leq 2 \tag{3.1}$$

Le lecteur pour s'en convaincre peut tester les 16 cas possibles, ou, remarquer que chacun des termes de la somme (3.1) vaut ± 1 et qu'ils sont reliés entre eux.

Mais certaines expériences quantiques sont en contradiction avec cette borne.

3.3.2.2 Cas Quantique

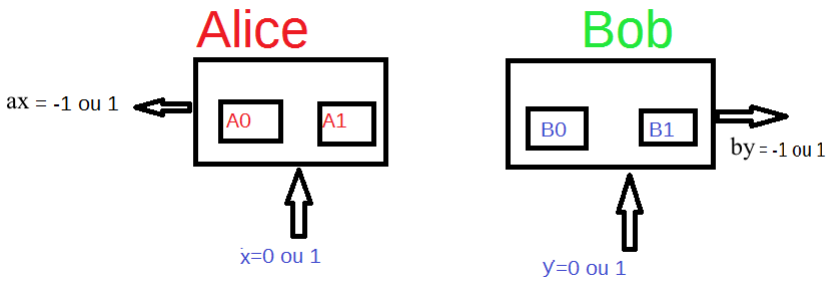

FIGURE 3.2 – Jeu de bell cas quantique

Le **cadre quantique** consiste en ce qui suit. Soient deux parties, Alice et Bob, auxquelles on associe respectivement les espaces de Hilbert $\mathbb{H}_A$ et $\mathbb{H}_B$. Ces deux parties partagent un même système quantique constitué de deux particules (une pour Alice et l'autre pour Bob). Ce système est représenté par l'état $|\phi\rangle \in \mathbb{H}_A \otimes \mathbb{H}_B$. Chaque partie dispose de deux mesures possibles représentées par les observables quantiques A_0, A_1 agissant sur $\mathbb{H}_A$ pour Alice, et B_0, B_1 agissant sur $\mathbb{H}_B$ pour Bob. Ces observables ont pour valeurs propres ± 1.

L'espérance des mesures conjointes d'Alice et de Bob est donnée par

$$E(A_iB_j) = \langle\phi|A_i \otimes B_j|\phi\rangle \tag{3.2}$$

Pour obtenir les différentes corrélations entre les mesures d'Alice et celles de Bob, et ainsi estimer l'espérance $E(I)$ (définie en(3.1)), on répète plusieurs fois l'expérience suivante :

- On tire au hasard (en utilisant de l'aléa publique) $x \in \{0\,,\,1\}$ (respectivement y).
- On effectue la mesure A_x (resp B_y) sur la particule d' Alice (resp Bob).
- On obtient alors le résultat $a_x \in \{-1\,,\,1\}$ (resp b_y).

On estime ainsi la quantité

$$E(I) = E(A_0B_0) \,+\, E(A_0B_1) \,+\, E(A_1B_0) \,-\, E(A_1B_1)$$

Borne de Tsirelson 1. *[27]*
Dans le cadre quantique posé plus haut, nous avons la borne quantique :

$$|E(I)| = |E(A_0B_0) \,+\, E(A_0B_1) \,+\, E(A_1B_0) \,-\, E(A_1B_1)| \leq 2\sqrt{2} \tag{3.3}$$

Avec

$$E(A_iB_j) = \langle\phi|A_i \otimes B_j|\phi\rangle$$

Il faut de plus noter que dans la référence [71], Stephanie Wehner retrouve cette borne quantique à l'aide de la méthode d'optimisation numérique qu'est la Programmation Semi-Definite-Programming (SDP).

Une configuration optimale pour atteindre cette borne quantique de $2\sqrt{2}$ est la suivante :

- Deux particules intriquées constituant un même système dans l'état dit *singlet* : $|\phi\rangle = \dfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.
- Avec les observables :

$$\begin{aligned} A_0 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad A_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ B_0 = \tfrac{1}{\sqrt{2}}(A_0 + A_1) \quad B_1 = \tfrac{1}{\sqrt{2}}(A_0 - A_1) \end{aligned} \tag{3.4}$$

3.3.3 Généralisations des inégalités et remarques

De nombreuses généralisations des inégalités de Bell sont proposées. Elles prennent notamment en compte plus de deux parties [73, 61] ou une dimension des observables $d \geq 2$ [12, 30] . Nous conseillons particulièrement la lecture de la référence [12]. Dans celle ci François Arnault donne un ensemble complet d'inégalités caractérisant les corrélations dans le cadre du réalisme local pour n-parties, 2-observables par parties et en dimension d quelconque.

Il est cependant important de noter que les violations de ces différentes inégalités induites par les expériences de la physique quantique ne font que montrer la non-localité de la physique quantique.

Bien que l'indéterminisme se déduise indirectement sous l'hypothèse que tout déterminisme serait local (et donc la non localité impliquerait l'indéterminisme) , il faut noter qu'il existe des interprétations déterministes mais Non-Locales en accord avec les prédictions de la physique quantique (voir les travaux de Bohm [19]).

Un premier apport direct en faveur de l'indéterminisme de certaines mesures quantiques réside dans le théorème Kochen Specker (voir section 3.4).

3.4 Théorème de Kochen Specker (KS)

Dans cette partie, nous proposons l'étude du théorème Kochen Specker (K.S) [47] qui aide à montrer le caractère indéterminé, et donc aléatoire, des résultats de mesures quantiques. Ce théorème s'attache à montrer qu'**il n'est pas possible, d'attribuer une valeur définie et non contextuelle à toute observable quantique**.
La conclusion généralement acceptée est qu'il existe au moins une observable quantique dont la valeur n'est pas définie d'avance, dont la valeur est indéterminée [1].

Définition 3.1. ***Contexte***
Dans cette section, nous définissons un contexte, suivant la référence [26], comme un ensemble de mesures compatibles. Le terme compatible désigne des mesures qui peuvent être effectuées simultanément ou, de manière équivalente, des mesures dont les observables (représentation matricielle) commutent.

Dans la section suivante (voir section 3.5) nous donnerons une définition plus détaillée, pour le besoin des démonstrations de cette section.

3.4.1 Énoncé

Les auteurs de [47] montrent précisément une contradiction entre les 3 assertions suivantes :

(i) Tout observable a une valeur prédéfinie (bien avant la mesure)

(ii) La valeur définie associée à une observable doit être non-contextuelle, c'est-à-dire indépendante des autres mesures compatibles avec lesquelles elle est effectuée simultanément.

(iii) Les résultats des mesures, pour un ensemble d'observables compatibles, doit être conforme aux prédictions de la physique quantique.

Pour montrer cette contradiction, ils exhibent un ensemble de 117 observables quantiques telles que l'attribution de valeur prédéfinie non contextuelle entraine une contradiction.

Ainsi, vu que les 3 points (i), (ii) et (iii) ne peuvent être simultanément vrais, et que le point (iii) est largement accepté, deux options se présentent :

- Soit (i) est faux. Alors il existe au moins une observable à valeur indéfinie.
- Soit (ii) est faux. Alors, la valeur prédéfinie d'avance dans le passé, associée à une observable, peut être contextuelle, c'est-à-dire dépendante des autres mesures compatibles avec lesquelles elle sera effectuée et donc dépendante du futur.

La conclusion la plus acceptée est le premier choix, c'est-à-dire **rejeter l'assertion (i)**, tout en gardant l'assertion (ii) vraie.

Cela signifie que sous l'hypothèse que les résultats des mesures ne soient pas prédéterminés en fonction du contexte, la physique quantique est effectivement indéterministe.

Il faut noter que le 2ème choix (rejeter l'assertion (ii)) reste une éventualité logiquement correcte analysée par Shimony dans la 3ème partie de la référence [66].

3.4.2 Implications du théorème K.S

En conclusion, la communauté retiendra que la contradiction montrée par le théorème (K.S) implique la négation de l'assertion (i) c'est à dire qu' **au moins l'une des observables quantiques est à valeur indéfinie, aléatoire** (pour un état donné, les résultats de mesure d'au moins une observable sont indéfinis, aléatoires). Du fait du théorème (K.S), la physique quantique est dite contextuelle, par opposition à la valeur définie non-contextuelle prônée par les opposants au formalisme quantique.
Il faut noter, qu'à l'image des inégalités de Bell, il existe des *inégalités contextuelles* (ou de la famille de K.S). Elles ont pour but de rendre ce théorème testable en laboratoire et donc utile aux usages courants de la physique quantique (comme la génération d'aléa). Parmi ces inégalités, nous pouvons citer l'inégalité KCBS [46] basée sur la théorie des graphes, et qui est la base de la sécurité du générateur quantique d'aléa présenté en [32].

3.5 Strong Kochen Specker ou théorème du résultat indéfini

La conclusion acceptée du théorème (KS) est qu'il existe une ou peut être plusieurs observables quantiques à valeur indéfinie. Quelles sont-elles ?

Cette question, détient une importance capitale dans la mesure où on affirme que la physique quantique, du fait de l'indéterminisme de certaines mesures, permet de produire des nombres vraiment aléatoires. Une propriété que ne peut offrir la physique classique. La question naturelle émanant de cette affirmation est donc :

Quelles sont les mesures indéterminées en physique quantique permettant de produire l'aléa vrai ?

Cette section s'attache donc à répondre à cette question par le biais du **théorème des résultats indéfinis** ou valeur indéfinie ou strong Kochen Specker défini en [1] (voir théorème 3.1). De plus, avec la notion de **d-bi-immunité** [6, section 6.1] on lie cet indéterminisme de la physique quantique au caractère aléatoire des nombres qu'elle produit.

3.5.1 Les définitions

Avant d'aborder le coeur des justifications de nos travaux, il est important de s'accorder sur les définitions des termes suivants : Contexte, fonction d'affectation de valeur, fonction admissible.

Soit un entier naturel $d \geq 2$ et $\mathbb{C}^d$, muni de la structure d'espace de Hilbert. Pour un vecteur $|\psi\rangle \in \mathbb{C}^d$, non nul, posons P_ψ le projecteur de dimension 1 relatif à $|\psi\rangle$ défini par

$$P_\psi := \frac{|\psi\rangle\langle\psi|}{|\ \langle\psi|\psi\rangle\ |}$$

Posés de plus

$$O \subseteq \{P_\psi : |\psi\rangle \in \mathbb{C}^d\}$$

un ensemble de projecteurs de dimension 1 sur $\mathbb{C}^d$.

Définition 3.2. *[1, P18]*
Un ensemble $C \subset O$ est un contexte si C possède d éléments et, pour tout P_ψ, $P_\phi \in C$ tels que $P_\psi \neq P_\phi$, on a P_ψ compatible avec P_ϕ

On en déduit la propriété

Propriété 3.1. *Un contexte est un ensemble Maximal de projecteurs de dimension* 1 *mutuellement compatibles.*

La preuve se base sur le lemme suivant :

lemme 3.1. *Les projecteurs P_ψ et P_ϕ, avec $P_\psi \neq P_\phi$, sont compatibles si et seulement si les vecteurs $|\psi\rangle$ et $|\phi\rangle$ sont orthogonaux. Deux vecteurs colinéaires ont le même projecteur.*

Démonstration. P_u et P_h sont compatibles (commutatifs) si et seulement si ils sont diagonalisables dans la même base (orthonormale) B. Cela signifie que $|u\rangle \in B$ et $|h\rangle \in B$ et donc $|u\rangle$ et $|h\rangle$ sont orthogonaux ou confondus. □

Pour achever la preuve de la proposition :

Démonstration. Supposons qu'à chaque projecteur P_ψ on associe un unique vecteur $|\psi\rangle$ ayant pour projecteur P_ψ. Soit $\tilde{C}$ un ensemble contenant $d+1$ projecteurs de dimension 1 mutuellement compatibles (donc plus grand qu'un contexte). Alors, sur la base du lemme précédent, on associe un ensemble de $d+1$ vecteurs mutuellement orthogonaux à $\tilde{C}$. On a donc un ensemble de $d+1$ vecteurs linéairement indépendants dans un espace de dimension d. **Contradiction**. Il ne peut y avoir d'ensemble de projecteurs de dimension 1 mutuellement compatibles plus grand qu'un contexte. □

Remarque 3.1.

- *À tout contexte C correspond un ensemble de vecteurs formant une base de $\mathbb{C}^d$. Il suffit de choisir, pour chaque P_ψ un unique représentant des vecteurs dont il est projecteur.*

- *Cette définition de contexte complète celle apparaissant dans [26] et donnée en définition 3.1 (" un contexte est un ensemble de projecteurs compatibles"). Ici nous considérons l'ensemble maximal.*

Définition 3.3. *[6]*
Une fonction d'attribution de valeur (sur O) est une fonction ***partielle*** $v : O \to \{0,1\}$ *attribuant des valeurs à des projecteurs dans O. La partialité de cette fonction v signifie que $v(P)$ peut être défini (c'est à dire $v(P)$ a toujours la même valeur 0 ou 1) ou indéfinie.*

Définition 3.4. *[6]*
Un projecteur $P \in O$ est à valeur définie (sous la fonction d'attribution de valeur v) si $v(P)$ est définie (égal à 0 ou 1). Autrement, il est à valeur indéfinie (sous v). De même on dira que O est à valeur définie (sous v) si tout projecteur $P \in O$ est à valeur définie

Définition 3.5. ***Admissible*** *[6]*

Soit $v : O \to \{0,1\}$ une fonction d'attribution de valeur. Alors v est admissible si, pour tout contexte C de O, on a

$$\sum_{P \in C} v(P) = 1$$

Autrement dit, seulement un projecteur dans un contexte peut avoir la valeur 1 *sous une fonction admissible.*

3.5.2 Résultat indéfini ou Strong (localised) kochen Specker

" Les résultats de presque toutes les mesures quantiques sont indéfinis" [1, P3]

Les définitions étant établies, énonçons le premier résultat fondamental.

3.5.2.1 Énoncé

Théorème 3.1. *Résultat indéfini ou Strong (Localised) Kochen Specker [1, P32]*
Soit un espace de Hilbert $\mathbb{H}$ *de dimension* $d \geq 3$.
Soient deux états $|\phi\rangle$ *et* $|\psi\rangle$ *de* $\mathbb{H}$ *tels que* P_ϕ *et* P_ψ *ne sont pas compatibles c'est-à-dire* $0 < |\langle\phi|\psi\rangle| < 1$ *(voir lemme 3.1). Alors, on peut trouver un ensemble* O *de projecteurs de dimension 1, contenant* P_ϕ *et* P_ψ *vérifiant l'assertion suivante :*

> *Il n'existe pas de fonction admissible non contextuelle* v *sur* O *telle que* $v(P_\psi) = 1$ *et* v *définie sur* P_ϕ.

Le paragraphe suivant nous permet, par une reformulation de ce théorème, de déduire que presque tous les résultats de mesures quantiques sont indéfinis.

3.5.2.2 Explication et adaptation

Pour déduire du théorème 3.1 (strong KS) le fait que, les résultats de presque toutes les mesures quantiques sont indéfinis, trois hypothèses sont nécessaires. Nous les détaillons ci-après.
Considérons la mesure avec le projecteur P_ψ où $|\psi\rangle \in \mathbb{H}$ et $\mathbb{H}$ un espace de Hilbert. Suivant le troisième postulat de la physique quantique (voir section 2.2), cette mesure correspond à la collection d'opérateurs $\{P_\psi, Id - P_\psi\}$ (avec Id la matrice identité sur $\mathbb{H}$).

Soit O un ensemble de projecteurs de dimension 1 sur $\mathbb{H}$ tel que $P_\psi \in O$.

On considère v_ψ la fonction d'attribution de valeur associée à la mesure avec le projecteur P_ψ :

$$v_\psi : O \to \{0, 1\}$$

telle qu'à tout projecteur P_ϕ elle associe la valeur de la mesure P_ψ sur l'état $|\phi\rangle$.

On considère alors donc les trois hypothèses suivantes :

(I) v_ψ est admissible sur O c'est-à-dire pour tout contexte C de O, on a $\sum_{P \in C} v_\psi(P) = 1$
(II) v_ψ est à valeur définie sur P_ψ et vaut 1.
(III) Toute fonction à valeur définie est non contextuelle.

Théorème 3.2. *Reformulation du théorème 3.1 [6]*
Soient $|\psi\rangle$ et $|\phi\rangle$ deux états de $\mathbb{C}^d$, $d \geq 3$, avec $0 < |\langle\psi|\phi\rangle| < 1$. Si les 3 conditions précédentes (I), (II) et (III) sont respectées alors la projection orthogonale sur P_ψ est à valeur indéfinie sur l'état $|\phi\rangle$ (ou la fonction v_ψ est à valeur indéfinie sur P_ϕ)

De plus, du fait que les observables soient constituées de projecteurs (voir section 2.2), nous déduisons le théorème suivant :

Théorème 3.3. *[4] Presque toutes les observables quantiques sont à valeur indéfinie (pour un état $|\phi\rangle$ fixé).*

Ce théorème, affirmant le caractère indétermininiste de la physique quantique, sert donc de base logique à la génération quantique d'aléa. Cependant il est nécessaire de lier ce caractère indéterministe des mesures au caractère aléatoire des nombres produits.

3.5.3 Relation entre l'indéterminisme et le caractère aléatoire des nombres produits

Pour exhiber cette relation, il nous faut introduire la notion de d-bi-immunité :

Définition 3.6. ***d-bi-immunité** [2]*
Soit $d \geq 2$ un entier. $A_d := \{0, 1, \cdots, d-1\}$ et $A_d^\infty := \{x = x_1 x_2 ...; \quad x_i \in A_d\}$ l'ensemble des séquences infinies sur A_d.
*Une séquence $x \in A_d^\infty$ est dite **d-bi-immune** si pour tout $a \in A_d$, aucun algorithme ne peut générer un nombre infini de paires $(i, x_i = a)$ ou $(i, x_i \neq a)$.*

Les auteurs de [2] montrent que cette propriété est plus forte que la notion classique d'incalculabilité.

Ainsi le caractère aléatoire des nombres générés par les expériences quantiques repose sur ce théorème :

Théorème 3.4. *[2, 6]*

*Toute répétition infinie d'une expérience de mesure par une observable à valeur indéfinie sur $\mathbb{C}^d$ génère toujours une séquence $x \in A_d^\infty$ **d-bi-immune***

Nous avons ainsi présenté les bases théoriques permettant de justifier l'utilisation de la physique quantique pour la production de l'aléa. Étudions ces générateurs quantiques d'aléa.

Chapitre 4

Différents types de générateurs quantiques d'aléa

Mots clés : Device independent, auto tests

Contents

4.1 Objectif et résumé du chapitre

Différents types de générateurs quantiques d'aléa sont répertoriés sur le marché. Nous choisissons la nomenclature suivante :

- Générateurs dont la fiabilité est basée sur la description détaillée des appareils utilisés
- Générateurs dont la fiabilité est basée sur des inégalités quantiques

Dans le cadre de cette thèse, nous choisissons la 2-ème option c'est à dire l'étude approfondie de générateurs, dont la fiabilité est basée sur des inégalités quantiques. Cela permet de s'affranchir de la dépendance à la description détaillée des appareils utilisés et de détecter d'éventuelles erreurs. De plus, nous travaillons ainsi dans un cadre plus formellement établi (voir par exemple (4.3)).

4.2 Générateurs dont la fiabilité est basée sur la description détaillée de l'appareil

4.2.1 Beamsplitter et schémas basiques de génération d'aléa quantique

L'un des moyens basiques de construction de générateur quantique d'aléa est l'utilisation d'une source de lumière et d'un Miroir semi-réfléchissant ou Beamsplitter suivant le schémas ci après (figure 4.1)

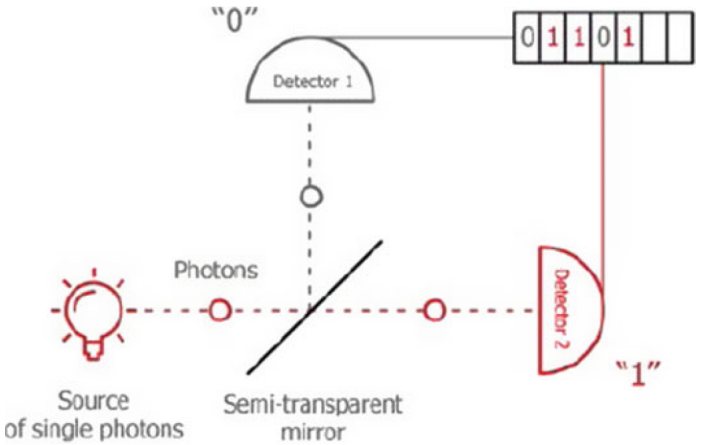

FIGURE 4.1 – QRNG basé sur un photon passant par un Beamsplitter. Le chemin du photon est aléatoire et détermine la valeur du bit de sortie [48]

Dans le schéma (4.1), le photon émis par la source de lumière est aléatoirement transmis ou reflété par le Beamsplitter. Chaque cas produit un bit aléatoire : 1 si le photon est transmis et 0 si le photon est reflété.

C'est ainsi le principe de base de la génération d'aléa à l'œuvre dans divers appareils de génération quantique d'aléa dont le populaire Quantis [42] de ID Quantique à Genève.

4.2.2 Autres méthodes

Bien d'autres principes de la physique quantiques sont à l'œuvre dans la production d'aléa. Le tableau suivant nous donne un aperçu de ces méthodes, ainsi que les références pour une description plus détaillée.

Méthode basée sur la description détaillée de l'appareil	Références détaillées
Beamsplitter	[42]
bruit quantique	[5]
Radioactivité	[41]
Raman scattering	[25]
Non optic quantum effects	[60]

TABLE 4.1 – Différents types de générateurs quantiques basés sur la description détaillée des appareils utilisés.

Un exemple assez prometteur est celui du générateur quantique utilisant un téléphone portable. Il est basé sur le bruit quantique, plus précisément, l'instant aléatoire d'émission du photon sur les capteurs de l'appareil photo [65]

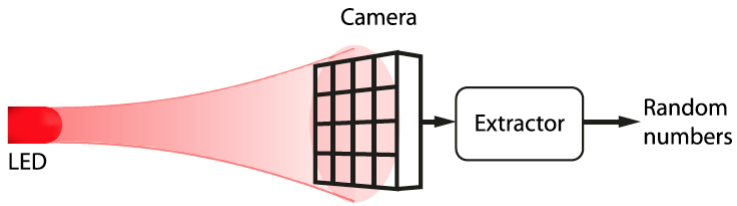

FIGURE 4.2 – Exemple de générateur quantique d'aléa utilisant un téléphone portable [65]

Mais cependant, il reste ardu, pour ces types de générateurs, de faire la distinction entre : l'aléa originel provenant du processus quantique, et les incertitudes qu'introduisent les imperfections des mesures. Ces incertitudes peuvent aussi être du fait d'intrusions malveillantes.

Ainsi donc, dans le cadre de **cette thèse**, nous choisissons plutôt l'étude des générateurs dont la fiabilité est basée sur des **inégalités quantiques**. Ces inégalités permettent de

détecter d'éventuelles erreurs et même, des intrusions malveillantes. L'exemple suivant (4.3.1) peut, à juste titre, être appelé l'exemple fondateur de cette thèse.

4.3 Générateurs dont la fiabilité est basée sur des inégalités quantiques

Nous proposons, dans cette sous partie, l'étude de générateurs quantiques dont la sécurité repose sur des inégalités quantiques. Ces inégalités font intervenir, pour la plupart, des produits d'observables quantiques **commutatives**. Les violations de ces inégalités rendent manifeste une propriété quantique particulière (comme la non localité). Elles permettent ainsi d'attester d'un taux d'erreur en dessous d'un seuil fixé. Cela aide à prévenir d'éventuelles intrusions malveillantes qui, nécessairement, introduirait des erreurs dans l'exécution du protocole. Il faut de plus noter, comme l'explique Zoé AMBLARD [7, Partie 2.4.4], qu'une plus grande violation d'inégalités quantiques permet une plus grande résistance aux bruits introduits par des attaquants.
NB : La preuve de cette dernière affirmation est explicitement faite dans le cadre de protocoles de distribution de clé quantique utilisant des particules intriqués.

4.3.1 Générateur *indépendant du système*

Définition 4.1. *[62, page 18]*
Le terme indépendant du système (device independant ou DI) signifie que la description du protocole est indépendante des appareils utilisés. Seule les trois hypothèses suivantes sont faites :

1. *Fonctionnement quantique du système (Les 4 axiomes de la physique quantique).*
2. *Le choix des mesures à effectuer est aléatoire et inconnu des appareils de mesure avant la mesure. Il n'est connu que juste au moment de la mesure.*
3. *Localité : les appareils sont séparés et ne communiquent pas pendant une étape donnée. De plus, les entrées x ne sont introduites que dans l'appareil A d'Alice, et, de même, les entrées y seulement dans l'appareil B de Bob.*

De plus, et même le plus important, un moyen formel est établi pour détecter d'éventuelles erreurs ou intrusions d'attaquants. Il s'agit de l'utilisation d'inégalités de Bell (défini en section 3.3). Lorsque ces inégalités ne sont pas violées au delà d'un certain seuil, la certitude est alors donnée de la présence d'erreurs dans l'exécution du protocole.
Dans ce cadre, nous proposons l'étude de l'exemple significatif qu'est le générateur d'aléa proposé par Pironio et compagnie dans [62]. On peut modéliser le dispositif comme suit :

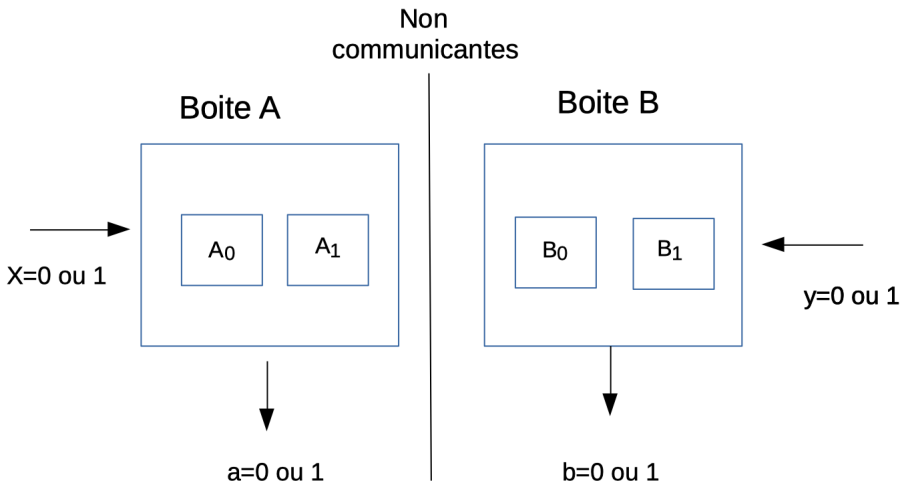

FIGURE 4.3 – Schémas de génération d'aléa certifié par les inégalités de Bell [62]

Le schémas de génération quantique d'aléa proposé par les auteurs de [62] est celui du jeu de Bell exposé à la section 3.2

La quantité de Bell E(I) est alors évaluée comme suit :

$$|E(I)| = |E(A_0 \otimes B_0) + E(A_0 \otimes B_1) + E(A_1 \otimes B_0) - E(A_1 \otimes B_1)| = 2\sqrt{2} > 2$$

NB : Le produit tensoriel utilisé dans l'inégalité est équivalent à l'utilisation de produit d'observables compatibles [58, partie 6.1] dans le cadre d'espaces de dimension finie. Dans notre cas, le produit tensoriel $A_i \otimes A_j = \tilde{A}_i \tilde{A}_j$ avec $\tilde{A}_i = A_i \otimes Id$ et $\tilde{A}_j = Id \otimes A_j$ où Id est l'identité sur l'espace concerné.

Cette évaluation permet de rendre le protocole ainsi détaillé indépendant du système (Device Independant DI). En effet, on a une relation analytique qui relie la qualité d'aléa produit (l'entropie) à la violation de Bell constatée :

$$H(AB|XY) \geq H_\infty(AB|XY) \geq 1 - log_2(1 + \sqrt{2 - \frac{I^2}{4}}) \tag{4.1}$$

Et, d'après cette relation, plus la quantité de Bell est proche de sa valeur maximale $2\sqrt{2}$, plus l'entropie se rapproche de sa valeur maximale 1. Ainsi, le fait d'atteindre, après évaluation de la quantité de Bell, la valeur maximale $2\sqrt{2}$, est une assurance sur le fait que l'entropie de l'expérience est maximale. À contrario, le fait de ne pas atteindre la violation maximale est une preuve d'éventuelles erreurs ou intrusions malveillantes.

La sécurité de ce protocole ne repose donc plus sur la description détaillée de l'appareil, mais plutôt sur la violation de l'inégalité de Bell c'est à dire sur le caractère **Non Local de la physique quantique**. Cela est le gage d'une entropie adéquate.
Cependant cette sécurité (device independent) est garantie sous les hypothèses de la définition 4.1.

4.3.2 Générateurs auto-tests

À l'image de la propriété *indépendant du système*, d'autres cadres de certification, basés sur des inégalités quantiques, peuvent être utilisés pour la sécurité des protocoles. C'est le cas du cadre *auto-test* (self-testing). Ce sont des propriétés plus faibles que la propriété "DI", qui, bien que basées sur des violations des inégalités quantiques, ont des hypothèses supplémentaires sur les appareils utilisés. C'est le cas du protocole auto-test (self-testing) présenté dans la référence [55]. Dans ce cadre, des hypothèses supplémentaires sont faites sur le système (Dans ce cas, l'hypothèse de la localité n'est pas faite). En effet, en plus du fonctionnement quantique du système et du choix aléatoire des mesures à effectuer, on suppose également :

1. L'état interne des appareils (de mesure et de préparation de l'état) n'est pas modifié pendant les différentes exécutions.
2. Indépendance entre l'appareil de préparation d'état et celui de mesure d'état.
3. Contraintes sur la dimension de l'espace des états.

Nous pouvons aussi citer le protocole de la référence [68] dont la sécurité est basée sur la violation de **l'inégalité contextuelle KCBS**. Cette dernière inégalité fait également intervenir des contextes c'est à dire des produits d'observables commutatives.

Aux termes de ce chapitre, nous avons donné un aperçu des différentes techniques de production quantique d'aléa. Partant des systèmes dont la sécurité repose sur la description détaillée des appareils utilisés, nous avons abouti aux systèmes dont la sécurité est plus formelle. Cette dernière sécurité repose sur des inégalités quantiques dont les violations, en dessous d'un certain seuil, permettent la détection d'éventuelles erreurs pouvant être du fait d'attaquants. Nous retenons de plus, comme l'explique l'auteur de [7], qu'une violation plus importante d'inégalités quantiques permet une meilleure résistance au bruit (cette analyse est prouvée dans le cadre des protocoles de distribution de clés quantiques utilisant des particules intriquées).

Or, les auteurs de [22] nous montrent qu'avec les observables non commutatives, il est possible d'atteindre des valeurs de violations des inégalités quantiques plus grandes que celles atteintes avec des observables commutatives. Ainsi nos différents travaux de thèse explorent l'emploi des observables non commutatives et leurs potentiels apports pour une meilleure sécurité de la production quantique d'aléa.

Deuxième partie

Apport des produits d'observables non commutatives

Chapitre 5

Inégalités basées sur des observables non commutatives et protocoles engendrés

Mots clés : *SDP, Réalisme macroscopique, cadre quantique non commutatif*

Contents

Les travaux présentés dans ce chapitre ont fait l'objet de poster notamment à Qcrypt 2020 (voir la liste des contributions dont le lien est donné en note de bas de page [1])

5.1 Objectif et résumé du chapitre

Dans le cadre de cette thèse, notre objectif est l'utilisation de produits de mesures potentiellement non commutatives. Nous le faisons pour produire de l'aléa dont la sécurité est basée sur des **violations plus grandes** d'inégalités, dans la perspective d'une meilleure résistance aux bruits et donc aux attaques comme c'est le cas pour les protocoles de distribution de clé quantique (QKD) [7, Partie 2.4.4].

Dans ce chapitre, pour la sécurité des protocoles que nous proposons, nous dérivons, à partir d'expressions déjà présentes dans la littérature (CHSH-2 [29] et CHSH-3 [30]), des inégalités faisant intervenir des observables quantiques non commutatives. De plus elles portent sur une seule partie.

5.1.1 Cadre de la physique classique

Dans ce cadre d'une seule partie, les bornes en physique classique des expressions que nous dérivons, ne sont plus obtenues sous l'hypothèse du réalisme local. Elles sont plutôt obtenues selon la **Notion de Réalité au niveau macroscopique** donnée par les auteurs de [52] (et aussi utilisée par les auteurs de [22] comme cadre classique des inégalités temporelles) :

Définition 5.1.

*La **Notion de Réalité au niveau macroscopique** implique les deux hypothèses suivantes :*

(A_1) *Les résultats de mesure sont prédéfinis (d'avance avant mesure) : Réalisme Macroscopique.*

(A_2) *Les résultats de mesure ne sont influencés par aucune mesure : Mesures non-invasives.*

Le cadre du réalisme local et celui défini par la notion de réalité au niveau macroscopique diffèrent en ces deux points :

- L'hypothèse de la localité, n'est pas nécessaire dans le cadre de la réalité au niveau macroscopique car il est défini dans le cas d'une seule partie.

1. item 90 https://2020.qcrypt.net/accepted-papers/#list-of-accepted-contributed-talks

- La notion de réalité au niveau macroscopique fait **explicitement** l'hypothèse que les résultats de mesures ne sont pas influencés par la mesure effectuée (mesures non invasives).

Dans ce cadre classique ainsi explicité, pour les inégalités que nous étudions (CHSH-2, CHSH-3) nous obtenons les mêmes bornes que dans le cadre du réalisme local.

5.1.2 Cadre de la physique quantique

Le cadre quantique est ici le cadre quantique non commutatif défini par :

Définition 5.2. *Le premier cadre quantique non commutatif est construit sur les hypothèses suivantes :*

- *Les 4 postulats de la physique quantique (voir partie 2.2 [59]). Nous utilisons en particulier le premier postulat, relatif aux états d'une seule particule, et le troisième postulat, relatif aux mesures (voir section 2.1).*
- *La possibilité de produits d'observables potentiellement non commutatives. (comme le font les auteurs des inégalités temporelles [22])*
- *Les fonctions de corrélation considérées sont de la forme*

$$\langle\phi|X_iX_j|\phi\rangle \tag{5.1}$$

avec $|\phi\rangle$ un état quantique et X_i, X_j des observables quantiques non nécessairement commutatives.

Dans ce cadre quantique, nous obtenons des bornes plus grandes que celles obtenues dans le cadre classique. Ce sont des **Violations de la physique classique**.

De plus, ces bornes sont égales et même plus grandes que dans le cadre quantique où nous n'autorisons que des produits d'observables commutatives.

5.1.3 Interprétation, avantages et limites

Ces violations de la borne classique, dans ce cadre quantique non commutatif, montrent que la **notion de réalité au niveau macroscopique** n'est pas applicable au monde microscopique de la physique quantique. On en déduit que :

- Soit les résultats de mesure ne sont pas prédéfinis (d'avance avant mesure).
- Soit les résultats de mesure sont prédéfinis mais influencés par les mesures effectuées.

Le théorème du résultat indéfini (voir Strong KS, théorème 3.1) nous permet de déduire que les résultats de mesure ne sont pas prédéfinis. De ce fait, la **violation des inégalités** que nous proposons est **une conséquence du caractère indéterminé des résultats** de mesure quantique.

L'avantage majeur de l'utilisation de produits d'observables non commutatives est la possibilité de violations quantiques plus grandes. Et cela, pourrait être utilisé comme arguments pour une meilleure sécurité (résistance aux bruits et donc aux attaques) comme c'est le cas pour les protocoles de distribution de clé quantique (QKD) [7, Partie 2.4.4]. Ainsi, ces inégalités aident à vérifier les protocoles que nous développons dans le cadre de cette thèse.

Une limite de ces travaux, réside dans le sens physique à donner aux fonctions de corrélations (5.1) optimisées. En effet, dans le cadre de produits de mesures commutatives, avec X_i et X_j les projecteurs sur des résultats de mesure, la quantité (5.1) correspond à la probabilité d'obtenir ces résultats (voir section 5.3.2 pour plus d'explications). Mais cela n'est pas le cas dans le cadre non commutatif.

Pour remédier à ces limites de nos travaux, nous proposons dans le chapitre 6, l'utilisation des inégalités temporelles. Pour ces dernières, les fonctions de corrélations, faisant intervenir des produits d'observables non commutatives ont un sens physique.

Une dernière perspective réside dans une preuve formelle selon laquelle, comme dans le cas des protocoles de distribution de clé quantique utilisant des particules intriquées, une meilleure violation des inégalités est vraiment gage d'une meilleure sécurité pour nos protocoles de génération d'aléa n'utilisant qu'une seule particule.

5.2 Cas particulier de variante non-commutative de l'inégalité CHSH-2 en dimension $d = 3$ (poster TQC 2020)[14]

Dans cette section, nous proposons une variante de l'inégalité CHSH-2 [29], faisant intervenir un **cas particulier de produits d'observables non commutatives**. Ce cas particulier de mesures non-commutatives est choisi pour avoir une extension directe

- des propriétés à l'oeuvre pour 2 qubits
- à cette fois-ci un seul qutrit (particule pouvant être dans 3 états possibles c'est à dire $d = 3$).

Ce passage permet, de bénéficier du **cadre formel du théorème du résultat indéfini** (voir Strong KS théorème 3.1). Ce dernier théorème permet de déduire qu'en dimension $d \geq 3$, les résultats des mesures de "presque" toutes les observables quantiques sont indéterminés (voir théorème 3.3).
La première partie de cette section consiste en la caractérisation des qutrits en terme de biphotons, c'est à dire des paires de photons indistinguables. Ensuite, nous procédons à l'étude de l'opérateur de symétrisation "Γ" permettant de transférer la violation du cadre des qubits à celui d'un seul qutrit. Nous déduirons enfin, dans ce cadre de mesures potentiellement non commutatives, l'expression de l'inégalité CHSH-2 pour un unique qutrit, ainsi que les propriétés essentielles. Celle-ci permet la génération d'aléa que on évalue grâce à une vérification d'état équivalent à la violation de l'inégalité CHSH-2 ci dessus.

5.2.1 Implémentation des qutrits avec des biphotons

Un qutrit est un objet physique modélisé par un vecteur de $\mathbb{C}^3$. Ces objets ont de nombreux avantages sur les qubits en terme de stockage de l'information. Entre autres exemples, ils conduisent à des inégalités de Bell plus résistantes aux bruits [43]. De plus, les auteurs de [3, 6] démontrent de manière formelle le caractère indéterminé des mesures quantiques pour des particules de dimension $d \geq 3$. Dans la pratique, les qutrits peuvent être implémentés par des particules de spin 1. Néanmoins, nous avons le plus souvent recours à des paires de photons indistinguables (biphotons) [24]. Les auteurs de [53] donnent une équivalence entre ces deux implémentations.
L'implémentation des qutrits à l'aide des biphotons se base sur le sous-espace symétrique défini comme suit :

> Soit l'état singlet donné par $|\psi\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$. Le sous-espace orthogonale à $|\psi\rangle$ est engendré par les vecteurs

$$|00\rangle, \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |11\rangle \tag{5.2}$$

Ces vecteurs, ainsi que chacun des vecteurs qu'ils engendrent, restent invariants par permutation des deux particules. L'espace ainsi décrit est l'espace des biphotons (ou photons symétriques) noté :

$$Sym(\mathbb{C}^2 \otimes \mathbb{C}^2) = \quad Vect\{|00\rangle, \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |11\rangle\} \tag{5.3}$$

Ces vecteurs de base peuvent être respectivement réécrits

$$|+\rangle, \quad |0\rangle, \quad |-\rangle$$

Ainsi donc, l'espace de deux qubits indistinguables est en bijection avec l'espace d'un seul qutrit : $Sym(\mathbb{C}^2 \otimes \mathbb{C}^2) \simeq \mathbb{C}^3$.

En règle générale, les transformations effectuées sur un qutrit sont modélisées par les opérateurs du groupe $SU(3)$. Mais cependant, les opérateurs de spin, faisant intervenir le groupe $SU(2)$, sont plus communs car plus faciles à implémenter. (Ils sont réalisés à l'aide d'éléments d'optique linéaire agissant sur des biphotons).

5.2.2 Symétrisation

Les auteurs de [50] définissent une application linéaire permettant de transformer les opérateurs sur un seul qubit en opérateurs sur un qutrit implémenté par des biphotons. Cette application va de l'ensemble des opérateurs sur un qubit (l'ensemble des opérateurs unitaires sur $\mathbb{C}^2$ nommé $U(2)$) vers l'ensemble des opérateurs sur une paire symétrique de qubits (que nous nommons $B = \{\text{Opérateurs sur } Sym(\mathbb{C}^2 \otimes \mathbb{C}^2) \simeq \mathbb{C}^3\}$) :

$$\begin{array}{rccl} \Gamma: & U(2) & \to & B \\ & V & \mapsto & \Gamma(V) = \frac{1}{2}(V \otimes I + I \otimes V) \end{array} \tag{5.4}$$

où l'opérateur $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est l'identité sur $\mathbb{C}^2$ Ainsi, pour un opérateur $V := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a

$$\Gamma(V) = \frac{1}{2}\begin{pmatrix} 2a & b & b & 0 \\ c & a+d & 0 & b \\ c & 0 & a+d & b \\ 0 & c & c & 2d \end{pmatrix}$$

De manière plus usuelle, elle s'écrit, dans la base de Qutrit ($|+\rangle$, $|0\rangle$, $|-\rangle$) : $\Gamma(V) = \frac{1}{\sqrt{2}}\begin{pmatrix} \sqrt{2}a & b & 0 \\ c & \frac{\sqrt{2}}{2}(a+d) & b \\ 0 & c & \sqrt{2}d \end{pmatrix}$ où la dernière matrice est obtenue par changement de base c'est à dire qu'on exprime l'image par $\Gamma(V)$ de $|+\rangle$, $|0\rangle$, $|-\rangle$ dans la base canonique de deux qubits. Puis nous réexprimons le tout dans la base d'un seul qutrit ($|+\rangle$, $|0\rangle$, $|-\rangle$).

Chacun des opérateurs $\Gamma(V) \in B$ a pour vecteurs propres $|v_\varepsilon\rangle \otimes |v_\eta\rangle$, relatifs aux valeurs propres $\frac{1}{2}(\varepsilon + \eta) \in \{-1, 0, 1\}$; avec $|v_\varepsilon\rangle$, $|v_\eta\rangle$ vecteurs propres de V pour les valeurs propres $\varepsilon, \eta \in \{\pm 1\}$.

5.2.3 CHSH-2 pour Qutrit

L'expression ici considérée est la suivante

$$\langle\psi|\Gamma(A_1)\Gamma(B_1) + \Gamma(A_1)\Gamma(B_2) + \Gamma(A_2)\Gamma(B_1) - \Gamma(A_2)\Gamma(B_2)|\psi\rangle \tag{5.5}$$

5.2.3.1 Borne classique

Il faut noter que dans le cadre de la physique classique c'est à dire sous l'hypothèse de la réalité au niveau macroscopique (défini plus haut) la borne classique est :

$$B_c = 2 \tag{5.6}$$

En effet, l'équation (5.5) se réécrit :

$$E(\Gamma(A_1)\Gamma(B_1)) + E(\Gamma(A_1)\Gamma(B_2)) + E(\Gamma(A_2)\Gamma(B_1)) - E(\Gamma(A_2)\Gamma(B_2))$$

Or, dans le cadre classique défini à la section 5.1.1, la mesure $\Gamma(A_i)$ sur l'état, a une valeur fixe α_i et ne modifie pas l'état. Ainsi, on réécrit l'équation (5.5) :

$$E(\alpha_1\beta_1) + E(\alpha_1\beta_2) + E(\alpha_2\beta_1) - E(\alpha_2\beta_2)$$

avec α_i, β_j des scalaires dans l'ensemble $\{-1,\ 0,\ 1\}$. Nous sous-entendons ainsi que les mesures sont effectuées l'une à la suite de l'autre $\Gamma(B_j)$ suivi de $\Gamma(A_i)$. On obtient alors la borne classique de 2, qui est la même borne classique que celle de l'inégalité habituelle de CHSH-2.

5.2.3.2 Valeur Quantique

Nous travaillons ici dans le cadre quantique exposé dans la définition 5.2. La particularité de cette expression réside dans le fait qu'elle fasse intervenir des produits d'observables potentiellement non commutatives formés d'observables $\Gamma(A_i)$ et $\Gamma(B_j)$ qui sont des extensions en dimension $d = 3$ d'observables A_i, B_j agissant en dimension $d = 2$. Dans ce cadre particulier de la physique quantique, la valeur quantique maximale est

$$B_q = 2\sqrt{2}$$

Cette valeur, qui correspond à la borne quantique de l'expression habituelle de CHSH-2 est atteinte pour l'état symétrique $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ou de manière équivalente avec le qutrit $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$. Les observables qui le permettent sont les suivantes :

- $\Gamma(A_1) = S_Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ représentée en dimension $d = 3$ avec $A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- $\Gamma(A_2) = S_X = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ avec $A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $\Gamma(B_1) = \frac{\Gamma(A_1)+\Gamma(A_2)}{\sqrt{2}}$ avec $B_1 = \frac{A_1+A_2}{\sqrt{2}}$
- $\Gamma(B_2) = \frac{\Gamma(A_1)-\Gamma(A_2)}{\sqrt{2}}$ avec $B_2 = \frac{A_1-A_2}{\sqrt{2}}$

5.2.4 Protocole déduit (Favor)

Dans cette section, nous proposons un protocole de génération d'aléa utilisant un seul qutrit. Dans ce cadre des qutrits, le théorème Strong Kochen Specker (voir 3.1) démontre le caractère (vraiment) aléatoire des résultats des mesures quantiques. De plus, ce protocole permet d'atteindre l'entropie maximale de 1 trit pour chaque trit produit. Son bon fonctionnement est évalué par une vérification d'état qu'on peut lier à l'inégalité CHSH-2 pour un qutrit, développée dans la section précédente (voir 5.2.3).

5.2.4.1 Exécution du protocole

1. On prépare la particule dans l'état $|\psi\rangle = \frac{1}{\sqrt{3}}(\xi|+\rangle + |0\rangle + \xi^3|-\rangle)$, avec $\xi = exp(i\pi/4)$. (voir explications au prochain paragraphe 5.2.4.2)

2. À l'aide d'une source d'aléa publique (celle du NIST [2]), on sélectionne une mesure parmi S_X, S_Y, S_Z avec $S_X = \frac{1}{\sqrt{2}}\begin{pmatrix}0&1&0\\1&0&1\\0&1&0\end{pmatrix}$, $S_Y = \frac{1}{\sqrt{2}}\begin{pmatrix}0&-i&0\\i&0&-i\\0&i&0\end{pmatrix}$, $S_Z = \begin{pmatrix}1&0&0\\0&0&0\\0&0&-1\end{pmatrix}$

3. La mesure donne le trit aléatoire $a_i \in \{1, \omega, \omega^2\}$ avec equiprobabilité $\frac{1}{3}$ (voir explications au prochain paragraphe 5.2.4.2).

4. Test de vérification d'état : On vérifie que l'état effectivement utilisé $|\phi_{used}\rangle$ est l'état $|\phi\rangle$ du premier item, grâce à l'espérance :

$$\langle\phi_{used}|S_p^2|\phi_{used}\rangle = 0; \quad \text{avec } S_p = \frac{1}{\sqrt{3}}\begin{pmatrix}1&-\xi&0\\-\xi^*&0&-\xi\\0&-\xi^*&-1\end{pmatrix}; \text{ et } \xi = exp(i\pi/4) \tag{5.7}$$

   Ce test de vérification d'état est lié à l'inégalité CHSH-2 développée à la section 5.2 (voir explications au prochain paragraphe 5.2.4.2)

5.2.4.2 Explications et vérification du protocole

L'état $|\psi\rangle = \frac{1}{\sqrt{3}}(\xi|+\rangle + |0\rangle + \xi^3|-\rangle)$ est non-biaisé pour les mesures S_X, S_Y, S_Z c'est à dire que chacune de ces mesures, effectuée sur cet état, donne le résultat 1 ou ω ou ω^2 avec probabilité $\frac{1}{3}$.

De plus, le bon fonctionnement du protocole est évalué par la vérification d'état reposant sur la propriété suivante :

Propriété 5.1. $\langle\phi_{used}|S_p^2|\phi_{used}\rangle = 0$ *si et seulement si*

$$|\phi_{used}\rangle = |\phi\rangle = \frac{1}{\sqrt{3}}(\xi|+\rangle + |0\rangle + \xi^3|-\rangle)$$

Pour tout autre état $|\phi_{used}\rangle \neq |\phi\rangle$, *on a* $\langle\phi_{used}|S_p^2|\phi_{used}\rangle > 0$

2. https ://csrc.nist.gov/projects/interoperable-randomness-beacons

Démonstration. S_p est un opérateur hermitien ce qui équivaut à $S_p^\dagger = S_p$ d'où

$$\begin{aligned} \langle \phi_{used} | S_p^2 | \phi_{used} \rangle &= \langle \phi_{used} | S_p^\dagger S_p | \phi_{used} \rangle \\ &= \| S_p | \phi_{used} \rangle \| \geq 0 \end{aligned} \tag{5.8}$$

Vu que les valeurs propres de S_p sont $\{-1, 0, 1\}$ et que $|\phi\rangle$ est vecteur propre pour 0, on déduit la propriété

□

Cette évaluation de l'espérance $\langle \phi_{used} | S_p^2 | \phi_{used} \rangle$ est équivalente [14, P3] à l'évaluation de l'expression CHSH-2 suivante :

$$CHSH(U,V) := U \, \frac{U+V}{\sqrt{2}} + U \, \frac{U-V}{\sqrt{2}} \; + V \, \frac{U+V}{\sqrt{2}} \; - V \, \frac{U-V}{\sqrt{2}} \tag{5.9}$$

Avec U, V et S_p des images par Γ d'opérateurs sur les qubits et vérifiant U, V et S_p mutuellement orthogonaux.

Nous avons ainsi montré une première dérivation d'inégalité quantique autorisant l'utilisation d'observables non commutative en dimension $d = 3$. Le fait d'étendre la dimension à un qutrit nous permet de bénéficier de la propriété des résultats indéfinis des mesures quantiques.

5.3 Inégalité CHSH-3 et sa variante non commutative Free-CHSH-3 (Poster Qcrypt 2020)

Le but de ces travaux est de déduire, au travers d'une inégalité sur les qutrits et autorisant des produits d'observables non commutatives, une borne quantique plus grande que dans le cadre quantique restreint aux observables commutatives. Cette violation plus grande permet de vérifier le bon fonctionnement du protocole de génération de nombre aléatoire que nous proposons : pour tous les observables et états permettant une violation maximale de l'inégalité, nous avons une entropie maximale. De plus, nous donnons des arguments d'auto-test, en ce sens que l'entropie est maximale si et seulement si la violation de l'inégalité est maximale.
Cependant, du fait du manque de réalité physique derrière les coefficients optimisés, notre méthode pour les estimer semble incomplète. Il s'en suit la nécessité, pour atteindre la propriété Self-Testing, de supposer ces coefficients réels.

Cette propriété n'est atteinte que sous l'hypothèse que les coefficients de corrélations entre les mesures sont réels. Deux pistes d'améliorations peuvent donc être proposées :

- Soit améliorer l'évaluation de l'inégalité
- Soit changer de type d'inégalité

5.3.1 Inégalité originelle CHSH-3

Les auteurs de [30] proposent une généralisation, CGLMP-d, de l'inégalité CHSH-2. Celle-ci fait intervenir 2 parties Alice et Bob, chacune pouvant effectuer 2 mesures. Les variables aléatoires A_1 et A_2 représentent les mesures d'Alice et, B_1 et B_2 celles de Bob. À la différence de CHSH-2, ces mesures ont d résultats possibles, avec $d \geq 2$.
En dimension $d = 3$, les mesures A_i et B_j (avec $i, j \in \{1, 2\}$) admettent comme résultats possibles : $1, \omega, \omega^2$ avec $\omega = exp(2i\pi/3)$, racine cubique de l'unité. On nomme alors l'expression **CHSH-3** [30, équation 5] l'expression suivante :

$$\begin{aligned} I_3 =& P(A_1 = B_1) + P(A_2 = \omega^2 B_1) + P(A_2 = B_2) + P(A_1 = B_2) \\ & - P(A_1 = \omega^2 B_1) - P(A_2 = B_1) - P(A_2 = \omega^2 B_2) - P(A_1 = \omega B_2) \end{aligned} \tag{5.10}$$

Dans le cadre de la physique classique, sous l'hypothèse du réalisme local, l'inégalité CHSH-3 stipule que :

$$I_3 \leq 2 \tag{5.11}$$

Ainsi, en faisant intervenir les probabilités conjointes d'Alice et Bob dans l'expression

(5.10), on obtient

$$\begin{aligned} I_3 = & P(1,1|A_1B_1) + P(\omega,\omega|A_1B_1) + P(\omega^2,\omega^2|A_1B_1) + P(\omega^2,1|A_2B_1) \\ & + P(1,\omega|A_2B_1) + P(\omega,\omega^2|A_2B_1) + P(1,1|A_2B_2) + P(\omega,\omega|A_2B_2) \\ & + P(\omega^2,\omega^2|A_2B_2) + P(1,1|A_1B_2) + P(\omega,\omega|A_1B_2) + P(\omega^2,\omega^2|A_1B_2) \\ & - P(1,\omega|A_1B_1) - P(\omega,\omega^2|A_1B_1) - P(\omega^2,1|A_1B_1) - P(1,1|A_2B_1) \\ & - P(\omega,\omega|A_2B_1) - P(\omega^2,\omega^2|A_2B_1) - P(1,\omega|A_2B_2) - P(\omega,\omega^2|A_2B_2) \\ & - P(\omega^2,1|A_2B_2) - P(\omega,1|A_1B_2) - P(\omega^2,\omega|A_1B_2) - P(1,\omega^2|A_1B_2) \end{aligned} \tag{5.12}$$

où $P(\omega^k,\omega^\ell|A_i,B_j)$ désigne la probabilité conjointe qu'Alice obtienne ω^k et Bob ω^ℓ, ayant respectivement effectué les mesures A_i et B_j (avec $i,j \in \{1,2\}$ et $k,\ell \in \{0,1,2\}$).

Soit le cadre quantique commutatif défini par :

Définition 5.3. *Cadre quantique commutatif est construit sur les hypothèses suivantes :*

- *Les 4 postulats de la physique quantique (voir partie 2.2 [59]). Nous utilisons en particulier le premier postulat, relatif aux états d'une seule particule, et le troisième postulat, relatif aux mesures (voir section 2.1).*
- *Seulement les produits d'observables commutatives*
- *Les fonctions de corrélation considérées sont de la forme*

$$\langle\phi|X_iX_j|\phi\rangle \tag{5.13}$$

avec $|\phi\rangle$ un état quantique et X_i, X_j des observables quantiques nécessairement commutatives (X_i commute avec X_j).

Dans ce cadre quantique commutatif, A_1, A_2, B_1 et B_2 sont des observables agissant sur un espace de Hilbert de dimension $d = 3$, avec comme valeurs propres $1, \omega, \omega^2$. Les vecteurs propres correspondant sont désignés par $|a_{i,1}\rangle, |a_{i,\omega}\rangle, |a_{i,\omega^2}\rangle$ pour A_i, $i = 1, 2$, de même pour B_1, B_2. On obtient ainsi les projecteurs,

$$\tilde{A}_{1,1} = |a_{1,1}\rangle\langle a_{1,1}| \quad \tilde{A}_{1,\omega} = |a_{1,\omega}\rangle\langle a_{1,\omega}| \quad \tilde{A}_{1,\omega^2} = |a_{1,\omega^2}\rangle\langle a_{1,\omega^2}|$$

$$\tilde{A}_{2,1} = |a_{2,1}\rangle\langle a_{2,1}| \quad \tilde{A}_{2,\omega} = |a_{2,\omega}\rangle\langle a_{2,\omega}| \quad \tilde{A}_{2,\omega^2} = |a_{2,\omega^2}\rangle\langle a_{2,\omega^2}|$$

$$\tilde{B}_{1,1} = |b_{1,1}\rangle\langle b_{1,1}| \quad \tilde{B}_{1,\omega} = |b_{1,\omega}\rangle\langle b_{1,\omega}| \quad \tilde{B}_{1,\omega^2} = |b_{1,\omega^2}\rangle\langle b_{1,\omega^2}|$$

$$\tilde{B}_{2,1} = |b_{2,1}\rangle\langle b_{2,1}| \quad \tilde{B}_{2,\omega} = |b_{2,\omega}\rangle\langle b_{2,\omega}| \quad \tilde{B}_{2,\omega^2} = |b_{2,\omega^2}\rangle\langle b_{2,\omega^2}|$$

Ainsi, l'opérateur A_1 (de même pour A_2, B_1, B_2) peut s'écrire :

$$A_1 = 1 \cdot |a_{1,1}\rangle\langle a_{1,1}| + \omega \cdot |a_{1,\omega}\rangle\langle a_{1,\omega}| + \omega^2 \cdot |a_{1,\omega^2}\rangle\langle a_{1,\omega^2}|.$$

On pose $A_{i,\omega^k} = \tilde{A}_{i,\omega^k} \otimes Id$ et $B_{j,\omega^\ell} = Id \otimes \tilde{B}_{j,\omega^\ell}$

Les opérateurs A_{i,ω^k} et B_{j,ω^ℓ} sont ainsi commutatifs et on a donc :

$$\langle\phi|A_{i,\omega^k}B_{j,\omega^\ell}|\phi\rangle = P(\omega^k, \omega^\ell|A_iB_j)$$

pour un état $|\phi\rangle \in \mathbb{H}_A \otimes \mathbb{H}_B$, $i, j \in \{1, 2\}$ and $k, \ell \in \{0, 1, 2\}$.
Dans le cadre de la physique quantique l'expression (5.12) peut donc se réécrire

$$\begin{aligned} I_3(|\,\phi\rangle, A_1, A_2, B_1, B_2) = \\ &\langle\phi|A_{1,1}B_{1,1} + A_{1,1}B_{2,1} - A_{1,1}B_{1,\omega} - A_{1,1}B_{2,\omega^2} \\ &+ A_{1,\omega}B_{1,\omega} + A_{1,\omega}B_{2,\omega} - A_{1,\omega}B_{1,\omega^2} - A_{1,\omega}B_{2,1} \\ &+ A_{1,\omega^2}B_{1,\omega^2} + A_{1,\omega^2}B_{2,\omega^2} - A_{1,\omega^2}B_{1,1} - A_{1,\omega^2}B_{2,\omega} \\ &+ A_{2,1}B_{1,\omega} + A_{2,1}B_{2,1} - A_{2,1}B_{1,1} - A_{2,1}B_{2,\omega} \\ &+ A_{2,\omega}B_{2,\omega} + A_{2,\omega}B_{1,\omega^2} - A_{2,\omega}B_{1,\omega} - A_{2,\omega}B_{2,\omega^2} \\ &+ A_{2,\omega^2}B_{1,1} + A_{2,\omega^2}B_{2,\omega^2} - A_{2,\omega^2}B_{1,\omega^2} - A_{2,\omega^2}B_{2,1}|\phi\rangle \end{aligned} \tag{5.14}$$

Dans ce cas d'observables commutatives, la borne quantique pour l'expression I_3 est de $1 + \sqrt{11/3} \approx 2.9149$. Cette borne est obtenue théoriquement dans [38] ou par optimisation numérique dans [58, table 1].

5.3.2 La variante Free CHSH-3

Dans cette section nous dérivons une expression, Free CHSH-3, à partir de l'expression CHSH-3. Cette nouvelle dérivation fait intervenir des produits d'observables potentiellement non-commutatives. La borne dans le cadre de la physique classique (la notion de réalité au niveau macroscopique, voir 5.1.1) est

$$B_{classique} = 2$$

la non-localité n'intervient pas pour cette borne.
La borne dans le cadre de la physique quantique est obtenue dans le cadre quantique non commutatif défini en début de chapitre (voir définition 5.2) permettant l'utilisation des produits d'observables non-commutatives :

$$B_{quantique} = 4$$

Elle est obtenue par méthode numérique (SDP). Ce dépassement de la borne classique dans le cadre de la physique quantique est dû au caractère indéterminé des résultats

de mesures quantiques. De plus, l'optimisation de cette inégalité permet de déduire, grâce aux observables et états donnant la plus grande borne quantique, un protocole de génération quantique d'aléa. La violation maximale de cette inégalité permet de vérifier le schémas proposé, le rendant, sous certaines hypothèses, auto-test.

Décrivons plus précisément notre cadre de travail. Nous proposons l'étude d'une version non-commutative de l'expression (5.14). De plus, la dimension d de l'espace de Hilbert sur lequel agissent les observables et états de cette expression n'est pas connue à priori. Cela permet de prendre en compte la remarque des auteurs de [63] dans l'introduction de la partie 5 de ce papier. Cette remarque stipule que, lors de l'optimisation numérique d'une expression de Bell, la dimension de l'espace solution n'est pas connue à priori. Nous nommons ainsi cette variante *" l'inégalité free CHSH-3 "*. Tandis que l'inégalité originelle CHSH-3 (voir section 5.3.1) fait intervenir deux parties (Alice et Bob), avec 4 observables, deux pour chaque partie, notre modèle consiste en une seule partie. Cette seule partie possède 4 observables X_1, X_2, X_3, X_4 agissant sur un état $|\phi\rangle$ de l'espace de Hilbert $\mathbb{H}$ de dimension d non fixée. Les observables X_i ne commutent pas forcement entre eux. De plus, comme dans la section 5.3.1 et comme le suggère la référence [59, §2.2.6], l'opérateur X_i s'écrit comme mesure projective :

$$X_i = 1 \cdot X_{i,1} + \omega \cdot X_{i,\omega} + \omega^2 \cdot X_{i,\omega^2} + 0 \cdot X_{i,k_4} + \cdots + 0 \cdot X_{i,k_d} \quad \text{for } i \in \{1,2,3,4\}$$

avec les variables $X_{i,j}$ $i \in \{1,2,3,4\}, j \in \{1, \omega, \omega^2, k_4, ..., k_d\}$ correspondant au projecteur $|x_{i,j}\rangle\langle x_{i,j}|$ sur le vecteur propre $|x_{i,j}\rangle$ de X_i relatif à la valeur propre j. Les valeurs propres $k_4, \dots k_d$, comme l'indique [59, §2.2.6], sont rajoutées pour atteindre la dimension d (elles sont ici fixées à 0). Ainsi, le polynôme définissant CHSH-3 peut s'écrire, en fonction de $X = (X_{1,1}, X_{1,\omega}, \dots, X_{4,\omega^2})$ et de l'état $|\phi\rangle$ via le polynôme

$$\begin{aligned} g(X) = & \\ & = X_{1,1}X_{3,1} + X_{1,1}X_{4,1} - X_{1,1}X_{3,\omega} - X_{1,1}X_{4,\omega^2} \\ & + X_{1,\omega}X_{3,\omega} + X_{1,\omega}X_{4,\omega} - X_{1,\omega}X_{3,\omega^2} - X_{1,\omega}X_{4,1} \\ & + X_{1,\omega^2}X_{3,\omega^2} + X_{1,\omega^2}X_{4,\omega^2} - X_{1,\omega^2}X_{3,1} - X_{1,\omega^2}X_{4,\omega} \\ & + X_{2,1}X_{3,\omega} + X_{2,1}X_{4,1} - X_{2,1}X_{3,1} - X_{2,1}X_{4,\omega} \\ & + X_{2,\omega}X_{4,\omega} + X_{2,\omega}X_{3,\omega^2} - X_{2,\omega}X_{3,\omega} - X_{2,\omega}X_{4,\omega^2} \\ & + X_{2,\omega^2}X_{3,1} + X_{2,\omega^2}X_{4,\omega^2} - X_{2,\omega^2}X_{3,\omega^2} - X_{2,\omega^2}X_{4,1} \end{aligned} \tag{5.15}$$

où les produits précédents ne sont pas commutatifs. Il faut noter que dans le cas d'opérateurs non commutatifs, $\langle\phi|X_{i,\omega^k}X_{j,\omega^\ell}|\phi\rangle$ ne correspond généralement pas à $P(\omega^k, \omega^\ell|X_iX_j)$ et, peuvent être des nombres complexes non réels. De ce fait, nous considérons la partie réelle de g c'est à dire le polynôme :

$$f = \frac{1}{2}(g + g^*). \tag{5.16}$$

L'inégalité Free-CHSH-3 fait intervenir l'expression $\langle\phi|f(X)|\phi\rangle$ et, du fait que $f(X)$ se réduise à l'équation (5.12) dans le cadre d'observables commutatives et donc à (5.10), on déduit la borne classique :

$$\langle\phi|f(X)|\phi\rangle \leq 2 \tag{5.17}$$

Mais cependant, on ne peut directement déduire la borne quantique de la littérature. Ainsi, par la suite, nous décrivons l'optimisation numérique permettant de déduire les différentes valeurs quantiques de référence pour cette inégalité.

5.3.3 Relaxation semi-définie de l'expression free CHSH-3

5.3.3.1 Programmation Semi-définie

La programmation semi-définie (SDP) est une classe de problèmes d'optimisation convexe qui a gagné en importance pendant ces dernières décennies. C'est une généralisation naturelle de la programmation linéaire (LP) consistant à minimiser des fonctions linéaires sur des sections affines du cône des matrices hermitiennes semi-définies positives :

Définition 5.4. *[9, Définition 9.1]*
Un programme semi-défini (complexe) est un problème d'optimisation de la forme

$$\begin{array}{ll} \min & C \bullet X \\ s.t. & A_i \bullet X = b_i, i = 1, ..., m \\ & X \succeq 0. \end{array} \tag{5.18}$$

où la variable $X \in \mathbb{C}^{n\times n}$ est hermitienne, c'est à dire $X = X^\dagger$, avec $X^\dagger$ la transconjuguée de X ($X^\dagger_{i\,j} = \bar{X_{j\,i}}$).
De plus, la condition $X \succeq 0$ signifie que la variable est semi-définie positive, ce qui signifie que pour tout vecteur $z \in \mathbb{C}^n$ on a $z^\dagger X z \geq 0$.
Les termes A_i, $(i = 1, \cdots, m)$ et C sont des matrices hermitiennes données (déjà connues). $(b_1, \cdots, b_m) \in \mathbb{R}^m$ est un vecteur donné.
L'expression $U \bullet V = Trace(V^\dagger U)$ désigne le produit scalaire hermitien.

Propriété 5.2. *Le produit scalaire hermitien de deux matrices hermitiennes est un nombre réel (ce qui légitime le calcul du minimum).*

Démonstration. Soient U et V deux matrices hermitiennes de $\mathbb{C}^{n\times n}$. Cela signifie que $U^\dagger = U$ (respectivement $V^\dagger = V$) et donc $\forall i,\, j \in \{1, ..., n\}$, $U_{i\,j} = \bar{U_{j,\,i}}$ (respectivement $V_{i,\,j} = \bar{V_{j,\,i}}$). En particulier les éléments diagonaux sont réels ($U_{ii} \in \mathbb{R}$).

$$\begin{array}{rl} U \bullet V = & \sum_{i,j} \bar{V_{ij}} U_{ij} \\ & = \sum_{i=1,...,n} \bar{V_{ii}} U_{ii} + \sum_{i<j} \bar{V_{ij}} U_{ij} + \sum_{i>j} \bar{V_{ij}} U_{ij} \end{array}$$

Pour i_0 et $j_0 \in \{1, ..., n\}$ fixés, avec $i_0 < j_0$, le terme $\bar{V_{i_0 j_0}} U_{i_0 j_0}$ est le conjugué du terme $\bar{V_{j_0 i_0}} U_{j_0 i_0}$. Autrement dit chaque terme de la deuxième somme est le conjugué d'un terme de la troisième somme (et vice versa). Ainsi la deuxième somme et la première sont conjuguées l'une de l'autre. Et, pour tout nombre complexe a, on obtient $a + \bar{a} = 2\Re(a)$ De plus, la première somme est constituée de termes réels, d'où on déduit le résultat. □

La SDP est aussi, comme la programmation linéaire, résolue efficacement par la méthode des points intérieurs (en temps polynomial pour une précision fixée) implémentée dans des outils tels que [8, 67].
Bien que la SDP soit une classe de problèmes d'optimisation convexe, on peut tout de même l'utiliser pour la résolution de problèmes d'optimisation non convexes de minimisation de fonctions polynomiales multivariées sous des contraintes polynomiales [9]. Cela, grâce à des relaxations (appelées hiérarchies) des problèmes initiaux et des propriétés de convergence de ces relaxations comme l'explique Lasserre dans [51]. De plus, la hiérarchie SDP est étendue au cas de variables non commutatives [23] et appliquée avec succès à l'informatique quantique comme nous le montrent [63] et [9, chapitre 21]. En effet, cette hiérarchie donne des bornes sur le minimum ou le maximum de l'action d'une fonction polynomiale d'observables non commutatives, soumise à des contraintes polynomiales d'égalités ou d'inégalités. Pour ce faire, la clé réside en la linéarisation de la quantité

$$\langle \phi, f(X)\phi \rangle = \langle \phi, \sum_w f_w w(X)\phi \rangle = \sum_w f_w \langle \phi, w(X)\phi \rangle$$

où $f(X) = \sum_w f_w w(X)$ est une fonction polynôme non commutative des n opérateurs de mesure $X = (X_1, \ldots, X_n)$. Ces opérateurs sont définis sur l'espace de Hilbert $\mathbb{H}$; le terme $w(X)$ désigne un monôme en X et $|\phi\rangle \in \mathbb{H}$ un état pur. La linéarisation consiste à remplacer l'action $\langle \phi, w(X)\phi \rangle$ du polynôme $w(X)$ sur l'état $|\phi\rangle$, par la nouvelle variable ou moment y_w. En d'autre termes, on remplace l'opérateur non linéaire en X par la fonction linéaire sur l'espace des variables y suivante :

$$\langle \phi, f(X)\phi \rangle = \sum_w f_w \langle \phi, w(X)\phi \rangle = \sum_w f_w y_w.$$

Pour tout entier naturel $D > 0$, les moments y_w d'un ordre inférieur ou égal à D (c'est à dire relatifs à des polynômes de degré inférieurs ou égaux à D), sont organisés en une matrice symétrique multi-hankel de moments $M_D(y) = (y_{vw})_{v,w}$ (ce qui signifie que l'entrée de $M_D(y)$ indexée par (v, w) est y_{vw}). Par construction du moment y_w, une condition nécessaire apparait : $M_D(y)$ doit être semi-définie positive, du fait que pour tout vecteur complexe $z = (z_w)$ l'assertion $z^* M_d(y) z \geq 0$ est vraie. De même les contraintes non linéaires peuvent aussi être linéarisées permettant ainsi l'ajout de contraintes semi-définies et linéaires sur les variables X de la relaxation. Un exemple remarquable d'application de la SDP est celui de l'inégalité CHSH-2 pour laquelle le premier niveau de la hiérarchie est suffisant pour expliciter la borne quantique [71].

Dans le cadre de cette thèse, nous utilisons la programmation semi-définie dans l'esprit de [63, 71] pour déduire des observables non-commutatives. Ces observables entrainent une violation de l'inégalité CHSH-3 **plus grande que** la borne quantique dans le cas d'observables commutatives : $1 + \sqrt{11/3} \approx 2.9149$.

Il faut cependant noter qu'un désavantage majeur de la relaxation semi-définie réside en la croissance démesurée de la taille de la sortie en fonction du niveau de la hiérarchie. Cela entraine, dans bien des cas, le caractère irrésolvable en temps raisonnable de niveaux assez bas dans la hiérarchie. Et ce, même par des outils numériques. On pourrait, par la suite, étudier certaines structures particulières des matrices des moments, comme le suggèrent les auteurs de [45, 70], pour améliorer la résolution.

5.3.3.2 Relaxation du premier ordre de l'expression free CHSH-3

Désignons par

$$X = (X_{1,1}, X_{1,\omega}, X_{1,\omega^2}, X_{2,1}, \ldots, X_{4,\omega}, X_{4,\omega^2})$$

les projecteurs (inconnus) sur les espaces propres des opérateurs X_1, X_2, X_3, X_4 relatifs aux valeurs propres $1, \omega, \omega^2$ comme défini à la section 5.3.2. Posons de plus $f(X)$ le polynome non commutatif défini dans l'équatuin (5.16). Notre objectif est d'obtenir la violation maximale d'une version de CHSH-3 sans contraintes de dimensions ni de commutativité. De ce fait, nous posons $k_4, k_5, \ldots, k_d$ des valeurs propres additionnelles pour atteindre la dimension d (voir [59, §2.2.6]). De même on pose X_{i,k_j} le projecteur relatif à la valeur propre k_j, pour $j \in \{4, \ldots, d\}$. Définissons les ensembles suivants :

$$T = \{(i,\mu) \mid i = 1,2,3,4, \quad \mu = 1, \omega, \omega^2, k_4, \ldots, k_d\}.$$

$$U = \{(i,\mu) \mid i = 1,2,3,4, \quad \mu = 1, \omega, \omega^2\}.$$

Ainsi, on peut écrire $X_{i,\mu} = X_\alpha$ avec $\alpha = (i,\mu) \in T$. On peut alors formuler le problème initial de maximisation quantique de l'expression free CHSH-3 comme suit :

$$\begin{array}{rlll} f^* := & \sup & \langle\phi|f(X)|\phi\rangle & \\ & \text{s.t.} & \langle\phi|\phi\rangle = 1 & \\ & & X_\alpha X_\beta = \delta_{\mu\nu} X_\alpha & \alpha = (i,\mu), \beta = (i,\nu) \in T \\ & & \sum_\mu X_\alpha = 1 & i \in \{1,2,3,4\}, \alpha = (i,\mu) \end{array} \tag{5.19}$$

où $\delta_{\mu\nu}$ est le symbole de Kronecker pour les indices $\mu, \nu \in \{1, \omega, \omega^2, k_4, \ldots, k_d\}$ ($\delta_{\mu\nu} = 1$ si $\mu = \nu$, et $= 0$ autrement). Les deux dernières contraintes traduisent l'égalité $X_{i,\mu} = |x_{i,\mu}\rangle\langle x_{i,\mu}|$ que nous imposons comme discuté plus haut.

Relaxons ce problème avec des variables linéaires. Posons

$$y_\alpha = \langle\phi|X_\alpha|\phi\rangle$$

pour $\alpha \in T$, le moment d'ordre un, associé à la variable X_α et à l'état $|\phi\rangle$ (omis). De même nous posons le moment d'ordre 2 associé au produit $X_\alpha X_\beta$

$$y_{\alpha\beta} = \langle\phi|X_\alpha X_\beta|\phi\rangle$$

La relaxation du premier ordre du problème (5.19) s'exprime donc ainsi :

$$\begin{array}{rlll} f_1^* := & \sup & \sum_{\alpha\beta} c_{\alpha\beta} y_{\alpha\beta} & \\ & \text{s.t.} & y_0 = 1 & \\ & & y_{\alpha\beta} = \delta_{\mu\nu} y_\alpha & \alpha = (i,\mu), \beta = (i,\nu) \in T \\ & & \sum_\mu y_\alpha = 1 & i \in \{1,2,3,4\}, \alpha = (i,\mu) \\ & & M_1(y) \succeq 0 & \end{array} \tag{5.20}$$

avec $c_{\alpha\beta} \in \{-1, 0, 1\}$ les coefficients de f tels que : $f(X) = \sum_{\alpha\beta} c_{\alpha\beta} X_\alpha X_\beta$. Et, $M_1(y)$ la matrice Hermitienne des moments de la relaxation à l'ordre 1,

$$M_1(y) = \langle\phi|v_1^\dagger v_1|\phi\rangle = \begin{bmatrix} y_0 & y_{\alpha_1} & y_{\alpha_2} & \cdots & y_{\alpha_{4d}} \\ y_{\alpha_1} & y_{\alpha_1\alpha_1} & y_{\alpha_1\alpha_2} & \cdots & y_{\alpha_1\alpha_{4d}} \\ y_{\alpha_2} & y_{\alpha_2\alpha_1} & y_{\alpha_2\alpha_2} & & \vdots \\ \vdots & & & & \\ y_{\alpha_{4d}} & y_{\alpha_{4d}\alpha_1} & \cdots & & y_{\alpha_{4d}\alpha_{4d}} \end{bmatrix}$$

Avec $v_1 = (1, X_{\alpha_1}, X_{\alpha_2}, \cdots, X_{\alpha_{4d}}) \in \mathbb{C}^{4d+1}$, le vecteur de monômes de degré inférieur ou égal à 1 ; où nous avons choisi un ordre pour les indices α dans T désigné par $\{\alpha_1, \ldots, \alpha_{4d}\}$.

Nous proposons une réécriture de (5.20) faisant intervenir des produits de matrices Hermitiennes : Pour deux matrices Hermitiennes C_1, C_2 on note $C_1 \bullet C_2 = \text{Trace}(C_1 C_2)$ le produit scalaire habituel de ces deux matrices (les matrices étant hermitiennes, le signe transconjuguée n'apparait donc pas). Posons $C, C_0, A_0, A_{\alpha\beta}, A_i$ les matrices $(1 + 4d) \times (1 + 4d)$ symétriques telles que $\sum_\alpha c_\alpha y_\alpha = C \bullet M_1(y)$, $y_0 = C_0 \bullet M_1(y)$, $y_{\alpha\beta} - \delta_{\mu\nu} y_\alpha = A_{\alpha\beta} \bullet M_1(y)$ (pour cette dernière égalité $\alpha = (i,\mu)$, $\beta = (i,\nu)$). Posons de plus, $\sum_\mu y_\alpha = A_i \bullet M_1(y)$ (où, la première composante de α est i). Ainsi donc, le problème (5.20) est équivalent au programme semi-définie suivant

$$\begin{array}{rlll} f_1^* := & \sup & C \bullet M_1(y) & \\ & \text{s.t.} & C_0 \bullet M_1(y) = 1 & \\ & & A_{\alpha\beta} \bullet M_1(y) = 0 & \alpha = (i,\mu), \beta = (i,\nu) \in T \\ & & A_i \bullet M_1(y) = 1 & i \in \{1,2,3,4\}, \alpha = (i,\mu) \\ & & M_1(y) \succeq 0. & \end{array} \tag{5.21}$$

Remarque 5.1. *La relaxation (5.20) du problème (5.19) est donc un problème moins contraint : (5.20) porte sur les moments d'ordre 1 et 2, tandis que (5.19) entraine en plus des contraintes sur les moments d'ordres supérieurs. On en déduit que :*

$$f_1^* \geq f^*$$

Remarque 5.2. *Valeur intermédiaire* 3.1547
La référence [58, table 1], fait état de la valeur 3.1547 *générée par la relaxation de premier ordre pour l'optimisation de l'expression originelle CHSH-3. Cette valeur n'est cependant pas la borne quantique de l'expression originelle. En effet, le critère d'égalité du rang des matrices solutions d'une étape à la suivante ne s'applique pas (la borne est dans ce cas obtenue au deuxième ordre de la relaxation et est* $1+\sqrt{11/3} \approx 2.9149$*).*
Néanmoins, cette valeur intermédiaire $2+2\sqrt{1/3} \approx 3.1547$ *peut être obtenue par modification de l'équation* (5.21)*. Ceci en y rajoutant les contraintes de positivité des entrées de* $M_1(y)$ *correspondant aux monômes* X_α, X_β *avec* $\alpha, \beta \in U$*. Ces entrées sont celles relatives aux monômes du polynôme* $f(x)$ *dans* (5.16)*. On a ainsi des contraintes supplémentaires de positivité, par rapport au cas d'observables non commutatives. Avec ces contraintes supplémentaires, on a exactement toutes les contraintes d'une relaxation du premier ordre dans le cadre d'observables commutatives.*
Ainsi, cette valeur 3.1547 *semble être à "mi-chemin" entre l'optimisation à observables commutatifs (cas originel CHSH-3) et celle à observables non forcément commutatifs (free CHSH-3).*

L'optimisation à mener est la suivante :

$$\begin{array}{rll} \gamma := \sup & C \bullet M_1(y) & \\ s.t. & C_0 \bullet M_1(y) = 1 & \\ & A_{\alpha\beta} \bullet M_1(y) = 0 & \alpha = (i,\mu), \beta = (i,\nu) \in T \\ & A_i \bullet M_1(y) = 1 & i \in \{1,2,3,4\}, \alpha = (i,\mu) \\ & B_{\alpha,\beta} \bullet M_1(y) \geq 0 & \alpha, \beta \in U \\ & H_{\alpha,\beta} \bullet M_1(y) = 0 & \alpha, \beta \in U \\ & M_1(y) \succeq 0. & \end{array} \tag{5.22}$$

Les colonnes de la matrice B *suivante permettent d'obtenir l'état optimal de même que les états propres des observables permettant d'atteindre la valeur* $2+2\sqrt{1/3} \approx 3.1547$ *: Posons* $s = \sin(\pi/12)$*,* $c = \cos(\pi/12)$*, on a alors*

$$\frac{1}{3}\begin{bmatrix} 3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & -c & s & \sqrt{1/2} & -\sqrt{1/2} & -s & c & 0 & 0 & 0 & -\sqrt{3/2} & 0 & \sqrt{3/2} \\ 0 & -s & c & -\sqrt{1/2} & -\sqrt{1/2} & c & -s & 0 & 0 & 0 & -\sqrt{1/2} & \sqrt{2} & -\sqrt{1/2} \\ 0 & -\sqrt{1/2} & -s & c & s & \sqrt{1/2} & -c & -\sqrt{3/2} & 0 & \sqrt{3/2} & 0 & 0 & 0 \\ 0 & -\sqrt{1/2} & c & -s & c & -\sqrt{1/2} & -s & -\sqrt{1/2} & \sqrt{2} & -\sqrt{1/2} & 0 & 0 & 0 \end{bmatrix} \tag{5.23}$$

Cette matrice est interprétée suivant le canevas proposé dans [9, Ch. 21] : La première colonne de B *est l'état* $|\phi\rangle$ *et pour* $i \in \{1,2,3,4\}$*, la normalisation des colonnes* $3i-1, 3i$ *et* $3i+1$ *de* B *constituent les vecteurs propres* $|x_{i,1}\rangle, |x_{i,\omega}\rangle$ *et* $|x_{i,\omega^2}\rangle$ *correspondant aux mesures projectives* X_i*. Comme l'indique [59, §2.2.6] :*

$$X_i = 1 \cdot |x_{i,1}\rangle\langle x_{i,1}| + \omega \cdot |x_{i,\omega}\rangle\langle x_{i,\omega}| + \omega^2 \cdot |x_{i,\omega^2}\rangle\langle x_{i,\omega^2}| + 0 \cdot E_{i,0}. \tag{5.24}$$

où $E_{i,0}$ *est le projecteur de rang 2 vérifiant :*

$$|x_{i,1}\rangle\langle x_{i,1}| + |x_{i,\omega}\rangle\langle x_{i,\omega}| + |x_{i,\omega^2}\rangle\langle x_{i,\omega^2}| + E_{i,0} = Id_5.$$

5.3.3.3 Borne quantique

Dans le cadre quantique défini à la section 5.2, l'optimisation (5.21) donne pour valeur (voir[10])

$$f_1^* = 4$$

Les colonnes de la matrice B suivante permettent d'obtenir l'état optimal de même que les états propres des observables permettant d'atteindre cette borne quantique.

$$\frac{\sqrt{3}}{9}\begin{bmatrix} 3 & 3 & 0 & 0 & 0 & 3 & 0 & 2 & -1 & 2 & 2 & 2 & -1 \\ 3 & 0 & 3 & 0 & 0 & 0 & 3 & 2 & 2 & -1 & -1 & 2 & 2 \\ 3 & 0 & 0 & 3 & 3 & 0 & 0 & -1 & 2 & 2 & 2 & -1 & 2 \end{bmatrix} \tag{5.25}$$

Cette matrice est interprétée suivant le canevas proposé dans [9, Ch. 21] : La première colonne de B est l'état optimal $|\phi^*\rangle$ et pour $i \in \{1,2,3,4\}$, la normalisation des colonnes $3i-1, 3i$ et $3i+1$ de B constituent les vecteurs propres $|x_{i,1}\rangle, |x_{i,\omega}\rangle$ et $|x_{i,\omega^2}\rangle$ correspondant aux mesures projectives X_i^*. Comme l'indique [59, §2.2.6] :

$$X_i^* = 1 \cdot |x_{i,1}\rangle\langle x_{i,1}| + \omega \cdot |x_{i,\omega}\rangle\langle x_{i,\omega}| + \omega^2 \cdot |x_{i,\omega^2}\rangle\langle x_{i,\omega^2}| \tag{5.26}$$

Ainsi, les observables optimaux sont ceux ci :

$$\begin{aligned} X_1^* = Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix} \quad X_2^* = \begin{bmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ X_3^* = \tfrac{1}{3}\begin{bmatrix} -\omega & 2 & 2\omega^2 \\ 2 & -\omega^2 & 2\omega \\ 2\omega^2 & 2\omega & -1 \end{bmatrix} \quad X_4^* = \tfrac{1}{3}\begin{bmatrix} -\omega^2 & 2\omega & 2 \\ 2\omega & -1 & 2\omega^2 \\ 2 & 2\omega^2 & -\omega \end{bmatrix} \end{aligned} \tag{5.27}$$

Par la suite, nous montrons que cette borne optimale f_1^* de la première relaxation (5.21) est égale à la borne optimale f^* du problème original (5.19).
Les codes matlab de l'optimisation menée peuvent être trouvés dans [11].

Théorème 5.1. *La valeur optimale du problème* (5.19) *est* 4 *et est atteinte par la configuration* (5.26) *et pour l'état* $|\phi^*\rangle = (1/\sqrt{3})(1,1,1)^\dagger$.

Démonstration. Dans un premier temps, nous remarquons que les opérateurs construits dans (5.26) satisfont les contraintes du problème (5.19). On a ainsi

$$4 = C \bullet M_1(y^*) = \langle\phi^*|f(X^*)|\phi^*\rangle \leq f^*.$$

Or (5.20) est une relaxation de (5.19). On en déduit que l'ensemble des observables et états vérifiant (5.20), contient l'ensemble de ceux qui vérifient (5.19). De ce fait, $f^* \leq f_1^* = 4$, d'où $f^* = f_1^* = 4$ □

Borne algébrique et non algébrique

L'expression initiale (5.12) de CHSH-3 et celle de free CHSH-3 (5.16) ne sont pas équivalentes, et ce, du fait que (5.12) n'est pas définie dans le cadre d'observables non commutatives. Ainsi, ces deux expressions n'ont à priori pas les mêmes bornes algébriques. Mais cependant, la borne quantique 4 de (5.16) est égale à la borne algébrique de l'expression (5.12). On pourrait se poser la question à savoir la borne algébrique de (5.16). Une piste de réflexion serait alors de considérer chacun des 24 termes de cette expression, sous la forme $\langle\phi|X_{i,\omega^\ell}X_{j,\omega^k}|\phi\rangle$ avec une valeur absolue de 1.

5.4 Gabriel : Protocole basé sur l'inégalité Free CHSH-3 (Poster Qcrypt 2020) [10]

Le but de cette section est d'exposer un protocole basé sur l'inégalité Free CHSH-3. Ce protocole fait intervenir des produits d'observables incompatibles implémentés séquentiellement. L'utilisation de mesures non commutatives implémentées de manière séquentielle a déjà été démontrée par les auteurs de [3, 6]

Dans notre cas, ce schéma de mesures séquentielles est couplé à l'évaluation de l'inégalité free-CHSH-3. Cela permet d'énoncer des arguments de sécurité notamment celui de l'auto test. Décrivons dans un premier temps, les propriétés de l'état et des mesures utilisés. Ils permettent, ensuite, de décrire l'exécution de ce protocole. Nous terminons par les preuves de sécurité avec notamment les arguments en faveur de la propriété auto test.

5.4.1 Propriétés des mesures et de l'état

Les mesures X_1, X_2, X_3, X_4 et l'état $|\phi\rangle$ utilisés dans cette sous-section sont les résultats de l'optimisation exposés dans les équations (5.26) et (5.27), c'est-à-dire :

$$
\begin{aligned}
X_1 = Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix} \quad X_2 = \begin{bmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \omega X_1 \\
X_3 = \tfrac{1}{3}\begin{bmatrix} -\omega & 2 & 2\omega^2 \\ 2 & -\omega^2 & 2\omega \\ 2\omega^2 & 2\omega & -1 \end{bmatrix} \quad X_4 = \tfrac{1}{3}\begin{bmatrix} -\omega^2 & 2\omega & 2 \\ 2\omega & -1 & 2\omega^2 \\ 2 & 2\omega^2 & -\omega \end{bmatrix} = \omega^2 X_3 \\
|\phi\rangle = (1/\sqrt{3})(1,1,1)^\dagger
\end{aligned}
\tag{5.28}
$$

Les mesures X_1 et X_2 (de même pour X_3 et X_4) commutent. Ainsi les cinq faits suivants sont équivalents :

a) Implémenter la mesure dont la matrice est donnée par $X_1X_2 = X_2X_1$.

b) Implémenter séquentiellement X_2 puis X_1.
c) Implémenter séquentiellement X_1 puis X_2.
d) Ne mesurer que X_1 puis inférer le résultat de X_2.
e) Ne mesurer que X_2 puis inférer le résultat de X_1.

Cette équivalence vient du fait que, dans le cas des mesures projectives, la mesure d'une observable entraine une projection sur l'un de ses vecteurs propres. Et, les observables X_1, X_2 ainsi que leurs produits ont les mêmes états propres.

$$|x_{1,\omega^k}\rangle = |x_{2,\omega^{k+1}}\rangle = |(x_1x_2)_{\omega^{2k+1}}\rangle = |(x_2x_1)_{\omega^{2k+1}}\rangle$$

avec $|(x_ix_j)_{\omega^{2k+1}}\rangle$ un vecteur propre de X_iX_j relatif à la valeur propre ω^{2k+1} et k, $k+1$ $2k+1$ sont pris modulo 3 . La différence ne réside que dans le résultat retourné :

$$\begin{array}{ll} X_1 \mapsto \omega^k & X_1X_2 \mapsto \omega^k\omega^{k+1} \\ X_2 \mapsto \omega^{k+1} & X_2, X_1 \text{ (sequentiellement)} \mapsto \omega^k \textit{ or } \omega^{2k+1} \end{array}$$

Le raisonnement précédent s'applique à X_3X_4.
Il faut de plus noter que X_1 et X_2 ne commutent pas avec X_3 et X_4.

Randomness generation

Une propriété essentielle dans la génération d'aléa est le fait que, la mesure de l'état $|\phi\rangle$ dans la base X_i, $i \in \{1,2,3,4\}$ donne pour résultats :

$$\begin{array}{rlll} 1 & \text{avec probabilité} & P(1 \mid (|\phi\rangle, X_i)) = |\langle\phi|x_{i,1}\rangle|^2 & = 1/3 \\ \omega & \text{avec probabilité} & P(\omega \mid (|\phi\rangle, X_i)) = |\langle\phi|x_{i,\omega}\rangle|^2 & = 1/3 \\ \omega^2 & \text{avec probabilité} & P(\omega^2 \mid (|\phi\rangle, X_i)) = |\langle\phi|x_{i,\omega^2}\rangle|^2 & = 1/3 \end{array}$$

Ainsi donc, un générateur de nombre aléatoire, basé sur ces mesures effectuées sur l'état $|\phi\rangle$ aura une qualité estimée par la min-entropie suivante (voir [49])

$$H_\infty = -log_3 \max_{\ell,i} P(\omega^\ell \mid (|\phi\rangle, X_i)) = -log_3\, 1/3 = 1 \text{ trit}$$

On en conclue que chaque trit produit a une min-entropie d'exactement 1 trit (et donc maximale). Cette remarque est utilisée à cet effet pour le protocole suivant de génération de nombres aléatoires.

5.4.2 Exécution du protocole

Considérons les états et mesures définis dans l'équation (5.28). On suppose que l'utilisateur a accès à une source publique d'aléa comme celle du NIST [3]. À l'aide de la discussion précédente, décrivons le fonctionnement pratique de notre protocole de génération de trits aléatoires. Les étapes suivantes sont itérées :

3. https ://csrc.nist.gov/projects/interoperable-randomness-beacons

1. L'utilisateur choisit de manière aléatoire (en utilisant l'aléa publique) un couple (X_i, X_j), $i, j \in \{1, 2, 3, 4\}$.
2. Si $i, j \in \{1, 2\}$ ou $i, j \in \{3, 4\}$ alors il mesure l'état $|\phi\rangle$ dans la base X_i. Le résultat est retourné comme **trit aléatoire**.
3. Autrement, on mesure séquentiellement X_j puis X_i sur l'état $|\phi\rangle$: On mesure X_j, on collecte l'état résultant $|x_{j,\omega^k}\rangle$, $k \in \{0, 1, 2\}$; puis cet état est lui-même mesuré dans la base X_i pour obtenir l'état $|x_{i,\omega^\ell}\rangle$, $\ell \in \{0, 1, 2\}$. Ces résultats sont consignés dans le but d'évaluer l'expression Free CHSH-3 comme expliqué dans la section (5.4.3).

5.4.3 Valeur maximale de l'évaluation de Free CHSH-3

Nous pouvons évaluer l'expression $\langle\phi|f(X)|\phi\rangle$ sur la configuration $(X, |\phi\rangle)$ exposée dans l'équation (5.28) et calculée par SDP dans la section 5.3.3.3 avec pour valeur quantique de 4. Ainsi, si cette violation n'est pas atteinte, on peut déduire la potentielle présence d'erreur voir, d'un espion.
Cependant, cette évaluation ne peut se faire de manière exacte que sous l'hypothèse que les moments produits par l'expérience sont réels.

Pour cette évaluation de l'expression Free CHSH-3, nous utilisons les sorties de l'étape 3, du protocole décrit dans la section (5.4.2). La valeur maximale quantique de l'évaluation de Free CHSH-3 est atteinte pour la configuration (5.28), qui donne les moments optimaux $y^*_{(i,\omega^\ell)(j,\omega^k)}$. De plus, ces moments peuvent être estimés expérimentalement. En effet, pour tout moment $y_{(i,\omega^\ell)(j,\omega^k)}$ on a :

$$\begin{aligned} y_{(i,\omega^\ell)(j,\omega^k)} &= \langle\phi|X_{i,\omega^\ell}X_{j,\omega^k}|\phi\rangle \\ &= \langle\phi|x_{i,\omega^\ell}\rangle\langle x_{i,\omega^\ell}|x_{j,\omega^k}\rangle\langle x_{j,\omega^k}|\phi\rangle \end{aligned}$$

Ainsi

$$\begin{aligned} |\, y_{(i,\omega^\ell)(j,\omega^k)}\,| = &\sqrt{|\,\langle\phi|x_{i,\omega^\ell}\rangle\,|^2}\,\sqrt{|\,\langle x_{i,\omega^\ell}|x_{j,\omega^k}\rangle\,|^2} \\ &\sqrt{|\,\langle x_{j,\omega^k}|\phi\rangle\,|^2} \end{aligned}$$

où $|\,\langle\phi \mid x_{i,\omega^\ell}\rangle\,|^2 = \langle\phi|X_{i,\omega^\ell}|\phi\rangle = P(|x_{i,\omega^\ell}\rangle \mid (|\phi\rangle, X_i))$ est la probabilité d'avoir l'état $|x_{i,\omega^\ell}\rangle$ après la mesure de $|\phi\rangle$ dans la base X_i. Nous avons donc :

$$\begin{aligned} |\, y_{(i,\omega^\ell)(j,\omega^k)}\,| = &\sqrt{P(|x_{i,\omega^\ell}\rangle \mid (|\phi\rangle, X_i))} \\ &\times \sqrt{P(|x_{j,\omega^k}\rangle \mid (|x_{i,\omega^\ell}\rangle, X_j))} \\ &\times \sqrt{P(|x_{j,\omega^k}\rangle \mid (|\phi\rangle, X_j))} \end{aligned}$$

La bonne valeur, dans le cas de moments réels, peut être retrouvée par la relation

$$\sum_{k=0..2} y_{(i,\omega^\ell)(j,\omega^k)} = \sum_k \langle\phi|X_{i,\omega^\ell}X_{j,\omega^k}|\phi\rangle = \langle\phi|X_{i,\omega^\ell}|\phi\rangle = P(|x_{i,\omega^\ell}\rangle \mid (|\phi\rangle, X_i))$$

où la probabilité peut être estimée grâce aux sorties du protocoles.

$$y_{(i,\omega^\ell)(j,1)} + y_{(i,\omega^\ell)(j,\omega)} + y_{(i,\omega^\ell)(j,\omega^2)} = P(|x_{i,\omega^\ell}\rangle \mid (|\phi\rangle, X_i)) \tag{5.29}$$

Propriété 5.3. *Pour retrouver cette bonne valeur du moment à l'aide de son module les* $\mid y_{(i,\omega^\ell)(j,\omega^k)} \mid$*, il suffit d'attribuer les signes de telle sorte à vérifier la relation 5.29*

Démonstration. En effet :

- Dans le premier cas où les bons signes sont attribués aux modules, la relation précédente est vérifiée.

- Dans le deuxième cas où l'un des signes n'est pas le bon (disons le dernier), la relation n'est pas vérifiée. En effet

  $$y_{(i,\omega^\ell)(j,1)} + y_{(i,\omega^\ell)(j,\omega)} - y_{(i,\omega^\ell)(j,\omega^2)} - P(|x_{i,\omega^\ell}\rangle = -2y_{(i,\omega^\ell)(j,\omega^2)} \neq 0$$

  (car sinon $y_{(i,\omega^\ell)(j,\omega^2)} = 0$ et il a le bon signe tandis qu'on a supposé qu'il ne l'avait pas)
- Dans le troisième cas où deux des signes ne sont pas les bons (disons les deux derniers) la relation n'est pas vérifiée non plus car la différence entre l'expression obtenue après affectation des signes et celle qui devrait l'être théoriquement donne :

  $$\begin{aligned} y_{(i,\omega^\ell)(j,1)} \quad & -y_{(i,\omega^\ell)(j,\omega)} - y_{(i,\omega^\ell)(j,\omega^2)} - P(|x_{i,\omega^\ell}\rangle \\ & = -2(y_{(i,\omega^\ell)(j,\omega)} + y_{(i,\omega^\ell)(j,\omega^2)}) \\ & = -2(\langle\phi|X_{i,\,\omega^\ell}X_{j,\,\omega}|\phi\rangle + \langle\phi|X_{i,\,\omega^\ell}X_{j,\,\omega^2}|\phi\rangle) \\ & = -2\langle\phi|X_{i,\,\omega^\ell} \quad (X_{j,\,\omega}|\phi\rangle + X_{j,\,\omega^2}|\phi\rangle) \end{aligned}$$

  Cette différence entre l'expression obtenue après affectation des signes et celle qui devrait l'être théoriquement serait nulle si
  - Si $\langle\phi|X_{i,\,\omega^\ell} = 0$ auquel cas, les moments seraient nuls et donc tous les signes seraient bons (en contradiction avec l'hypothèse de ce point)
  - ou Si $(X_{j,\,\omega}|\phi\rangle + X_{j,\,\omega^2}|\phi\rangle) = 0$. Ce qui signifie que

    $$\begin{aligned} & (X_{j,\,\omega}|\phi\rangle + X_{j,\,\omega^2}|\phi\rangle) = 0 \text{ ce qui signifie que} \\ & X_{j,\,\omega}|\phi\rangle = -X_{j,\,\omega}|\phi\rangle \\ & |x_{j,\,\omega}\rangle\langle x_{j,\,\omega}|\phi\rangle = -|x_{j,\,\omega^2}\rangle\langle x_{j,\,\omega^2}|\phi\rangle \end{aligned}$$

    Et donc soit : l'un des produits scalaires $\langle x_{j,\,\omega}|\phi\rangle$ ou $\langle x_{j,\,\omega^2}|\phi\rangle$ est nul, auquel cas, l'un des deux moments est nul et on a le bon signe. Ce qui est en contradiction avec l'hypothèse du 3 ème cas disant que les deux moments ne sont

pas du bon signe.
Ou soit, les vecteurs $|x_{j,\omega}\rangle$ et $|x_{j,\omega^2}\rangle$ sont colinéaires. Ce qui n'est pas possible non plus car ce sont des vecteurs propres différents de la mesure X_j et sont donc orthogonaux.

Ainsi il n'est point possible, dans ce cas de deux mauvais signes des moments, d'avoir la bonne valeur lors de la vérification.

- Dans le quatrième cas, lorsque les 3 moments sont évalués par des signes contraires à ce qu'ils devraient être, on obtient évidemment l'opposé de la probabilité.

Ainsi on vient, au travers de ces cas, de montrer que les moments sont uniquement déterminés par la relation 5.29 sous l'hypothèse qu'ils sont réels.

□

Ce processus nous permet donc d'évaluer expérimentalement les moments, dans le cas où ceux-ci sont réels. Cela vient du fait que la probabilité utilisée dans l'expression précédente peut être déduite des résultats de l'étape 3 du protocole.

Par conséquent, si l'état et les mesures sont ceux exposés dans l'équation (5.28), nous avons une valeur quantique de 4.

Dans la section suivante, nous montrerons les déductions qui peuvent être faites, dans le cas où l'évaluation donne une valeur quantique maximale.

5.4.4 Propriété auto-test, limites et voies améliorations possibles

Dans cette section, nous exhibons un indicateur de la qualité de l'aléa produit, dépendant de la valeur de l'évaluation de l'expression Free CHSH-3. Cet indicateur repose sur la relation entre la valeur de l'évaluation de Free CHSH-3 et la borne inférieure de la quantité d'aléa produit dans le cadre quantique. Cette relation, déterminée grâce aux statistiques sur les sorties, permet d'inférer la qualité des nombres aléatoires ainsi générés. Pour cela nous procédons comme expliqué dans la référence [31] en adaptant la méthode à notre contexte :

Nous exprimons ci-après, au travers d'une heuristique, la min-entropie comme fonction de la valeur de l'expression Free CHSH-3 : pour une configuration donnée $(B_1, ..., B_4, |\psi\rangle)$ la min-entropie est donnée par

$$H_{min}(B_1, ..., B_4, |\psi\rangle) = log_3 \max_{\ell,i} P(\omega^\ell \mid (|\psi\rangle, B_i))$$

où $\ell \in \{0, 1, 2\}$, $i \in \{1, 2, 3, 4\}$, $P(\omega^\ell \mid (|\psi\rangle, B_i)) = \langle\psi|B_{i,\ell}|\psi\rangle$

On souhaite ainsi, trouver une borne minimale (le minimum) de la min-entropie pour une valeur donnée L d'évaluation de Free CHSH-3. Ce minimum doit être valide pour toute configuration ayant comme valeur d'évaluation L. Cela équivaut à résoudre le problème suivant

$$\begin{aligned} \max_{i,\ell} \quad & \langle\psi|B_{i,\ell}|\psi\rangle \\ \text{s.t.} \quad & \langle\psi|f(B)|\psi\rangle = L \\ & \text{les mêmes contraintes que dans (5.19)} \end{aligned} \tag{5.30}$$

où $B = (B_1, ..., B_4)$.
Nous réutilisons itérativement la même méthode à l'œuvre pour la résolution de (5.19). En pratique, pour chaque valeur L, on optimise tous les moments d'ordre 1. Et alors, on retient la plus grande valeur de toutes ces valeurs " max du max". Ce processus est itéré pour différentes valeur de L, on obtient alors le graphe suivant

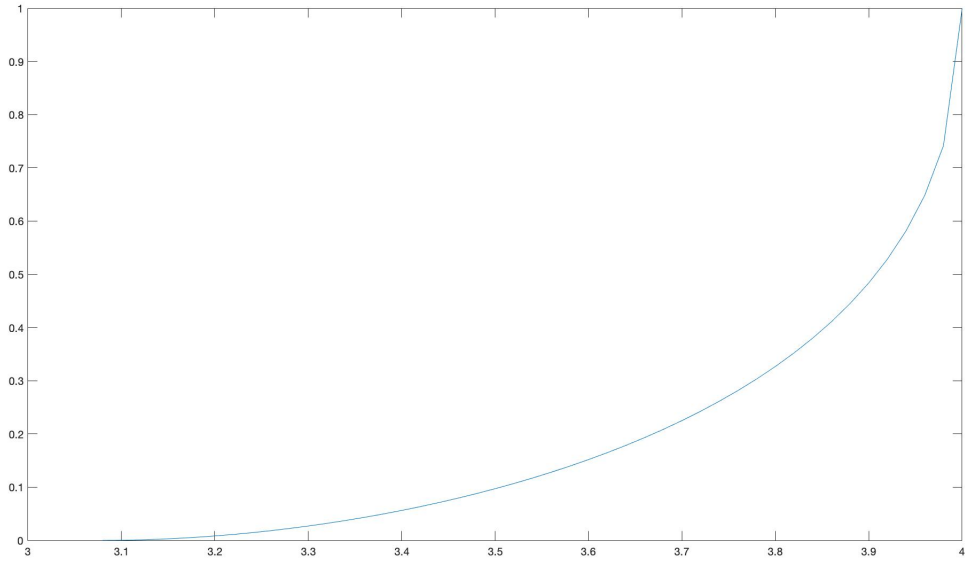

FIGURE 5.1 – Le minimum de la min-entropie f(L) versus différentes valeurs L de violation de Free CHSH-3

La courbe précédente, comme celle de [31, Figure 1], atteint l'entropie maximale pour la plus grande valeur 4 de Free-CHSH-3. Mais, à la différence de la précédente référence, la valeur de la min-entropie reste nulle pour des valeurs L plus grandes que la borne classique. Les valeurs non nulles apparaissent pour $L > 3.08$. Dans notre contexte, et dans le cadre quantique, l'heuristique 5.1 nous montre que, atteindre la valeur maximale $L = 4$ est équivalent à obtenir une min-entropie $H_{min} = 1\,trit$ pour chaque trit produit. Pour atteindre la notion d'indépendant du système (device independent), il nous faudra passer la contrainte de la preuve de sécurité 5.4.3 selon laquelle l'évaluation ne peut

se faire de manière exacte que pour les moments réels. Dans cette perspective, nous nous tournons vers les inégalités temporelles qui, elles aussi, font intervenir des produits d'observables potentiellement non-commutatives. Elles nous offrent de plus l'avantage que les moments optimisés sont des probabilités.

Les codes matlab de l'optimisation menée peuvent être trouvés dans [11].

Aux termes du chapitre 6 nous récapitulons, sous forme de tableaux, les inégalités étudiées et les protocoles qui en sont déduits.

Chapitre 6

Inégalités temporelles, cadre formel des produits d'observables incompatibles

Mots clés : *inégalités temporelles mesures séquentielles*

Contents

6.1 Objectif et résumé du chapitre

Le but de ce chapitre est la description des inégalités temporelles [21, 37]. Celles-ci sont similaires aux inégalités de Bell mais, à la différence, font intervenir des produits **d'observables éventuellement incompatibles**. Ces produits d'observables sont implémentés à l'aide de mesures séquentielles c'est-à-dire l'une à la suite de l'autre. Ces inégalités donnent des facteurs de violation plus importants que les inégalités de Bell classiques. Nous exposons ci-après les implications conceptuelles de ces violations. De plus, la notion de *résultat indéfini* étudiée précédemment (3.5.2) nous permet de déduire la cause de ces violations qui est, le caractère indéfini des résultats de mesures quantiques.

6.2 Inégalités temporelles, utilisation d'observables incompatibles

6.2.1 Principes généraux

Les inégalités temporelles sont développées notamment par les auteurs de [21, 37]. Ces inégalités ont la forme d'inégalités de Bell, dont les termes sont constitués de produits d'observables potentiellement non commutatives.

Ces inégalités temporelles peuvent ne faire intervenir que le produit d'une même observable, dont les mesures sont effectuées à des temps séparés, sur un ensemble de particules dans le même état. C'est le cas de l'inégalité de Leggett-Garg [52].

Elles peuvent aussi faire intervenir des produits d'observables incompatibles implémentées de manière séquentielle, c'est-à-dire l'une à la suite de l'autre : sur le système préparé dans l'état $|\psi\rangle$ on effectue la première mesure A_1. Et, sur le système résiduel, on effectue la mesure A_2. Ce deuxième cas permet la réécriture d'inégalités de Bell classiques en terme d'inégalités temporelles. C'est le cas de l'inégalité CHSH temporelle [37] ou l'inégalité KCBS temporelle [21]. Nos analyses, le long de cette thèse, porteront sur ce deuxième cas d'inégalités temporelles, implémentées avec des mesures projectives.

6.2.2 Corrélations et bornes temporelles

Dans cette sous-partie, nous explicitons le fait que l'ensemble des corrélations à l'œuvre dans les inégalités temporelles (les corrélations temporelles) est plus grand que l'ensemble des corrélations quantiques habituelles aussi appelées corrélations spatiales [37]. On atteint ainsi des bornes quantiques plus importantes, et cela du fait de la possible non commutativité des observables.

Définition 6.1. *Vecteur de corrélations (ou comportement)* ***quantiques habituelles ou spatiales***

Soit le vecteur $(C_{i,j})_{i=1,\dots,n;\ j=1,\dots,n;} \in \mathbb{C}^{n^2}$. *Ce vecteur est un comportement spatial (ou vecteur de corrélations quantiques habituelles) s'il existe des observables* A_i, B_j *agissant sur un espace de Hilbert* $\mathbb{H}$, *et un état* $|\psi\rangle \in \mathbb{H}$ *telles que :*

$$\forall i,j, \quad A_i \text{ commute avec } B_j \text{ et } C_{i,j} = \langle\psi|A_iB_j|\psi\rangle$$

Définition 6.2. *Vecteur de corrélations (ou comportement)* ***QUANTIQUES TEMPORELLES*** *pour qubits* $(d = 2)$ *[37, Proposition 2.1].*

Soit le vecteur $(C_{i,j})_{i=1,...,n;\ j=1,...,n;} \in \mathbb{C}^{n^2}$. *Ce vecteur est un comportement temporel (ou vecteur de corrélations quantiques temporelles) pour qubits, s'il existe des observables* A_i, B_j *agissant sur un espace de Hilbert* $\mathbb{H}$ *de valeurs propres* $\{\pm 1\}$, *et un état* $|\psi\rangle \in \mathbb{H}$ *telles que :*

$$\forall i, j,\ C_{i,j} = \frac{1}{2}\langle\psi|A_iB_j + B_jA_i|\psi\rangle \tag{6.1}$$

lemme 6.1. *Tout vecteur de corrélations quantiques spatiales est un vecteur de vecteur de corrélations temporelles. Mais l'inverse n'est cependant pas vrai.*

Démonstration. En effet, par la commutativité de A_i et B_j

$$C_{i,j} = \langle\psi|A_iB_j|\psi\rangle = \frac{1}{2}\langle\psi|A_iB_j + A_iB_j|\psi\rangle = \frac{1}{2}\langle\psi|A_iB_j + B_jA_i|\psi\rangle$$

À l'inverse, de manière générale, si A_i et B_j ne commutent pas,

$$\frac{1}{2}(A_iB_j + B_jA_i) \neq A_iB_j$$

□

Définition 6.3. *Généralisation [22, General Method] :*

Vecteur de corrélations (ou comportement) ***QUANTIQUES TEMPORELLES*** *pour qudits* $(d \geq 2$ *quelconque) et n mesures faites séquentiellement.*

Soit le vecteur $(C_{r,s})_{r=r_1,...,r_n;\ s=s_1,...,s_n;} \in \mathbb{C}^{n^d}$. *Ici, les* s_i *sont des observables sur* $\mathbb{C}^d$ *de valeurs propres* r_i. *Ce vecteur* $(C_{r,s})$ *est un comportement temporel (ou vecteur de corrélations quantiques temporelles) pour qudits, s'il existe des observables* s_1, ..., s_n *agissant sur un espace de Hilbert* $\mathbb{H}$ *de dimension d, et un état* $|\psi\rangle \in \mathbb{H}$ *telles que :*

$$\begin{aligned} C_{r,s} &= P(r|s) \\ Avec\ \ P(r|s) &= \langle\psi|\Pi(r|s)\Pi(r|s)^\dagger|\psi\rangle \\ Et\ \Pi(r|s) &= \Pi_{r_1}^{s_1}\Pi_{r_2}^{s_2}\cdots\Pi_{r_n}^{s_n} \end{aligned} \tag{6.2}$$

Le terme $P(r|s) = P(r_1, r_2, ..., r_n|s_1, s_2, ..., s_n)$ *est une probabilité séquentielle. Le tuple* $(r_1, r_2, ..., r_n|s_1, s_2, ..., s_n)$ *s'interprète comme étant le fait d'obtenir* r_1 *en effectuant la mesure* s_1 *sur l'état de départ, puis,* r_2 *en effectuant la mesure* s_2 *sur l'état résultant de la précédente mesure. Et ce jusqu'à obtenir* r_n *en effectuant la mesure* s_n *sur l'état résultant de la mesure* s_{n-1}. *De plus les* $\Pi_{r_i}^{s_i}$ *sont des projecteurs de dimension 1 (sur le vecteur propre de la mesure* s_i *relatif à la valeur propre* r_i*).*

En annexe (voir IV), nous montrons le lien entre la définition 6.2 et 6.3, c'est-à-dire le fait que la formule (6.2) généralise l'équation (6.1). Nous y montrons aussi que cette formule 6.2 traduit bien l'intuition décrite à la fin de la définition précédente.

Il faut noter que les vecteurs de corrélations temporelles permettent d'atteindre des bornes quantiques plus grandes. C'est le cas de l'inégalité KCBS qui est telle que la borne quantique spatiale est $4\sqrt{5} - 5 \approx 3.94$ [46] et la borne temporelle est $\frac{5}{4}(1 + \sqrt{5}) \approx 4.04$ [22]. Ainsi donc l'ensemble de corrélations temporelles contient strictement celui des corrélations quantiques spatiales (ou habituelles).

6.2.3 Borne en physique classique et interprétation, lien avec la valeur indéfinie

Les inégalités temporelles ont pour but premier de montrer une incompatibilité entre les deux assertions que devrait vérifier toute extrapolation directe des propriétés quantiques au cadre macroscopique [52]. De ce fait, la borne en physique classique pour les inégalités temporelles est établie sous ces deux assertions qui sont :

(A_1) Réalisme macroscopique : pour tout système ; dans toute base de l'espace des états de ce système, avec au moins deux états, ce système doit être continuellement et exactement dans un seul des états de base. (L'état d'un système est toujours le même avant mesure)

(A_2) Mesures non invasives à l'échelle macroscopique : pour toute mesure, il est possible, en principe, de déterminer l'état des systèmes avec une précision arbitraire sans introduire la moindre perturbation dans leur dynamique. (L'état d'un système est toujours le même, même après mesure)

Ainsi, lorsqu'on considère une inégalité temporelle, la borne classique est établie sous les deux hypothèses précédentes. Dans le cas de $KCBS_{seq}$ on a

$$S_5 = \langle B_1|B_2\rangle_{seq} + \langle B_2|B_3\rangle_{seq} + \langle B_3|B_4\rangle_{seq} + \langle B_4|B_5\rangle_{seq} - \langle B_5|B_1\rangle_{seq} \tag{6.3}$$

avec $\langle B_i|B_j\rangle_{seq}$ l'espérance de la mesure séquentielle du produit des observables B_i et B_j qui ont pour valeurs propres $\{\pm 1\}$. Et, sous les deux hypothèses précédentes on a [21],

$$S_5 \leq 3$$

Mais cependant, les mesures quantiques séquentielles permettent d'atteindre $S_5 = \frac{5}{4}(1 + \sqrt{5}) \approx 4.04$. Ainsi donc, au moins l'une des hypothèses (A_1) ou (A_2) est fausse dans le cadre quantique. Grâce au théorème de la valeur indéfinie (3.5.2), nous savons que l'hypothèse (A_1) n'est pas vérifiée. Il s'en suit que l'hypothèse (A_2) ne l'est pas. En effet, si le système peut être dans l'un ou l'autre des états de base, c'est bien le mécanisme de la mesure qui le transporte dans un état précis. On en déduit que la mesure introduit des perturbations.

6.2.4 Cas pratique de l'inégalité CHSH-3 temporelle et perspectives pour la production d'aléa

L'expression quantique CHSH-3 est décrite initialement dans [30] pour deux parties séparées. Cependant, dans la section 5.3.1 nous avons donné les détails techniques pour dériver une inégalité CHSH-3 pour une seule partie. Il en a résulté l'expression Free CHSH-3 (voir (5.15)) portant sur les corrélations du type $\langle\phi|X_{i\omega^k}X_{j\omega^\ell}|\phi\rangle$

Ici, dans le cadre des inégalités temporelles, nous dérivons une expression de CHSH-3 où les fonctions de corrélations sont désormais du type

$$\langle\phi|X_{i\omega^k}X_{j\omega^\ell}X_{i\omega^k}|\phi\rangle$$

Il faut aussi rappeler que ces corrélations sont des probabilités : $\langle\phi|X_{i\omega^k}X_{j\omega^\ell}X_{i\omega^k}|\phi\rangle = P(\omega^k,\omega^\ell|X_i,X_j)$.

Ainsi dans le cadre des inégalités temporelles, on a la formule suivante pour l'espérance du polynôme CHSH-3 :

$$\begin{aligned}
&\langle\phi|H_{seq}(X)|\phi\rangle = \\
&= \langle\phi|(\ X_{1,1}X_{3,1}X_{1,1} + X_{1,1}X_{4,1}X_{1,1} - X_{1,1}X_{3,\omega}X_{1,1} - X_{1,1}X_{4,\omega^2}X_{1,1} \\
&+ X_{1,\omega}X_{3,\omega}X_{1,\omega} + X_{1,\omega}X_{4,\omega}X_{1,\omega} - X_{1,\omega}X_{3,\omega^2}X_{1,\omega} - X_{1,\omega}X_{4,1}X_{1,\omega} \\
&+ X_{1,\omega^2}X_{3,\omega^2}X_{1,\omega^2} + X_{1,\omega^2}X_{4,\omega^2}X_{1,\omega^2} - X_{1,\omega^2}X_{3,1}X_{1,\omega^2} - X_{1,\omega^2}X_{4,\omega}X_{1,\omega^2} \\
&+ X_{2,1}X_{3,\omega}X_{2,1} + X_{2,1}X_{4,1}X_{2,1} - X_{2,1}X_{3,1}X_{2,1} - X_{2,1}X_{4,\omega}X_{2,1} \\
&+ X_{2,\omega}X_{4,\omega}X_{2,\omega} + X_{2,\omega}X_{3,\omega^2}X_{2,\omega} - X_{2,\omega}X_{3,\omega}X_{2,\omega} - X_{2,\omega}X_{4,\omega^2}X_{2,\omega} \\
&+ X_{2,\omega^2}X_{3,1}X_{2,\omega^2} + X_{2,\omega^2}X_{4,\omega^2}X_{2,\omega^2} - X_{2,\omega^2}X_{3,\omega^2}X_{2,\omega^2} - X_{2,\omega^2}X_{4,1}X_{2,\omega^2}\ )|\phi\rangle
\end{aligned} \tag{6.4}$$

6.2.4.1 Cadre temporel : borne en physique classique

La borne de l'expression temporelle de CHSH-3 dans le cadre de la physique classique est obtenue sous les deux assertions (A_1) et (A_2) (voir 6.2.3). Celles-ci peuvent être résumées comme suit :
L'état d'un système est toujours le même, à la fois avant et après mesure.
Ainsi, nous déduisons la borne classique en attribuant une valeur immuable à chaque observable. On obtient alors la borne classique :

$$B_{chsh3_{classique-temporelle}} = 2 \tag{6.5}$$

Nous donnons une analyse plus approfondie de la dérivation de cette borne en annexes (voir IV).

6.2.4.2 Cadre temporel : borne quantique

Pour obtenir la borne quantique séquentielle de l'inégalité CHSH-3, nous utilisons la méthode exposée à la section 5.3.3.3. Dans notre cas, l'optimisation porte sur les probabilités $P(\omega^k, \omega^\ell | X_i, X_j) = \langle \phi | X_{i\omega^k} X_{j\omega^\ell} X_{i\omega^k} | \phi \rangle$. Cela revient à effectuer une relaxation à mi-chemin entre le premier et le deuxième ordre, en l'occurrence l'ordre "1+AB" comme nommée dans [58, table 1]. Nous obtenons la borne séquentielle suivante

$$B_{chsh3_{seq}} \approx 3.235$$

Cette borne quantique du polynôme CHSH-3 dans le **cadre temporel** est plus grande que la borne quantique $1 + \sqrt{11/3} \approx 2.91$ obtenue dans le cas des observables commutatives. Ceci vient simplement du fait qu'en plus des observables commutatives, on s'autorise aussi les observables non commutatives. Il y a donc plus de choix et donc une borne maximale potentiellement plus grande.
Cependant, cette valeur est inférieure à la borne 4 obtenue dans le cadre free-CHSH3. Il faut noter en effet que les termes optimisés ne sont pas les mêmes. Tandis que dans le cadre des inégalités temporelles, l'optimisation est portée sur des probabilités, le sens physique des termes optimisés dans le cadre free CHSH-3 reste ardu à percevoir avec des mesures non commutatives.

6.2.4.3 Perspectives pour la production d'aléa sécurisée par les inégalités temporelles

Par l'optimisation précédente, nous extrayons, de la matrice de la relaxation d'ordre "$1 + AB$" la sous-matrice de la relaxation d'ordre 1.

1.0000	0.3333	0.3333	0.3333	0.3333	0.3333	0.3333	0.3333	0.3333	0.3333	0.3333	0.3333	0.3333
0.3333	0.3333	0	0	0.1194	0.0945	0.1194	0.2710	0.0452	0.0171	0.2710	0.0171	0.0452
0.3333	0	0.3333	0	0.1194	0.1194	0.0945	0.0171	0.2710	0.0452	0.0452	0.2710	0.0171
0.3333	0	0	0.3333	0.0945	0.1194	0.1194	0.0452	0.0171	0.2710	0.0171	0.0452	0.2710
0.3333	0.1194	0.1194	0.0945	0.3333	0	0	0.0452	0.2710	0.0171	0.2710	0.0452	0.0171
0.3333	0.0945	0.1194	0.1194	0	0.3333	0	0.0171	0.0452	0.2710	0.0171	0.2710	0.0452
0.3333	0.1194	0.0945	0.1194	0	0	0.3333	0.2710	0.0171	0.0452	0.0452	0.0171	0.2710
0.3333	0.2710	0.0171	0.0452	0.0452	0.0171	0.2710	0.3333	0	0	0.1800	-0.0267	0.1800
0.3333	0.0452	0.2710	0.0171	0.2710	0.0452	0.0171	0	0.3333	0	0.1800	0.1800	-0.0267
0.3333	0.0171	0.0452	0.2710	0.0171	0.2710	0.0452	0	0	0.3333	-0.0267	0.1800	0.1800
0.3333	0.2710	0.0452	0.0171	0.2710	0.0171	0.0452	0.1800	0.1800	-0.0267	0.3333	0	0
0.3333	0.0171	0.2710	0.0452	0.0452	0.2710	0.0171	-0.0267	0.1800	0.1800	0	0.3333	0
0.3333	0.0452	0.0171	0.2710	0.0171	0.0452	0.2710	0.1800	-0.0267	0.1800	0	0	0.3333

TABLE 6.1 – Sous-matrice de la relaxation d'ordre 1 de l'expression CHSH-3 séquentielle

Au vu de cette matrice 6.1, on peut extraire des observables et états permettant d'atteindre la valeur quantique séquentielle maximale avec de plus la propriété suivante :

- les moments de la forme $\langle \phi | X_{i,\omega^k} | \phi \rangle$ (qui sont les probabilités $P(\omega^k | X_{i\omega^k} | \phi \rangle))$ sont tous égaux à $\frac{1}{3}$, pour les projecteurs optimaux X_{i,ω^k}.

De ce fait, mesurer l'état optimal avec l'une des observables optimales donne le résultat 1, ω, ou ω^2, avec équiprobabilité (probabilité de $\frac{1}{3}$). On aurait alors une entropie maximale.

Les codes matlab de l'optimisation menée peuvent être trouvés dans [11].

Ainsi il serait intéressant de construire un générateur d'aléa sur cette propriété de ces états et mesures, dont la sécurité serait basée sur la violation maximale de l'expression CHSH3 séquentielle.

Le bémol est qu'il reste assez ardu de trouver les valeurs exactes de ces observables et états, du fait que l'optimiseur ne nous en donne que des valeurs approchées. Nous pourrons, pour de futurs travaux, utiliser les récentes améliorations proposées par les auteurs de [45, 70] permettant d'avoir des approximations plus précises.
De plus, nous sommes encouragés par la proposition de protocole "device independant" [56] basée sur une inégalité temporelle de Leggett–Garg.

Inégalité	**Physique Classique**		**Physique Quantique**		
	Hypothèses de départ	Borne	Hypothèse de départ	Borne	Conclusion vérifiée
CHSH-2 Originel (voir section 3.3.2) (Pour 2 parties de dimension $d = 2$)	Réalisme Local : • Résultats de mesures prédéfinis • Résultats non influencés par un environnement non immédiat	2	• Les 4 postulats de la physique quantique • **Produit d'observables commutatives** • Termes optimisés : $\langle\phi\|A_iB_j\|\phi\rangle$	$2\sqrt{2} \approx 2.828$	Non localité de la physique quantique
CHSH-2 pour un qutrit par $\Gamma()$ (voir section 5.2)	Réalité au niveau Macroscopique : • Résultats de mesures prédéfinis (Réalisme macroscopique) • Résultats non modifiés par la mesure (Mesure non invasive)	2	• Les 4 postulats de la physique quantique • **Produit d'observables potentiellement non-Commutatives** • Termes optimisés : $\langle\phi\|\Gamma(A_i)\Gamma(B_j)\|\phi\rangle$	$2\sqrt{2}$	• **Résultats indéfinis** ou bien • *Résultats préexistants mais modifiés par les mesures* (Hypothèse infirmée par le théorème du Résultat indéfini (Voir Strong KS 3.1))
CHSH-3 Originel (voir section 5.3.1). (CGLMP $d = 3$; 2 parties de dimension $d = 3$)	Réalisme Local : • Résultats de mesures prédéfinis • Résultats non influencés par un environnement non immédiat	2	• Les 4 postulats de la physique quantique • **Produit d'observables commutatives** • Termes optimisés : $P(\omega^k, \omega^\ell\|A_iB_j) = \langle\phi\|A_{i,\omega^k}B_{j,\omega^\ell}\|\phi\rangle$	$1 + \sqrt{11/3} \approx$ 2.915	Non Localité de la physique quantique

Inégalité	**Physique Classique**		**Physique Quantique**		
	Hypothèses de départ	Borne	Hypothèse de départ	Borne	Conclusion vérifiée
Free CHSH-3 (voir section 5.3.2) ou (Free CHSH-3 avec positivité, voir remarque de la section 5.3.2)	Réalité au niveau Macroscopique : • Résultats de mesures prédéfinis (Réalisme macroscopique) • Résultats non modifiés par la mesure (Mesure non invasive)	2	• Les 4 postulats de la physique quantique • **Produit d'observables potentiellement non-commutatives** • Termes optimisés : $\langle\phi\|X_{i,\omega^k}X_{j,\omega^\ell}\|\phi\rangle$ Ne correspondant pas à une probabilité dans le cas non commutatif (ou, avec de plus la positivité des coefficients $\langle\phi\|X_{i,\omega^k}X_{j,\omega^\ell}\|\phi\rangle \geq 0$)	4 ou 3.155	• **Résultats indéfinis** ou bien • *Résultats préexistants mais modifiés par les mesures* (Hypothèse infirmée par le théorème du Résultat indéfini (3.1))
CHSH-3 temporelle (séquentielle) voir section 6.2.4	Réalité au niveau Macroscopique : • Résultats de mesures prédéfinis (Réalisme macroscopique) • Résultats non modifiés par la mesure (Mesure non invasive)	2	• Les 4 postulats de la physique quantique • **Produit d'observables potentiellement non-commutatives** • Termes optimisés : $\langle\phi\|X_{i,\omega^k}X_{j,\omega^\ell}X_{i,\omega^k}\|\phi\rangle = P(\omega^k,\omega^\ell \mid X_i, X_j)$	3.235	• **Résultats indéfinis** ou bien • *Résultats préexistants mais modifiés par les mesures* (Hypothèse infirmée par le théorème du Résultat indéfini (voir Théorème Strong KS, Thm 3.1))

TABLE 6.3 – Inégalités étudiées ou développées dans cette thèse pour la sécurité de la production quantique d'aléa

Dans le tableau précédent, nous récapitulons les différentes inégalités travaillées au cours de cette thèse. Pour cela, nous donnons tout d'abord le cadre dans lequel la borne classique est obtenue ainsi que cette borne classique. Ensuite, nous donnons les hypothèses de la physique quantique utilisées pour chacune de ces inégalités ainsi que la valeur de cette borne quantique en question. Nous terminons par donner les conclusions vérifiées par ces valeurs quantiques.

Protocole	Inégalité utilisée	État et Observables utilisés	Sécurité
Favor (5.2.4)	CHSH-2 en dimension $d = 3$ 5.2	$\|\psi\rangle = \frac{1}{\sqrt{3}}(\xi\|+\rangle + \|0\rangle + \xi^3\|-\rangle)$; $\Gamma(A_1) = S_Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ avec $A_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $\Gamma(A_2) = S_X = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ avec $A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\Gamma(A_3) = S_y = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix}$ avec $A_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	Test de vérification d'état (indirectement lié à l'évaluation de CHSH-2 en dimension $d = 3$)
Gabriel (voir 5.4.2)	Free CHSH-3	$\|\phi\rangle = (1/\sqrt{3})(1,1,1)^\dagger$ $X_1 = Z = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}$ $X_2 = \begin{bmatrix} \omega & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ $X_3 = \frac{1}{3} \begin{bmatrix} -\omega & 2 & 2\omega^2 \\ 2 & -\omega^2 & 2\omega \\ 2\omega^2 & 2\omega & -1 \end{bmatrix}$ $X_4 = \frac{1}{3} \begin{bmatrix} -\omega^2 & 2\omega & 2 \\ 2\omega & -1 & 2\omega^2 \\ 2 & 2\omega^2 & -\omega \end{bmatrix}$	• Violation maximale de free CHSH-3 • Propriété de self-testing sous la condition des moments réels,
Réhoboth	CHSH-3 séquentiel	(en cours d'achèvement)	(en cours d'achèvement)

TABLE 6.4 – Protocoles de génération quantique d'aléa développés dans le cadre de cette thèse

Dans le tableau précédent, nous récapitulons les différentes protocoles développés au cours de cette thèse. Nous donnons les inégalités utilisées pour la sécurité ainsi que les configurations optimales utilisées.

Troisième partie

Autres travaux de la thèse

Chapitre 7

Autres aspects de la cryptographie quantique

Mots clés : *QKD, polynômes de Mermin*

Nous y abordons, en plus de la génération quantique d'aléa, des sujets connexes de la cryptographie quantique comme la distribution de clé quantique (QKD)

7.1 Protocole d'échange de clé quantique : Flat six-States (Poster TQC 2017)

7.1.1 Résumé

Nous présentons ici un protocole d'échange de clé (QKD), qui est une version basée sur l'intrication du protocole six-states [20] comme le font les auteurs de [36]. À la différence des précédents auteurs, nous utilisons la violation de l'inégalité quantique I3322 [75, equation 4] comme avantage pour la sécurité.

7.1.2 Idée de base

La distribution de clé quantique (QKD) permet la distribution de clé entre deux parties en utilisant des mécanismes basés sur la physique quantique. Pour ce faire, il existe essentiellement deux types de protocoles

1. Protocoles "Prepare and Measure" initiés par Bennett et Brassard (BB84) en [18]
2. Protocoles basés sur les propriétés d'intrication, initié par Ekert dans [35].

Le premier type de protocole peut aussi faire usage de paires de photons intriqués comme nous le montrent les auteurs de [36]. Dans ce cas, l'intrication n'est qu'une option et ne sert pas à vérifier la non-localité aux travers des inégalités de Bell. Les attaquants sont alors détectés par le sacrifice de certains bits de clé où les deux parties vérifient, publiquement, la similarité de ces données. La plupart du temps, un certain seuil t de bits d'erreur parmi n bits est toléré avec $t \ll n$.

La deuxième famille utilise essentiellement l'intrication comme base de sécurité au travers de violations d'inégalités de Bell.

Dans notre cas, nous étudions le protocole "Six States" [20], en testant de plus la non-localité au travers de l'inégalité I3322 suivante [75, equation 4] :

$$4 + E(A_1) + E(A_2) + E(B_1) + E(B_2) \\ + E(A_1B_1) + E(A_1B_2) + E(A_1B_3) + E(A_2B_2) - E(A_2B_3) + E(A_3B_1) - E(A_3B_2) \geq 0 \tag{7.1}$$

Dans notre cas, l'espérance $E(A_iB_j)$ désigne l'espérance du produit tensoriel $A_i \otimes B_j$ et, l'espérance $E(A_i)$ (ou $E(B_j)$) celle du produit tensoriel $A_i \otimes Id$ (ou $Id \otimes B_j$) avec Id l'identité sur l'espace.

7.1.3 Violation maximale et Protocole

Les auteurs de [75] nous indiquent que la violation maximale de cette inégalité est atteinte pour les mesures et l'état suivants :

$$\begin{aligned} A_1 = B_1 = -X &= \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \\ A_2 = B_2 = J = \tfrac{-1}{2}X + \tfrac{\sqrt{3}}{2}Y &= \begin{bmatrix} 0 & \omega^2 \\ \omega & 0 \end{bmatrix} \\ A_3 = B_3 = J^* = \tfrac{-1}{2}X - \tfrac{\sqrt{3}}{2}Y &= \begin{bmatrix} 0 & \omega \\ \omega^2 & 0 \end{bmatrix} \\ |S\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) & \end{aligned} \tag{7.2}$$

avec $\omega = exp(2i\pi/3)$ et $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Les bases propres de ces observables sont respectivement :
$(|+\rangle, |-\rangle)$ avec $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
la base $|\pm j\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm j|1\rangle)$ et enfin la base $|\pm j^*\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm j^*|1\rangle)$

Ainsi, l'état singlet $|S\rangle$ se réécrit dans ces bases :

$$|S\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) = \frac{1}{\sqrt{2}}(|j,-j\rangle - |-j,j\rangle) = \frac{1}{\sqrt{2}}(|j^*,-j^*\rangle - |-j^*,j^*\rangle)$$

À l'aide de cet état et des mesures précédentes (voir équation 7.2), la violation maximale est atteinte et vaut $\frac{5}{4}$. En effet, le membre de gauche de l'équation 7.2 vaut -1, ce qui signifie que la somme des espérances vaut -5 et donc un facteur de violation de $\frac{5}{4}$ (par rapport à la borne 4 de ces espérances).

Exécution :

Pour produire n qubits :

- Alice choisit 6n qubits dans six états choisis aléatoirement parmi les bases précédentes : $|-\rangle, |j\rangle, |j^*\rangle$ pour 0 et $|+\rangle, |-j\rangle, |-j^*\rangle$ for 1 (Elle choisit ainsi une certaine mesure et sa sortie). Pour chacun des qubits, elle envoie à Bob l'état opposé de la même mesure (par exemple $|-j^*\rangle$ si elle choisit $|j^*\rangle$). Cela est équivalent à distribuer les deux particules d'un état singlet ($|S\rangle$) entre Alice et Bob. Ainsi, si une mesure d'Alice (par exemple $A_1 = -X$) donne un état (par exemple $|+\rangle$) alors Bob a automatiquement l'état opposé de la même mesure (ici $|-\rangle$).

- Bob choisit $b \in \{1, 2, 3\}$, fait la mesure correspondante $B_1 = -X$, $B_2 = J$, et $B_3 = J^*$.

- Si $a = b$, les bits obtenus par Alice et Bob sont parfaitement corrélés et forment la CLÉ. En moyenne, $2n$ fois (c'est à dire $\frac{1}{3}$ des fois), Alice et Bob choisissent les mêmes mesures (3 mesures équiprobables). On a ainsi $2n$ bits de clé. On en sacrifie n bits pour la vérification de l'expression de I3322.

- Les autres choix, ainsi que les bits de clé sacrifiés, sont utilisés pour la vérification de l'inégalité I3322. Il faut noter que les espérances se calculent avec les valeurs propres (± 1) relatives aux états propres des observables A_i et B_j et non avec les bits $(0, 1)$ que ces états propres encodent.

7.1.4 Sécurité du protocole contre les attaques "Man in the middle"

La probabilité pour Bob d'obtenir le bon bit de clé après attaque d'Ève, disposant des mesures $B_e \in \{-X, J, J^*\}$, est :

$$P_b = \frac{3}{4} \simeq 0.75 \quad \text{(voir explication plus bas)}$$

Pour obtenir cette probabilité, considérons A_a la mesure choisie par Alice, et $|-\alpha_a\rangle$ l'état qu'elle choisit pour elle (correspondant à l'état $|\alpha_a\rangle$ qu'elle envoie à Bob). Lorsque l'attaquante Ève intercepte cet état, elle y effectue la mesure B_e et obtient l'état $|\varepsilon_e\rangle$ qu'elle envoie à Bob. Bob à son tour effectue la mesure $B_b = B_a$ (car pour la clé, $a = b$) et obtient l'état $|\beta\rangle$. On cherche la probabilité P_b d'avoir $|\beta\rangle = |\alpha_a\rangle$:

$$P_b \quad = \sum_{a,\alpha_a,e} P(A_a)\, P(\alpha_a)\, P(e) \sum_{\varepsilon_e} P(\varepsilon_e|\alpha_a, e) P(\alpha_a|\varepsilon_e, a)$$

avec $P(A_a)$ la probabilité pour Alice de choisir la mesure A_a, $P(\alpha_a)$ la probabilité que cette mesure (sur la portion du singlet chez Alice) donne l'état $|\alpha_a\rangle$. De plus, $P(e)$ désigne la probabilité pour Ève d'effectuer la mesure B_e. Le terme $P(\varepsilon_e|\alpha_a, e)$ désigne la

probabilité que la mesure B_e sur l'état $|\alpha_a\rangle$ donne l'état $|\varepsilon_e\rangle$. Enfin, le terme $P(\alpha_a|\varepsilon_e, a)$ désigne la probabilité que la mesure $B_b = A_a$ sur l'état $|\varepsilon_e\rangle$ donne l'état $|\alpha_a\rangle$.

$$P_b = \sum_{a,\alpha_a,e} \frac{1}{3}\frac{1}{2}\frac{1}{3} \sum_{\varepsilon_e} |\langle\alpha_a|\varepsilon\rangle|^2 |\langle\varepsilon|\alpha_a\rangle|^2 = \frac{1}{18} \sum_{a,\alpha_a,e,\varepsilon_e} |\langle\alpha_a|\varepsilon_e\rangle|^4$$

$$= \frac{1}{18}(6 \cdot 1 + 6 \cdot 0 + 12 \cdot 1/16 + 12 \cdot 9/16) = \frac{3}{4}$$

Avec un raisonnement similaire au précédent, nous obtenons la probabilité qu'un attaquant Êve obtienne le bon bit encodé par Alice :

$$P_e = \frac{13}{18} \simeq 0.722$$

Ces résultats sont un peu moins attrayants que ceux du protocole original six-states ($P_e = P_b = \frac{2}{3}$) car l'attaquant Êve a plus de chance d'obtenir le bon résultat. Mais cependant, on bénéficie de l'avantage de sécurité qu'est la vérification de l'expression de Bell $I3322$

	Standard six states	Flat six states
Probabilité de Bon résultat pour Êve	2/3	13/18
Probabilité de Bon résultat pour Bob après attaques	2/3	3/4

Test de l'inégalité de Bell
Nous pouvons de plus exploiter l'outil du test de non-localité avec l'expression de Bell $I3322$ (7.1). Nous obtenons une violation de $v = \frac{5}{4}$(voir explication au début de la section 7.1.3) et donc une résistance au bruit de $1 - \frac{1}{v} = 1/5$.

7.2 Généralisation des polynômes de Mermin

Dans cette recherche, nous nous intéressons à cet indicateur de non localité que constituent les polynômes de Mermin [57]. Il permettent de quantifier l'intrication multi-partite.

Notre contribution consiste à montrer que les polynômes de Mermin sont des polynômes homogènes de Bell introduits par François ARNAULT dans [12]. Cela nous permet de proposer, aux travers des inégalités homogènes de Bell, une généralisation en dimension $d > 2$ des polynômes de Mermin, basée sur la transformée de Fourier.

7.2.1 Définition propriétés

Dans cette section $d = 2$ ce qui signifie que nous travaillons dans le cas des qubits. Par la suite, nous étendrons aux dimensions $d > 2$;

Définition 7.1.

Les polynômes de Mermin sont définis sur $\mathbb{C}$ *ainsi :*

$$\begin{aligned} M_1 &= a_1 \qquad ; \qquad M_1' = a_1' \\ M_n &= \frac{1}{2}[(M_{n-1} + M_{n-1}')a_n + (M_{n-1} - M_{n-1}')a_n'] \end{aligned} \tag{7.3}$$

avec M_n' *obtenu à partir de* M_n *en interchangeant les observables prime et non-prime des* a_i*.*

Exemple 7.1.

$$\begin{aligned} M_2 &:= \frac{1}{2}[a_1a_2 + a_1a_2' + a_1'a_2 - a_1'a_2'] \\ M_2' &:= \frac{1}{2}[a_1'a_2' + a_1'a_2 + a_1a_2' - a_1a_2] \end{aligned}$$

Nous montrons par la suite, qu'en utilisant la définition précédente, les polynômes de Mermin M_n de degré n peuvent être vus comme des polynômes homogènes de Bell définis comme suit :

Définition 7.2. *Posons* ω*, racine d-ième de l'unité (*$\omega = e^{2i\pi/d}$*). Soient n parties ayant deux observables chacune (*A_i *et* B_i*) dont les issues (*a_i *et* b_i*) sont éléments de* $\omega^{\mathbb{Z}_d} := \{1, \omega, \cdots, \omega^{d-1}\}$*.*
Soit f une fonction $f : \{0,1\}^n \to \{1, \omega, \omega^2, ..., \omega^{d-1}\} = \{1, -1\}$ *(pour* $d = 2$*,* $\omega = -1$*) dont la transformée de Fourier est notée* $\hat{f} : \{0,1\}^n \to \mathbb{C}$*.*
Un polynôme homogène de Bell en dimension d sur n parties est donné par

$$P_f = \sum_{r \in \mathbb{Z}_d^n} \hat{f}(r) \prod_{i=1}^{n} A_i^{d-1-r_i} B_i^{r_i} \tag{7.4}$$

Il nous faut donc montrer que pour chaque M_n, $n \in \mathbb{N}$, il existe une fonction $f : \{0,1\}^n \to \{1, \omega, \omega^2, ..., \omega^{d-1}\} = \{1, -1\}$ (pour $d = 2$, $\omega = -1$) telle que sa transformée de Fourier $\hat{f} : \{0,1\}^n \to \mathbb{C}$ vérifie

$$M_n = cst_n\Big(\sum_{r \in \{0,1\}^n} \hat{f(r)} \prod_{i=1}^{n} a_i^{1-r_i} a_i'^{r_i}\Big)$$

avec cst_n une constante dans $\mathbb{C}$.

De plus chaque monôme a_i apparait à la puissance au plus 1.
Pour cela, nous utilisons la formule de construction itérative des polynômes homogènes de Bell (voir [12, page 8]) permettant de construire des polynômes à n variables (d'ordre n) en utilisant d polynômes d'ordre $n-1$:

$$P_0 \bowtie P_1 \bowtie ... \bowtie P_{d-1} = \sum_{r_n=0}^{d-1} a_n^{d-1-r_n} a'^{r_n} \sum_{t=0}^{d-1} \omega^{r_n.t} P_t$$

avec $\omega = e^{2i\pi/d}$.
Le polynôme résultant de cette opération est homogène d'ordre n et de degré $(d-1)n$
Dans le cas originel des polynômes de Mermin $d = 2$, et nous posons
$HB_{n-1} := c_{n-1}M_{n-1}$, $\quad HB'_{n-1} := c_{n-1}M'_{n-1}$, On obtient :

$$\begin{aligned} HB_{n-1} \bowtie HB'_{n-1} &= (c_{n-1}M_{n-1} + c_{n-1}M'_{n-1})a_n + (c_{n-1}M_{n-1} - c_{n-1}M'_{n-1})a'_n \\ &= 2c_{n-1}M_n \end{aligned}$$

et pour $n = 1$ nous avons $HB_1 = 2a_1 = 2M_1$; $\quad HB'_1 = 2a'_1 = 2M'_1$. Ainsi

$$c_n = 2^n$$

et on a

$$M_n = (1/2)^n HB_{n-1} \bowtie HB'_{n-1}$$

$cst_n = \frac{1}{c_n} = (1/2)^n$. Par la même démonstration et, en échangeant HB_{n-1} and HB'_{n-1} on trouve la même formule pour M'_n.

Ainsi nous avons montré que les polynômes de Mermin sont, à une constante près, de polynômes homogènes de Bell car ils vérifient la formule de récurrence (voir [12, page 8]). Il existe donc une fonction $f : \{0,1\}^n \to \{-1,1\}$ telle que sa transformée de Fourier $\hat{f} : \{0,1\}^n \to \mathbb{C}$ vérifie

$$M_n = (1/2)^n \Big(\sum_{r \in \{0,1\}^n} \hat{f}(r) \prod_{i=1}^{n} a_i^{1-r_i} a'^{r_i}_i \Big) \tag{7.5}$$

On peut, de la sorte, directement identifier un polynôme de Mermin à un vecteur de taille 2^n.

$$mat_{\hat{f}} = \begin{pmatrix} \hat{f}(0,0,...,0) \\ \hat{f}(1,0,...,0) \\ \vdots \\ \hat{f}(0,1,...,1) \\ \hat{f}(1,1,...,1) \end{pmatrix}$$

L'ordre originel de ce vecteur a été modifié pour avoir une meilleure vision de ce qui suit. Pour retrouver l'ordre originel, il suffit d'appliquer une matrice de permutation.

Exemple 7.2.
$M_2 := \frac{1}{2}[a_1a_2 + a_1a_2' + a_1'a_2 - a_1'a_2']$
M_2 est identifiée au vecteur :

$$\begin{pmatrix} \hat{f}(0,0) \\ \hat{f}(1,0) \\ \hat{f}(0,1) \\ \hat{f}(1,1) \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

Nous noterons cette représentation $\hat{f}_2()$
De même pour $M_3 = a_1a_2a_3' + a_1a_2'a_3 + a_1'a_2a_3 - a_1'a_2'a_3'$ identifié au vecteur

$$\hat{f}_3() = 8 \begin{pmatrix} \hat{f}(0,0,0) \\ \hat{f}(1,0,0) \\ \hat{f}(0,1,0) \\ \hat{f}(1,1,0) \\ \hat{f}(0,0,1) \\ \hat{f}(1,0,1) \\ \hat{f}(0,1,1) \\ \hat{f}(1,1,1) \end{pmatrix} = 4 \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

Pour étendre ces polynômes de Mermin en dimension $d > 2$, nous étudions les particularités des fonctions $\hat{f}$ auxquelles les polynômes sont identifiés.

7.2.2 Propriétés approfondies

Pour avoir une vision pratique de la construction du vecteur $\hat{f}_n()$, nous associons le terme a_i à 0 à la position i et le terme a_i' à 1 à la position i. Par exemple le monôme $a_1a_2a_3' \mapsto (0,0,1)$ et son coefficient dans M_3 est 1.

Nous pouvons aussi avoir un vecteur pour M_n' noté $\hat{f}_n(^-)$ qui est $\hat{f}_n()$ mais pris dans l'ordre inverse (du bas vers le haut). Ceci vient du fait que nous obtenons M_n' à partir de M_n en interchangeant les termes en prime avec ceux sans prime. On a donc

$$\begin{aligned} M_n' &= (1/2)^n \Big(\sum_{r \in \{0,1\}^n} \hat{f}(r) \Pi_{i=1}^n a_i'^{1-r_i} a_i^{r_i} \Big) \\ &= (1/2)^n \Big(\sum_{r \in \{0,1\}^n} \hat{f}(\bar{r}) \Pi_{i=1}^n a_i^{1-r_i} a_i'^{r_i} \Big) \end{aligned}$$

où $\bar{r}$ est obtenu à partir de r en échangeant 0 et 1.

7.2.2.1 Recurrence sur le vecteur $\hat{f}_n()$ et sur $f_n()$

Du fait qu'on ait :

$$\begin{aligned} M_n &= \frac{1}{2}(M_{n-1} + M'_{n-1})a_n + \frac{1}{2}(M_{n-1} - M'_{n-1})a'_n \\ &= (1/2)^n[\sum_{s\in\{0,1\}^{n-1}} (\hat{f}(s) + \hat{f}(\bar{s}))\ \Pi_{i=1}^{n-1}\ a_i^{1-s_i}a'^{s_i}_i)]\ a_n + \\ &\quad (1/2)^n[\sum_{s\in\{0,1\}^{n-1}} (\hat{f}(s) - \hat{f}(\bar{s}))\ \Pi_{i=1}^{n-1}\ a_i^{1-s_i}a'^{s_i}_i)]\ a'_n \end{aligned}$$

Nous ajoutons ainsi une autre composante au vecteur "s" : s_n.

$$= (1/2)^n \sum_{s_n\in\{0,1\}} [\sum_{s\in\{0,1\}^{n-1}} (\hat{f}(s) + (-1)^{s_n}\hat{f}(\bar{s}))\ \Pi_{i=1}^{n-1} a_i^{1-s_i}a'^{s_i}_i)]a_n^{1-s_n}a'^{s_n}_n$$

Et donc pour $r \in \{0,1\}^n$ on pose R le vecteur sans la composante r_n. Ainsi :

$$\hat{f}_n(r) = [\hat{f}_{n-1}(R) + (-1)^{r_n}\hat{f}_{n-1}(\bar{R})] \tag{7.6}$$

Au vu de l'équation précédente, nous pouvons avoir la vision selon laquelle, pour construire $\hat{f}_n(r)$, il y a deux groupes de r à distinguer : Ceux avec des 0 à la fin et ceux avec des 1. Pour le premier nous faisons une addition et pour le dernier, une soustraction. On obtient ainsi le vecteur suivant :

$$\hat{f}_n() = \begin{pmatrix} \hat{f}_{n-1}() + \hat{f}_{n-1}(^-) \\ \\ \hat{f}_{n-1}() - \hat{f}_{n-1}(^-) \end{pmatrix}$$

Qui peut se réécrire

$$\hat{f}_n() = \begin{pmatrix} Id_{2^{n-1}} & Id_{2^{n-1}} \\ \\ Id_{2^{n-1}} & -Id_{2^{n-1}} \end{pmatrix} \begin{pmatrix} \hat{f}_{n-1}() \\ \\ \hat{f}_{n-1}(^-) \end{pmatrix}$$

Ce qui signifie que

$$\hat{f}_n() = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes Id_{2^{n-1}} \cdot \begin{pmatrix} \hat{f}_{n-1}() \\ \\ \hat{f}_{n-1}(^-) \end{pmatrix} \tag{7.7}$$

avec

$$\hat{f}_1() = 2\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

On reconnait en la première matrice, la matrice de la transformée de Fourier H_2 pour $d = 2, n = 1$.

Par définition,

$$\hat{f}_n() = F_n f_n()$$

où F_n est la matrice de Fourier d'ordre n pour $d = 2$:

$$F_n = H_2^{\otimes n}$$

Nous avons

$$\begin{aligned} f_n() &= F_n^{-1} \hat{f}_n() \\ &= (1/2) \begin{pmatrix} F_{n-1}^{-1} & F_{n-1}^{-1} \\ \\ F_{n-1}^{-1} & -F_{n-1}^{-1} \end{pmatrix} . \begin{pmatrix} \hat{f}_{n-1}() + \hat{f}_{n-1}(^-) \\ \\ \hat{f}_{n-1}() - \hat{f}_{n-1}(^-) \end{pmatrix} \\ &= (1/2) \begin{pmatrix} 2 * f_{n-1}() \\ \\ 2 * f_{n-1}() + f_{n-1}(^-) \end{pmatrix} . \\ &= \begin{pmatrix} f_{n-1}() \\ \\ (-1)^{\omega(t)} f_{n-1}() \end{pmatrix} . \end{aligned}$$

nous obtenons

$$f_n(t) = (-1)^{\lfloor \frac{w(t)}{2} \rfloor} \tag{7.8}$$

Ainsi donc, une extension des polynômes de Mermin en dimension $d > 2$ peut être basée sur la matrice de la transformée de Fourier. Nous la présentons dans la section suivante.

7.2.3 Formule pour l'extension des polynômes de Mermin

Comme nous l'avons vu dans l'équation (7.7) pour le cas $(n, m, d) = (n, 2, 2)$ (avec n le nombre de parties, m le nombre de mesures, d la dimension de l'espace des parties), nous avons l'expression suivante pour le vecteur de Mermin donnant le polynôme de Mermin.

$$\hat{f}_n() = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes Id_{2^{n-1}} \cdot \begin{pmatrix} \hat{f}_{n-1}() \\ \\ \hat{f}_{n-1}(^-) \end{pmatrix} \text{ avec } \hat{f}_1() = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ \hat{f}_1(^-) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Pour avoir $\hat{f}_1(^-)$ nous inversons le vecteur $\hat{f}_1()$

Pour étendre au cas $(n, 2, d)$, on utilise H_d (matrice de Fourier avec d>2) telle que :

$$\hat{f}_n() = H_d \otimes Id_{d^{n-1}} \cdot \begin{pmatrix} \hat{f}_{n-1}() \\ \hat{f}_{n-1}(^1) \\ . \\ . \\ . \\ \hat{f}_{n-1}(^{d-1}) \end{pmatrix} \text{ avec } \hat{f}_1() = \begin{pmatrix} 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}, \hat{f}_1(^1) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}, ..., \hat{f}_1(^{d-1}) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ . \\ . \\ . \\ 1 \end{pmatrix} \tag{7.9}$$

Cela signifie que :

$$M_1 := a_1; \quad M_1' := a_1'; \quad M_1'' := a_1''; \quad ... \quad ; M_1^{(d)} := a_1^{(d)} \tag{7.10}$$

Pour construire l'extension du polynôme de Mermin, nous pouvons nous baser sur le point de vue suivant : Dans le polynôme initial de Mermin, pour passer de M_n à M_n' nous ajoutons un prime à tous les termes modulo 2 (2 primes = no prime). Ainsi, dans notre cas, pour passer de $M_1()$ à $M_1'()$ nous ajoutons un prime à tous les termes. Pour généraliser, le passage de $M_1^{(k)}()$ à $M_1^{(k+h)}()$ se fait en ajoutant h primes modulo n (n primes = no prime).

Nous définissons aussi les termes suivants pour tout d. Pour plus de lisibilité, nous commençons par décrire explicitement le cas $d = 3$. Puis nous donnons les formules pour d quelconque.

$$\begin{aligned} M_2 &= \frac{1}{3}[(a_1 + a_1' + a_1'')\, a_2 + (a_1 + \omega a_1' + \omega^2 a_1'')\, a_2' + (a_1 + \omega^2 a_1' + \omega a_1'')\, a_2''] \\ &= (\sum_{k=0}^{2} M_1^{(k)})\, a_2 + (\sum_{k=0}^{2} M_1^{(k)} \omega^k)\, a_2' + (\sum_{k=0}^{2} M_1^{(k)} \omega^{2k})\, a_2'' \\ &= \sum_{j=0}^{2} (\sum_{k=0}^{2} M_1^{(k)} \omega^{jk})\, a_2^{(j)} \end{aligned} \tag{7.11}$$

Cette formule est une implication de l'équation (7.9). On définit M_2' à partir de M_2 en ajoutant un prime modulo 3

$$M_2' = \frac{1}{3}[(a_1' + a_1'' + a_1)\, a_2' + (a_1' + \omega a_1'' + \omega^2 a_1)\, a_2'' + (a_1' + \omega^2 a_1'' + \omega a_1)\, a_2]$$

De même pour M_2'' à partir de M_2'

$$M_2'' = \frac{1}{3}[(a_1'' + a_1 + a_1')\, a_2'' + (a_1'' + \omega a_1 + \omega^2 a_1')\, a_2 + (a_1'' + \omega^2 a_1 + \omega a_1')\, a_2']$$

On a l'écriture contractée suivante :

$$M_2^{(\alpha)} = \frac{1}{3}\sum_{j=0}^{2}(\sum_{k=0}^{2} M_1^{(k+\alpha)}\omega^{jk})\, a_2^{(j+\alpha)}$$

Pour tout n nous avons cette formule de récurrence :

$$\begin{aligned} M_n = \frac{1}{3}[&(M_{n-1} + M'_{n-1} + M''_{n-1})\, a_n + (M_{n-1} + \omega M'_{n-1} + \omega^2 M''_{n-1})\, a'_n + \\ &(M_{n-1} + \omega^2 M'_{n-1} + \omega M''_{n-1})\, a''_n] \end{aligned} \tag{7.12}$$

$$M_n^{(\alpha)} = \frac{1}{3}\sum_{j=0}^{2}(\sum_{k=0}^{2} M_{n-1}^{(k+\alpha)}\omega^{jk})\, a_n^{(j+\alpha)}$$

Par extension, pour tout $d \in \mathbb{N},\ d > 1$:

Définition 7.3.
Pour tout $d \in \mathbb{N},\ d > 1$, avec ω racine d-ième de l'unité, le polynôme de Mermin en dimension d est défini pour tout $n \in \mathbb{N}$ par :

$$\begin{aligned} &M_1 := a_1; \quad M'_1 := a'_1; \quad M''_1 := a''_1; \quad \ldots \quad ; M_1^{(d)} := a_1^{(d)} \\ &M_n^{(\alpha)} = (\frac{1}{d})^n \sum_{j=0}^{d-1}(\sum_{k=0}^{d-1} M_{n-1}^{(k+\alpha)}\omega^{jk})\, a_n^{(j+\alpha)} \end{aligned} \tag{7.13}$$

Cette généralisation n'est pas toujours un polynôme homogène de Bell, du fait du nombre de mesures utilisées. Ainsi, nous rajoutons des contraintes sur les observables utilisées : Pour C_i et D_i deux observables unitaires de la 'i' ème partie, on pose , la k-ième observable de la partie 'i' :

$$A_i^{(k)} = C_i^k D_i^{d-1-k}$$

Propriété 7.1. *Avec la configuration décrite ci dessus, les polynômes de Mermin étendus que nous définissons, sont des polynômes homogènes de Bell (à une constante près).*

Démonstration. Grâce à la formule de récurrence nous le montrons que pour $n = 1$. En effet, l'application de cette formule permet de passer d'un polynôme de Bell sur n parties, à un polynôme de Bell sur $n+1$ parties. Nous donnons la preuve en dimension $d = 3$. Celle-ci est facilement généralisable à $d > 3$.
Nous avons, $M_1 = \frac{1}{3}(3A_1)$, $M'_1 = \frac{1}{3}(3A'_1)$, $M''_1 = \frac{1}{3}(3A''_1)$. M_1 est un polynôme homogène de Bell, cela revient à dire qu'il existe $f : \mathbb{Z}_d \mapsto \mathbb{U} = \{1, \omega, \omega^2\}$ telle que

$$M_1 = \frac{1}{3}\sum_{r\in\mathbb{Z}} \hat{f}(r) A^r B^{d-1-r} = \frac{1}{3}(\hat{f}(0)B^2 + \hat{f}(1)AB + \hat{f}(2)A^2) = \frac{1}{3}(3A^2)$$

avec $\vec{\hat{f}} = \begin{pmatrix} \hat{f}(0) \\ \hat{f}(1) \\ \hat{f}(2) \end{pmatrix} = 3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Ainsi, étant donné cette fonction $\hat{g} = 3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} g(0) \\ g(1) \\ g(2) \end{pmatrix}$ nous cherchons $f : \mathbb{Z}_d \mapsto \mathbb{U}$. Pour la trouver $f = \begin{pmatrix} f(0) \\ f(1) \\ f(2) \end{pmatrix}$ nous appliquons la transformée de Fourier inverse à "g" : $\frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix}$.
Du fait que nous eûmes trouvé une fonction de $\mathbb{Z}_d$ dans $\mathbb{U}$, nous avons une fonction f bien définie.

Ainsi donc, nous pouvons affirmer que M_1 et donc tous les polynômes de Mermin ainsi définis sont des polynômes homogènes de Bell. □

7.2.4 Bornes des polynômes

Avec le formalisme des polynômes homogènes, en dimension $d = 2$ nous déduisons la borne classique dans le cadre du réalisme local (défini dans la section 3.2).

$$M_n \in Hull(\mathbb{U}) \tag{7.14}$$

avec $Hull(\mathbb{U})$ l'enveloppe convexe de $(\mathbb{U}) = \{1, -1\}$ racine d-ième de l'unité $d = 2$ (voir [12, Page 6]).
Dans ce cas, on peut aussi écrire :

$$-1 \leq M_n \leq 1$$

qui est la borne classique du polynôme originel de Mermin.
On déduit ainsi la borne classique des polynômes de Mermin généralisés à travers les polynômes homogènes.

$$\forall d \text{ et } n, \qquad Re(e^{i\pi/d} M_n) \leq cos(\pi/d) \tag{7.15}$$

Borne Quantique
Nous n'avons malheureusement pas pu déterminer les bornes quantiques pour ces inégalités, cela, par manque de temps.

Chapitre 8

Conclusion

La production de nombres aléatoires (ou aléa) est une tâche de grande importance pour la sureté des protocoles de sécurisation de données. C'est pourquoi, au travers de ce manuscrit de thèse, nous avons montré l'apport que pourrait avoir l'utilisation de produits d'observables non commutatives pour une meilleure production quantique d'aléa.
En prélude, nous avons étudié les générateurs d'aléa n'étant pas basés sur la physique quantique. Ce faisant, nous avons mis en lumière le caractère déterministe des expériences utilisées par ces générateurs. Ainsi, bien que l'aléa généré nous soit imprédictible, cette imprédictibilité émane d'un manque d'information sur ces expériences dont les résultats sont déterminés d'avance. De ce fait, ces générateurs basés sur des expériences non quantiques, ne peuvent être considérés comme des candidats idéaux pour la génération d'aléa. On se doit donc de baser la génération d'aléa sur des expériences dont les résultats sont indéterminés. C'est cette propriété que nous offre la physique quantique, dont le caractère indéterminé des résultats de mesure est formellement montré (voir chapitre3).
La physique quantique est alors la base de protocoles de génération d'aléa (voir chapitre 4) essentiellement de deux types :

1) Les générateurs dont la sécurité est basée sur la description détaillée des appareils utilisés.

2) Les générateurs dont la sécurité est basée sur des inégalités quantiques.

Du fait de la difficulté à distinguer l'aléa intrinsèque de l'expérience quantique, et le bruit introduit par les imperfections des appareils, nous n'optons pas pour la première classe de générateurs. Nous nous focalisons alors sur le deuxième type de générateurs, ceux ci, basés sur des inégalités quantiques. Par conséquent, nos travaux de recherche portent essentiellement sur l'analyse et le développement d'inégalités quantiques pour la sécurité des protocoles. Nous en déduisons des protocoles de génération quantique d'aléa.

Dans ces travaux, nous partons de la remarque selon laquelle plus la violation (rapport entre la valeur de l'expression et sa borne en physique classique) entrainée par l'inégalité est grande, meilleure est la résistance aux bruits qu'elle permet (remarque démontrée dans le cas des protocoles utilisant l'intrication ; démonstration à étendre dans le cas de nos protocoles n'utilisant qu'une seule particule). Ainsi, nous déduisons, à partir d'inégalités déjà existantes pour deux parties (CHSH-2 et CHSH-3), des expressions en dimension $d = 3$ pour une partie, faisant intervenir des produits d'observables

potentiellement non commutatives. Cela permet d'obtenir des **violations aussi, voir plus élevées** que ne permettent les expressions originelles, tout en bénéficiant du **théorème du résultat indéfini** (voir théorème 3.1), qui est le cadre formel du caractère indéfini de presque tous les résultats de mesures quantique.

À cet effet, nous commençons par l'étude de l'inégalité CHSH-2, de laquelle nous déduisons une expression dans le cas d'un seul qutrit. Cela par le moyen de la fonction de symétrisation (Γ) permettant de transformer un opérateur sur qubit en un opérateur sur un qutrit (biphoton symétrique) (voir chapitre 5). Cette nouvelle expression atteint la même borne quantique que l'expression initiale, c'est à dire $2\sqrt{2}$. Sur cette valeur quantique, mais de manière indirecte, nous basons la sécurité du protocole de génération d'aléa présenté dans la section 5.2.4. Ce protocole donne de plus une entropie maximale.

Nous étudions aussi l'inégalité CHSH-3 (CGLMP d=3), initialement établie pour deux parties, chacune de dimension $d = 3$. Nous en déduisons une inégalité, Free CHSH-3 (voir section 5.15), pour une seule partie en dimension $d = 3$. De plus, on y autorise l'utilisation de produits d'observables non commutatives. Cette dernière possibilité permet d'atteindre une borne plus grande de 4, à défaut de 2.91 dans le cas d'observables uniquement commutatives. Sur cette borne, nous basons la sécurité du protocole de génération d'aléa GABRIEL, présenté dans la section 5.4. Ce protocole a de plus une entropie maximale. En outre, nous donnons des arguments pour le caractère "Self-testing". Ceux-ci sont basés sur le fait que, l'évaluation de l'expression Free-CHSH-3 donne une valeur maximale si et seulement si, le protocole mis en œuvre a une entropie maximale.
Néanmoins, ces arguments sont obtenus sous une hypothèse assez lourde : *" Les corrélations, générées par les observables et états utilisés dans le protocole, sont réelles"*. De plus, il est assez ardu de trouver un sens physique direct aux corrélations optimisées dans cette inégalité CHSH-3.

Au vu de ces limites que présentent nos protocoles précédemment exposés, nous explorons, en cette fin de thèse, la perspective des **les Inégalités Temporelles**. Celles-ci implémentent, dans un cadre plus formellement établi, les produits d'observables potentiellement non commutatives ; et cela de manière séquentielle (l'une à la suite de l'autre). Les corrélations utilisées dans ce cadre ont un sens physique et sont réelles (même positives), puisqu'elles sont des probabilités. Dans ce contexte, nous déduisons l'expression CHSH-3 temporelle ainsi que sa borne quantique qui est approximativement 3.235
Nous espérons construire un protocole de génération d'aléa basé sur les observables et états permettant d'atteindre cette borne maximale. Cela est motivé par les probabilités prometteuses qu'exhibe la matrice des moments. Celles-ci permettraient de construire un protocole avec une entropie maximale en sortie.
Cependant, ce chantier reste assez abrupte, du fait qu'on n'ait que les valeurs approchées

des optimiseurs de cette inégalité.
De futures recherches pourraient consister à étudier les spécificités des polynômes que nous développons pour utiliser les récentes solutions d'optimisation exposées en [45, 70]. Cela permettrait d'avoir des approximations plus précises des optimums et, plus facilement, leurs valeurs exactes.

Enfin, dérogeant à l'accoutumée, je ne saurais conclure sans remercier mon directeur, François ARNAULT ainsi que Simone NALDI pour leur aide inestimable dans l'accomplissement de cette thèse.

Quatrième partie

Annexes

Exemples, Démonstrations et Explications approfondies

Vision des produits scalaires et tensoriels

Exemple 8.1. *Utilisation du formalisme pour un calcul*

Considérons $\{|w_i\rangle\}$ une base orthonormale de W. L'application $(|w_j\rangle\langle w_j|)$ de W dans W a pour représentation dans la base $\{|w_i\rangle\}$ une matrice avec tous ses coefficients nuls sauf le seul coefficient (j,j) qui est égal à 1. (Le lecteur pour s'en convaincre pourra écrire la représentation dans la base et se rappeler que $\langle w_i|w_j\rangle = \delta_{i,j}$ c'est-à-dire 0 si $i \neq j$ et 1 si $i = j$).
Ainsi on a $I_w = \sum_j |w_j\rangle\langle w_j|$ qui est l'identité sur W. De même $I_v = \sum_j |v_j\rangle\langle v_j|$ où on considère $\{|v_j\rangle\}$ comme une base orthonormale de l'espace V. D'où , si $A : V \to W$, on aura $A = I_w A I_v$. Cela implique que

$$A = \sum_{i,j} |w_i\rangle\langle w_i|A|v_j\rangle\langle v_j|.$$

Ainsi si on applique A à $|v_k\rangle on\ a$

$$\begin{aligned} A|v_k\rangle &= \sum_i |w_i\rangle\langle w_i|A|v_k\rangle \\ &= \sum_i |w_i\rangle(\langle w_i|A|v_k\rangle), \text{ où la parenthèse est un produit scalaire donc un scalaire} \end{aligned}$$

l'on aura comme représentation matricielle pour A : $\begin{pmatrix} \langle w_1|A|v_1\rangle & ... & \langle w_1|A|v_m\rangle \\ \langle w_2|A|v_1\rangle & ... & \langle w_2|A|v_m\rangle \\ ... & & \\ \langle w_n|A|v_1\rangle & ... & \langle w_n|A|v_m\rangle \end{pmatrix}$

Grâce à la représentation précédente, l'on voit que

$$(|w\rangle\langle v|)^\dagger = |v\rangle\langle w|$$

En effet, en développant l'on constatera que si $|w\rangle = \begin{pmatrix} b_1 \\ b_2 \\ ... \\ b_m \end{pmatrix}$ et $|v\rangle = \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_n \end{pmatrix}$ alors $|w\rangle\langle v|$

a pour représentation

$$\begin{pmatrix} b_1 \\ b_2 \\ ... \\ b_m \end{pmatrix} \begin{pmatrix} a_1^* & a_2^* & ... & a_n^* \end{pmatrix} = \begin{pmatrix} b_1a_1^* & b_1a_2^* & ... & b_1a_n^* \\ b_2a_1^* & b_2a_2^* & ... & b_2a_n^* \\ ... & & & \\ b_ma_1^* & b_ma_2^* & ... & b_ma_n^* \end{pmatrix}$$

et $|v\rangle\langle w|$ a pour représentation

$$\begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_n \end{pmatrix} \begin{pmatrix} b_1^* & b_2^* & ... & b_m^* \end{pmatrix}$$

qui est exactement la transconjuguée de la précédente matrice .

De plus , l'on peut voir que le produit extérieur est linéaire par rapport à la première composante :

$$\forall\, a \,et\, b \,\in\, \mathbb{C} \,: (a\,|w_1\rangle + b\,|w_2\rangle)\langle v| = a\,|w_1\rangle\langle v| + b\,|w_2\rangle\langle v|$$

De même , l'on a une pseudo linéarité par rapport à la deuxième composante en ce sens que si l'on part de $c\,|v_1\rangle + d\,|v_2\rangle$ en lieu et place de $|v\rangle$ alors l'on a

$$|w\rangle(c^*\,\langle v_1| + d^*\,\langle v_2|) \;=\; c^*|w\rangle\langle v_1| + d^*|w\rangle\langle v_2|$$

On a c^* *et* d^* car l'on utilise à droite la transconjuguée du deuxième vecteur en l'occurrence dans notre cas $c\,|v_1\rangle + d\,|v_2\rangle$.

En règle générale, étant données deux matrices A et B , on a

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & ... & a_{1n}B \\ a_{21}B & a_{22}B & ... & a_{2n}B \\ ... & & & \\ a_{n1}B & a_{n2}B & ... & a_{nn}B \end{pmatrix}$$

Propriété 8.1. $\forall\, \lambda \in \mathbb{C}$ *on a*

$$\begin{aligned} (\lambda\, A) \otimes B &= \lambda\,(A \otimes B) \\ A \otimes (\lambda\, B) &= \lambda\,(A \otimes B) \\ (A_1 + A_2) \otimes B &= A_1 \otimes B + A_2 \otimes B \\ A \otimes (B_1 + B_2) &= A \otimes B_1 + A \otimes B_2 \end{aligned}$$

En revanche, le produit tensoriel est loin d'être commutatif.

Une dernière propriété du produit tensoriel très importante pour la suite des événements est la suivante :

Propriété 8.2. *Considérons* $|v\rangle \in V$, $|w\rangle \in W$, A *une matrice* $n \times n$ *agissant sur* V, *et* B *une matrice* $m \times m$ *agissant sur* W. *Alors, multiplier* $A \otimes B$ *par* $|v\rangle \otimes |w\rangle$ *revient à faire le produit tensoriel* $A|v\rangle \otimes B|w\rangle$.

En effet, en utilisant la notation d'Einstein qui permet d'écrire

$$\sum_{i_1} a_{1i_1} v_{i_1} = a_{1i_1} v_{i_1}$$

où deux termes indicés par les mêmes indices impliquent une somme sur cet indice, l'on a

$$A|v\rangle = \begin{pmatrix} \sum_{i_1} a_{1i_1} v_{i_1} \\ \\ ... \\ \sum_{i_n} a_{ni_n} v_{i_n} \end{pmatrix} = \begin{pmatrix} a_{1i_1} v_{i_1} \\ \\ ... \\ a_{ni_n} v_{i_n} \end{pmatrix}$$

D'où
On a d'une part

$$A|v\rangle \otimes B|w\rangle = \begin{pmatrix} a_{1i_1} v_{i_1} B|w\rangle \\ a_{2i_2} v_{i_2} B|w\rangle \\ ... \\ a_{ni_n} v_{i_n} B|w\rangle \end{pmatrix}$$

Et, d'autre part,

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = (A \otimes B) \begin{pmatrix} v_1|w\rangle \\ ... \\ v_n|w\rangle \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}B & a_{12}B & ... & a_{1n}B \\ a_{21}B & a_{22}B & ... & a_{2n}B \\ ... & & & \\ a_{n1}B & a_{n2}B & ... & a_{nn}B \end{pmatrix} \begin{pmatrix} v_1|w\rangle \\ ... \\ v_n|w\rangle \end{pmatrix}$$

$$= \begin{pmatrix} a_{1i_1} B\, v_{i_1}|w\rangle \\ a_{2i_2} B\, v_{i_2}|w\rangle \\ ... \\ a_{ni_n} B\, v_{i_n} B|w\rangle \end{pmatrix}$$

$$= \begin{pmatrix} a_{1i_1} v_{i_1} B|w\rangle \\ a_{2i_2} v_{i_2} B|w\rangle \\ ... \\ a_{ni_n} v_{i_n} B|w\rangle \end{pmatrix}$$ On peut permuter B et v_{i_j} car v_{i_j} est un scalaire.

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$$

De cela, l'on voit que si une transformation linéaire A est faite sur $|v\rangle$ dans V et une transformation linéaire B sur $|w\rangle$ dans W, cela revient à faire la transformation linéaire $A \otimes B$ sur $|v\rangle \otimes |w\rangle$.

Définitions des correlations temporelles et leurs implications

Les auteurs de [21] [37] considèrent, dans le cas $d = 2$, des expressions temporelles faisant intervenir des espérances de mesures séquentielles :

$$\sum_{i,j} f_{i,j}\, E(A_i A_j)_{seq} \tag{8.1}$$

avec

$$E(A_i A_j)_{seq} = \frac{1}{2}\langle\psi|A_i A_j + A_j A_i|\psi\rangle$$

représentant l'espérance de la mesure séquentielle $A_i A_j$.
En dimension d quelconque, une généralisation de la formule précédente est proposée,

considérant des corrélations sur les probabilités séquentielles

$$\sum_{r,s} C_{r,s} P(r|s) \tag{8.2}$$

avec les probabilités séquentielles $P(r|s) = P(r_1, r_2, ..., r_n|s_1, s_2, ..., s_n)$ où $r = (r_1, r_2, ..., r_n)$ représente les résultats des mesures $(s_1, s_2, ..., s_n)$. Le tuple $(r_1, r_2, ..., r_n|s_1, s_2, ..., s_n)$ s'interprète comme étant le fait d'obtenir r_1 en effectuant la mesure s_1 sur l'état de départ, puis, r_2 en effectuant la mesure s_2 sur l'état résultant de la précédente mesure. Et ce jusqu'à obtenir r_n en effectuant la mesure s_n sur l'état résultant de la mesure s_{n-1}.

Cette probabilité s'exprime à l'aide des projecteurs comme suit :

$$P(r|s) = \langle\psi|\Pi(r|s)\Pi(r|s)^\dagger|\psi\rangle \tag{8.3}$$

avec $\Pi(r|s) = \Pi_{r_1}^{s_1}\Pi_{r_2}^{s_2}\cdots\Pi_{r_n}^{s_n}$, et les Π_r^s des projecteurs de dimension 1.

Par la suite nous montrons le lien entre les formules du type (8.1) et celle du type (8.2)

Cas de deux mesures consécutives

Équivalence des formules (8.1) et (8.2) dans le cadre binaire

Le but de ce qui suit est de montrer l'équivalence entre les formules (8.1) et (8.2) dans le cadre de deux mesures binaires consécutives. Il s'agit plus particulièrement, de montrer, qu'en utilisant les probabilités séquentielles de (8.2) l'on aboutit à la formule

d'espérance apparaissant dans (8.1).
Par définition des espérances

$$E(A_iA_j)_{seq} = \sum_{k,\,\ell=+\,ou\,-} a_{i,k}a_{j,\ell}P(a_{i,k},\, a_{j,\ell} \mid (A_iA_j)_{seq})$$

avec $a_{i+} = +1,\ a_{i-} = -1,\ a_{j+} = +1,\ a_{j-} = -1,$ les valeurs propres des mesures A_i et A_j.
(La classique somme des issues multipliées par la probabilité de l'issue)

En utilisant la formule des probabilités séquentielles (8.3) en fonction des projecteurs, on a

$$E(A_iA_j)_{seq} = \sum_{k,\,\ell=+\,ou\,-} a_{i,k}a_{j,\ell}\ \langle\phi|A_{i,k}A_{j,\ell}A_{j,\ell}A_{i,k}|\phi\rangle$$

où $A_{i,k}$ est le projecteur de A_i sur sa valeur propre $a_{i,k}$

$$\begin{aligned} E(A_iA_j)_{seq} &= \sum_{k,\,\ell=+\,ou\,-} a_{i,k}a_{j,\ell}\ \langle\phi|A_{i,k}A_{j,\ell}A_{j,\ell}A_{i,k}|\phi\rangle \\ &= +\langle\phi|A_{i+}A_{j+}A_{i+}|\phi\rangle - \langle\phi|A_{i+}A_{j-}A_{i+}|\phi\rangle \\ &\quad - \langle\phi|A_{i-}A_{j+}A_{i-}|\phi\rangle + \langle\phi|A_{i-}A_{j-}A_{i-}|\phi\rangle \\ &= \langle\phi|(A_{i+}A_{j+}A_{i+} - A_{i+}A_{j-}A_{i+} - A_{i-}A_{j+}A_{i-} + A_{i-}A_{j-}A_{i-})|\phi\rangle \end{aligned}$$

D'autre part, l'expression $\frac{1}{2}\langle\psi|A_iA_j + A_jA_i|\psi\rangle$ donne

$$\begin{aligned} \frac{1}{2}\langle\phi|A_iA_j + A_jA_i|\phi\rangle = \quad & \frac{1}{2}\langle\phi|(A_{i+} - A_{i-})(A_{j+} - A_{j-}) \\ & + (A_{j+} - A_{j-})(A_{i+} - A_{i-})|\phi\rangle \end{aligned}$$

Or du fait du 3 ème postulat de la physique quantique (voir [59, section 2.2.3]), la somme de tous les projecteurs d'une même mesure est égale à l'identité. Plus particulièrement $A_{i+} + A_{i-} = Id$. Ainsi donc

$$
\begin{aligned}
\frac{1}{2}\langle\phi|A_iA_j + A_jA_i|\phi\rangle = \quad & \frac{1}{2}\langle\phi|(A_{i+} - A_{i-})(A_{j+} - A_{j-})(A_{i+} + A_{i-}) \\
& \quad + (A_{i+} + A_{i-})(A_{j+} - A_{j-})(A_{i+} - A_{i-})|\phi\rangle \\
= \quad & \frac{1}{2}\langle\phi|A_{i+}A_{j+}A_{i+} - A_{i+}A_{j-}A_{i+} - A_{i-}A_{j+}A_{i-} + A_{i-}A_{j-}A_{i-} \\
& \quad A_{i+}A_{j+}A_{i-} - A_{i+}A_{j-}A_{i-} - A_{i-}A_{j+}A_{i+} + A_{i-}A_{j-}A_{i+} \\
& \quad A_{i+}A_{j+}A_{i+} - A_{i+}A_{j-}A_{i+} - A_{i-}A_{j+}A_{i-} + A_{i-}A_{j-}A_{i-} \\
& \quad - A_{i+}A_{j+}A_{i-} + A_{i+}A_{j-}A_{i-} + A_{i-}A_{j+}A_{i+} - A_{i-}A_{j-}A_{i+}|\phi\rangle \\
= \quad & \langle\phi|A_{i+}A_{j+}A_{i+} - A_{i+}A_{j-}A_{i+} - A_{i-}A_{j+}A_{i-} + A_{i-}A_{j-}A_{i-}|\phi\rangle \\
= \quad & E(A_iA_j)_{seq}
\end{aligned}
$$

Ainsi, en utilisant la formule des probabilités séquentielles (8.3) l'on montre que l'on a effectivement $E(A_iA_j)_{seq} = \frac{1}{2}\langle\phi|A_iA_j + A_jA_i|\phi\rangle$. Le lien entre les formules (8.1) et (8.2) est ainsi établi.

Formules explicites et implications Dans le cas de deux mesures consécutives, on a effectivement la formule que l'on souhaite intuitivement pour des mesures séquentielles :

$$P(r_1, r_2|s_1, s_2) = P(r_1|s_1)P(r_2|r_1, s_1, s_2) \tag{8.4}$$

En effet,

$$
\begin{aligned}
P(r_1, r_2|s_1, s_2) &= \langle\psi|\Pi_{r_1}^{s_1}\Pi_{r_2}^{s_2}(\Pi_{r_1}^{s_1}\Pi_{r_2}^{s_2})^\dagger|\psi\rangle \\
&= \langle\psi|\Pi_{r_1}^{s_1}\Pi_{r_2}^{s_2}\Pi_{r_2}^{s_2}\Pi_{r_1}^{s_1}|\psi\rangle \\
&= \langle\psi|\,|x_{r_1}^{s_1}\rangle\langle x_{r_1}^{s_1}|\,|x_{r_2}^{s_2}\rangle\langle x_{r_2}^{s_2}|\,|x_{r_2}^{s_2}\rangle\langle x_{r_2}^{s_2}|\,|x_{r_1}^{s_1}\rangle\langle x_{r_1}^{s_1}|\,|\psi\rangle \\
&= \langle\psi|x_{r_1}^{s_1}\rangle\langle x_{r_1}^{s_1}|\psi\rangle \quad \langle x_{r_1}^{s_1}|x_{r_2}^{s_2}\rangle\langle x_{r_2}^{s_2}|x_{r_1}^{s_1}\rangle \quad \langle x_{r_2}^{s_2}|x_{r_2}^{s_2}\rangle \\
&= P(r_1|s_1) \quad P(r_2|r_1, s_1, s_2)
\end{aligned}
$$

Borne en physique classique de l'expression temporelle de CHSH-3

L'on souhaite obtenir la borne en physique classique de l'expression temporelle de CHSH-3. Pour cela nous étudions la structure du polynôme dans le cadre séquentiel et déduisons, sous les hypothèses de la physique classique spécifiques aux inégalités temporelles, la borne classique. L'inégalité originelle CHSH-3 fait intervenir deux parties distinctes et s'écrit [30, equation 5] :

$$\begin{aligned} I_3 =& P(A_1 = B_1) + P(A_2 = \omega^2 B_1) + P(A_2 = B_2) + P(A_1 = B_2) \\ & - P(A_1 = \omega^2 B_1) - P(A_2 = B_1) - P(A_2 = \omega^2 B_2) - P(A_1 = \omega B_2) \end{aligned} \tag{8.5}$$

Dans le cadre des inégalités temporelles, les mesures sont effectuées séquentiellement, on ne distinguera donc pas les parties (de même que dans le cas de l'inégalité free CHSH-3, voir 5.3.2). Ainsi les mesures sont ré-indicées : $A_1 \mapsto X_1$ $A_2 \mapsto X_2$, $B_1 \mapsto X_3$, $B_2 \mapsto X_4$. Par conséquent dans le cadre des inégalités temporelles on a l'expression suivante pour CHSH-3

$$\begin{aligned} I_{3\ seq} =& P(X_1 = X_3) + P(X_2 = \omega^2 X_3) + P(X_2 = X_4) + P(X_1 = X_3) \\ & - P(X_1 = \omega^2 X_3) - P(X_2 = X_3) - P(X_2 = \omega^2 X_4) - P(X_1 = \omega X_4) \end{aligned} \tag{8.6}$$

De ce fait, en terme de probabilités de résultats de mesures on a :

$$\begin{aligned} I_{3\ seq} =& P(1,1|X_1B_1) + P(\omega,\omega|X_1X_3) + P(\omega^2,\omega^2|X_1X_3) + P(\omega^2,1|X_2X_3) \\ & + P(1,\omega|X_2X_3) + P(\omega,\omega^2|X_2X_3) + P(1,1|X_2X_4) + P(\omega,\omega|X_2X_4) \\ & + P(\omega^2,\omega^2|X_2X_4) + P(1,1|X_1X_4) + P(\omega,\omega|X_1X_4) + P(\omega^2,\omega^2|X_1X_4) \\ & - P(1,\omega|X_1X_3) - P(\omega,\omega^2|X_1X_3) - P(\omega^2,1|X_1X_3) - P(1,1|X_2X_3) \\ & - P(\omega,\omega|X_2X_3) - P(\omega^2,\omega^2|X_2X_3) - P(1,\omega|X_2X_4) - P(\omega,\omega^2|X_2X_4) \\ & - P(\omega^2,1|X_2X_4) - P(\omega,1|X_1X_4) - P(\omega^2,\omega|X_1X_4) - P(1,\omega^2|X_1X_4) \end{aligned} \tag{8.7}$$

Cependant, contrairement au cas de l'expression free-CHSH-3, cette expression (8.7) est équivalente à l'expression faisant intervenir les projecteurs. Cette équivalence prévaut

même dans le cas de mesures non commutatives. On a ainsi :

$$\begin{aligned}
&I_{3\,seq} = \langle\phi|H_{seq}(X)|\phi\rangle = \\
&= \langle\phi|(\ X_{1,1}X_{3,1}X_{1,1} + X_{1,1}X_{4,1}X_{1,1} - X_{1,1}X_{3,\omega}X_{1,1} - X_{1,1}X_{4,\omega^2}X_{1,1} \\
&+ X_{1,\omega}X_{3,\omega}X_{1,\omega} + X_{1,\omega}X_{4,\omega}X_{1,\omega} - X_{1,\omega}X_{3,\omega^2}X_{1,\omega} - X_{1,\omega}X_{4,1}X_{1,\omega} \\
&+ X_{1,\omega^2}X_{3,\omega^2}X_{1,\omega^2} + X_{1,\omega^2}X_{4,\omega^2}X_{1,\omega^2} - X_{1,\omega^2}X_{3,1}X_{1,\omega^2} - X_{1,\omega^2}X_{4,\omega}X_{1,\omega^2} \\
&+ X_{2,1}X_{3,\omega}X_{2,1} + X_{2,1}X_{4,1}X_{2,1} - X_{2,1}X_{3,1}X_{2,1} - X_{2,1}X_{4,\omega}X_{2,1} \\
&+ X_{2,\omega}X_{4,\omega}X_{2,\omega} + X_{2,\omega}X_{3,\omega^2}X_{2,\omega} - X_{2,\omega}X_{3,\omega}X_{2,\omega} - X_{2,\omega}X_{4,\omega^2}X_{2,\omega} \\
&+ X_{2,\omega^2}X_{3,1}X_{2,\omega^2} + X_{2,\omega^2}X_{4,\omega^2}X_{2,\omega^2} - X_{2,\omega^2}X_{3,\omega^2}X_{2,\omega^2} - X_{2,\omega^2}X_{4,1}X_{2,\omega^2}\ )|\phi\rangle
\end{aligned} \tag{8.8}$$

Déduction de la borne en physique classique

Au vu de l'équivalence des expressions (8.6) $\Leftrightarrow$ (8.7) $\Leftrightarrow$ (8.8), nous utilisons l'expression (8.6) plus intuitive pour la déduction de la borne classique. Ainsi, en assignant une valeur fixe et immuable à chaque observable dans l'ensemble $\{1, \omega, \omega^2\}$ on obtient la borne classique :

$$I_{3\,seq} \leq 2$$

Bibliographie

[1] Alastair A. Abbott. *Value Indefiniteness, Randomness and Unpredictability in Quantum Foundations. (De la Valeur Indéfinie aux Notions d'Aléatoire et d'Imprévisibilité Quantiques)*. PhD thesis, École Normale Supérieure, Paris, France, 2015. (Cité en pages 27, 29 et 31.)

[2] Alastair A. Abbott, Cristian S. Calude, Jonathan Conder, and Karl Svozil. Strong kochen-specker theorem and incomputability of quantum randomness. *Physical Review A*, 86(6), Dec 2012. (Cité en page 32.)

[3] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil. A quantum random number generator certified by value indefiniteness. *Math. Struct. Comput. Sci.*, 24(3), 2014. (Cité en pages 46 et 61.)

[4] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil. Value-indefinite observables are almost everywhere. *Phys. Rev. A*, 89 :032109, Mar 2014. (Cité en pages 2, 3 et 32.)

[5] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Optics Express*, 22(2) :1645, Jan 2014. (Cité en page 35.)

[6] José Manuel Agüero Trejo and Cristian S. Calude. A new quantum random number generator certified by value indefiniteness. *Theoretical Computer Science*, 2020. (Cité en pages 2, 3, 29, 30, 32, 46 et 61.)

[7] Zoé Amblard. Cryptographie quantique et applications spatiales. 2016. (Cité en pages 37, 39, 43 et 45.)

[8] E.D. Anderson and K.D. Anderson. MOSEK : High performance software for large-scale LP, QP, SOCP, SDP and MIP including interfaces to C, Java, MATLAB, .NET and Python. *MOSEK, Copenhagen*, 2012. (Cité en page 56.)

[9] M.F. Anjos and J.B. Lasserre. *Introduction to Semidefinite, Conic and Polynomial Optimization*. Springer US, Boston, MA, 2012. (Cité en pages 55, 56, 59 et 60.)

[10] Don Jean Baptiste Anoman, François Arnault, and Simone Naldi. Quantum random number generator based on violations of the free chsh-3 inequality. `https://arxiv.org/abs/2003.00124`, 2020. (Cité en pages 2, 3, 5, 42, 60, 61, 63, 65 et 67.)

[11] Don Jean Baptiste Anoman, François Arnault, and Simone Naldi. Codes matlab. `https://github.com/donakou/SDPfreeCHSH3`, 2021. (Cité en pages 60, 67 et 74.)

[12] François Arnault. A complete set of multidimensional bell inequalities. *Journal of Physics A : Mathematical and Theoretical*, 45(25) :255304, may 2012. (Cité en pages 3, 17, 26, 86, 88 et 94.)

[13] François Arnault, Thierry Pierre Berger, Marine Minier, and Benjamin Pousse. Revisiting LFSRs for Cryptographic Applications. *IEEE Transactions on Information Theory*, 57(12) :8095–8113, 2011. (Cité en page 5.)

[14] François ARNAULT and Don ANOMAN. Random generation with the spin of a qutrit. https://arxiv.org/abs/2002.07675, 2020. (Cité en pages 2, 3, 5, 42, 45, 47, 49 et 50.)

[15] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment : A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49 :91–94, Jul 1982. (Cité en pages 15 et 24.)

[16] Lawrence (NIST) Bassham, Andrew (NIST) Rukhin, Juan (NIST) Soto, James (NIST) Nechvatal, Miles (NIST) Smid, Elaine (NIST) Barker, Stefan (NIST) Leigh, Mark (NIST) Levenson, Mark (NIST) Vangel, David (NIST) Banks, N. (NIST) Heckert, and James (NIST) Dray. Computer security resource center. https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final, 2010. (Cité en page 5.)

[17] JOHN S. BELL. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, 38 :447–452, Jul 1966. (Cité en pages 2, 3, 22 et 24.)

[18] Charles H. Bennett and Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *Theoretical Computer Science*, 560 :7–11, Dec 2014. (Cité en page 83.)

[19] David Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. i. *Phys. Rev.*, 85 :166–179, Jan 1952. (Cité en pages 22 et 27.)

[20] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14) :3018–3021, Oct 1998. (Cité en page 83.)

[21] C. Budroni. *Temporal Quantum Correlations and Hidden Variable Models*. Springer Theses. Springer International Publishing, 2015. (Cité en pages 68, 69, 71 et 104.)

[22] Costantino Budroni, Tobias Moroder, Matthias Kleinmann, and Otfried Gühne. Bounding temporal quantum correlations. *Physical Review Letters*, 111(2), Jul 2013. (Cité en pages 39, 43, 44, 70 et 71.)

[23] S. Burgdorf, I. Klep, and J. Povh. *Optimization of polynomials in non-commuting variables*. Springer, 2016. (Cité en page 56.)

[24] A. V. Burlakov, M. V. Chekhova, O. A. Karabutova, D. N. Klyshko, and S. P. Kulik. Polarization state of a biphoton : Quantum ternary logic. *Physical Review A*, 60(6) :R4209–R4212, Dec 1999. (Cité en page 46.)

[25] Philip J. Bustard, Doug Moffatt, Rune Lausten, Guorong Wu, Ian A. Walmsley, and Benjamin J. Sussman. Quantum random bit generation using stimulated raman scattering. *Opt. Express*, 19(25) :25173–25180, Dec 2011. (Cité en page 35.)

[26] Adan Cabello, Simone Severini, and Andreas Winter. (non-)contextuality of physical theories as an axiom, 2010. (Cité en pages 27 et 30.)

[27] B. S. Cirel'Son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2) :93–100, March 1980. (Cité en page 26.)

[28] J F Clauser and A Shimony. Bell's theorem. experimental tests and implications. *Reports on Progress in Physics*, 41(12) :1881–1927, dec 1978. (Cité en pages 23 et 24.)

[29] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23 :880–884, Oct 1969. (Cité en pages 3, 4, 21, 22, 24, 43 et 45.)

[30] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Physical Review Letters*, 88(4), Jan 2002. (Cité en pages 2, 3, 26, 43, 51, 72 et 107.)

[31] D. Deng, Chong Zu, X. Chang, Panyu Hou, H. Yang, Y. Wang, and L. Duan. Exploring quantum contextuality to generate true random numbers. 01 2013. (Cité en pages 65 et 66.)

[32] D. L. Deng, C. Zu, X. Y. Chang, P. Y. Hou, H. X. Yang, Y. X. Wang, and L. M. Duan. Exploring quantum contextuality to generate true random numbers, 2013. (Cité en page 28.)

[33] M. Drutarovsky and P. Galajda. A robust chaos-based true random number generator embedded in reconfigurable switched-capacitor hardware. In *2007 17th International Conference Radioelektronika*, pages 1–6, 2007. (Cité en page 6.)

[34] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete ? *Phys. Rev.*, 47 :777–780, May 1935. (Cité en page 22.)

[35] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67 :661–663, Aug 1991. (Cité en page 83.)

[36] Daphna G Enzer, Phillip G Hadley, Richard J Hughes, Charles G Peterson, and Paul G Kwiat. Entangled-photon six-state quantum cryptography. *New Journal of Physics*, 4 :45–45, jul 2002. (Cité en page 83.)

[37] Tobias Fritz. Quantum correlations in the temporal clauser–horne–shimony–holt (chsh) scenario. *New Journal of Physics*, 12(8) :083055, Aug 2010. (Cité en pages 2, 3, 68, 69, 70 et 104.)

[38] L-B. Fu, J-L. Chen, and X-G. Zhao. Maximal violation of Clauser-Horne-Shimony-Holt inequality for two qutrits. *Physical Review A*, 68, 09 2002. (Cité en page 53.)

[39] Solomon W. Golomb. *Shift Register Sequences*. Aegean Park Press, USA, 1981. (Cité en page 5.)

[40] Z. Gutterman, B. Pinkas, and T. Reinman. Analysis of the linux random number generator. In *2006 IEEE Symposium on Security and Privacy (S P'06)*, pages 15 pp.–385, 2006. (Cité en page 6.)

[41] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1), Feb 2017. (Cité en page 35.)

[42] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4) :1675–1680, Apr 2000. (Cité en page 35.)

[43] D. Kaszlikowski, L.C. Kwek, J-L. Chen, M. Żukowski, and C.H. Oh. Clauser-Horne inequality for three-state systems. *Phys. Rev. A*, 65 :032118, Feb 2002. (Cité en page 46.)

[44] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX :5–38, févr 1883. (Cité en page 1.)

[45] Igor Klep, Victor Magron, and Janez Povh. Sparse noncommutative polynomial optimization. *Mathematical Programming*, 2021. (Cité en pages 57, 74 et 97.)

[46] Alexander A. Klyachko, M. Ali Can, Sinem Binicioğlu, and Alexander S. Shumovsky. Simple test for hidden variables in spin-1 systems. *Phys. Rev. Lett.*, 101 :020403, Jul 2008. (Cité en pages 28 et 71.)

[47] Simon Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17 :59–87, 1967. (Cité en pages 22 et 27.)

[48] C. Kollmitzer, S. Schauer, S. Rass, and B. Rainer. *Quantum Random Number Generation : Theory and Practice*. Quantum Science and Technology. Springer International Publishing, 2020. (Cité en pages 8, 2 et 34.)

[49] R. Konig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9) :4337–4347, 2009. (Cité en page 62.)

[50] Paweł Kurzyński, Adrian Kołodziejski, Wiesław Laskowski, and Marcin Markiewicz. Three-dimensional visualization of a qutrit. *Phys. Rev. A*, 93 :062126, Jun 2016. (Cité en page 46.)

[51] J-B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3) :796–817, 2001. (Cité en page 56.)

[52] A. J. Leggett and Anupam Garg. Quantum mechanics versus macroscopic realism : Is the flux there when nobody looks ? *Phys. Rev. Lett.*, 54 :857–860, Mar 1985. (Cité en pages 2, 3, 43, 69 et 71.)

[53] Qing Lin and Bing He. Bi-directional mapping between polarization and spatially encoded photonic qutrits. *Physical Review A*, 80(6), Dec 2009. (Cité en page 46.)

[54] E.N. Lorenz. *The Essence Of Chaos*. Jessie and John Danz lectures. Taylor & Francis, 1995. (Cité en page 9.)

[55] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner. Self-testing

quantum random number generator. *Physical Review Letters*, 114(15), Apr 2015. (Cité en page 39.)

[56] Shiladitya Mal, Manik Banik, and Sujit K. Choudhary. Temporal correlations and device-independent randomness. *Quantum Information Processing*, 15(7) :2993–3004, 2016. (Cité en page 74.)

[57] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65 :1838–1840, Oct 1990. (Cité en page 86.)

[58] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7) :073013, jul 2008. (Cité en pages 38, 53, 59 et 73.)

[59] M.A. Nielsen and I.L. Chuang. Quantum computation and quantum information. *Phys. Today*, 54 :60–2, 2001. (Cité en pages 12, 18, 44, 52, 54, 57, 59, 60 et 105.)

[60] M. Oestreich, M. Römer, R. J. Haug, and D. Hägele. Spin noise spectroscopy in gaas. *Phys. Rev. Lett.*, 95 :216603, Nov 2005. (Cité en page 35.)

[61] A. Peres. All the bell inequalities. *Foundations of Physics*, 29 :589–614, 1999. (Cité en page 26.)

[62] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and et al. Random numbers certified by bell's theorem. *Nature*, 464(7291) :1021–1024, Apr 2010. (Cité en pages 2, 3, 8, 19, 37 et 38.)

[63] S. Pironio, M. Navascués, and A. Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM J. on Optimization*, 20(5) :2157–2180, May 2010. (Cité en pages 54, 56 et 57.)

[64] Henri Poincaré. *SCIENCE ET MÉTHODE*. Pages 64-65 FB Editions, 1920. (Cité en page 7.)

[65] Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, and Nicolas Gisin. Quantum random number generation on a mobile phone. *Physical Review X*, 4(3), Sep 2014. (Cité en pages 8 et 35.)

[66] Abner Shimony. *Contextual hidden variables theories and Bell's Inequalities*, volume 2, page 104–129. Cambridge University Press, 1993. (Cité en page 28.)

[67] J.F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optim. Methods Softw.*, 11/12(1-4) :625–653, 1999. (Cité en page 56.)

[68] Mark Um, Xiang Zhang, Zhang Junhua, Ye Wang, Yangchao Shen, D-L Deng, Lu-Ming Duan, and Kihwan Kim. Experimental certification of random numbers via quantum contextuality. *Scientific reports*, 3 :1627, 04 2013. (Cité en page 39.)

[69] Jase Vincent. Météo et théorie du chaos. `https://www.sciencepresse.qc.ca/blogue/vincent-jase/2016/09/20/meteo-theorie-chaos#`, 2020. (Cité en page 9.)

[70] J. Wang and V. Magron. Exploiting term sparsity in noncommutative polynomial optimization. *Computational Optimization and Applications*, 2021. (Cité en pages 57, 74 et 97.)

[71] S. Wehner. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Phys. Rev. A*, 73 :022110, Feb 2006. (Cité en pages 26, 56 et 57.)

[72] Charlotte Werndl. What are the new implications of chaos for unpredictability ?, 2013. (Cité en pages 7 et 9.)

[73] R. F. Werner and M. M. Wolf. All-multipartite bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64 :032112, Aug 2001. (Cité en page 26.)

[74] John A. Winnie. Computable chaos. *Philosophy of Science*, 59(2) :263–275, 1992. (Cité en pages 8 et 9.)

[75] Cezary Śliwa. Symmetries of the bell correlation inequalities. *Physics Letters A*, 317(3-4) :165–168, Oct 2003. (Cité en pages 83 et 84.)