Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés

Hamza Jaffali

THESE DE DOCTORAT DE L'ETABLISSEMENT UNIVERSITE BOURGOGNE FRANCHE-COMTE

PREPAREE A L'UNIVERSITE DE TECHNOLOGIE DE BELFORT-MONTBELIARD (UTBM)

Ecole doctorale n°37

SPIM (Sciences Pour l'Ingénieur et Microtechniques)

Doctorat d'informatique

Par

M. Jaffali Hamza

Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés

Thèse présentée et soutenue à Belfort, le 16 Octobre 2020

Composition du Jury :

M. Couturier Raphaël	Professeur – Université de Franche-Comté	Président
M. Perdrix Simon	Chargé de recherche – Loria	Rapporteur
M. Safey El Din Mohab	Professeur – Université de Sorbonne	Rapporteur
M. Franz Uwe	Professeur – Université de Franche-Comté	Examinateur
M. Jauslin Hans-Rudolf	Professeur – Université de Bourgogne	Examinateur
M. Luque Jean-Gabriel	Professeur – Université de Rouen	Examinateur
M. Nechita Ion	Chargé de recherche – IRSAMC	Examinateur
M. Holweck Frédéric	Maître de Conférences – UTBM	Directeur de thèse
M. Merolla Jean-Marc	Chargé de recherche – Femto-ST	Codirecteur de thèse

Remerciements

Je me dois de remercier en premier lieu mes parents, pour m'avoir ouvert les portes du savoir et de la sagesse. Je leur dois un remerciement profond pour m'avoir enseigné, accompagné, supporté et aidé durant toutes ces années. Mes paroles ne seront jamais à la hauteur de leurs sacrifices, mais je sais qu'ils seront rétribués à leurs justes valeurs. Je remercie également mes frères et sœurs, ma belle-mère, mes oncles et cousins, et le reste de ma famille, qui m'ont toujours soutenu dans ce projet et m'ont permis d'aborder certains problèmes sous un angle différent. Ils trouveront en ce manuscrit le produit de ces trois dernières années de travail, et je leur dédie sincèrement cette trace fugace.

C'est un honneur pour moi de pouvoir adresser ici toute ma gratitude et ma reconnaissance à Frédéric Holweck pour ces trois années durant lesquelles il a été mon directeur de thèse. Mais notre collaboration a débuté bien avant : je le remercie également pour m'avoir partagé l'amour des mathématiques et de la recherche tout au long de mes études d'ingénieur, et de m'avoir fait découvrir différents domaines où les mathématiques apparaissent aussi belles qu'indispensables. C'est en grande partie grâce à cet encadrement de qualité, tant sur le plan humain, pédagogique que scientifique, que j'ai pu arriver aussi loin dans mon voyage dans le monde des sciences. Frédéric m'a toujours fait confiance tout au long de nos échanges, et ce depuis les premiers instants, et m'a procuré une liberté d'action et une autonomie qui m'a permis de m'épanouir dans mes recherches. Il a également su être là dans les moments difficiles, pour m'aiguiller, m'accompagner et me conseiller avec justesse et bienveillance. Aussi, il a toujours fait en sorte de prendre les décisions qui m'étaient les plus bénéfiques en tant que chercheur et étudiant, ce qui en fait un directeur de thèse et un enseignant comme il en existe très peu, et je suis fier d'avoir été l'élève de ce chercheur talentueux. "Pour tout cela donc un grand merci".

Je tiens de même à remercier sincèrement Jean-Marc Merolla pour ces trois années durant lesquelles il a également été mon directeur de thèse. L'expérience et la maîtrise de Jean-Marc dans son domaine ont été une source d'inspiration pour moi, tout comme sa capacité à partager avec passion ses expériences éblouissantes. Jean-Marc a toujours su me conseiller avec sagesse afin que je puisse progresser dans ma manière de communiquer, de restituer et d'organiser les informations dans mes prises de parole. Il a toujours fait tout son possible pour me permettre de bénéficier des meilleurs conditions de travail, et je le remercie également pour cela. L'humour et la bonne humeur constante de Jean-Marc ont également été pour moi une confirmation que l'on pouvait atteindre l'excellence scientifique tout en entretenant des relations chaleureuses avec ses collaborateurs.

It is also a pleasure for me to switch in english in order to pay my special regards to Luke Oeding, who had the kindness to invite me at Auburn University for sharing great knowledge and great moments. He supervised me during my stay at Auburn, and allowed me to progress in the best environment, to supervise at my turn the learning of our neural networks. A talented mathematician with whom I had the honor to work. Loved the city, loved the man, and loved his family : thank you for all.

Je voudrais poursuivre par des remerciements distingués à mes rapporteurs de thèse Simon Perdrix et Mohab Safey El Din. Je les remercie tout d'abord d'avoir accepté de rapporter mon travail, et les remercie de même pour le temps qu'ils ont consacré à la lecture de mon manuscrit, à la formulation des remarques et à la production du rapport.

J'ai eu l'occasion de rencontrer Simon Perdrix durant les différentes Journées Information Quantique organisées par le GDR-IM, durant les colloques organisés par le GRD-IQFA, ainsi que lors de sa visite à Belfort et Besançon. J'ai pu apprécier les différentes discussions que l'on a pu avoir, les encouragements et les retours positifs dont il m'a fait part concernant mes travaux sur l'apprentissage supervisé de l'intrication et l'étude de l'intrication dans les algorithmes quantiques. Sans le savoir, et de par le travail qu'il développe avec son équipe au sein du Loria, il n'a fait que confirmer ma motivation à vouloir développer la connaissance et la recherche dans le domaine de l'information quantique en France.

À l'heure où je rédige ces remerciements, je n'ai pas encore eu l'occasion de rencontrer Mohab Safey El Din, mais ses travaux dans le domaine de la géométrie algébrique m'ont déjà conquis. En effet, je suis à la fois passionné d'informatique et de mathématiques, et les contributions de Mohab Safey El Din viennent encore une fois démontrer que ces deux domaines peuvent s'associer pour laisser émerger des solutions à des problèmes variés, tant dans leur formulation que dans leur difficulté. Je suis ravi de pouvoir lui présenter mes humbles travaux alliant informatique quantique et géométrie algébrique, et le remercie pour son retour et son intérêt.

Je remercie Jean-Gabriel Luque, Uwe Franz, Hans Jauslin, Ion Nechita et Raphael Couturier d'avoir accepté de faire partie de mon jury thèse, et je suis honoré par leur présence. J'ai eu l'opportunité d'échanger avec Jean-Gabriel Luque lors de mes deux présentations sur les algorithmes quantiques dans le cadre des séminaires du projet Moustic. Je le remercie pour ces invitations et pour les indications précieuses qu'il a pu me partager en début de thèse. En effet, j'ai commencé mes travaux à partir de ceux déjà développés par Frédéric et Jean-Gabriel, et leur article sur la classification des 4-qubits et l'utilisation de la théorie des invariants fut pour moi un document de chevet. J'ai également pu rencontrer Uwe Franz et Hans Jauslin à diverses occasions, car étant investis dans le même projet de recherche régional. Je n'oublierai pas le cours de Uwe Franz sur les inégalités de Bell qui me permit d'atteindre un niveau de compréhension qui m'a été utile pour le développement de travaux en lien avec la détection de l'intrication. J'ai également pu rencontrer Ion Nechita lors des dernières Journées Information Quantique à Besançon, où j'ai pu recevoir de nombreux conseils, questions et suggestions après une présentation de mes travaux sur l'apprentissage machine. Enfin, à l'heure où je finalise ce manuscrit, j'ai pu intégrer l'équipe de recherche de Raphael Couturier au laboratoire Femto-ST. Je le remercie pour son accueil lors de mon arrivée, et pour les conseils et les questions pertinentes dont il a pu me faire part avant ma soutenance de thèse. Je garde un très bon souvenir de ces différentes rencontres.

Durant ma thèse, j'ai eu l'occasion de voyager et d'être accueilli par différents instituts et universités. Ces voyages ont été riches en rencontres et en expériences, et je tenais ici à remercier toutes les personnes qui ont rendu ces déplacements possibles, et dans de si bonnes conditions. En particulier, je tiens tout d'abord à remercier Adil Belhadj

pour son accueil chaleureux à l'Université de Sultan Moulay Slimane à Beni Mellal, et je remercie également les différents doctorants ainsi que les professeurs organisateurs. Je me dois également de remercier Metod Saniga qui a toujours été très bienveillant et accueillant lors de nos visites à l'Institut Astronomique de Tatranská Lomnica. J'ai pu découvrir le domaine de la géométrie finie, et la passion que Metod développait pour ce domaine. Je remercie également l'Université d'Auburn, et plus particulièrement le département COSAM et ses membres pour l'accueil et l'aide apportée tout au long de mon séjour. J'ai une pensée particulière pour Mark Carpenter et ses cours d'apprentissage statistique, pour Hans-Werner Van Wykainsi, ainsi que pour Philippe Gaillard qui également a fait preuve d'une hospitalité qui m'a touché. Je me dois également de remercier le CIAD et son directeur Stéphane Galland pour l'accueil au sein de ses locaux durant mes premières années de thèse, et pour l'invitation à une présentation en séminaire. Je remercie par la même occasion les différents membres du laboratoire Femto-ST, de l'observatoire et du laboratoire de mathématiques de Besançon, pour leur accueil lors de mes différentes visites.

Ces années d'études et ces années de thèse ont également été enrichissantes pour moi sur le plan de la collaboration scientifique et aussi du point de vue de l'enseignement. Je tenais à remercier ici chaque personne avec qui j'ai pu échanger et travailler tout au long de mon doctorat. Je pense en particulier à Fabrice Lauri, mon premier voisin de bureau, avec qui j'ai eu des discussions passionnantes sur différents sujets scientifiques, et avec qui j'ai pu partager des parties d'échecs durant les pauses. J'ai également eu l'occasion d'y jouer avec Henri de Boutray, avec qui j'ai eu l'honneur de collaborer durant ma thèse sur la question de l'intrication et des algorithmes quantiques. Je remercie Peter Lévay, physicien et mathématicien hors pair, avec qui j'ai pu partager des discussions sur divers sujets profonds et toujours intéressants. Je pense aussi à Franck Gechter, enseignant exceptionnel que j'ai eu la chance d'avoir, et qui m'a motivé à poursuivre mes études en doctorat, et qui continue également de m'inspirer à travers sa vision de l'informatique, de l'enseignement et de la science de manière générale. Je remercie également Alain Giorgetti et Pierre-Alain Masson pour leur collaboration dans la recherche et pour les différentes discussions et conseils précieux. J'ai également une pensée pour Marc Bataille, avec qui j'ai pu partager des discussions intéressantes sur l'intrication générée par les circuits quantiques et les algèbres sous-jacentes. Julien Barbier a également été mon voisin de bureau, et nous avons pu partager différentes discussions autour de l'informatique 3D et divers autres sujets très intéressants. Enfin plus récemment, ce fut un plaisir pour moi de collaborer et de partager des moments avec Joeffrey Boffelli et Grâce Amouzou, et je leur souhaite une grande réussite dans leurs études. Je remercie par la même occasion tout le département informatique de l'UTBM, et notamment Denise Simon pour leur accueil et leur bienveillance.

Enfin, je remercie mes amis et mes proches pour m'avoir soutenu et supporté durant ces années. Je pense bien entendu à Zine, présent depuis le début de l'aventure, et m'ayant toujours conseillé, mais également inspiré par son sens du travail sérieux et bien accompli, et par sa curiosité intellectuelle. C'est en partie grâce à lui que je suis actuellement arrivé au point de soutenir ma thèse de doctorat. J'ai aussi une pensée particulière pour Ismaël, à l'intelligence et à la vivacité d'esprit impressionnante, aussi co-auteur de mon premier article scientifique. C'est avec lui que j'ai mis la première

fois le pied dans le monde quantique, et nous avons toujours été avec Ismaël comme une paire de particules intriquées : l'excitation de l'un engendrait instantanément l'excitation de l'autre. Je pense également à Hedi, doctorant au laboratoire Femto-St, avec qui j'ai partagé des discussions intéressantes sur divers sujets, et qui a toujours été à mes côtés tout au long de mon doctorat. J'admire son sérieux et sa remise en question permanente, et j'espère qu'il atteindra les hautes sphères de la recherche et de l'enseignement en France. Je pense aussi à Salah-Eddine, m'ayant accompagné durant mes études d'ingénieur et au delà, et ayant un sens de l'innovation et du marketing hors-pair. Il a souvent su me faire comprendre de manière subtile que j'allais dans la mauvaise direction, et a toujours été de bon conseil. Une partie de moi est aussi toujours connectée à Hamid, que je remercie pour les exercices de pensée et les méditations qui m'ont inspiré dans mes travaux de recherche. Je n'oublie pas Kevin, mon binôme inséparable, m'ayant accompagné durant mes diverses péripéties mathématiques et humoristiques, et avec qui je continue d'entretenir des liens fraternels. Je remercie enfin Radouan, qui a été à mes côtés durant toutes ces années et a su me motiver, mon conseiller et m'ouvrir la porte d'idées de recherche que j'ai hâte de développer et de vous partager. Je remercie le *cinq de légende* : lieu d'amitié, de partage et de motivation quotidienne. Je remercie aussi Youcef, qui a participé considérablement à ma formation et mon éducation, et qui m'a appris à appréhender différemment La Science. Je remercie aussi une personne qui se reconnaîtra dans cette phrase, et que je n'oublie pas.

Mes remerciements vont également à toutes les personnes qui m'ont aidé à la relecture de ce manuscrit. Je les remercie pour m'avoir offert mes erreurs et défauts dans la rédaction ou dans la présentation des idées.

Je ne peux bien entendu citer tous ceux qui m'ont accompagné tout au long de mon doctorat, mais je tenais tout de même à remercier explicitement un maximum de personnes, et de prendre le temps ... De nos jours, il est difficile de prendre son temps, et c'est pourquoi je tiens pour terminer à remercier mes *frères* pour l'étude et le partage autour de la notion du temps.

Je salue enfin le lecteur de ce manuscrit, et espère qu'il y trouvera une science utile pour lui et pour les vivants.

"*Le soleil ne peut rattraper la lune, ni la nuit devancer le jour, et chacun vogue dans* ***une orbite***" [121].

Je dédie ce manuscrit
À toute ma famille
Et à la *vraie famille*

Propos préliminaire

Depuis les origines de la vie humaine, l'Homme n'a cessé d'évoluer et de progresser dans la contrée des Sciences et des Connaissances, à la recherche d'une réponse, d'une compréhension et d'une explication des divers phénomènes qu'il peut rencontrer ou observer dans le monde qui l'entoure. Cet héritage ne cesse d'évoluer, et peut parfois converger, vers une description plus précise et plus générale de la réalité observée ou conçue, mais demeurera indéniablement incomplet et inconsistant. En revanche, cela n'empêche pas l'émergence de nouvelles idées et concepts, motivés par de nouveaux constats pratiques et résultats théoriques. Parmi les théories et disciplines modernes, émergentes et bouleversantes de ce dernier siècle, figure celle de la Mécanique Quantique (MQ), s'attachant à étudier et décrire les phénomènes physiques fondamentaux à l'œuvre à l'échelle atomique et subatomique [280].

C'est de cette dernière discipline qu'est née la Théorie de l'Information Quantique (TIQ), domaine alliant à la fois physique, mathématiques et informatique. Prolongeant la Théorie de l'Information, discipline tout aussi bouleversante développée par Shannon, elle vise à exploiter les propriétés quantiques des particules utilisées comme support de l'information. Toute la discipline se développe donc autour de la manipulation théorique et expérimentale de cette information quantique, et des différents phénomènes physiques pouvant intervenir.

La TIQ s'est développée depuis sa première suggestion par les travaux de Feynman, et permit l'émergence de divers domaines d'études : la cryptographie quantique, les codes correcteurs d'erreurs quantiques, les algorithmes quantiques, la communication quantique, l'internet quantique, la téléportation quantique, les mémoires quantiques, la théorie des jeux quantiques, l'apprentissage machine quantique, la simulation et conception d'ordinateurs quantiques, etc.

Discipline aujourd'hui en pleine évolution, elle ne laisse pas indifférentes les grandes entreprises et les grandes instances de recherche dans le monde. Du point de vue national, un rapport ministériel a été publié (Janvier 2020) regroupant un certain nombre de propositions concernant la stratégie de la France en ce qui concerne les Technologies Quantiques. En 2018, l'Europe lançait le Quantum Flagship, initiative européenne visant à développer les technologies quantiques dans le continent, doté d'un budget de 1 milliard d'euros. En septembre 2019, IBM annonçait la mise à disposition d'un ordinateur quantique, via le cloud, d'une puissance de 53 qubits. En octobre 2019, Google a annoncé avoir démontré la suprématie quantique (supériorité de l'ordinateur quantique sur les machines classiques). Nous pouvons également citer des entreprises comme D-Wave ou encore Atos qui travaillent activement dans la réalisation ou la simulation d'ordinateurs quantiques.

Ainsi, l'étude théorique de certains phénomènes quantiques comme l'intrication, présente sous différents aspects dans cette technologie quantique, permettrait de faciliter la conception et le développement de telles applications, tout en apportant de nouvelles clés de compréhension et d'analyse de ce phénomène non-classique.

Organisation du manuscrit

Pour plus de clarté dans la présentation des principes théoriques utilisés, des recherches menées et des résultats, ce manuscrit de thèse a été divisé en trois parties.

En Partie I, nous introduisons les principes fondamentaux de la théorie de l'information quantique, qui seront réutilisés tout au long de la thèse. Nous introduisons ensuite des notions de géométrie algébrique, notamment les variétés algébriques en lien avec le phénomène d'intrication quantique. Enfin, nous présentons justement les définitions et outils utilisés pour étudier ce dernier phénomène.

En Partie II nous étudions l'intrication quantique dans les algorithmes quantiques. Nous menons à la fois une étude qualitative et quantitative de l'intrication pour les algorithmes de Grover et de Shor, afin d'apporter de nouveaux éléments pour expliquer le comportement de l'intrication au cours de ces algorithmes.

Enfin, en Partie III, nous étudions l'intrication du point de vue de la géométrie algébrique sous trois axes différents. Le premier axe est d'étudier l'intrication de manière originale en étudiant les singularités d'hypersurfaces associées aux états quantiques, et ce dans le cas des 3-qutrits. La seconde approche vise à utiliser les polynômes invariants comme mesure de l'intrication, et de chercher à les maximiser pour proposer ou confirmer des candidats pour les états maximalement intriqués. Enfin, le dernier axe vise à développer des outils d'apprentissage supervisé à l'aide de réseaux de neurones pour apprendre à reconnaître certaines variétés algébriques directement liées à certaines classes d'intrication.

Nous renseignons en Annexe A l'ensemble des algorithmes et codes utilisés pour les calculs et les implémentations informatiques.

Liste des articles et travaux

Articles publiés

- Frédéric Holweck, Hamza Jaffali, and Ismaël Nounouh, *Grover's algorithm and the secant varieties*, Quantum Information Processing **15** (2016), no. 11, 4391–4413
- Frédéric Holweck and Hamza Jaffali, *Three-qutrit entanglement and simple singularities*, Journal of Physics A **49** (2016), no. 46, 465301
- Hamza Jaffali and Frédéric Holweck, *Quantum entanglement involved in grover's and shor's algorithms : the four-qubit case*, Quantum Information Processing **18** (2019), no. 5, 133
- Metod Saniga, Frédéric Holweck, and Hamza Jaffali, *Taxonomy of three-qubit mermin pentagrams*, Symmetry **12** (2020), no. 4, 534
- Hamza Jaffali and Luke Oeding, *Learning algebraic models of quantum entanglement*, Quantum Information Processing **19** (2020), no. 9, 279

Articles en cours de publication

- Henri de Boutray, Hamza Jaffali, Frédéric Holweck, Alain Giorgetti, and Pierre-Alain Masson, *Mermin polynomials for entanglement evaluation in grover's algorithm and quantum fourier transform*, 2020
- Grâce Amouzou, Jeoffrey Boffelli, Hamza Jaffali, Kossi Atchonouglo, and Frédéric Holweck, *Entanglement and non-locality of four-qubit connected hypergraph states*, 2020

Articles en cours de rédaction

- Frédéric Holweck, Hamza Jaffali, and Luke Oeding, *Entanglement of fermionic systems from hyperpfaffians*, 2021
- Frédéric Holweck, Hamza Jaffali, and Jean-Gabriel Luque, *Maximally entangled symmetric states from invariants of binary forms*, 2021

Mémoires

- Lucas Budai, Hamza Jaffali, and Ismaël Nounouh, *Principes fondamentaux de l'information quantique*, June 2014
- Hamza Jaffali and Ismaël Nounouh, *Théorie de l'information quantique : Applications à l'energie*, January 2017

Vue globale des disciplines impliquées

Table des matières

Table des figures

Liste des tableaux

Première partie

Introduction et Notions Fondamentales

Cette thèse étant à l'intersection de plusieurs disciplines (information quantique, mathématiques, informatique), il convient d'introduire les notions fondamentales nécessaires à la compréhension de ce travail pour que ce dernier soit accessible au plus grand nombre. Nous voulions regrouper et centraliser dans cette partie l'ensemble des définitions et concepts de base, qui pourraient être sollicités dans les différents chapitres de la thèse, afin notamment de permettre au lecteur de s'attarder sur les notions qu'il découvre, et de moins le faire pour les notions avec lesquelles il est plus familier. Aussi, nous voulions dédier les autres parties à la présentation des résultats de recherche pour plus de clarté.

Dans le premier chapitre de cette partie, nous présentons succinctement les notions fondamentales de la théorie de l'information quantique liées à cette thèse. Nous y incluons la définition du qubit et des différents postulats de la mécanique quantique, ainsi qu'une présentation des algorithmes quantiques étudiés en seconde partie. Enfin, nous abordons également la question de la représentation de certains systèmes quantiques.

Dans le second chapitre de cette partie, nous abordons à la fois des notions de géométrie algébrique et d'intrication quantique. Nous introduisons les différentes variétés algébriques auxquelles nous ferons référence tout au long de la thèse. Nous définissons ensuite la notion d'intrication quantique du point de vue mathématique, et précisons sous quel angle nous l'étudions dans ce travail. Enfin nous rappelons quelques classifications connues de l'intrication pour certains systèmes quantiques, et nous présentons diverses mesures de l'intrication exploitées dans les parties suivantes.

Chapitre 1

Bases de la Théorie de l'Information Quantique

"I think I can safely say that nobody understands quantum mechanics", Richard Feynman.

Dans ce chapitre, nous introduirons les notions de bases et les outils nécessaires à la compréhension de la Théorie de l'Information Quantique. La notion de qubit sera introduite, tout en généralisant la définition aux systèmes à plusieurs particules. Les postulats de la mécanique quantique seront rappelés du point de vue de la TIQ et du point de vue mathématique. Nous nous attarderons également sur certains aspects liés au calcul quantique, en présentant notamment les algorithmes quantiques de Grover et de Shor. Enfin, nous introduirons certaines représentations géométriques liées à la notion de qubit et d'états symétriques.

1.1 Principes fondateurs

1.1.1 Le bit quantique

La première notion de base qu'il convient d'introduire afin de pouvoir appréhender la Théorie de l'Information Quantique est celle de bit quantique. Elle est définie par analogie au bit, unité de mesure élémentaire de l'information, en Informatique ou Théorie de l'Information classique. Ce dernier est défini comme une variable dont la valeur appartient à un ensemble à deux éléments. L'aspect binaire de cette variable est ce qui la caractérise fondamentalement : un bit aura comme valeur **soit** le premier élément de l'ensemble, **soit** le second élément de l'ensemble. Le bit sert donc à caractériser une propriété d'un système classique ne pouvant être que dans deux états différents : ouvert ou fermé, actif ou inactif, orienté vers la droite ou vers la gauche, noir ou blanc, etc. Le "ou" ici doit être compris au sens exclusif. Généralement, on adoptera la notation binaire, représentant donc un bit b comme étant un élément dans l'ensemble binaire $\mathcal{B} = \{0, 1\}$.

Le bit quantique vient étendre les possibilités et l'espace des valeurs possibles d'un bit classique. En effet, un bit quantique pourra *soit être égal à 0, soit être égal à 1, soit* ***être dans une superposition des états 0 et 1***. Cette différence fondamentale

entre le bit quantique et le bit classique est directement issue des lois de la Mécanique Quantique, et est la première responsable de la différence entre les deux philosophies et manières de manipuler l'information.

En effet, un bit quantique représentera l'état d'un système quantique, ou l'état d'une propriété spécifique d'un système quantique : orientation du spin d'un électron, polarisation d'un photon, etc. Chacune de ces propriétés ne peuvent prendre que deux valeurs (polarisé verticalement ou horizontalement, pour le photon par exemple), ce qui justifie l'appellation d'un bit quantique. La mécanique quantique étant linéaire, un système quantique à deux états peut être donné par une combinaison linéaire de ces deux états : c'est le principe de *superposition*.

Le bit quantique est souvent appelé *qubit*, venant de l'anglais *quantum bit*, et dispose d'une convention de notation, proposée par Dirac[1], appelée "bra-ket". On notera alors $|0\rangle$ et $|1\rangle$ les deux états de base associés à un qubit. Le qubit $|\psi\rangle$, représentant l'état du système quantique ψ, sera donc défini comme une superposition des deux états de base, modélisée par la combinaison linéaire

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

avec α et β deux nombres complexes appelés les *amplitudes de probabilité* de l'état $|\psi\rangle$, vérifiant la contrainte de normalisation

$$|\alpha|^2 + |\beta|^2 = 1 \ . \tag{1.2}$$

En fixant $\alpha = 0$ ou $\beta = 0$, on retrouve les valeurs de base d'un bit classique $|\psi\rangle = |0\rangle$ ou $|\psi\rangle = |1\rangle$, impliquant que le modèle du bit classique est compris dans le modèle de représentation d'un qubit.

En considérant les états de base $|0\rangle$ et $|1\rangle$ comme des vecteurs formant une base orthonormée, un qubit peut alors être vu comme un vecteur dans un espace de Hilbert $\mathcal{H} = \mathbb{C}^2$. Tout au long de ce manuscrit, la base $\{|0\rangle, |1\rangle\}$ sera appelée base de calcul (*computational basis* en anglais) ou la base canonique de l'espace de Hilbert associé à un qubit. Ces vecteurs sont usuellement exprimés par

$$|0\rangle \sim \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \sim \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ , \tag{1.3}$$

permettant effectivement de voir l'état $|\psi\rangle$ comme un vecteur dans un espace vectoriel complexe de dimension 2 (voir Figure 1.1) :

$$|\psi\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathcal{H} = \mathbb{C}^2 \ . \tag{1.4}$$

À chaque qubit $|\psi\rangle \in \mathcal{H}$ on peut associer l'état dual $\langle\psi| \in \mathcal{H}^*$, s'écrivant avec la notation "bra", défini par

1. Paul Adrien Maurice Dirac (1902 – 1984) est un mathématicien et un physicien britannique, considéré comme un des pères de la mécanique, ayant également prévu l'existence de l'antimatière.

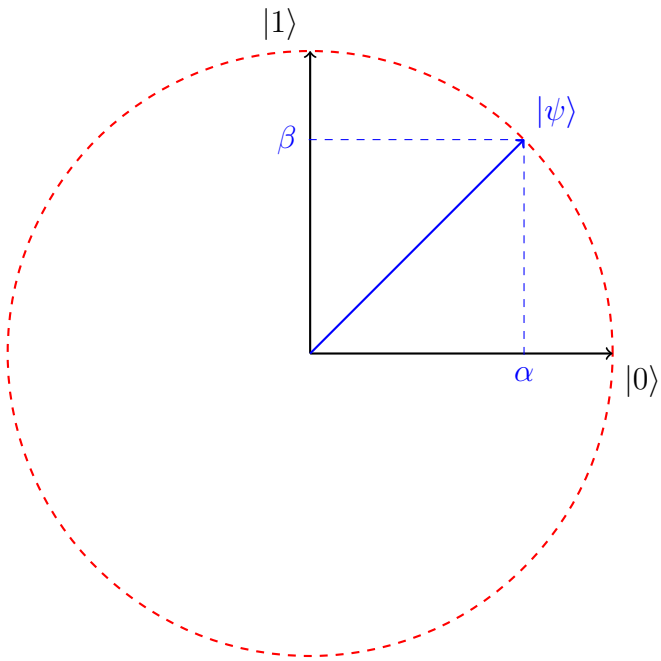


FIGURE 1.1 – Représentation graphique dans le plan du qubit $|\psi\rangle$ (en bleu) dans la base de calcul (en noir). La condition de normalisation est représentée par le cercle rouge.

$$\langle\psi| = \overline{\alpha}\langle 0| + \overline{\beta}\langle 1| \ , \tag{1.5}$$

avec $\langle 0|$ et $\langle 1|$ les vecteurs lignes suivants :

$$\langle 0| \sim \begin{pmatrix} 1 & 0 \end{pmatrix}, \ \langle 1| \sim \begin{pmatrix} 0 & 1 \end{pmatrix} \quad \text{et donc } \langle\psi| = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix} \ . \tag{1.6}$$

De plus, une forme sesquilinéaire hermitienne $\langle\cdot|\cdot\rangle$ est naturellement associée à l'espace de Hilbert complexe, définissant un produit scalaire hermitien sur $\mathbb{C}^2$. La notation "bra-ket" permet astucieusement d'effectuer le produit hermitien de deux qubits $|\psi\rangle$ et $|\varphi\rangle = \gamma|0\rangle + \delta|1\rangle$, défini comme :

$$\langle\psi|\varphi\rangle = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \overline{\alpha}\gamma + \overline{\beta}\delta \ . \tag{1.7}$$

Ce produit scalaire hermitien définit une forme sesquilinéaire vérifiant un certain nombre de propriétés :

- Pour tout état $|\psi\rangle \in \mathcal{H}$, on a $\langle\psi|\psi\rangle \geq 0$ (positive),
- Pour tout état $|\psi\rangle \in \mathcal{H}$, $\langle\psi|\psi\rangle = 0 \implies |\psi\rangle = 0_{\mathcal{H}}$ (définie),
- Pour tout $\lambda_1, \lambda_2 \in \mathbb{C}$, et pour tout $|\psi\rangle, |\varphi_1\rangle, |\varphi_2\rangle \in \mathcal{H}$, on a $\langle\psi|\Big(\lambda_1|\varphi_1\rangle + \lambda_2|\varphi_2\rangle\Big) = \lambda_1\langle\psi|\varphi_1\rangle + \lambda_2\langle\psi|\varphi_2\rangle$ (linéaire à droite),
- Pour tout $\lambda_1, \lambda_2 \in \mathbb{C}$, et pour tout $|\psi_1\rangle, |\psi_2\rangle, |\varphi\rangle \in \mathcal{H}$, on a $\Big(\lambda_1\langle\psi_1| + \lambda_2\langle\psi_2|\Big)|\varphi\rangle = \overline{\lambda_1}\langle\psi_1|\varphi\rangle + \overline{\lambda_2}\langle\psi_2|\varphi\rangle$ (sesquilinéaire à gauche),
- On peut définir une norme sur $\mathcal{H}$, dite norme hermitienne : la norme de $|\psi\rangle$ est égale à $\|\psi\| = \sqrt{\langle\psi|\psi\rangle}$,
- Pour tout $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$, $|\psi\rangle$ et $|\varphi\rangle$ sont orthogonaux si et seulement si $\langle\psi|\varphi\rangle = 0$.

La condition de normalisation $|\alpha|^2 + |\beta|^2 = 1$ est donc équivalente à imposer que tout qubit soit de norme 1. La base orthonormée $\{|0\rangle, |1\rangle\}$ doit alors vérifier les relations suivantes :

$$\langle 0|1\rangle = \langle 1|0\rangle = 0, \text{ et } \langle 0|0\rangle = \langle 1|1\rangle = 1 \ . \tag{1.8}$$

1.1.2 Systèmes à plusieurs particules

En informatique classique, il convient de définir des registres de données composés de plusieurs bits pour pouvoir encoder plus d'information. Un registre binaire de taille n est donc composé de n bits, et l'état global du registre est totalement décrit par l'état de chaque bit. On écrit généralement l'état d'un registre binaire en concaténant la valeur de chaque bit.

En théorie de l'information quantique, mais en physique quantique aussi, il est nécessaire de pouvoir modéliser des systèmes quantiques composés de plusieurs particules, et de pouvoir décrire l'état global du système, éventuellement en fonction des états possibles de chaque particule.

À titre de premier exemple, on se propose d'étudier les systèmes quantiques à 2 particules, où chaque particule ne peut prendre que deux états. Il est clair que chaque particule peut être modélisée par un qubit, et par conséquent, le système quantique composé de ces deux particules sera modélisé comme un système à 2-qubits. Soit donc $|\psi_{AB}\rangle$ l'état représentant le système quantique composé des particules A et B. La particule A peut être représentée par un qubit, exprimé comme une superposition des deux états possibles $|0_A\rangle$ et $|1_A\rangle$ de la particule A. Le qubit représentant la particule A sera donc considéré comme un vecteur de l'espace de Hilbert $\mathcal{H}_A$ associé à cette particule. De même, le qubit associé à la particule B sera exprimé dans la base $\{|0_B\rangle, |1_B\rangle\}$ de l'espace de Hilbert $\mathcal{H}_B$.

L'état $|\psi_{AB}\rangle$ du système global sera aussi considéré comme un vecteur dans un espace de Hilbert $\mathcal{H}_{AB}$ de dimension $2^2 = 4$, défini comme étant le produit tensoriel des espaces de Hilbert de chaque particule. On a alors $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Le *principe de superposition* (premier postulat de la mécanique quantique [200]), stipule que tout état d'un système quantique s'exprime comme une superposition de tous les états possibles du système quantique. Le système étant composé de deux particules, l'état de ce système s'exprimera donc comme la combinaison de toutes les possibilités associées aux états de base de chaque particule. Par exemple, la première particule peut être dans l'état de base $|0_A\rangle$, et la seconde particule dans l'état $|1_B\rangle$, ce qui implique que le système est dans l'état $|0_A\rangle \otimes |1_B\rangle = |0_A\rangle|1_B\rangle$ (le symbole produit tensoriel est souvent omis). De manière générale, on ne connaît pas forcément l'état de chaque particule, et elles peuvent être dans une superposition de leur états de base également. L'état du système global s'exprime alors de manière générale comme une combinaison linéaire des états possibles du système :

$$|\psi_{AB}\rangle = a_{00}|0_A\rangle|0_B\rangle + a_{01}|0_A\rangle|1_B\rangle + a_{10}|1_A\rangle|0_B\rangle + a_{11}|1_A\rangle|1_B\rangle \ . \tag{1.9}$$

On omettra souvent d'indiquer les indices correspondants à chaque particule pour la suite du manuscrit, l'ordre d'écriture des états de base permettra d'identifier la particule considérée. De plus, on concaténera (comme dans le cas classique) l'écriture des états de base pour simplifier l'écriture des états quantiques. La ré-écriture de l'état $|\psi_{AB}\rangle$ suivant ces conventions donne alors :

$$|\psi_{AB}\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \ , \tag{1.10}$$

avec $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$, vérifiant la condition de normalisation

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1 \ . \tag{1.11}$$

Lorsque l'état $|\psi_A\rangle = \alpha_A|0\rangle + \beta_A|1\rangle$ de la particule A est connu, et que l'état $|\psi_B\rangle = \alpha_B|0\rangle + \beta_B|1\rangle$ de la particule B est aussi connu, alors on peut exprimer l'état du système global $|\psi_{AB}\rangle$ à partir du produit tensoriel suivant :

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = (\alpha_A|0\rangle + \beta_A|1\rangle) \otimes (\alpha_B|0\rangle + \beta_B|1\rangle) \ , \tag{1.12}$$

$$|\psi_{AB}\rangle = \alpha_A\alpha_B|00\rangle + \alpha_A\beta_B|01\rangle + \beta_A\alpha_B|10\rangle + \beta_A\beta_B|11\rangle \ . \tag{1.13}$$

On passe alors d'une écriture factorisée à une écriture développée de l'état $|\psi_{AB}\rangle$. En revanche, il n'est pas toujours possible de passer d'une écriture développée, où l'état du système est écrit comme une superposition d'états de base, à une écriture factorisée, où l'écriture de l'état des particules composant le système est exprimée de manière indépendante. Ceci est notamment le cas de l'état de Bell $|\psi_{Bell}\rangle$ (voir Équation 1.14), qui présente des propriétés intéressantes, notamment liées à la notion d'intrication (voir Section 2.2).

$$|\psi_{Bell}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \ . \tag{1.14}$$

On peut aussi généraliser la notion de système quantique à des dimensions supérieures. On définit l'état $|\psi_n\rangle$ d'un système à n-qubits comme un système composé de n particules, chacune possédant deux états de base possibles. Cet état sera également vu comme un vecteur $|\psi_n\rangle$ d'un espace de Hilbert $\mathcal{H}_n$ de dimension $N = 2^n$, défini comme le produit tensoriel de n copies de $\mathcal{H} = \mathbb{C}^2$, c'est à dire $\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$. L'état $|\psi_n\rangle$ s'écrira alors comme une superposition de tous les états de base possibles :

$$|\psi_n\rangle = a_0|0\ldots00\rangle + a_1|0\ldots01\rangle + a_2|0\ldots10\rangle + \cdots + a_{N-1}|1\cdots11\rangle \ , \tag{1.15}$$

avec $\forall i \in [\![0, N-1]\!], a_i \in \mathbb{C}$ et $\sum_{i=0}^{N-1} |a_i|^2 = 1$. On peut également adopter la notation décimale à la place de la notation binaire pour écrire les états de base intervenant dans l'expression d'un état quantique. Ainsi un état de base s'écrivant $|b_1b_2\ldots b_n\rangle$ en notation binaire avec $b_j \in \mathcal{B} = \{0, 1\}$, pourra s'écrire $|B\rangle$ avec $B = 2^{n-1}b_1 + 2^{n-2}b_2 + \cdots + 2^0b_n$ un entier naturel. On pourra alors ré-exprimer $|\psi_n\rangle$ comme suit :

$$|\psi_n\rangle = a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + \cdots + a_{N-1}|N-1\rangle \ . \tag{1.16}$$

1.1.3 Manipuler l'état d'un système quantique

Tant qu'un système quantique n'est pas soumis à une mesure ni projeté sur un état classique, l'état de ce dernier peut évoluer. Cette transformation du système est en effet régie par le postulat d'évolution.

L'évolution d'un système quantique (fermé), c'est à dire sans interaction extérieure, est décrit par une transformation unitaire. Cette évolution de l'état provient de l'application d'un opérateur linéaire, nommé opérateur d'évolution. Si $|\psi(t_1)\rangle$ désigne l'état d'un système quelconque au temps t_1, il est alors lié à l'état $|\psi(t_2)\rangle$ du système au temps t_2 par un opérateur d'évolution U, tel que $|\psi(t_2)\rangle = U|\psi(t_1)\rangle$.

Géométriquement, une transformation unitaire est une rotation dans l'espace de Hilbert, c'est à dire une transformation de l'état du système laissant invariant sa norme, et est alors l'analogue complexe d'un opérateur orthogonal pour les espaces vectoriels réels. Contrairement aux opérateurs classiques (par exemple les opérateurs logiques sur des bits ou registres binaires) qui ne sont pas toujours réversibles, les opérateurs unitaires admettent toujours une transformation inverse.

Un opérateur unitaire, agissant sur un espace de Hilbert de dimension finie, est une application linéaire pouvant être représentée à l'aide d'une matrice. Soit une matrice $U \in M_n(\mathbb{C})$, alors les conditions suivantes sont équivalentes :

- la matrice U est unitaire,
- $UU^\dagger = U\overline{U}^t = I_n$,
- $U^\dagger U = \overline{U}^t U = I_n$,
- les vecteurs colonnes de U forment une base orthonormée (au sens du produit hermitien) de $\mathbb{C}^n$,
- les vecteurs lignes de U forment une base orthonormée de $\mathbb{C}^n$.

Un des problèmes résidera alors dans la difficulté à déterminer l'opérateur d'évolution U, en connaissant les états $|\psi(t_1)\rangle$ et $|\psi(t_2)\rangle$. Le sixième (et dernier) postulat de la mécanique quantique [281] stipule que l'évolution de l'état d'un système quantique est gouvernée par l'équation de Schrödinger[2]

$$i\hbar\frac{\partial}{\partial t}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle \ , \tag{1.17}$$

où i représente l'imaginaire complexe, $\hbar$ la constante de Planck réduite et $\hat{H}$ l'opérateur hamiltonien (associé à l'observable "énergie totale du système").

L'équation de Schrödinger est une équation différentielle du premier ordre par rapport au temps. Ce qui signifie que la donnée d'un état initial $|\psi(t_0)\rangle$ suffit à déterminer $|\psi(t)\rangle$ à tout instant ultérieur t. Ceci n'est valable que si l'évolution n'est pas interrompue par une mesure du système.

2. Erwin Rudolf Josef Alexander Schrödinger (1887 – 1961) est un physicien, philosophe et théoricien scientifique autrichien, ayant participé à l'élaboration du formalisme théorique de la mécanique quantique, notamment connu pour son équation d'évolution de la fonction d'onde, ou pour l'expérience de pensée liée à son chat.

Cette équation est également linéaire et homogène. Il existe donc une correspondance linéaire entre $|\psi(t_0)\rangle$ et $|\psi(t)\rangle$. De ce fait, il existe un opérateur linéaire $U(t, t_0)$ tel que $|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle$. On peut alors en déduire une solution de l'équation temporelle de Schrödinger :

$$U(t, t_0) = exp\left(-\frac{i(t - t_0)}{\hbar}\hat{H}\right) . \tag{1.18}$$

Cette "explication simplifiée" de l'évolution de l'état d'un état quantique nous permet de comprendre qu'il est possible d'ajuster physiquement l'opérateur hamiltonien pour *piloter* l'évolution de l'état quantique. On pourra définir et réaliser des opérateurs permettant de transformer un état quantique en un état cible par un choix approprié d'interactions avec le système. On se propose dans la suite de présenter les différentes portes quantiques utilisées dans le domaine du calcul quantique notamment.

Opérateurs sur un qubit

Comme explicité précédemment, il est toujours possible d'exprimer un qubit comme un vecteur dans une base d'un espace de Hilbert. Ainsi, un opérateur unitaire agissant sur un qubit ordinaire prendra la forme d'une matrice carrée d'ordre 2 unitaire. Nous travaillons usuellement dans la base canonique $\{|0\rangle, |1\rangle\}$, mais il peut parfois arriver d'exprimer les états dans une autre base pour simplifier les calculs ou les représentations.

Par exemple, l'opérateur associé à la matrice identité I_2 laissera le qubit inchangé. L'opérateur de négation, connu en informatique sous le nom de porte NON (ou NOT en anglais), mais noté opérateur X dans le contexte de l'information quantique, modifie en effet les vecteurs de la base comme suit :

$$X|0\rangle = |1\rangle \text{ et } X|1\rangle = |0\rangle . \tag{1.19}$$

La représentation matricielle associée est donc la suivante.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \tag{1.20}$$

Si on applique cet opérateur à un état quelconque, on obtient :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{X} |\psi\rangle_X = \alpha|1\rangle + \beta|0\rangle . \tag{1.21}$$

On définit également deux autres opérateurs Y et Z, dont l'action est représentée par les matrices

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} . \tag{1.22}$$

Ces trois opérateurs X, Y et Z sont appelés les opérateurs (ou les matrices) de Pauli[3], permettant de prendre en compte l'interaction du spin d'une particule avec un

3. Wolfgang Ernst Pauli (1900 – 1958) est un physicien autrichien connu pour sa définition du principe d'exclusion en mécanique quantique, ou principe de Pauli, ce qui lui valut le prix Nobel de physique de 1945.

champ magnétique externe (dans l'équation de Pauli notamment). On prouve que ces matrices sont hermitiennes et unitaires, et constituent des opérateurs fondamentaux en théorie de l'information quantique.

Un autre opérateur important est celui d'Hadamard[4], souvent utilisé pour générer des états complètement parallélisés (dont l'écriture fait intervenir tous les états de base du système avec la même amplitude de probabilité). La porte de Hadamard, souvent notée H, est définie par la transformation suivante de la base canonique :

$$\begin{aligned} |0\rangle &\to \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ , \\ |1\rangle &\to \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \ . \end{aligned} \tag{1.23}$$

Cette porte H peut être représentée sous forme matricielle comme suit :

$$H = \frac{X+Z}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \ . \tag{1.24}$$

On notera les deux états issus de l'application de la porte d'Hadamard à la base canonique par $|+\rangle$ et $|-\rangle$. On aura alors

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \ . \tag{1.25}$$

Les quatre matrices X, Y, Z et H sont en effet étroitement liées. On peut ainsi rapidement établir les relations suivantes :

- $X^2 = Y^2 = Z^2 = H^2 = I_2$,
- $XY = iZ$, $YZ = iX$ et $ZX = iY$,
- $HXH = Z$, $HYH = -Y$ et $HZH = X$.

Enfin, on définit la matrice R_k, utile dans le contexte de l'algorithme de Shor, permettant d'introduire une phase à l'état $|1\rangle$, lorsqu'il est en entrée :

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix} \ . \tag{1.26}$$

Opérateurs sur un système à plusieurs qubits

Tout comme un système à un qubit, un système à 2-qubits évolue selon une transformation unitaire. Un opérateur unitaire agissant sur un système à 2-qubits sera alors représenté par une matrice carrée d'ordre 4. De façon générale, toute opération unitaire sur un système à n-qubits peut être représentée par une matrice carrée d'ordre $N = 2^n$. On pourra ainsi manipuler des états à plusieurs qubits, et réaliser des opérations plus complexes sur ces derniers.

De plus, un opérateur U agissant sur un état à 2-qubits peut être vu comme un opérateur global agissant sur tout le système, mais peut aussi parfois être décomposé

4. Jacques Salomon Hadamard (1865 – 1963) est un mathématicien français, notamment connu pour ses travaux en théorie des nombres, en analyse complexe, en analyse fonctionnelle et en géométrie différentielle.

en deux opérateurs U_1 et U_2 agissant respectivement sur le premier et le second qubit du système. La transformation globale U s'exprimera alors $U = U_1 \otimes U_2$ comme le produit tensoriel des deux opérateurs **locaux**.

Plus précisément, et afin d'expliciter le calcul du produit tensoriel, si les deux matrices U_1 et U_2 s'expriment explicitement comme

$$U_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad U_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} , \tag{1.27}$$

alors la matrice U sera égale à

$$U = \begin{pmatrix} a_1 \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} & b_1 \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \\ c_1 \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} & d_1 \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 & b_1a_2 & b_1b_2 \\ a_1c_2 & a_1d_2 & b_1c_2 & b_1d_2 \\ c_1a_2 & c_1b_2 & d_1a_2 & d_1b_2 \\ c_1c_2 & c_1d_2 & d_1c_2 & d_1d_2 \end{pmatrix} . \tag{1.28}$$

Ceci servira notamment à la compréhension et à la mise en place d'algorithmes et de circuits quantiques, notions qui seront introduites dans la Section 1.2.

Il apparaît donc intéressant d'étudier les principales portes logiques réversibles agissant sur des états à plusieurs qubits. La première est la porte *c-NOT*, ou *controlled-NOT*, utilisée pour appliquer la porte *NOT* (ou X) en fonction de la valeur du premier qubit. Elle fonctionne de la manière suivante :

État d'entrée	État de sortie
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

(1.29)

La porte *c-NOT* agit en effet sur un système à deux qubits. Elle repose sur le principe de porte contrôlée, c'est à dire que le premier bit sert de contrôle (bit de *contrôle*) et le second bit (bit *cible*) subit ou non la transformation associée (ici la porte X), en fonction de l'état du bit de *contrôle*. Comme nous savons comment l'opérateur *c-NOT* transforme les vecteurs de la base de calcul $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, on peut alors le représenter par la matrice suivant :

$$c\text{-}NOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} . \tag{1.30}$$

Ainsi, la valeur du bit *cible* est inchangée, si le bit de *contrôle* vaut 0 ; et la valeur du bit *cible* est changée, si le bit de *contrôle* vaut 1. En fait, le bit *cible* vaut à la sortie la somme, modulo 2, des deux bits d'entrée, tandis que le bit de *contrôle* reste inchangé. On note alors, *c-NOT* : $(x, y) \to (x, x \oplus y)$. Il est également possible de définir la porte *c-NOT* en intervertissant le rôle des qubits pour le contrôle et la cible (voir plus tard la porte SWAP)

En plus de la représentation matricielle, on peut introduire la représentation sous forme de circuit pour les opérateurs à plusieurs qubits (voir Figure 1.2). Les fils horizontaux matérialisent un qubit ou une particule, et les fils verticaux correspondent à une interaction entre les qubits, comme le fait qu'un qubit puisse contrôler l'action sur un second qubit. Le symbole de somme entouré représente la somme binaire modulo 2 pour la porte *c-NOT*.

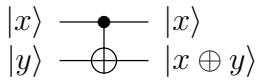


Figure 1.2 – Représentation sous la forme d'un circuit quantique de l'opérateur à 2-qubits *c-NOT*.

Enfin, l'application de l'opérateur *c-NOT*, qui est un opérateur linéaire et unitaire, à un état à 2-qubits quelconque $|\psi\rangle$ donne :

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \xrightarrow{c-NOT} \alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle \ . \quad (1.31)$$

Nous souhaitons également introduire une autre porte à 2-qubits souvent utilisée dans le contexte des calculs, circuits et algorithmes quantiques. La porte $SWAP$, comme son nom l'indique, échange la place des deux qubits passés en paramètre : SWAP : $(x, y) \to (y, x)$. La porte $SWAP$ se compose d'une succession de 3 portes *c-NOT*, avec alternance du bit de *contrôle* :

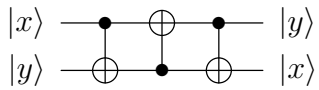


Figure 1.3 – Représentation sous la forme d'un circuit quantique de la porte $SWAP$

Le lecteur pourra vérifier que la matrice associée à l'action de la porte $SWAP$ sous un registre à 2-qubits est bien la suivante :

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \ . \quad (1.32)$$

Le circuit nous dit que la porte $SWAP$ est en fait une triple application de la porte *c-NOT*, en alternant la place du bit de *contrôle*. On appellera $c\text{-}NOT_1$ la porte *c-NOT* avec premier qubit en bit de *contrôle*, et $c\text{-}NOT_2$ la porte *c-NOT* en prenant l'autre qubit en *contrôle*. On a donc :

$$c\text{-}NOT_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad c\text{-}NOT_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \ .$$

La succession de portes quantiques revient à leur composition en terme d'opérateur, ce qui implique que $SWAP = c\text{-}NOT_1 \circ c\text{-}NOT_2 \circ c\text{-}NOT_1$. Ceci se traduit aussi au

niveau matriciel. En effet, la matrice de l'application $SWAP$ sera égale au produit des trois matrices représentant les portes $c\text{-}NOT$ le composant :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

Enfin, l'application de l'opérateur SWAP à un état quelconque $|\psi\rangle$ donne :

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \xrightarrow{SWAP} \alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \delta|11\rangle .$$

De manière plus générale, il existe une porte agissant sur des registres quantiques à 3-qubits, permettant d'introduire plus de flexibilité et de possibilités dans la réalisation d'opérations sur des registres quantiques. L'opérateur TOF, mis en place par Tommaso Toffoli[5] en 1980, peut être considéré comme un $c\text{-}c\text{-}NOT$ (*controled-controled-NOT*). Cette porte apporte une grande aide dans la résolution du problème de réversibilité des portes logiques classiques.

Cette porte prend 3 qubits en entrée : les deux premiers servant pour le *contrôle* et le troisième étant le qubit *cible*. Cet opérateur réalise ainsi l'application unitaire suivante, TOF : $(x, y, z) \to (x, y, z \oplus xy)$. Le circuit correspondant à la porte de Toffoli est donc le suivant :

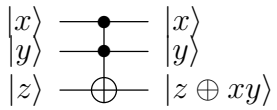


FIGURE 1.4 – Représentation sous la forme d'un circuit quantique de la porte TOF

La porte de Toffoli transforme les états de base d'un système à trois qubits comme suit :

État d'entrée	État de sortie
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|101\rangle$
$\|110\rangle$	$\|111\rangle$
$\|111\rangle$	$\|110\rangle$

, et donc $TOF = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$. (1.33)

La porte de Toffoli permettra, en considérant certains qubits comme auxiliaires, de modéliser toutes les portes logiques classiques qui ne sont pas facilement modélisables à l'aide des portes quantiques usuelles. Enfin, cette porte, ainsi que la porte X et $SWAP$, feront partie d'un ensemble universel permettant la génération de toutes les portes unitaires à n-qubits.

5. Tommaso Toffoli (né en 1943) est un scientifique et un universitaire italien. Il est professeur de génie électronique et d'informatique à l'université de Boston depuis 1995.

Théorème 1.1.1 (Kitaev-Shen-Vialyi). *Soit $n \geq 2$ et $N = 2^n$. Toute matrice unitaire $U_N \in SU(N)$, vue comme une porte à n-qubits, est calculée par un circuit sur l'ensemble de portes :*

$$\{X, SWAP, TOF\} \cup \{U \mid U \in U(2)\} \ .$$

Ce théorème nous informe donc que les portes réversibles de base (traduites en transformations unitaires) ainsi que toutes les portes unitaires agissant sur un qubit, suffisent pour calculer n'importe quelle transformation unitaire sur un système à n-qubits.

1.1.4 Mesurer un système quantique

En plus de pouvoir manipuler et guider l'évolution de l'état d'un système quantique, il convient aussi de pouvoir *mesurer*, ou *observer*, ses grandeurs ou propriétés physiques. En mécanique quantique, mesurer l'état d'un système quantique revient à projeter cet état dans une base de mesure (on mesure le spin d'un électron par rapport à une direction, la polarisation d'un photon selon des axes de polarisation, etc.)

Le résultat de cette mesure est probabiliste, et lorsque l'état est en superposition des états de base, la probabilité d'obtenir un état de base précis est donnée par le module au carré de l'amplitude correspondante. Par exemple, si le système étudié est un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ alors la probabilité d'obtenir $|0\rangle$ (respectivement $|1\rangle$) lorsqu'on mesure $|\psi\rangle$ dans la base canonique est de $|\alpha|^2$ (respectivement $|\beta|^2$).

De manière plus générale, le principe de *mesure* en mécanique quantique est aussi associé à la notion d'*observable*, permettant de déterminer de manière probabiliste la valeur de la grandeur mesurée. Il est admit par la communauté scientifique que l'on ne peut généralement pas établir de manière déterministe le résultat d'une mesure pour un état quantique, mais seulement déterminer les résultats possibles et les probabilités associées à chaque résultat. Toutes ces informations sont encodées dans le concept d'observable [4].

On définit un observable, que l'on notera A, comme étant un *opérateur hermitien linéaire*, associé à une propriété d'un système physique, agissant sur des vecteurs de l'espace de Hilbert $\mathcal{H}$ (second postulat [281, 200]). Un opérateur A est hermitien si et seulement s'il vérifie la relation $A = \overline{A}^t$.

L'ensemble des résultats possibles de la mesure d'une grandeur physique par un observable A est égal à l'ensemble des valeurs propres $\{\lambda_i\}_i$ de l'opérateur A. De plus, les vecteurs propres $\{|\Phi_i\rangle\}_i$ de A décrivent tous les états possibles du système quantique immédiatement après la mesure (troisième postulat [281, 200]). On dira alors que l'état $|\psi\rangle$ sera projeté sur le vecteur propre $|\Phi_i\rangle$ (ou le sous-espace propre associé) après une mesure ayant donné pour résultat la valeur propre λ_i.

On rappelle la relation liant les valeurs propres et le vecteur propre d'une matrice d'un opérateur A en Équation 1.34.

$$A|\Phi_i\rangle = \lambda_i|\Phi_i\rangle \ . \tag{1.34}$$

Une des propriétés des vecteurs propres de tout observable est qu'ils forment une base orthonormée de l'espace de Hilbert. Ainsi, tout état $|\psi\rangle \in \mathcal{H}$ pourra s'écrire de manière unique comme étant

$$|\psi\rangle = c_1|\Phi_1\rangle + c_2|\Phi_2\rangle + \cdots + c_N|\Phi_N\rangle \ . \tag{1.35}$$

La mesure de l'état $|\psi\rangle$ par l'observable A donnera comme résultat la valeur propre λ_i avec une probabilité $|c_i|^2$. En effet, et de manière générale, le produit hermitien $\langle\varphi|\psi\rangle$ représente l'amplitude de probabilité que l'état $|\psi\rangle$ soit dans l'état $|\varphi\rangle$ après la mesure (quatrième postulat [281]). Le module au carré de cette amplitude représente la probabilité associée. On peut remarquer ici que d'après la loi des probabilités totales, la somme des probabilités $\sum_i |c_i|^2$ doit être égale à 1, ce qui nous permet notamment de retrouver la condition de normalisation associée à la représentation du vecteur $|\psi\rangle$ dans l'Équation 1.35.

D'autre part, dans ce contexte probabiliste de la mesure, il est possible de déterminer la valeur moyenne théorique de la mesure associée à un observable. Ainsi la prédiction théorique de la valeur moyenne de la mesure de l'état $|\psi\rangle$ par l'observable A est donnée par la quantité $\langle A\rangle_{|\psi\rangle}$, définie comme étant égale à

$$\langle A\rangle_{\psi} = \langle\psi|A|\psi\rangle \ . \tag{1.36}$$

En d'autres termes, l'observable définit une base dans laquelle on mesurera un système à un ou plusieurs qubits $|\psi\rangle$, qui sera projeté sur un des vecteurs de cette base. À titre d'exemple, l'opérateur Z (porte de Pauli) est l'observable associé à la base de calcul $\{|0\rangle, |1\rangle\}$ (étant donc ses vecteurs propres) ayant les valeurs propres 1 et -1. L'observable X (porte de Pauli) est lui associé à la base $\{|+\rangle, |-\rangle\}$, et de valeur propre 1 et -1.

Dans la base canonique, si on considère l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, on retrouve alors la probabilité que l'état $|\psi\rangle$ soit projeté sur le vecteur propre $|0\rangle$ (respectivement $|1\rangle$) est égale à $|\alpha|^2$ (respectivement $|\beta|^2$).

Les observables sont souvent étudiés dans la littérature en imposant la condition que les valeurs propres d'un observable à un qubit A doivent appartenir à l'ensemble $\{-1, 1\}$ (impliquant que $A^2 = I_2$). Ceci est équivalent à dire que l'observable A est un opérateur unitaire (comme les matrices de Pauli, par exemple).

Il convient ici de faire la distinction entre les opérateurs utilisés dans le contexte du calcul quantique et de la manipulation des qubits, et les opérateurs utilisés comme observables de mesure. Les portes de Pauli, par exemple, sont à la fois des matrices hermitiennes et unitaires, et sont à la fois étudiées pour leur intégration dans les circuits quantiques, ainsi que pour leur habilité à modéliser une configuration de mesure dans une base spécifique. Il conviendra alors de distinguer les deux interprétations possibles de ces opérateurs en fonction du contexte étudié.

Ces portes de Pauli constituent également une base des observables dont le spectre est égal à $\{-1, 1\}$ (n'incluant donc pas l'identité). Ainsi, tout observable A dont les valeurs propres sont -1 et 1, peut s'exprimer comme

$$A = a_X X + a_Y Y + a_Z Z \ , \tag{1.37}$$

avec X, Y et Z les matrices de Pauli, et $a_X, a_Y, a_Z \in \mathbb{R}$, tels que

$$a_X{}^2 + a_Y{}^2 + a_Z{}^2 = 1 \ . \tag{1.38}$$

Enfin, il est important de préciser que l'opération de mesure implique une projection de l'état sur un des états de base, et donc une modification ou une détérioration de l'information initiale de l'état $|\psi\rangle$. La mesure est donc dans la plupart du temps destructive, et n'est pas un processus réversible comme peut l'être l'application d'un opérateur d'évolution [200].

1.2 Algorithmes quantiques

En 1982, Richard Feyman[6] émit l'idée qu'aucun calculateur classique ne pourrait simuler correctement un système quantique du fait des différences fondamentales entre la physique classique et la physique quantique. Aussi selon Feyman, seule une machine exploitant les effets de la mécanique quantique serait en mesure de modéliser un système quantique [100].

Depuis le début des années 1980, de nombreux mathématiciens et informaticiens travaillent sur l'élaboration d'algorithmes adaptés aux simulateurs et ordinateurs quantiques. De nouveaux algorithmes sont régulièrement proposés à la communauté scientifique, et on en dénombre aujourd'hui pas moins de 420 références[7] concernant de nouveaux algorithmes quantiques proposés dans la littérature [193].

L'algorithmique est l'étude des processus systématiques de résolution d'un problème, permettant de décrire précisément les étapes pour résoudre un problème donné [279]. C'est une discipline centrale et primordiale de l'informatique, et elle a également su se développer dans le domaine de l'information quantique. En effet, les algorithmes quantiques ont contribué à faire connaître et démontrer le potentiel de l'information quantique, notamment en remettant en question les algorithmes de sécurité classiques et en démontrant une efficacité et une complexité surpassant certains algorithmes et calculs classiques.

Une notion importante présente dans le calcul quantique est la réversibilité des transformations des états, à l'exception des mesures ou autres projections. C'est pourquoi les algorithmes quantiques ou autres protocoles de communication peuvent adopter la représentation sous forme de circuit pour simplifier l'étude, et également rendre compte des actions locales et parallèles sur les registres quantiques.

Ainsi, un algorithme quantique s'assurera tout d'abord d'initialiser correctement les données de départ, notamment les différents registres de données et les registres

6. Richard Phillips Feyman (1918 – 1988) est un physicien américain, l'un des plus influents du siècle dernier, en raison notamment de ses travaux sur l'électrodynamique quantique, les quarks et l'hélium superfluide.

7. http://quantumalgorithmzoo.org

auxiliaires. Il n'est pas impossible d'introduire des registres classiques dans un algorithme quantique lorsque l'aspect quantique de modélisation de l'information n'est pas utile. Durant l'algorithme, on connaîtra alors diverses manipulations de qubits, sous la forme de portes quantiques à un ou plusieurs qubits, certaines pouvant modéliser des fonctions classiques ou d'autres correspondants à des Oracles ou portes contrôlées. Il sera également nécessaire de pouvoir mesurer certains qubits ou certains registres manipulés par l'algorithme, en milieu ou en fin d'algorithme. Enfin, dans la description globale d'un algorithme quantique, il est courant de faire apparaître les éventuels pré et post-traitements classiques sur les données d'entrées ou de sortie (voir Figure 1.5).

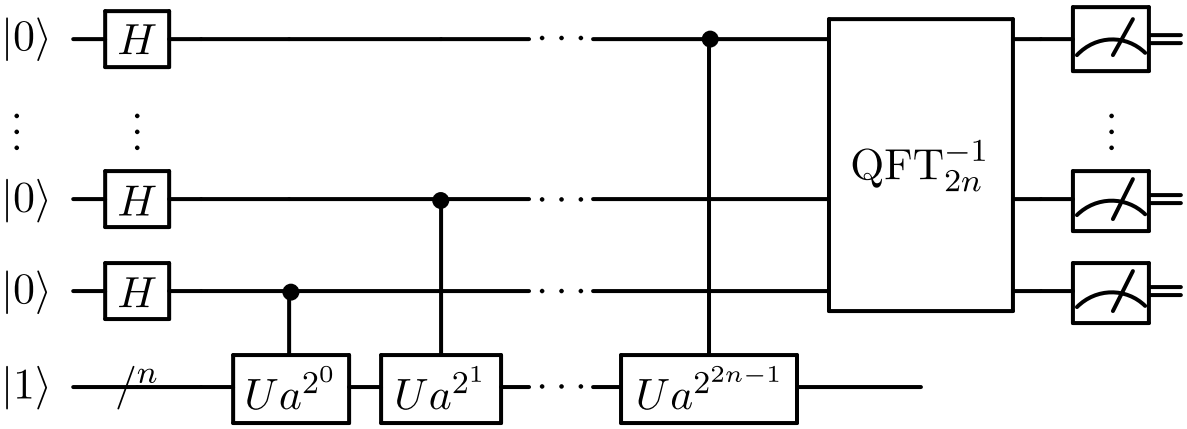


FIGURE 1.5 – Exemple de circuit quantique, se lisant de la gauche vers la droite. Chaque ligne horizontale permet de modéliser un ou plusieurs qubits. Les lignes verticales représentent une combinaison de qubits pour la réalisation d'opérations (ici un contrôle). Une opération peut également s'appliquer sur plusieurs qubits à la fois, et sera représenté par un bloc intersectant verticalement plusieurs lignes [200].

Dans cette section, nous nous proposons d'introduire et de présenter de manière générale les deux algorithmes de Grover et de Shor, qui seront étudiés en Chapitres 3 et 4.

1.2.1 Algorithme de Grover

Proposé par Lov Grover[8] en 1996 [117], cet algorithme a pour but de résoudre le problème de recherche d'un élément dans une base de données non-ordonnée de taille N. Aucun a priori n'est connu sur l'élément recherché, mais on définit une fonction $f_{\mathcal{O}}$, appelée communément $\mathcal{O}racle$, permettant de reconnaître l'élément recherché.

La meilleure stratégie classique est équivalente à parcourir un par un les éléments de la base de données, évaluer l'oracle pour chacun des éléments, jusqu'à le trouver. En moyenne, cela prend $\frac{N}{2}$ évaluations de l'oracle, et dans le pire des cas N évaluations. La complexité est donc linéaire en N ici, en terme d'évaluations de l'oracle. L'un des grands avantages de l'algorithme de Grover est de proposer une complexité de l'ordre de $\mathcal{O}(\sqrt{N})$ évaluation de l'oracle, pour la recherche d'un élément.

8. Lov Grover (1961) est un informaticien indo-américain aux Laboratories Bell, reconnu notamment pour son algorithme de recherche quantique.

L'algorithme quantique de Grover propose de représenter l'ensemble de la base de données comme un registre quantique de taille N. On supposera que $N = 2^n$ pour des raisons de simplification. On représente donc la base de données à l'aide d'un système quantique à n qubits. Chaque état de base correspond à un élément de la base de données.

On dénombre quatre étapes principales dans l'algorithme de Grover : l'initialisation, l'opérateur d'Oracle, l'opérateur de Diffusion et la mesure finale. On notera $\mathcal{S}$ l'ensemble des éléments recherchés lors du lancement de l'algorithme, et $|\mathcal{S}|$ désignera le nombre d'éléments recherchés. En fonction de $|\mathcal{S}|$ et N, les opérateurs d'Oracle et de Diffusion seront répétés plusieurs fois.

Le circuit correspondant aux différentes étapes de l'algorithme est représenté en Figure 1.6. La première étape est celle de l'initialisation, c'est-à-dire la préparation du premier registre pour obtenir un état totalement parallélisé $|+\rangle^{\otimes n}$. Ceci peut se faire en initialisant le premier registre quantique à l'état $|0\rangle^{\otimes n}$ puis en appliquant la porte de Hadamard à chaque qubit. Le second registre est composé d'un seul qubit, généralement initialisé à $|-\rangle$, et sert en pratique pour l'implémentation de l'opérateur d'Oracle.

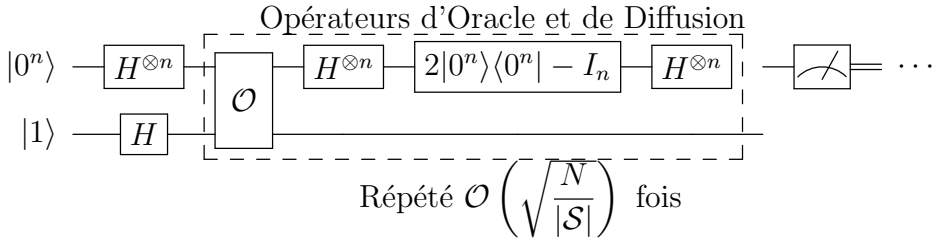


Figure 1.6 – Représentation de l'algorithme de Grover sous la forme d'un circuit [133]

Ensuite, l'opérateur d'Oracle va marquer le (ou les) élément(s) recherché(s) dans la base de données. Ce marquage consiste à multiplier par -1 l'amplitude associée aux états de base représentant les éléments marqués. L'état du premier registre est alors modifié. Nous ne nous attarderons pas sur l'implémentation effective de l'Oracle (nous considérerons l'opérateur d'Oracle comme une boite noire et un opérateur unitaire). Plusieurs études théoriques et expérimentales ont été néanmoins menées sur le sujet [200, 218]. Le lecteur prendra tout de même soin de distinguer le fait de *connaître* la solution, et le fait de pouvoir *reconnaître* la solution. On peut être capable de reconnaître la bonne solution lorsqu'elle se présente à nous, sans pour autant être en mesure de la déterminer [200]. L'opérateur d'Oracle agit donc comme suit sur les états de base :

$$|x\rangle \xrightarrow{\mathcal{O}racle} (-1)^{f_{\mathcal{O}}(x)}|x\rangle \ , \tag{1.39}$$

avec $f_{\mathcal{O}}(x) = 1$ si x est l'élément recherché, $f_{\mathcal{O}}(x) = 0$ sinon.

L'opérateur de diffusion $\mathcal{D}$ intervient ensuite. Il a pour but d'amplifier le module des amplitudes correspondantes aux éléments marqués. Il correspond à effectuer une symétrie de toutes les amplitudes autour de la moyenne des amplitudes (voir Équations 1.40 et 1.41) :

$$\mathcal{D} = H^{\otimes n} \cdot \left(2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - I_n\right) \cdot \left(H^{\otimes n}\right) , \tag{1.40}$$

$$\mathcal{D}\Big(\sum_{x=0}^{2^n-1} c_x|x\rangle\Big) = \sum_{x=0}^{2^n-1} \left(2\overline{c} - c_x\right)|x\rangle , \tag{1.41}$$

avec $\overline{c}$ la moyenne de toutes les amplitudes c_x.

Combiné avec l'opérateur d'Oracle (qui signe les amplitudes des états recherchés), cela permet d'amplifier les amplitudes des états recherchés et de réduire les amplitudes des états non-recherchés (voir Figure 1.7). Ces deux opérations sont répétées k_{opt} fois, défini tel que :

$$k_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{N}{|\mathcal{S}|}} \rceil , \tag{1.42}$$

avec $\lfloor x \rceil$ désignant l'entier le plus proche de $x \in \mathbb{R}$ [200]. On supposera ici que le nombre d'éléments marqués $|\mathcal{S}|$ est négligeable devant la quantité $N = 2^n$ pour assurer l'approximation de l'index de l'itération optimale. Au delà de l'itération optimale k_{opt}, l'amplitude devant les éléments recherchés commence à décroître. En effet on peut observer un comportement périodique de l'algorithme de Grover si on poursuit les itérations après l'itération optimale [133, 147]. La complexité de l'algorithme est donc en $\mathcal{O}(\sqrt{\frac{N}{|\mathcal{S}|}})$ (voir Equation 1.42).

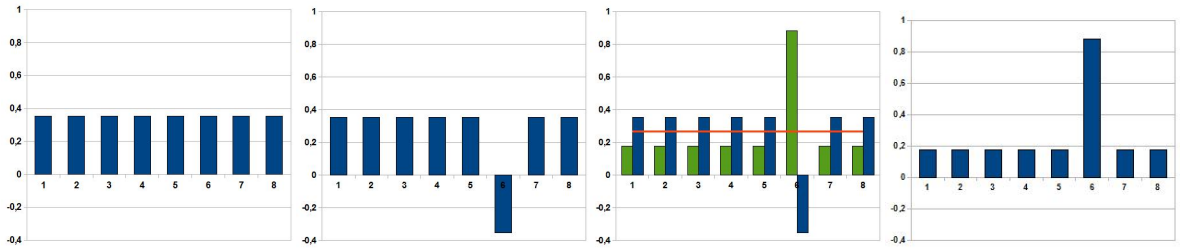


FIGURE 1.7 – Représentation de l'évolution des amplitudes du premier registre au cours de la première itération l'algorithme de Grover pour $n = 3$ et $\mathcal{S} = \{|101\rangle\}$ [278]. De gauche à droite, le premier histogramme représente l'état $|+\rangle^{\otimes 3}$ d'initialisation, le second histogramme l'application de l'Oracle marquant l'élement recherché et les deux derniers histogrammes représentent l'application de l'opérateur de Diffusion.

L'algorithme de Grover présente un avantage par rapport aux algorithmes naifs de recherche, et ceci en particulier pour tout problème de décision dont la complexité est de classe **NP** (problèmes pour lesquels on peut vérifier si une proposition de solution en est bien une, et ceci en un temps polynomial) [193].

Par exemple, l'utilisation de l'algorithme de Grover pour la résolution du problème d'*Amplitude amplification* [44], permet un gain quadratique en terme de complexité, comparé aux algorithmes classiques basés sur des heuristiques.

L'algorithme de Grover peut en outre être utilisé pour trouver le minimum parmi n nombres [90], pour déterminer la connectivité d'un graphe à n sommets [89] et pour accélérer les méthodes de type Monte-Carlo [122]

1.2.2 Algorithme de Shor

L'algorithme de Shor[9], est un des algorithmes quantiques les plus célèbres, connu notamment pour l'avancée considérable qu'il propose : passer d'une complexité sous-exponentielle à une complexité polynomiale pour le célèbre problème de factorisation des entiers. Cet algorithme contribua grandement à faire connaître les disciplines de l'information et du calcul quantique, que ce soit auprès du grand public comme de la communauté scientifique, et constitua un des arguments en faveur de leur développement. L'algorithme a été publié il y a plus d'une vingtaine d'années [245], mais il continue d'être étudié jusqu'à aujourd'hui, et a bouleversé la discipline de la sécurité informatique, permettant l'émergence de la cryptographie post-quantique notamment [153, 35, 111, 36].

Une des spécificités de l'algorithme de Shor est qu'il redéfinit le problème de factorisation comme un problème de recherche de la période d'une fonction, et fait alors appel à la Transformée de Fourier Quantique pour le résoudre. On se propose tout d'abord d'introduire formellement le problème de factorisation, puis de présenter la Transformée de Fourier Quantique pour enfin aborder explicitement l'algorithme de Shor et les discussions associées.

Mise en place du problème

L'objectif de l'algorithme de Shor est de permettre la résolution du problème de factorisation des entiers. Ce problème est reconnu comme un problème difficile à résoudre, et c'est pour cette raison que certains algorithmes de cryptographie informatique exploitent ce fait pour sécuriser les communications et transactions informatiques.

Supposons que nous cherchons à factoriser un entier M. Le principe de l'algorithme repose principalement sur l'utilisation du théorème d'Euler-Fermat comme formulé ci-dessous :

Théorème 1.2.1 (Euler-Fermat)**.** *Soit M un entier strictement positif et a un entier premier avec M. Alors nous avons*

$$a^{\varphi(n)} \equiv 1 \mod M \text{ aussi noté } a^{\varphi(n)} \equiv 1[M] \ ,$$

avec φ la fonction indicatrice d'Euler.

Ceci implique notamment que pour tout entier a premier avec M, il existe un entier positif r tel que :

$$a^r \equiv 1[M] \iff a^r - 1 \equiv 0[M] \ . \tag{1.43}$$

Le plus petit entier r vérifiant cette propriété est appelé *l'ordre de a modulo M*. La détermination de cet entier a en effet un lien direct avec le problème de factorisation de l'entier M. Si l'on suppose que r est un entier pair, alors on peut procéder à la factorisation suivante :

$$(a^{r/2} - 1)(a^{r/2} + 1) \equiv 0 \mod M \ . \tag{1.44}$$

9. Peter Shor (né en 1959) est actuellement professeur au MIT et membre du CSAIL. Il est connu pour ses contributions majeures dans le domaine du calcul quantique

En posant $\alpha = a^{r/2} - 1$ et $\beta = a^{r/2} + 1$, nous pouvons en déduire que M divise le produit $\alpha\beta$. Cependant, le facteur α ne peut pas être un multiple de M, car cela impliquerait qu'il existe un ordre de a modulo M plus petit que r, ce qui contredit la définition de r. De ce fait, soit β est un multiple de M, soit α et/ou β renferment des facteurs de M.

Dans le second cas, en calculant le $PGCD(\alpha, M)$ et $PGCD(\beta, M)$, nous récupérerons au moins un facteur du nombre M. De cette manière, on pourra en déduire une factorisation du nombre M. La principale difficulté de cette approche pour résoudre le problème de factorisation de M repose dans la difficulté à déterminer l'entier r, ordre de a modulo M.

C'est ici que le calcul quantique apporte une solution non réalisable de manière classique, en résolvant le problème de recherche de l'ordre r, par un algorithme de recherche de la période ayant une complexité de l'ordre de $\mathcal{O}(n^3)$ avec n le nombre de qubits sur système quantique utilisé pour résoudre le problème [200]. Pour faire le lien entre ces deux problèmes nous définissons une fonction périodique f, agissant sur l'espace de Hilbert à n qubits, dont la période est exactement égale à l'ordre r. Ceci sera abordé plus en détail en Section 1.2.2, après avoir introduit le Transformée de Fourier Quantique en sous-section suivante.

Transformée de Fourier Quantique

Dans le domaine de l'information et du calcul quantique, l'analogue de la Transformée de Fourier[10] Discrète (TFD) est la Transformée de Fourier Quantique (TFQ). La Tranformée de Fourier Quantique agit de manière linéaire sur un registre quantique, et constitue une étape clé de l'algorithme de Shor, permettant notamment de révéler la période de la fonction définissant le problème de factorisation (comme nous le verrons par la suite).

En effet, la TFQ présente des propriétés intéressantes dans le contexte de l'information quantique et des algorithmes quantiques [200] :

- c'est un opérateur unitaire,
- elle transforme l'état $|0\rangle^{\otimes n}$ en l'état parallélisé $|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$,
- *Linear Shift Invariant property* : elle transforme un état périodique en un autre état périodique, sans prendre en compte le *shift* initial (voir Chapitre 4 pour de plus amples informations sur les états périodiques).

Lorsqu'elle est appliquée sur un des états de la base canonique $|k\rangle \in \{|0\rangle, |1\rangle, \dots |N-1\rangle\}$ (exprimés ici en notation décimale), avec $N = 2^n$ le nombre d'états de base et n le nombre de qubits, le résultat de la TFQ peut être décrit comme suit :

$$|k\rangle \xrightarrow{\mathcal{TFQ}} QFT\ |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2i\pi}{N}kj} |j\rangle\ . \tag{1.45}$$

10. Jospeh Fourier (1768 – 1830) est un mathématicien et physicien français, notamment connu pour avoir déterminé, par le calcul, la diffusion de la chaleur en utilisant la décomposition d'une fonction quelconque à l'aide de ses célèbres séries de Fourier.

Ainsi, pour un système à n-qubit quelconque $|\psi\rangle$, nous avons :

$$|\psi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{\mathcal{TFQ}} \left|\widetilde{\psi}\right\rangle = \sum_{k=0}^{N-1} y_k |k\rangle \ , \tag{1.46}$$

avec,

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \cdot \omega^{kj} \ , \text{ avec } \quad \omega = e^{\frac{2i\pi}{N}} \ . \tag{1.47}$$

Étant une application unitaire, la Transformée de Fourier Quantique peut aussi être écrite sous la forme d'une matrice carrée (à coefficients complexes souvent) de taille $2^n \times 2^n$:

$$TFQ_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix} \ , \tag{1.48}$$

avec $\omega = e^{\frac{2i\pi}{N}}$ la racine N-ième de l'unité.

La Transformée de Fourier Quantique peut aussi être décomposée à l'aide de plusieurs portes quantiques de base agissant sur un ou deux qubits, permettant de la représenter aisément sous la forme d'un circuit quantique, représentation qui s'avère souvent utile dans le contexte de calculs et algorithmes quantiques. La TFQ peut être définie comme une combinaison et une succession de trois différentes portes : la porte de Hadamard, la porte SWAP et la porte *controlled-*R_k (définie ci-dessous, voir Équation 1.49). Le circuit complet de la TFQ est représenté en Figure 1.8, où la porte $SWAP_n$ à n-qubits consiste à échanger le qubit $|x_1\rangle$ avec $|x_n\rangle$, le qubit $|x_2\rangle$ avec $|x_{n-1}\rangle$, et ainsi de suite.

$$cR_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix} \qquad \begin{array}{l} |x\rangle \\ |y\rangle \end{array} \quad \Qcircuit @C=1em @R=1em { & \multigate{1}{R_k} & \qw \\ & \ctrl{-1} & \qw } \tag{1.49}$$

Une des raisons rendant l'algorithme de Shor efficace, et amenant de l'intérêt pour la version quantique de la TFQ, est que la complexité de la Transformée de Fourier Quantique est quadratique en le nombre d'opérations et de portes quantiques présentes dans le circuit. En effet, en observant le circuit (Figure 1.8), on remarque que :

- sur la première ligne, correspondant au qubit $|x_1\rangle$, on applique une fois la porte d'Hadamard, et $n-1$ differents cR_k opérateurs,
- sur la ligne de $|x_2\rangle$: une fois la porte d'Hadamard, et $n-2$ differents cR_k opérateurs,
- $\ldots$,
- sur la ligne de $|x_n\rangle$: une fois la porte d'Hadamard,
- enfin, on applique au plus $\frac{n}{2}$ fois l'opérateur SWAP (agissant sur deux qubits).

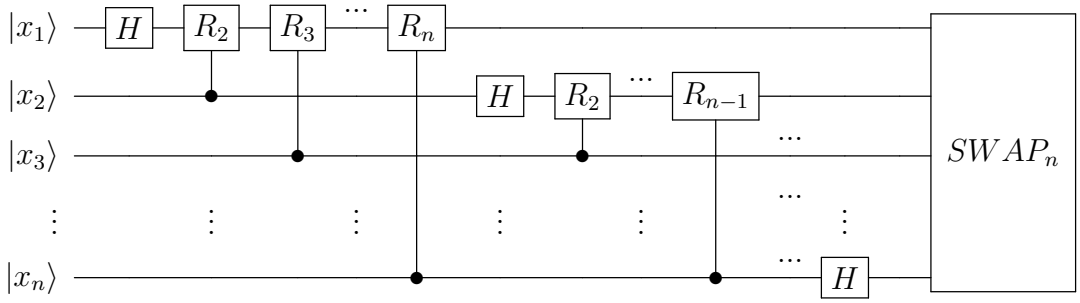


FIGURE 1.8 – Représentation de la Transformée de Fourier Quantique, appliquée à un registre à n-qubit, sous la forme d'un circuit quantique.

Au total, au plus $\frac{n(n+1)}{2} + \frac{n}{2}$ opérations sont effectuées (ou portes quantiques sont appliquées), ce qui entraîne une complexité de l'ordre de $\mathcal{O}(n^2)$ opérations, avec n le nombre de qubits. Avec $N = 2^n$ états de base, on obtient une complexité de l'ordre de $\mathcal{O}(\log(N)^2)$ opérations

Il peut paraître maladroit de comparer, en terme de complexité, la Transformée de Fourier Quantique, qui agit sur des registres quantiques, et la Transformée de Fourier Discrète ou la *Fast Fourier Transform* qui eux agissent sur des vecteurs classiques, et coûtent respectivement $\mathcal{O}(m2^m)$ et $\mathcal{O}(m \log m)$ portes, avec m le nombre de bits. Cependant, l'exploitation de la superposition quantique, et éventuellement l'intervention de l'intrication quantique dans ce processus, peuvent expliquer l'intéressante complexité de la TFQ, et par conséquent l'avantage qu'elle permet d'apporter dans l'algorithme de recherche de la période de l'algorithme de Shor [154, 147]. Cette question sera discutée plus en profondeur dans le Chapitre 4.

Recherche de la période

Dans cette sous-section, nous présentons l'algorithme de recherche de la période, nécessaire à l'implémentation de l'algorithme de Shor. Cet algorithme peut être représenté sous la forme d'un circuit quantique (voir Figure 1.9).

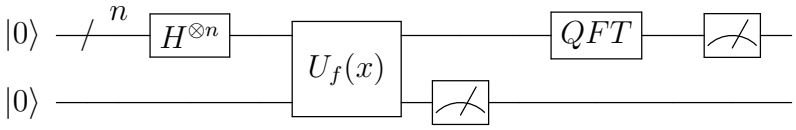


FIGURE 1.9 – Représentation de l'algorithme de recherche de la période, sous la forme d'un circuit quantique.

On définit tout d'abord une fonction $f : \mathcal{H}_N \to \mathcal{H}_N$ avec $\mathcal{H}_N = \{|x\rangle \ / \ x \in \mathbb{N}, x < N\}$. On dit que f est périodique de période $r < N$, lorsque :

$$\forall x \in [\![0, N - r - 1]\!],\ f(|x + r\rangle) = f(|x\rangle)\ . \tag{1.50}$$

On suppose par ailleurs que f ne prend jamais deux fois la même valeur dans une même période. On pose alors $f(|x\rangle) = |a^x\ [M]\rangle$ qui prend un état $|x\rangle$ en paramètre

et renvoie l'état $|a^x \text{ modulo } M\rangle$. Cette fonction permet de modéliser le problème de recherche de l'ordre de a modulo M. On remarque que la fonction f est en effet périodique, et on notera r la période de la fonction f. On définit également une porte $U_f : (x, y) \to (x, y \oplus f(x))$, permettant d'appliquer la fonction f à un registre quantique, avec x le registre de données. Le résultat sera contenu dans le registre de résultats $y \oplus f(x)$.

L'algorithme commence par initialiser le premier registre dans l'état totalement parallélisé $|+\rangle^{\otimes n}$ et le second registre dans l'état $|0\rangle$. Le système quantique $|\psi_0\rangle$ modélisant les deux premiers registres après l'intialisation s'exprime comme décrit dans l'équation suivante :

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle|0\rangle \ . \tag{1.51}$$

Ensuite la porte U_f est appliquée à l'ensemble des 2 registres. Cela a pour effet de transformer le second registre qui associe, à chaque état de base dans l'expression du premier registre, l'application de la fonction f à cet état de base. On récupère alors l'état $|\psi_1\rangle$ exprimé comme suit :

$$|\psi_1\rangle = U_f|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle\left|a^k[M]\right\rangle \ . \tag{1.52}$$

L'algorithme continue ensuite en effectuant une mesure sur le second registre. Après la mesure, on récupère une valeur particulière $\left|a^{k_0}\right\rangle$ parmi toutes les valeurs $\left|a^k[M]\right\rangle$ calculées précédemment. Or la valeur a^{k_0} n'est pas atteinte, à travers la fonction périodique f, seulement pour $k = k_0$, mais pour toutes les valeurs périodiques associées à k_0, c'est à dire pour tous les k pouvant s'écrire $k = k_0 + jr$, avec $j \in \mathbb{N}$. Il en résulte qu'il ne reste pas seulement l'état $|k_0\rangle$ dans le premier registre, après la mesure, mais tous les autres états donnant la même valeur a^{k_0} modulo l'entier M. On récupère alors l'état global noté $|\psi_2\rangle$ tel que :

$$|\psi_2\rangle = \frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |k_0 + jr\rangle\left|a^{k_0}\right\rangle \ . \tag{1.53}$$

Afin d'extraire la période r, on se concentre sur l'état du premier registre qui est en effet un état périodique de shift égal à k_0 et de période r. Un état périodique (à coefficients positifs et équilibrés) $\left|\Psi^n_{l,r}\right\rangle$ à n-qubits, avec un shift l et une période r, est défini par son écriture comme suit :

$$\left|\Psi^n_{l,r}\right\rangle = \frac{1}{\sqrt{A}} \sum_{i=0}^{A-1} |l + ir\rangle, \quad \text{avec } A = \left\lceil \frac{N-l}{r} \right\rceil, \ N = 2^n \ . \tag{1.54}$$

Effectuer une mesure sur le premier registre ne permet pas d'extraire la période r de l'état périodique, car nous n'avons pas l'information du nombre k_0 (qui aurait pu nous permettre de déduire j_0 et r après la mesure). À la place, l'algorithme de recherche de période propose d'appliquer la Transformée de Fourier Quantique sur le

premier registre, afin justement de contourner le problème lié à la connaissance de k_0, et de travailler avec un état dont le shift est nul. Cette propriété découle directement de l'application de la TFQ sur un état périodique.

Pour la suite des calculs, et pour simplifier la présentation de l'algorithme dans ce manuscrit, nous supposerons que la période r divise $N = 2^n$. Le cas où r ne divise pas N implique un certain nombre de traitements supplémentaires, ne changeant pas fondamentalement la complexité globale de l'algorithme de recherche de la période [200]. Notons $K = \frac{N}{r}$. Nous appliquons alors la TFQ sur le premier registre de l'état périodique $|\psi_2\rangle$ en omettant d'écrire l'état du second registre :

$$|\psi_3\rangle = TFQ_N|\psi_2\rangle = \frac{1}{\sqrt{K}}\sum_{j=0}^{K-1} y_j|k_0 + jr\rangle \ , \tag{1.55}$$

avec

$$y_j = \frac{1}{\sqrt{N}}\sum_{k=0}^{K-1} e^{\frac{2i\pi}{N}j(k_0+kr)} = \frac{1}{\sqrt{N}}e^{\frac{2i\pi}{N}jk_0}\sum_{k=0}^{K-1} e^{\frac{2i\pi}{N}jkr} \ . \tag{1.56}$$

Après simplifications de l'état obtenu suite à l'application de la TFQ nous obtenons l'état suivant :

$$|\psi_3\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{\frac{2i\pi}{r}jk_0}\left|j\frac{N}{r}\right\rangle \ . \tag{1.57}$$

Si l'on effectue de nouveau une mesure, mais cette fois sur le premier registre, nous obtiendrons un état $|z\rangle$ où z est un multiple de $\frac{N}{r}$. De ce fait il existe un $j_0 \in \mathbb{N}$ tel que $z = j_0\frac{N}{r}$. Ceci est équivalent à considérer cette égalité de fraction $\frac{z}{N} = \frac{j_0}{r}$.

La prochaine étape consiste à déterminer concrètement la période r. On cherchera alors à réduire la fraction $\frac{z}{N}$. Si j_0 et r sont premiers entre eux alors on peut immédiatement en déduire la période r comme dénominateur. Si ce n'est pas le cas, différentes procédures seront nécessaires, sans rentrer d'avantage dans les détails, comme notamment la relance du processus pour mesurer une valeur différente de z et utiliser l'algorithme des fractions continues pour simplifier la fraction [200]. Il demeure que la probabilité que $j_0 \in [0, r-1]$ soit premier avec r est de l'ordre de $\frac{1}{2\log(r)}$ qui reste strictement supérieure à la quantité $\frac{1}{n}$. De ce fait, on peut espérer qu'en répétant le processus un certain nombre de fois, il sera bien possible de déterminer la période r.

À partir de la valeur de la période r, on pourra la réutiliser dans un algorithme plus gobal pour déterminer la décomposition en facteurs du nombre M. Ceci constitue notamment l'objet de notre prochaine sous-section, visant à présenter l'algorithme de Shor dans sa globalité.

L'algorithme de Shor explicite

Dans cette sous-section, nous nous proposons de résumer tous les différents aspects de l'algorithme de Shor vus précédemment en présentant l'algorithme global de factorisation.

Algorithme 1 Algorithme de Shor

Require: M l'entier naturel à factoriser
Ensure: Un facteur de M

1. Si M est pair, **retourner 2**, sinon on poursuit,
2. Choisir aléatoirement un entier $a \in [\![1, M-1]\!]$. Si $PGCD(a, M) = d > 1$, alors **retourner d**, sinon on poursuit,
3. On utilise l'algorithme de recherche de la période pour trouver l'ordre r tel que $a^r \equiv 1\ [M]$,
4. Si r est impair, *retour à l'étape 2*,
5. Sinon, on calcule $PGCD(a^{r/2} \pm 1, M)$, qui nous donne un facteur non trivial de M.

Ainsi l'algorithme de Shor fait principalement appel à des principes issus de la théorie des nombres, et à des algorithmes classiques pour déterminer le PGCD par exemple. La partie quantique de l'algorithme réside dans la recherche de la période, problème seulement résolvable en une complexité sous-exponentielle de manière classique.

En terme de complexité, nous pouvons subdiviser l'algorithme en plusieurs modules et évaluer la complexité de chacun comme suit :

- La Transformée de Fourier Quantique nécessite $\mathcal{O}(n^2)$ opérations,
- L'application de la fonction f, par exponentiation modulaire, coûte $\mathcal{O}(n^3)$ opérations,
- L'algorithme de recherche de la période r est donc en $\mathcal{O}(n^3)$ opérations (deux points précédents),
- L'algorithme d'Euclide, utilisé pour calculer le $PGCD$, coûte $\mathcal{O}(\log(M)^3)$ opérations,
- L'algorithme de Shor nécessite alors globalement $\mathcal{O}(n^3) = \mathcal{O}(\log(N)^3)$ opérations.

En Partie II Chapitre 4, nous étudierons les états générés par la procédure de recherche de la période, plus précisément l'intrication des états périodiques générés après la mesure du second registre. Nous tenterons de présenter des résultats d'études à la fois qualitatives et quantitatives pour apporter des nouveaux éléments à la compréhension de l'intrication dans l'algorithme de Shor.

1.3 Représentation des qubits

1.3.1 Sphère de Bloch

Une des représentations alternatives d'un qubit est celle de la sphère de Bloch[11]. C'est une représentation dans un espace à 3 dimensions, faisant appel à la sphère $\mathbb{S}^2$ unitaire dans $\mathbb{R}^3$. Un qubit sera alors vu comme un vecteur défini de manière unique par un point sur la sphère unitaire.

Soit $|\psi\rangle \in \mathcal{H} = \mathbb{C}^2$ un qubit défini par $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec α et β, vérifiant la relation de normalisation usuelle (voir Section 1.1.1). On choisit d'adopter la notation

11. Felix Bloch (1905 – 1983) est un physicien suisse, récompensé du prix Nobel de physique en 1952.

exponentielle pour définir ces deux complexes. On pose alors $\alpha = r_1 e^{i\varphi_1}$ et $\beta = r_2 e^{i\varphi_2}$, avec $(r_1, r_2) \in \mathbb{R}^2$ et $(\varphi_1, \varphi_2) \in [0, 2\pi[^2$.

On ré-écrit alors l'état $|\psi\rangle$ comme suit :

$$|\psi\rangle = r_1 e^{i\varphi_1}|0\rangle + r_2 e^{i\varphi_2}|1\rangle \iff |\psi\rangle = e^{i\varphi_1}\left(r_1|0\rangle + r_2 e^{i(\varphi_2-\varphi_1)}|1\rangle\right) . \tag{1.58}$$

On montre que l'état résultant de l'introduction d'une phase globale dans l'écriture d'un état quantique, représentée ici par le facteur $e^{i\varphi_1}$, est physiquement indiscernable de l'état initial, dans la mesure où cette phase ne modifie pas les probabilités de mesures associées aux vecteurs de base. Ceci reste valide quelque soit la base considérée [56, 200]. On peut alors négliger cette phase globale. En rappelant que les coefficients définissant $|\psi\rangle$ doivent vérifier la condition de normalisation, en introduisant la variable $\theta \in [0, 2\pi[$ et en posant $\varphi = \varphi_2 - \varphi_1$, on peut ré-écrire l'actuelle expression de l'état $|\psi\rangle$ comme suit :

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle . \tag{1.59}$$

Les réels θ et φ (considérés comme l'angle polaire et azimutal) définissent un point unique sur la sphère $\mathbb{S}^2$ (voir Figure 1.10). Cette représentation graphique d'un qubit se révèle souvent utile dans le contexte de l'information quantique ou des calculs quantiques.

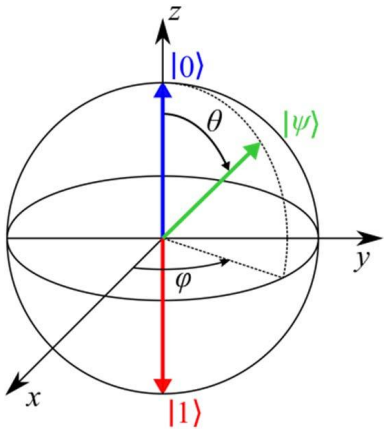


FIGURE 1.10 – Représentation d'un qubit sur la sphère de Bloch [239]

On montre en effet que deux vecteurs opposés sur la sphère de Bloch sont orthogonaux au sens du produit hermitien de $\mathbb{C}^2$. D'autre part, plusieurs portes agissant sur un qubit se décrivent de manière intuitive sur la sphère de Bloch. Appliquer les opérateurs de Pauli X, Y ou Z, revient à effectuer une rotation autour de l'axe x, y ou z. Appliquer la porte d'Hadamard revient alors à réaliser une rotation de 90° autour de l'axe y, puis de 180° autour de l'axe x (voir Figure 1.11).

Des difficultés sont néanmoins rencontrées pour généraliser cette représentation à un système à n-qubits quelconque, mais des représentations similaires existent pour des états spécifiques. Ceci est justement l'objet de la sous-section suivante.

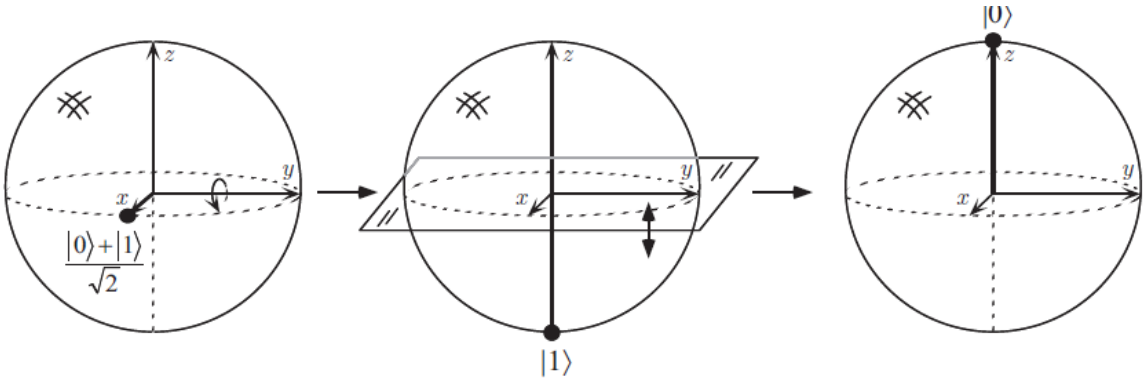


Figure 1.11 – Visualisation de la porte d'Hadamard sur la shpère de Bloch, appliquée à l'état $|+\rangle$ [200].

1.3.2 Représentation de Majorana

Il est possible de représenter, du point du vue de la mécanique quantique, un état pur à $2j$ états de base (ou état pur de spin j) par $2j$ points indiscernables sur la sphère. C'est en effet une généralisation de la représentation d'un qubit sur la sphère de Bloch [16, 192]. Une représentation similaire, appelée représentation de Majorana[12] [185], peut être adoptée pour les états symétriques à n-qubits.

Un état symétrique à n-qubits $|\psi_{sym}\rangle$ est un vecteur de l'espace de Hilbert $\mathcal{H}_{sym} = \mathrm{Sym}^n \mathbb{C}^2$, dont une base orthonormée est donnée par les $n+1$ états de Dicke $|D_k\rangle$. Ces états sont définis comme la somme pondérée équilibrée de toutes les permutations des états de la base canonique avec $n-k$ qubits à $|0\rangle$ et k qubits à $|1\rangle$, c'est-à-dire

$$|D_k\rangle = \frac{1}{\sqrt{\binom{n}{k}}} \sum_{perm} \underbrace{|0\rangle|0\rangle\cdots|0\rangle}_{n-k} \underbrace{|1\rangle|1\rangle\cdots|1\rangle}_{k} . \tag{1.60}$$

Tout état symétrique $|\psi_{sym}\rangle$ pourra alors s'exprimer comme :

$$|\psi_{sym}\rangle = \sum_{i=0}^{n} a_i |D_k\rangle \ , \tag{1.61}$$

avec $a_i \in \mathbb{C}$. La représentation de Majorana d'un état $|\psi_{sym}\rangle$ consiste à trouver l'unique ensemble composé de n qubits $|p_1\rangle, |p_2\rangle, \ldots, |p_n\rangle$ tel que, à une phase près,

$$|\psi_{sym}\rangle = |p_1\rangle \circ |p_2\rangle \circ \cdots \circ |p_n\rangle \ , \tag{1.62}$$

avec $\circ$ désignant ici le produit symétrique de tenseurs, tel que, pour toutes les permutations $\sigma \in S_n$,

$$|p_1\rangle \circ |p_2\rangle \circ \cdots \circ |p_n\rangle = \frac{1}{\sqrt{K}} \left|p_{\sigma(1)}\right\rangle \circ \left|p_{\sigma(2)}\right\rangle \circ \cdots \circ \left|p_{\sigma(n)}\right\rangle \ , \tag{1.63}$$

12. Ettore Majorana (1906 – 1959) est un physicien italien. Il est surtout connu pour ses travaux en physique des particules, avec des applications particulières de la théorie des neutrinos.

avec K le coefficient de normalisation dépendant de l'état considéré. Par ailleurs, comme cela est explicité dans la section précédente (Section 1.3.1), on peut ré-écrire les états $|p_i\rangle$ comme étant

$$|p_i\rangle = \cos\frac{\theta_i}{2}|0\rangle + e^{i\varphi_i}\sin\frac{\theta_i}{2}|1\rangle \ . \tag{1.64}$$

On peut alors voir chaque $|p_i\rangle$ comme un point sur la sphère, et donc représenter l'état $|\psi_{sym}\rangle$ comme une constellation de n points sur la surface $\mathbb{S}^2$. Ces points seront alors appelés *Majorana Points* (MP, ou points de Majorana), et la sphère correspondante la sphère de Majorana.

À titre d'exemple, on peut exprimer les deux premiers états de Dicke sous forme de produits symétriques, tel que $|D_0\rangle = |0\rangle \circ |0\rangle \circ |0\rangle$ et $|D_1\rangle = |0\rangle \circ |0\rangle \circ |1\rangle$. La représentation de Majorana de ces états consistera donc ici en 3 points, positionnés différemment aux pôles nord ou sud (voir Figure 1.12).

(a) Dicke state $|D_0\rangle$ (b) Dicke state $|D_1\rangle$

FIGURE 1.12 – Représentation de Majorana pour les deux premiers états de Dicke, dans le cas des 3-qubits. Le pôle nord désigne l'état $|0\rangle$, tandis que le pôle sud désigne l'état $|1\rangle$.

À partir de la représentation sous forme de produit symétrique de l'état $|\psi_{sym}\rangle$, il n'est pas difficile de retrouver sa décomposition dans la base de Dicke. En revanche, déterminer les $|p_1\rangle, |p_2\rangle, \ldots, |p_n\rangle$ associés à l'état $|\psi_{sym}\rangle$ (voir Équation 1.62), et donc déterminer la représentation de Majorana associée n'est pas aussi direct. Pour ce faire, on définit un polynôme, appelé polynôme de Majorana :

$$p_{|\psi_{sym}\rangle}(z) = \sum_{k=1}^{n}(-1)^k\sqrt{\binom{n}{k}}a_k z^k \ . \tag{1.65}$$

En effet, les quotients des coefficients $\frac{\cos\frac{\theta_i}{2}}{e^{i\varphi_i}\sin\frac{\theta_i}{2}} = e^{-i\varphi_i}\cot\frac{\theta_i}{2}$, définissant les états $|p_i\rangle$, correspondent exactement aux racines z_i du polynôme $p_{|\psi_{sym}\rangle}$ (appelées racines de Majorana) [104]. On établit alors une correspondance directe, pour un état symétrique, entre l'ensemble de ses points sur la sphère de Marojana, ses coefficients dans la base de Dicke et les racines du polynôme de Majorana associé :

$$\text{Points de Majorana } \{|p_i\rangle\}_i \iff \text{Coefficients } \{a_k\}_k \iff \text{Racines de Majorana } \{z_k\}_k \ . \tag{1.66}$$

La correspondance entre les points de Majorana et les racines de Majorana peut aussi être interprétée géométriquement. En effet, si l'on représente les racines de Majorana dans le plan complexe, en plaçant la sphère de Majorana de manière tangente à ce plan, les points de Majorana correspondront alors à la projection stéréographique par rapport au pôle nord des points représentant les racines dans le plan complexe (voir Figure 1.13).

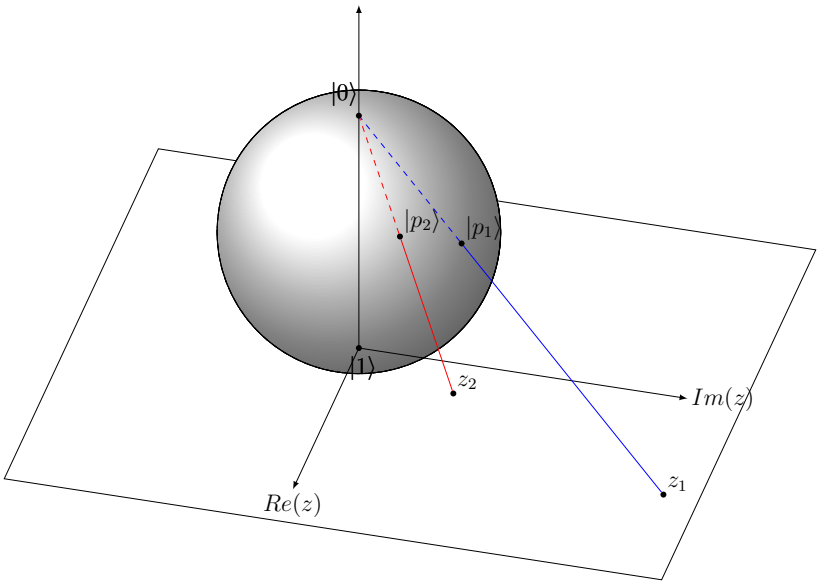


Figure 1.13 – Projection stéréographique associée au pôle nord, établissant la correspondance entre la représentation stellaire des états symétriques et les racines du polynôme de Majorana.

Chapitre 2

Intrication Quantique et Géométrie Algébrique

"One of the exciting things about an entanglement puzzle is there's no end to it. Once you solve how to take it apart, you have to solve how to put it back together", T. J. Miller.

2.1 Notions de Géométrie Algébrique

Dans cette section, nous nous proposons d'introduire les notions de géométrie algébrique utiles dans le cadre de l'étude et de la caractérisation de l'intrication sous l'action du groupe SLOCC et des interprétations géométriques associées. Cela passe par la définition de variétés algébriques modélisant certaines propriétés liées à l'intrication.

La géométrie est l'étude des propriétés d'un ensemble de points, ou d'éléments, qui sont invariantes par un certain groupe de transformations. Ces éléments forment ce que l'on peut appeler des objets géométriques, et certains de ces objets peuvent trouver une définition précise d'un point de vue algébrique. On dira alors que la géométrie algébrique est l'étude d'objets géométriques (tels que des courbes ou des surfaces), formés par ensemble de points dont les cordonnées vérifient un ensemble d'équations algébriques.

2.1.1 Espace projectif

Soit V un espace vectoriel de dimension $n+1$. On appelle espace projectif issu de V, et on note $\mathbb{P}(V)$ ou $\mathbb{P}V$, l'ensemble des droites vectorielles de V, c'est à dire l'ensemble des sous-espaces de dimension 1 de V [246]. On dit que $\mathbb{P}(V)$ est un espace projectif de dimension n, et on pourra noter $\mathbb{P}^n = \mathbb{P}(V)$ et on le définit [160] tel que :

$$\mathbb{P}(V) = \{[v] \mid v \in V \backslash \{0_V\}\} \ , \tag{2.1}$$

où $[v]$ désigne l'ensemble des vecteurs colinéaires à v. Si le vecteur v s'exprime par les coordonnées $(v_0, v_1, \ldots, v_n)$ dans une base de l'espace vectoriel V, alors la projectivisation $[v]$ de ce vecteur pourra s'exprimer par les coordonnées homogènes $[v_0 : v_1 : \ldots : v_n]$. Si on considère la relation d'équivalence $\mathbb{C}^\times$, représentée par l'action du produit par un

scalaire non nul $\lambda \in \mathbb{C}^*$, alors v est un représentant de la classe d'équivalence $[v]$, définie comme l'ensemble des vecteurs de V pouvant s'écrire λv.

À titre d'exemple, si V est de dimension 2, alors $\mathbb{P}(V) = \mathbb{P}^1$ sera appelé droite projective, et chaque point de cette droite projective $\mathbb{P}(V)$ représentera une direction (une droite passant par l'origine) dans l'espace vectoriel V. Dans le cas où V est de dimension 3, on appelera alors $\mathbb{P}(V)$ le plan projectif.

Dans le contexte de l'information quantique, et de l'étude de l'intrication plus particulièrement (voir Section 2.2), considérer les états quantiques comme des points de l'espace projectif associé à l'espace de Hilbert, c'est considérer tous les vecteurs (dans l'espace de Hilbert) proportionnels (au sens de la multiplication par un scalaire non nul) comme un même point dans l'espace projectif. La multiplication externe ne changeant pas la nature de l'état (un état quantique est défini à une phase prêt), et de surcroît sa classe d'intrication, il est alors intéressant de se placer dans l'espace projectif.

2.1.2 Variété Projective

Dans cette section, nous introduisons la notion de variété projective, qui nous permettra ensuite d'associer différentes variétés à différentes classes d'intrication quantique. Ces variétés sont les objets de base étudiés en géométrie projective, et sont les analogues projectifs des variétés affines [62]. Dans le contexte de l'information quantique et du reste de ce manuscrit, lorsque cela n'est pas précisé c'est que nous travaillerons sur le corps des complexes.

Les variétés algébriques sont définies comme le lieu des zéros de polynômes. Cependant, en se plaçant dans l'espace projectif, il en résulte que les coordonnées (homogènes) d'un point de l'espace projectif ne sont pas définies de manière unique, mais à un scalaire près. De ce fait, un polynôme ne sera pas considéré comme une fonction car ne renvoyant pas la même valeur pour plusieurs représentants d'une même classe d'états colinéaires [83]. En revanche, dans le cadre de la définition de variétés projectives, seulement les zéros des polynômes nous intéressent. Ceci nous motive donc à nous intéresser aux polynômes homogènes définis ci-dessous [62].

Définition 1. Un polynôme $p \in \mathbb{C}[x_0, \ldots, x_N]$ est dit *homogène* de degré d si, et seulement si, il s'écrit comme une combinaison linéaire de monômes de degré d. Ainsi pour tout élément $\lambda \in \mathbb{C}$, on a

$$p(\lambda x_0, \ldots, \lambda x_n) = \lambda^d p(x_0, \ldots, x_n) \ .$$

On en déduit alors que si un polynôme homogène s'annule pour un point donné de l'espace projectif, il s'annulera pour tout représentant de la classe d'équivalence associée. En effet, pour tout $\lambda \neq 0$, nous aurons alors l'équivalence suivante

$$p(x_0, \ldots, x_n) = 0 \iff p(\lambda x_0, \ldots, \lambda x_n) = 0 \ . \tag{2.2}$$

Nous définissons alors à présent la notion de variété projective.

Définition 2. Soit $S \subset \mathbb{C}[x_0, \ldots, x_N]$ un ensemble formé de polynômes homogènes. On définit $\mathcal{V}(S)$ comme le sous-ensemble de $\mathbb{P}^N$ formé des zéros communs à tous les éléments de S. Les sous-ensembles $\mathcal{V}(S)$ de $\mathbb{P}^N$ de ce type définissent les *variétés projectives*.

$$\mathcal{V}(S) = \left\{ [x] = [x_0, x_1, \ldots, x_n] \in \mathbb{P}^N \mid f(x_0, x_1, \ldots, x_n) = 0, \ \forall f \in S \right\} .$$

Deux ensembles distincts de polynômes S et S' peuvent définir la même variété $\mathcal{V}(S) = \mathcal{V}(S')$. Par exemple, il est clair que $\mathcal{V}(x) = \mathcal{V}(x^2)$. Pour préciser l'ensemble des polynômes s'annulant sur une variété il faut introduire la notion d'idéal, que nous définissons succinctement ci-dessous.

Définition 3. Soit $\mathcal{V}$ une variété projective, sous-ensemble de $\mathbb{P}^N$. On appelle *idéal* de $\mathcal{V}$, et on le note $I(\mathcal{V})$, l'ensemble des polynômes homogènes de $\mathbb{C}[x_0, \ldots, x_N]$ s'annulant sur $\mathcal{V}$.

Un théorème clé que l'on doit à Hilbert implique que tout idéal de $\mathbb{C}[x_0, \ldots, x_N]$ est généré par un nombre fini de polynômes. À partir d'une variété il sera alors possible de déterminer son idéal, comme il sera aussi possible de déterminer la variété associée à un idéal quelconque. Ceci indique une correspondance entre variété et idéal, et il sera alors possible de générer de différentes manières l'idéal d'une variété algébrique [77].

Enfin, et dans le cadre de cette thèse et de l'étude de l'intrication quantique, lorsque nous considérerons des variétés complexes projectives lisses, nous les noterons généralement X.

2.1.3 Variété de Segre

Dans le contexte de l'information quantique, la variété de Segre joue un rôle pour la description mathématique de l'intrication quantique. Elle paramétrise en effet tous les états séparables (et donc non-intriqués) de l'espace de Hilbert, et les variétés auxiliaires associées permettent également de mettre en évidence différents aspects ou classes d'intrication [128, 135].

Nous proposons d'étudier comme premier objet géométrique la surface quadrique afin d'introduire sous forme d'exemple cette variété. Nous considérons alors dans $\mathbb{P}^3$ la surface quadrique d'équation $z_0 z_3 - z_2 z_1 = 0$. Nous nous proposons de voir dans quelle mesure cette surface peut être vue comme le produit cartésien $\mathbb{P}^1 \times \mathbb{P}^1$ de deux droites projectives plongé dans $\mathbb{P}^3$.

L'idée est d'identifier $\mathbb{P}^3$ avec la projectivisation de l'espace des matrices carrées d'ordre 2 à coefficients complexes, c'est-à-dire $\mathbb{P}^3 = \mathbb{P}\left(\mathcal{M}_2(\mathbb{C})\right) = \mathbb{P}(\mathbb{C}^2 \otimes \mathbb{C}^2)$. Pour ce faire, on définit un ensemble S, et on propose deux définitions équivalentes ci-dessous :

$$\begin{aligned} S &= \{(a_{ij}) \in \mathcal{M}_2(\mathbb{C}) \mid \mathsf{Rang}(a_{ij}) = 1\} \\ &= \left\{(a_{ij}) \neq 0_{M_2(\mathbb{C})} \mid det(a_{ij}) = 0\right\} , \end{aligned} \tag{2.3}$$

représentant toutes les matrices carrées d'ordre 2 à coefficients complexes de rang 1. On associe à S, l'ensemble $\widetilde{S} = S/\mathbb{C}^\times$ des classes d'équivalence pour la relation de

colinéarité. Toutes les matrices de S définies à un facteur multiplicatif près seront donc dans la même orbite. Ainsi l'ensemble $\widetilde{S}$ peut être vu comme la projectivisation des matrices carrées d'ordre 2 complexes de rang 1.

On définit alors une application φ de $\mathbb{P}^1 \times \mathbb{P}^1$ dans $\widetilde{S}$ comme

$$\begin{array}{rccc} \varphi\colon & \mathbb{P}^1 \times \mathbb{P}^1 & \to & \widetilde{S} \\ & ([x_0 : x_1], [y_0 : y_1]) & \mapsto & \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \begin{pmatrix} y_0 & y_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 & x_0 y_1 \\ x_1 y_0 & x_1 y_1 \end{pmatrix}, \end{array} \tag{2.4}$$

et on peut démontrer qu'il s'agit en fait d'un isomorphisme entre les deux ensembles [20, 63]. Ainsi, tout couple de lignes projectives, défini par deux paires de coordonnées homogènes, peut être associé à une classe d'équivalence pour les matrices de rang 1. Il est possible d'aller plus loin, et de plonger notre ensemble $\widetilde{S}$ dans l'espace projectif $\mathbb{P}^3$ en considérant la transformation suivante :

$$\begin{array}{rccc} \varphi_2\colon & \widetilde{S} & \hookrightarrow & \mathbb{P}^3 \\ & \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} & \mapsto & [a_{00} : a_{01} : a_{10} : a_{11}]. \end{array} \tag{2.5}$$

Ce plongement revient à ré-écrire les coefficients de la matrice comme un vecteur ligne exprimant des coordonnées homogènes dans $\mathbb{P}^3$. En effet, comme les matrices de $\widetilde{S}$ sont définies à un scalaire près, l'image d'une matrice sera bien la classe d'équivalence représentée par le point de $\mathbb{P}^3$ correspondant. Par ailleurs, on peut déduire de la définition de S que la matrice nulle n'appartient pas à l'ensemble, et cela est cohérent avec le fait que l'origine $[0 : 0 : 0 : 0]$ n'appartient pas à $\mathbb{P}^3$.

Ainsi, en combinant ces deux transformations φ et φ_2, il est possible de plonger le produit $\mathbb{P}^1 \times \mathbb{P}^1$ dans $\mathbb{P}^3$, et on appelle ce plongement **le plongement de Segre**[1] de deux droites projectives [20] :

$$\begin{array}{rccc} \mathrm{Seg}\colon & \mathbb{P}^1 \times \mathbb{P}^1 & \hookrightarrow & \mathbb{P}^3 \\ & ([x_0 : x_1], [y_0 : y_1]) & \mapsto & [x_0 y_0 : x_0 y_1 : x_1 y_0 : x_1 y_1], \end{array} \tag{2.6}$$

D'autre part, l'image de $\mathbb{P}^1 \times \mathbb{P}^1$ par le plongement de Segre dans $\mathbb{P}^3$ peut être définie à l'aide de polynômes homogènes. En effet, on rappelle que de part l'application φ, on peut associer à tout point de $\mathbb{P}^1 \times \mathbb{P}^1$ une classe de matrice de rang 1, et ensuite la voir comme un point en coordonnées homogènes dans l'espace projectif $\mathbb{P}^3$. De plus, la seconde définition de l'ensemble S, nous indique aussi que ce plongement permet de voir de manière équivalente les matrices 2×2 complexes de déterminant nul comme des points de $\mathbb{P}^3$. Or cette condition de nullité du déterminant s'exprime justement comme un polynôme homogène de degré 2.

Si on dénote par $[z_0 : z_1 : z_2 : z_3]$ les coordonnées homogènes des points de $\mathbb{P}^3$, alors nous pouvons en effet voir $\mathbb{P}^1 \times \mathbb{P}^1$ comme la variété projective $Q = \mathcal{V}(z_0 z_3 - z_2 z_1) \subset \mathbb{P}^3$. On appelle cette variété Q la surface quadrique [57, 63]. Si l'on s'intéresse à l'image de toutes les matrices non nulles de $\mathcal{M}_2(\mathbb{C})$ alors on obtient tout $\mathbb{P}^3$. Si l'on ne s'intéresse

1. Corrado Segre (1863 – 1924) est un mathématicien italien connu pour ses contributions majeures au développement de la géométrie algébrique.

qu'à l'image des matrices de rang 1 (et donc de déterminant égal à 0), alors on obtient la variété Q qui est un sous-ensemble de $\mathbb{P}^3$. On appelle aussi, de manière générale, cette variété la **variété de Segre**.

On peut généraliser le plongement de Segre afin de considérer le produit cartésien de n espaces projectifs comme une variété projective. Prenons l'espace de Hilbert $\mathcal{H}_n$ tel que $\mathcal{H}_n = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \cdots \otimes \mathbb{C}^{d_n}$, et considérons l'espace projectif associé à chaque facteur par $\mathbb{P}^{d_i-1} = \mathbb{P}(\mathbb{C}^{d_i})$. On définit alors le plongement de Segre du produit de n espace projectifs comme suit [57] :

$$\begin{array}{rccc} \text{Seg}: & \mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1} & \hookrightarrow & \mathbb{P}(\mathcal{H}_n) \\ & ([v_1], [v_2], \ldots, [v_n]) & \mapsto & [v_1 \otimes v_2 \otimes \cdots \otimes v_n] \end{array}, \tag{2.7}$$

où v_i est un vecteur de $\mathbb{C}^{d_i}$, et $[v_i]$ le point correspondant dans $\mathbb{P}^{d_i-1} = \mathbb{P}(\mathbb{C}^{d_i})$. On plonge alors le produit cartésien $\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1}$ dans l'espace projectif $\mathbb{P}(\mathcal{H}_n) = \mathbb{P}^{d_1 d_2 \ldots d_n - 1}$. De ce point de vue, les points $\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1}$ peuvent être vus comme des matrices multidimensionnelles, ou des tenseurs, et la variété de Segre $\text{Seg}(\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1})$ correspondra alors à l'ensemble des tenseurs de $\mathcal{H}_n$ de rang 1 [165, 57] (voir Section 2.1.6 pour une définition et discussion sur le rang de tenseurs).

Exemple 1. En guise d'exemple, on considère le produit $\mathbb{P}^a \times \mathbb{P}^b$. Le plongement de Segre à deux facteurs s'exprimera alors :

$$\begin{array}{rccc} \text{Seg}: & \mathbb{P}^a \times \mathbb{P}^b & \hookrightarrow & \mathbb{P}^{(a+1)(b+1)-1} \\ & ([x_0 : \ldots : x_a], [y_0 : \ldots : y_b]) & \mapsto & [x_0y_0 : x_0y_1 : \ldots : x_iy_j : \ldots : x_ay_b] \end{array}. \tag{2.8}$$

On peut alors montrer que l'image $\text{Seg}(\mathbb{P}^a \times \mathbb{P}^b) \subset \mathbb{P}^{(a+1)(b+1)-1}$ est une variété projective définie par l'ensemble des équations de la forme $x_iy_j \times x_ky_l - x_iy_l \times x_ky_j = 0$ [83]. La variété de Segre à 2 facteur $\text{Seg}(\mathbb{P}^a \times \mathbb{P}^b)$ est donc définie comme le lieu des zéros de l'idéal généré par tous les 2×2 mineurs des matrices de taille $(a+1)(b+1)$. La variété de Segre est donc la projectivisation de l'ensemble de matrices de rang 1 [165]. ♢

La variété de Segre modélisera alors tous les tenseurs de $\mathcal{H}_n$ de rang 1, c'est-à-dire pouvant se décomposer en produit tensoriel de vecteurs de chaque espace vectoriel définissant $\mathcal{H}_n$. Cette notion de factorisation trouve un lien direct avec la notion de séparabilité des systèmes quantiques, et donc un lien avec la notion d'intrication étudiée en Section 2.2. Enfin, la variété de Segre définit une orbite fermée pour l'action du groupe $\text{GL}_{d_1} \times \cdots \times \text{GL}_{d_n}$.

2.1.4 Variété de Veronese

De manière analogue au plongement de Segre, on peut définir l'application de Veronese[2] permettant de plonger un espace projectif $\mathbb{P}^n$ dans un espace projectif plus grand $\mathbb{P}^N$ [83].

2. Giuseppe Veronese (1854 – 1917) est un mathématicien italien, ayant, entre autres, publié de remarquables ouvrages concernant la géométrie multidimensionnelle.

Les premiers exemples présentés dans la littérature sont la *twisted cubic curve* et la surface de Veronese [57]. Le premier exemple présente une manière de plonger un espace projectif $\mathbb{P}^1$ dans $\mathbb{P}^3$, et peut être décrit par la transformation ν_3 suivante :

$$\begin{array}{rccc} \nu_3 : & \mathbb{P}^1 & \hookrightarrow & \mathbb{P}^3 \\ & [x:y] & \mapsto & [x^3 : x^2y : xy^2 : y^3] \end{array} . \tag{2.9}$$

L'étude du second exemple par la communauté a été motivée par l'étude des quadriques, polynômes de degré 2, de la forme homogène suivante [282] :

$$Ax^2 + By^2 + Cz^2 + Dxy + Exz + Fyz = 0 . \tag{2.10}$$

En effet, le plongement de Veronese de degré 2 de $\mathbb{P}^2$ dans $\mathbb{P}^5$ permet de représenter l'ensemble des quadriques de la forme décrite en Équation 2.10. Cette variété de Veronese correspond à l'ensemble des quadriques qui s'écrivent $Q = L^2$, avec $L = ax+by+cz$, et est définie par

$$\begin{array}{rccc} \nu_2 : & \mathbb{P}^2 & \hookrightarrow & \mathbb{P}^5 \\ & [x:y:z] & \mapsto & [x^2 : y^2 : z^2 : xy : xz : yz] \end{array} . \tag{2.11}$$

L'image par l'application $\nu_2 : \mathbb{P}^2 \to \mathbb{P}^5$ s'appelle la surface de Veronese [83], et peut aussi être vue comme la variété projective modélisant toutes les matrices symétriques de rang 1 de la forme

$$\begin{pmatrix} x^2 & xy & xz \\ xy & y^2 & yz \\ xz & yz & z^2 \end{pmatrix} . \tag{2.12}$$

De manière générale, le plongement de Veronese quadratique $\nu_2(\mathbb{P}(\mathcal{H}))$ est la projectivisation des matrices symétriques de rang 1 [165], et explicitement si $v = (v_1, \ldots, v_k) \in \mathcal{H}$ alors

$$\nu_2([v]) = \left[\begin{pmatrix} v_1v_1 & v_1v_2 & \cdots & v_1v_k \\ v_2v_1 & v_2v_2 & \cdots & v_2v_k \\ \vdots & \vdots & \vdots & \vdots \\ v_kv_1 & v_kv_2 & \cdots & v_kv_k \end{pmatrix} \right] . \tag{2.13}$$

Le plongement de Veronese, ou la variété de Veronese associée, se généralise en dimensions supérieures en considérant $n+1$ variables, et à tout degré d. Le plongement de Veronese de degre d, $\nu_d : \mathbb{P}^n \to \mathbb{P}^N$, enverra alors $[x_0 : \ldots : x_n]$ sur tous les monômes possibles de degré d. La variété sera alors un sous ensemble de l'espace projectif $\mathbb{P}^N$, avec $N = \binom{n+d}{d} - 1$ correspondant au nombre de monômes de degré d à $n+1$ variables, auquel on soustrait 1 par définition de l'espace projectif [83].

Exemple 2. Par exemple, dans le cas où $n = 1$, le plongement de Veronese de degré d définit une variété projective appelée **variété de Veronese de degré** d, pouvant notamment définir un isomorphisme entre la droite projective $\mathbb{P}^1$ et son image dans $\nu_d(\mathbb{P}^1)$ comme décrit ci-dessous :

$$\begin{array}{rccc} \nu_d : & \mathbb{P}^1 & \hookrightarrow & \mathbb{P}^d \\ & [x:y] & \mapsto & [x^d : x^{d-1}y : \ldots : xy^{d-1} : y^d] \end{array} . \tag{2.14}$$

Cette variété $\nu_d(\mathbb{P}^1)$ est souvent appelée la *rational normal curve* dans la littérature [165]. ♢

Il est également possible de voir la variété de Veronese sans utiliser de coordonnées explicites. En effet, pour un espace de Hilbert donné $\mathcal{H}$, la variété de Veronese de degré d plonge l'espace projectif $\mathbb{P}(\mathcal{H})$ dans $\mathbb{P}(\mathrm{Sym}^d \mathcal{H})$, avec $\mathrm{Sym}^d \mathcal{H}$ définissant les puissances symétriques de degré d sur $\mathcal{H}$ [165]. En d'autres termes, on peut écrire :

$$\begin{array}{rccc} \nu_d\colon & \mathbb{P}(\mathcal{H}) & \hookrightarrow & \mathbb{P}(\mathrm{Sym}^d \mathcal{H}) \\ & [v] & \mapsto & [v \circ v \circ \cdots \circ v] = [v^{\circ n}] \end{array} , \tag{2.15}$$

voir Équation 1.63 pour une définition du produit symétrique $\circ$.

La variété de Veronese, du point de vue de l'intrication, est l'équivalent de la variété de Segre mais pour les états (ou tenseurs) symétriques. En effet, la variété de Veronese modélise les états séparables symétriques (donc non-intriqués), et peut alors aussi se définir comme la restriction de la variété de Segre aux états symétriques [165].

En considérant l'espace de Hilbert à n-qubits $\mathcal{H}_n = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, et en rappelant que $\mathbb{P}^1 = \mathbb{P}(\mathbb{C}^2)$, on peut définir l'image du plongement de Veronese de degré n appliqué à $\mathbb{P}(\mathbb{C}^2)$ comme étant :

$$\nu_n(\mathbb{P}(\mathbb{C}^2)) = \ \mathrm{Seg}(\mathbb{P}^1 \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1) \cap \mathbb{P}(\mathrm{Sym}^n \mathbb{C}^2) \ \subset \ \mathbb{P}(\mathcal{H}_n) \ . \tag{2.16}$$

La variété de Veronese peut de ce fait également être définie par un ensemble de 2×2 mineurs d'une matrice symétrique. Nous nous intéresserons plus en profondeur à cette variété, dans le contexte de l'étude de l'intrication des états symétriques, notamment en étudiant les variétés auxiliaires associées dans les Chapitres 6 et 7. Enfin, la variété de Veronese est une orbite fermée pour l'action du groupe $\mathrm{SL}_d(\mathbb{C})$.

2.1.5 Variété Grassmannienne

Dans le contexte de la théorie de l'information quantique, la variété de Grassmann[3], ou variété Grassmannienne, modélise les états fermioniques séparables. Dans cette section nous définissons la notion de produit externe nécessaire à l'introduction de la variété Grassmannienne. En Chapitre 6, nous définissons une mesure de l'intrication pour les états fermioniques, comme une distance à cette variété, et étudions les états fermioniques maximalement intriqués.

Soit V un espace vectoriel de dimension n. Soient $e_1, e_2, \ldots, e_n$ des vecteurs de V formant une base orthonormée de V. Le produit extérieur de deux vecteurs e_1 et e_2 de V, noté $e_1 \wedge e_2$, n'est pas un vecteur du même espace vectoriel V, mais d'un nouvel espace noté $\bigwedge^2 V$. Ce produit extérieur est bilinéaire, alterné ($e_1 \wedge e_1 = 0$) et antisymétrique ($e_1 \wedge e_2 = -(e_1 \wedge e_2)$).

On définit également le produit extérieur de k vecteurs $e_1 \wedge \cdots \wedge e_k$ de V comme un vecteur de l'espace $\bigwedge^k V$, ensemble des produits externes de degré k dans l'espace V.

3. Hermann Günther Grassmann (1809 – 1877) est un mathématicien allemand, considéré aujourd'hui comme le fondateur du calcul tensoriel et de la théorie des espaces vectoriels.

Dans le cas des états fermioniques, on prendra $V = \mathbb{C}^n$, et on modélisera donc un état fermionique à k particules à n états comme un vecteur $|\psi\rangle$ de $\bigwedge^k \mathbb{C}^n$, tel que :

$$|\psi\rangle = \sum_{1\leq i_1,\dots,i_k\leq n} a_{i_1,\dots,i_k}\ e_{i_1} \wedge \cdots \wedge e_{i_k}\ , \tag{2.17}$$

avec les amplitudes complexes $a_{i_1,\dots,i_k}$ vérifiant $\sum_{1\leq i_1,\dots,i_k\leq n} |a_{i_1,\dots,i_k}|^2 = 1$. Il est courant de voir le produit extérieur de k vecteurs $e_1 \wedge \cdots \wedge e_k$ noté de manière raccourcie $e_{i_1 i_2 \dots i_k}$. Pour $k = 3$, on aura par exemple $e_{ijk} = e_i \wedge e_j \wedge e_k$.

D'autre part, il est possible de voir l'espace $\bigwedge^k \mathbb{C}^n$ comme un sous-espace de $(\mathbb{C}^n)^{\otimes k}$. En particulier, il est possible d'établir une relation entre le produit extérieur et le produit tensoriel (néanmoins peu recommandée par Laurent Schwartz [238]). Dans le cas $k = 2$, cette relation s'exprime comme suit :

$$e_1 \wedge e_2 = e_1 \otimes e_2 - e_2 \otimes e_1\ . \tag{2.18}$$

Il est alors possible, de ce point de vue, de voir le vecteur $e_1 \wedge e_2$ de $\bigwedge^2 \mathbb{C}^n$ comme un tenseur antisymétrique de $\mathbb{C}^n \otimes \mathbb{C}^n$.

Nous pouvons à présent définir la variété projective Grassmannienne [165].

Définition 4. Soit $G(k,n) \subset \mathbb{P}\left(\bigwedge^k \mathbb{C}^n\right)$ l'ensemble des éléments de le forme $[e_1 \wedge \cdots \wedge e_k]$, avec $e_1, \dots, e_k \in \mathbb{C}^n$. Alors $G(k,n)$ est appelée la variété de Grassmann, ou la Grassmannienne, et son plongement dans l'espace projectif est appelé le plongement de Plücker.

La Grassmannienne $G(k,n)$ modélise donc l'ensemble des états de $\bigwedge^k \mathbb{C}^n$ pouvant s'écrire de manière factorisée, et représente donc tous les états fermioniques non-intriqués ou séparables.

Enfin, d'un point de vue géométrique, de la même manière que l'ensemble $\mathbb{P}(\mathbb{C}^n)$ paramétrise les sous-espaces de dimension 1 (droites) de $\mathbb{C}^n$, la variété $G(k,n)$ paramétrise les sous-espaces de dimension k de $\mathbb{C}^n$.

2.1.6 Variété des sécantes et rang de tenseur

Variété des sécantes

Nous choisissons ici d'introduire la notion de variété de sécantes à travers la notion de joint. On définit alors ci-dessous le joint de deux variétés.

Définition 5. Le *joint* $J(X,Y)$ de deux variétés $X \subset Y \subset \mathbb{P}^N$ est défini comme la clôture de Zariski de l'union des droites projectives passant par des points distincts de X et Y [165], c'est à dire plus précisément :

$$J(X,Y) = \overline{\bigcup_{\substack{x\in X, y\in Y \\ x\neq y}} \mathbb{P}^1_{xy}}\ .$$

La première variété des sécantes, souvent notée $\sigma(X)$ ou $\sigma_2(X)$ se définit comme l'ensemble des droites projectives reliant deux points d'une même variété. De ce fait, il est possible de définir cette première variété des sécantes à l'aide du concept de joint en observant que $\sigma_2(X) = J(X, X)$. De ce fait, la variété projective $\sigma_2(X)$ contiendra tous les points de toutes les lignes sécantes et tangentes à la variété projective X [165].

La dimension de la variété $J(X, Y)$ peut être calculée en raisonnant par construction. En effet, pour obtenir un point $j \in J(X, Y)$, on dispose de $\dim(X)$ degrés de liberté pour choisir un point de X, puis $\dim(Y)$ degrés de liberté pour choisir un point de Y, puis enfin un degré de liberté en choisissant un point sur la ligne joignant les deux points précédents. Il peut aussi arriver que la variété $J(X, Y)$ remplis tout l'espace ambiant dans ce cas $J(X, Y) = \mathbb{P}^N$. De ce fait, la dimension attendue de la variété $J(X, Y)$, s'exprime comme $\min\big(\dim(X) + \dim(Y) + 1, N\big)$. Il est néanmoins possible que la variété de joint $J(X, Y)$ soit dégénérée et que la dimension attendue ne soit pas atteinte. On en déduit en outre que la dimension attendue de la variété des sécantes $\sigma_2(X)$ est donnée par $\min\big(2\dim(X) + 1, N\big)$ [165, 57].

De même, la notion de variété des sécantes se généralise à l'ordre supérieur, en considérant plus de 2 points pour définir les droites sécantes parcourues par la variété des sécantes. Pour ce faire, on généralise également la notion de joint à l'ordre supérieur.

Définition 6. Le joint de k variétés $X_1, \ldots, X_k \subset \mathbb{P}^N$ est défini comme étant la clôture (au sens de Zariski) de l'union des espaces projectifs $\mathbb{P}^{k-1}$ correspondant, ou par induction $J(X_1, \ldots, X_k) = J(X_1, J(X_2, \ldots, X_k))$.

On pourra alors définir la k-ème variété des sécantes de X, comme étant $\sigma_k(X) = J(X, \ldots, X)$, le joint de k copies de X [165].

Il peut arriver que la dimension de la k-ième variété des sécantes $\sigma_k(X)$ ne soit pas égale à la dimension attendue, dans ce cas on dira que X est k-défective ou seulement défective. On peut alors prouver que si X est k-défective, alors X est aussi j-défective pour tout $j \geq k$. Ceci est notamment le cas de la surface de Veronese (voir Équation 2.11) qui est un des exemples les plus connus de variété défective. De manière générale, si $X \subset \mathbb{P}^N$ est une variété de dimension n, alors la dimension attendue de la k-ième sécante $\sigma_k(X)$ est donnée par le $\min\big(k\dim(X) + 1, N\big)$ [165, 57].

Dans le cadre de cette thèse, nous nous intéresserons principalement aux variétés des sécantes associées à la variété de Segre et à la variété de Veronese. En effet, ces variétés sont liées à la notion d'intrication, comme suggéré dans les sous-sections précédentes, et les variétés des sécantes associées permettent une stratification, une classification et une interprétation géométrique des différentes classes d'intrication des systèmes quantiques [128, 133].

Remarque 7. Les variétés des sécantes de variétés de Segre trouvent un lien direct avec la notion de rang, comme abordé plus tard dans cette section, et permet en effet de voir les points de ces variétés comme des points d'un espace sécant engendré par un certain nombre d'état séparables. L'étude de ces variétés de sécantes liées aux variétés de Segre

trouve une grande motivation auprès de la communauté de géométrie algébrique car directement liée au problème de détermination du nombre minimal de multiplication nécessaire pour calculer un produit matriciel de taille donnée [164].

Remarque 8. D'autre part, les variétés des sécantes liées aux variétés de Veronese intéressent grandement les chercheurs en géométrie algébrique, notamment pour leur lien avec le problème de décomposition de polynômes homogènes. En effet, la variété des sécantes $\sigma_p(\nu_d(\mathbb{P}^n))$ est la fermeture de Zariski de l'ensemble des polynômes homogènes à $n+1$ variables pouvant s'exprimer comme la somme de p formes linéaires à la puissance d [165, 57]. Un problème associé est celui de Waring (*Waring problem for forms*), mettant en jeu la dimension des variétés des sécantes des variétés de Veronese. En effet, le problème consiste à déterminer quel est le plus petit entier r_0 tel qu'un polynôme homogène à $n+1$ variable de degré peut s'écrire comme la somme de r_0 de formes linéaires élevées à la puissance d. En d'autres termes, cela revient à déterminer le plus petit r_0 tel que $\sigma_{r_0}(\nu_d(\mathbb{P}^n)) = \mathbb{P}(\mathrm{Sym}^d \mathbb{P}^n)$, c'est à dire déterminer la variété des sécantes de plus petit ordre telle qu'elle remplit tout l'espace [57]. La valeur attendue est fournie par le théorème d'Alexander-Hirschowitz, et ceci sera notamment discuté en Chapitre 7.

Rang d'un tenseur

Lorsque l'on étudie les tenseurs d'un point de vue mathématique, une des principales propriétés associée à ces objets est celle du rang, généralisant la notion de rang (bien connue) pour les matrices. De plus le rang d'un tenseur, lorsqu'il est associé à l'état d'un système quantique, peut servir de mesure algébrique de l'intrication, et ceci nous motive entre autres à l'étudier dans le contexte de l'informatique quantique [55].

La notion de rang de tenseur généralise la notion de rang pour les matrices multi-dimensionnelles. Nous commençons par définir les tenseurs de rang 1.

Définition 9. Soient $|\psi_1\rangle \in \mathcal{H}_1, \ldots, |\psi_m\rangle \in \mathcal{H}_m$ des vecteurs d'espaces de Hilbert respectifs. Un tenseur $|\psi\rangle$ de $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m$ est dit de *rang* 1 (ou élémentaire, indécomposable ou factorisé) si, et seulement si, il peut s'écrire sous la forme $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_m\rangle$ [165].

On définit alors le rang général d'un tenseur comme suit :

Définition 10. Soit un tenseur $|\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m$. On définit le rang du tenseur $|\psi\rangle$, et on le note $\mathsf{Rang}(|\psi\rangle) = r$, comme étant l'entier naturel minimum r tel que $|\psi\rangle = \sum_{i=1}^{r} |\Phi_i\rangle$, avec tous les $|\Phi_i\rangle \in \mathcal{H}$ étant de rang 1 [165].

Remarque 11. Les tenseurs de rang 1 peuvent être vus comme les blocs de base de $\mathcal{H}$. En effet, il existe toujours une base de $\mathcal{H}$ composée de tenseurs de rang 1 tel que tout tenseur de $\mathcal{H}$ peut s'exprimer comme une combinaison de tenseurs de rang 1.

La détermination de cette valeur minimale r correspondant au rang peut être vue comme un analogue du problème de Waring pour les tenseurs [57]. Une propriété intéressante du rang d'un tenseur $|\psi\rangle \in \mathcal{H}$, notamment lorsqu'il est lié à la notion d'intrication, est qu'il reste inchangé si l'on effectue un changement de base sur l'espace de Hilbert $\mathcal{H}_i$. Ceci en fait donc un invariant intéressant par transformation locale de l'état des systèmes quantiques, qui permettra en effet de caractériser l'intrication quantique.

La notion de rang se définit également pour les tenseurs symétriques, et on parle alors de *rang symétrique*. En effet, les tenseurs appartenant à la variété de Veronese, par exemple, modélisent les tenseurs symétriques de rang 1. La notion de rang symétrique se définit alors de manière analogue, comme suit :

Définition 12. Le rang symétrique d'un tenseur $|\psi_{sym}\rangle \in \mathrm{Sym}^d \mathcal{H}$, noté $\mathsf{Rang}_{Sym}(|\psi_{sym}\rangle)$, est le plus petit entier r tel que pour tout $|\varphi_i\rangle \in \mathcal{H}$ on a :

$$|\psi_{sym}\rangle = \underbrace{|\varphi_1\rangle \circ |\varphi_1\rangle \circ \cdots \circ |\varphi_1\rangle}_{\text{d fois}} + \cdots + \underbrace{|\varphi_r\rangle \circ |\varphi_r\rangle \circ \cdots \circ |\varphi_r\rangle}_{\text{d fois}} \ .$$

Remarque 13. Pour tout tenseur $|\psi_{sym}\rangle \in \mathrm{Sym}^d \mathbb{C}^n \subset (\mathbb{C}^n)^{\otimes d}$, le rang symétrique vérifie toujours l'inégalité $\mathsf{Rang}_{Sym}(|\psi_{sym}\rangle) \leq \binom{n+d-1}{d}$. Le rang symétrique d'un tenseur symétrique peut être aussi être comparé au rang d'un tenseur symétrique. En effet, nous avons toujours $\mathsf{Rang}_{Sym}(|\psi_{sym}\rangle) \geq \mathsf{Rang}(|\psi_{sym}\rangle)$ [165].

Enfin, la notion de rang peut également être définie pour les tenseurs antisymétriques, et on parlera alors de *rang antisymétrique*. Les tenseurs antisymétriques de rang 1 sont en effet les états de la variété Grassmannienne, et on peut définir le rang antisymétrique comme suit :

Définition 14. Le rang antisymétrique d'un tenseur $|\psi_{asym}\rangle \in \bigwedge^k \mathcal{H}$, noté $\mathsf{Rang}_{ASym}(|\psi_{asym}\rangle)$, est le plus petit entier r tel que pour tout $|\varphi_{i,j}\rangle \in \mathcal{H}$, en précisant que pour tout i les vecteurs $\{|\varphi_{i,1}\rangle, |\varphi_{i,2}\rangle, \ldots |\varphi_{i,k}\rangle\}$ sont indépendants, on a :

$$|\psi_{asym}\rangle = \sum_{i=1}^{r} \underbrace{|\varphi_{i,1}\rangle \wedge |\varphi_{i,2}\rangle \wedge \cdots \wedge |\varphi_{i,k}\rangle}_{\text{k fois}} \ .$$

Rang de bord

Une notion dérivant de la notion de rang est celle du rang de bord. Elle sous-entend une notion de bord, et de points limites, et se définit en effet comme suit :

Définition 15. Un tenseur $|\psi\rangle$ est de *rang de bord* r, et on note $\mathsf{Rang}_{Bord}(|\psi\rangle) = r$ si, et seulement si, il est la limite de tenseurs de rang r, mais n'est pas la limite de tenseurs de rang s, pour tout $s < r$ [165]. En d'autres termes, $|\psi\rangle$ est de rang de bord r s'il existe une famille de tenseurs $\{|\psi_\epsilon\rangle \mid \epsilon > 0\}$ de rang r tels que $\lim_{\epsilon \to 0} |\psi_\epsilon\rangle = |\psi\rangle$, et s'il n'existe pas une telle famille d'états de rang $r-1$.

La notion de rang de bord trouve en effet un lien direct avec les variétés de sécantes. En effet, si X désigne la variété de Segre (des tenseurs de rang 1, et donc de rang de bord 1), alors r-ième variété des sécantes $\sigma_r(X)$ définira l'ensemble des tenseurs $|\psi\rangle$ de rang de bord au plus r [165]. De ce fait, nous avons l'équivalence suivante :

$$\mathsf{Rang}_{Bord}(|\psi\rangle) = r \iff |\psi\rangle \in \sigma_r(X) \textbf{ et } |\psi\rangle \notin \sigma_{r-1}(X) \ . \tag{2.19}$$

Remarque 16. Pour tout tenseur $|\psi\rangle \in \mathcal{H}$, nous avons toujours l'inégalité suivante : $\mathsf{Rang}(|\psi\rangle) \geq \mathsf{Rang}_{Bord}(|\psi\rangle)$ [165].

Exemple 3. À titre d'exemple, on considère le tenseur $T = |001\rangle + |010\rangle + |100\rangle$ de rang 3. On se propose de démontrer que ce tenseur est de rang de bord égal à 2. En effet, on peut trouver une famille de tenseurs $|\psi_\varepsilon\rangle$ de rang 2 tendant vers le tenseur T lorsque ε tend vers 0.

$$T_\varepsilon = \frac{1}{K_\varepsilon}\left(\frac{1}{\varepsilon}\left(|0\rangle + \varepsilon|1\rangle\right)^{\otimes 3} - \frac{1}{\varepsilon}|000\rangle\right) \ , \tag{2.20}$$

avec $\varepsilon > 0$ et K_ε le facteur de normalisation dépendant d'ε. Il est clair qu'à partir de l'écriture de T_ε (voir Équation 2.20) que c'est un état de rang 2, quelque soit ε positif non nul. Il peut être moins évident que ce tenseur tend vers T. On peut développer et ré-écrire le tenseur T_ε comme suit :

$$\begin{aligned} T_\varepsilon = \frac{1}{K_\varepsilon}\Big(\frac{1}{\varepsilon}|000\rangle + |001\rangle + |010\rangle + |100\rangle + \varepsilon|011\rangle + \varepsilon|101\rangle + \varepsilon|101\rangle \\ +\varepsilon^2|111\rangle - \frac{1}{\varepsilon}|000\rangle\Big) \ . \end{aligned} \tag{2.21}$$

Il apparaît à présent plus clairement que les termes $|000\rangle$ se simplifient, et que les termes avec ε en facteur seront éliminés en passant à la limite. Il ne restera donc que les vecteurs de base $|001\rangle$, $|010\rangle$ et $|100\rangle$ formant le tenseur T, et donc on a bien :

$$\lim_{\varepsilon \to 0} T_\varepsilon = T \ . \tag{2.22}$$

♢

D'autre part, il est également possible de définir le rang de bord symétrique et antisymétrique d'un tenseur comme suit :

Définition 17. Le *rang de bord symétrique* r d'un tenseur symétrique $|\psi_{sym}\rangle$, et on note $\mathsf{Rang}_{Bord,Sym}(|\psi\rangle) = r$, est défini comme le plus petit entier r tel que $|\psi_{sym}\rangle$ est la limite de tenseurs symétriques de rang symétrique r [165].

Remarque 18. Pour tout tenseur $|\psi_{sym}\rangle \in \mathrm{Sym}^d \mathbb{C}^n \subset (\mathbb{C}^n)^{\otimes d}$, le rang de bord symétrique d'un tenseur symétrique peut être aussi être comparé au rang de bord d'un tenseur symétrique. En effet, nous avons toujours $\mathsf{Rang}_{Bord,Sym}(|\psi_{sym}\rangle) \geq \mathsf{Rang}_{Bord}(|\psi_{sym}\rangle)$ [165].

Définition 19. Le *rang de bord antisymétrique* r d'un tenseur symétrique $|\psi_{asym}\rangle$, et on note $\mathsf{Rang}_{Bord,ASym}(|\psi\rangle) = r$, est défini comme le plus petit entier r tel que $|\psi_{asym}\rangle$ est la limite de tenseurs antisymétriques de rang antisymétrique r.

2.1.7 Variété des tangentes

La variété des tangentes, comme son nom l'indique, est la variété algébrique définie comme l'union des espaces tangents. Soit une variété algébrique lisse $X \subset \mathbb{P}(\mathcal{H}) = \mathbb{P}^N$. On définit la projectivisation de l'espace tangent $T_x X$ au point $x \in X$ comme étant l'ensemble

$$T_x X = \left\{ v \in \mathbb{P}^N \mid \operatorname{grad}_x F(v) = 0,\ \forall F \in I(X) \right\} , \tag{2.23}$$

avec $I(X)$ l'idéal de X, ensemble de polynômes généré par les polynômes définissant la variété X [101]. On définit alors la variété des tangentes de X, notée $\tau(X) \subset \mathbb{P}^N$ comme étant

$$\tau(X) = \bigcup_{x \in X} T_x X \ . \tag{2.24}$$

La variété des tangentes $\tau(X)$ est toujours incluse dans la variété des sécantes $\sigma_2(X)$, et la dimension de la variété des tangentes est l'objet du théorème suivant :

Théorème 2.1.1 (Fulton et Hansen)**.** *Soit $X \subset \mathbb{P}^N$ une variété algébrique de dimension n, alors une de ces deux affirmations est vraie [165] :*

- $\dim \sigma_2(X) = 2n + 1$ *et* $\dim \tau(X) = 2n$,
- $\sigma_2(X) = \tau(X)$.

Il est également possible de définir la variété des tangentes en introduisant la notion d'union de limites de droites projectives, dans un esprit similaire à la notion de joint (voir Section 2.1.6).

Soit Y une seconde variété algébrique telle que $Y \subset X \subset \mathbb{P}^N$. On définit l'objet $T^\star_{X,Y,y_0}$ comme étant l'union des droites projectives $\mathbb{P}^1_\star$, avec $\mathbb{P}^1_\star$ définie comme étant la limite de la droite $\mathbb{P}^1_{xy}$, avec $x \in X$, $y \in Y$ et $y \to y_0 \in Y$. De plus, on définit la variété $T(Y, X)$ des tangentes relatives de X par rapport à Y comme étant justement l'union des $T^\star_{X,Y,y_0}$ [101, 135] :

$$T(Y, X) = \bigcup_{y \in Y} T^\star_{X,Y,y} \ . \tag{2.25}$$

La variété des tangentes pourra alors aussi être définie par l'égalité $\tau(X) = T(X, X)$. De même, on peut généraliser la notion de variété des tangentes à des ordres supérieurs, permettant notamment d'introduire la notion de variété osculatoire $Osc_k(X)$ [165]. Enfin, il est possible de décrire les relations entre les variétés des tangentes et des sécantes d'ordres supérieurs et leurs dimensions sous la forme d'une chaîne d'inclusion, comme cela est décrit dans la proposition suivante [135] :

Proposition 2.1.1. *Soit $X \subset \mathbb{P}^N$ une variété algébrique non-dégénérée de dimension n. Supposons que la k-ième variété des sécantes est non-défective et ne remplit pas l'espace ambiant. Alors nous avons la chaîne d'inclusion suivante, avec les dimensions correspondantes :*

$$\underbrace{X}_{dim=n} \subset \underbrace{\tau(X)}_{=2n} \subset \underbrace{\sigma_2(X)}_{=2n+1} \subset \underbrace{T(X, \sigma_2(X))}_{=3n+1} \subset \underbrace{\sigma_3(X)}_{=3n+2} \subset \underbrace{T(X, \sigma_3(X))}_{=4n+2} \subset \cdots \subset \underbrace{\sigma_k(X)}_{=kn+k-1} \subset \mathbb{P}^N$$

.

2.1.8 Variété duale

La notion de dualité projective, et notamment les variétés projectives appelées variétés duales, ont été intensivement étudiées dans le domaine de la géométrie algébrique, car permettant notamment de reconstruire n'importe quelle variété projective à partir de ses hyperplans tangents [256].

Pour tout espace de Hilbert $\mathcal{H}$, on note par $\mathcal{H}^*$ l'espace de Hilbert *dual*, c'est à dire l'espace vectoriel défini par les formes linéaires sur $\mathcal{H}$. D'autre part, en se plaçant dans le contexte de la géométrie projective, le dual $\mathbb{P}(\mathcal{H})^*$ de l'espace projectif lié à l'espace de Hilbert $\mathcal{H}$ correspond à l'espace projectif du dual de $\mathcal{H}$ [256]. En d'autres termes on a $\mathbb{P}(\mathcal{H})^* = \mathbb{P}(\mathcal{H}^*)$, et tous les points de l'espace projectif dual $\mathbb{P}(\mathcal{H}^*)$ correspondent aux hyperplans de $\mathbb{P}(\mathcal{H})$.

On rappelle ci-dessous la notion générale de vecteur dual dans un espace équipé d'une forme hermitienne [165], La notion de vecteur dual a été rapidement esquissée en Équations 1.5 et 1.6 dans le cadre du qubit.

Définition 20. Soit $\mathcal{H}$ un espace de Hilbert et $\mathcal{H}^*$ son espace dual. Alors pour tout $\langle\alpha| \in \mathcal{H}^*$, l'hyperplan H_α, dual du point $[\alpha] \in \mathbb{P}(\mathcal{H}^*)$, est le sous-espace de $\mathbb{P}(\mathcal{H})$ défini par $H_\alpha = \mathbb{P}(\alpha^\perp)$ avec

$$\alpha^\perp = \{|v\rangle \in \mathcal{H} \mid \langle\alpha|v\rangle = 0\} \ .$$

Inversement, on peut aussi associer à tout point $[\beta]$ de $\mathbb{P}(\mathcal{H})$, associé au vecteur $|\beta\rangle$, un hyperplan dans $\mathbb{P}(\mathcal{H}^*)$, c'est à dire l'ensemble des hyperplans de $\mathbb{P}(\mathcal{H})$ passant par $[\beta]$. Il vient alors que le dual du dual est l'espace initial, c'est à dire que $\mathbb{P}(\mathcal{H}^*)^* = \mathbb{P}(\mathcal{H})$. Cette dualité entre point d'un espace et hyperplan de l'espace dual est illustrée dans le cas de $\mathbb{P}^2$ en Figure 2.1.

(a) Un point dans $(\mathbb{P}^2)^*$ (b) Une ligne dans $(\mathbb{P}^2)^*$

Figure 2.1 – Représentation graphique dans $\mathbb{P}^2$, de la dualité entre points et lignes de l'espace projectif dual $(\mathbb{P}^2)^*$ [106].

À partir de ces définitions de base, nous pouvons à présent définir la notion de variété projective duale. Soit $X \subset \mathbb{P}(\mathcal{H})$ une variété algébrique. Nous renvoyons le lecteur à la Section 2.1.7 pour la définition de l'espace tangent T_xX à X au point $x \in X$. Pour tout hyperplan $H \subset \mathbb{P}(\mathcal{H})$, on dit que H est tangent à X au point x, si H contient l'espace tangent T_xX. On définira alors la variété duale de la variété X, et on notera $X^* \subset \mathbb{P}(\mathcal{H}^*)$, la fermeture (au sens de Zariski) de l'ensemble des hyperplans tangents à X [106, 256, 165] :

$$X^* = \overline{\{H \in \mathbb{P}(\mathcal{H}^*) \mid \exists x \in X,\ T_xX \subset H\}} \subset \mathbb{P}(\mathcal{H}^*) \ . \tag{2.26}$$

Une manière équivalente de voir la variété duale est de la définir comme l'ensemble des hyperplans $H \in \mathbb{P}(\mathcal{H}^*)$ tels que la section $X \cap H$ ne soit pas lisse et comporte des singularités [106, 256, 135, 137]. Cet aspect sera notamment développé au Chapitre 5 pour permettre une classification de l'intrication par l'étude des singularités de cette section hyperplane.

La variété duale X^* est une variété projective à part entière, et son dual est donné par $(X^*)^* = X$ d'après le théorème de bidualité [106, 135]. D'une manière générale, on s'attend à ce que X^* soit une hypersurface : on a $\dim(X)$ degrés de liberté pour choisir x, et $\mathrm{codim}(X) - 1$ degrés de liberté pour choisir H qui contient $T_x X$. Lorsque la variété duale est une hypersurface, un unique (à un scalaire près) polynôme homogène irréductible définit X^* et est appelé X-déterminant ou **hyperdéterminant**, noté Δ_X ou Det_X, définissant la variété duale par l'équation $Det_X = 0$. Les points appartenant à la variété duale X^* sont dits *dégénérés* et les points à l'extérieur de cette variété sont dit *non-dégénérés*.

Exemple 4. Dans le cas où la variété considérée $X = \mathrm{Seg}(\mathbb{P}^n \times \mathbb{P}^n)$ est la variété de Segre à 2 facteurs, alors la variété duale X^* est l'hypersurface définie par le fait que le déterminant (de la matrice associée) est égal à 0. La variété duale dans le cas où $X = \mathrm{Seg}(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)$ a été étudiée par Cayley, et son équation est définie par l'annulation d'un polynôme quartique appelé l'hyperdéterminant de Cayley [59, 58]. ♢

Exemple 5. Un autre exemple est celui de la variété duale de la variété de Veronese, et le polynôme associé sera alors appelé *discriminant* [106, 202]. L'étude et la détermination des hyperdéterminants pour différentes variétés duales a beaucoup intéressé les géomètres algébriques, et demeure un problème difficile lorsque les dimensions des variétés considérées augmentent [106, 180, 143, 48, 202, 50]. ♢

La variété duale de la variété de Segre, ou d'autres variétés, et l'hyperdéterminant associé peuvent être utilisés pour caractériser ou étudier les classes d'intrication des systèmes à plusieurs qubits [190, 135, 137, 136, 131, 138, 149]. Cet objet qu'est l'hyperdéterminant reviendra de manière récurrente tout au long de ce manuscrit, car permettant de discriminer qualitativement certaines classes d'intrication en fournissant une interprétation géométrique, et permet aussi de quantifier l'intrication et d'être vu comme une mesure possible de ce phénomène non-local.

2.2 Intrication quantique

L'intrication quantique, aussi appelée enchevêtrement quantique, est un phénomène physique apparaissant à l'échelle subatomique et n'ayant pas d'équivalent (connu à ce jour) dans le monde macroscopique. Ce phénomène a été historiquement questionné et formalisé par Einstein et Schrödinger notamment, et cela depuis 1935 déjà [234, 235, 94]. Il est souvent interprété comme une liaison non-classique entre plusieurs particules quantiques, constituant une corrélation et une dépendance entre les états des différents systèmes quantiques, et ce, indifféremment de la distance séparant ces systèmes dans l'espace. La notion d'intrication invite souvent celui qui l'étudie à considérer l'état des

particules intriquées comme un système unique, sans pouvoir exprimer explicitement l'état d'une seule de ces particules.

La nature et la réalité physique de l'intrication quantique n'est toujours pas connue à ce jour, et différentes théories sont mises en avant pour expliquer ou interpréter ce phénomène à la lumière de la "physique moderne" [107, 120, 15, 252, 186, 151, 249, 105].

Une des manières les plus intuitives de définir l'intrication, d'un point de vue mathématique, est d'introduire la notion de séparabilité. Un système quantique est dit séparable, si l'on peut justement séparer chaque composante, chaque particule, formant le système quantique, et si l'on peut considérer l'état de chaque particule indépendamment de l'état des autres particules du système. Mathématiquement, cette séparation est synonyme de factorisation de l'écriture du système complet en produit de vecteurs représentant l'état de chaque particule. En effet, si pour un système $|\psi\rangle$ à n-qubits, on connaît l'état $|\psi_i\rangle$ de chaque particule, alors l'état $|\psi\rangle$ peut toujours s'écrire :

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle \ . \tag{2.27}$$

Un état $|\psi\rangle$ sera donc séparable s'il peut toujours s'écrire comme le produit tensoriel des états $|\psi_i\rangle$ représentant chaque particule. Il apparaît ici clairement que les points de la variété de Segre (voir Section 2.1.3) correspondent effectivement aux états séparables. Ceci implique que tous les états purs n'appartenant pas à la variété de Segre sont intriqués, ce qui est théoriquement relativement simple à vérifier (même si la difficulté augmente avec la dimension de l'espace de Hilbert). Ceci contraste avec la difficulté d'établir des critères nécessaires et suffisants, et implémentables en pratique, pour l'intrication des états mixtes sous le formalisme des matrices de densité.

Historiquement, c'est l'état de Bell (voir Equation 1.14, aussi appelé état EPR) qui fut le premier état intriqué introduit dans la littérature. Le cas des états à 2 particules et deux états de base par particule (2-qubits) est considéré comme le cas le plus simple d'étude de l'intrication, et sert souvent d'exemple pour introduire explicitement la notion d'intrication (voir Section 2.2.2). En travaillant en dimensions supérieures, l'étude théorique de l'intrication devient plus difficile, et de nombreux efforts sont actuellement mis en œuvre pour développer de nouveaux outils.

Dans cette section, nous présentons les principales notions ayant permis l'étude qualitative et quantitative de l'intrication quantique dans le cadre de cette thèse.

2.2.1 Étude de l'intrication

Afin de caractériser l'intrication quantique à travers différentes classes d'intrication, il convient de partitionner l'espace de Hilbert en différentes classes d'équivalences, où la relation d'équivalence est définie par rapport aux opérations appliquées aux états quantiques [16]. En fonction des différentes natures des transformations (ou opérations) considérées, les classifications associées, et la difficulté de leur mise en place, peut varier. Nous nous proposons de rappeler les principales abordées dans la littérature.

Transformations LU

Une propriété fondamentale de l'intrication quantique est qu'elle reste invariante quelque soit le changement de base local. Plus particulièrement, la classe d'intrication d'un état reste inchangée sous l'application d'opérations unitaires locales (changement de base préservant les bases orthonormales), appelées *Local Unitary* (LU) *transformations*.

Une transformation U agissant sur un système quantique à n particules est dite de type LU si elle se définit comme le produit de n matrices unitaires locales $U_i \in U(d_i, \mathbb{C})$, de taille $d_i \times d_i$, tel que

$$U = U_1 \otimes U_2 \otimes \cdots \otimes U_n \ . \tag{2.28}$$

De ce fait, deux états $|\varphi\rangle, |\psi\rangle \in \mathcal{H}_n$ sont dit LU-équivalents, s'il existe une transformation LU U telle que $|\varphi\rangle = U|\psi\rangle$. Ces deux états quantiques partageront alors les mêmes propriétés physiques, dont l'intrication, du fait de l'impossibilité de la créer ou de la détruire à l'aide de transformations LU. Différents travaux ont été menés afin de déterminer des critères nécessaires ou suffisants en ce qui concerne la LU-équivalence de deux états arbitraires, et des outils permettant de déterminer les formes normales liées à chaque orbite sous l'action du groupe LU [115, 19, 169, 182, 171].

LOCC et SLOCC *operations*

Malgré l'aspect local de certaines transformations agissant de manière locale sur les particules, il est toujours possible de coordonner les différentes opérations quantiques à distance, en utilisant un canal de communication classique (le téléphone typiquement).

C'est ainsi que l'on définit le groupe des *Local Operations and Classical Communication* (LOCC), représentant au plus près les actions réalisées lors des expérimentations : transformations locales unitaires, coordination par communications classiques et mesure des systèmes quantiques manipulés. Le groupe LOCC permet alors de modéliser plus largement les actions sur les systèmes quantiques, par rapport au groupe LU. D'autre part, dans le cas des états purs (ce qui nous intéresse dans ce travail), il est connu que deux états sont LOCC-équivalents s'ils sont LU-équivalents [263, 16]. Plusieurs études de la classification de l'intrication sous l'action du groupe LOCC ont pu être menées [199, 32, 33, 108], et c'est un problème difficile qui intéresse toujours la communauté [254].

C'est de ce concept que découle le groupe d'opérations SLOCC (*Stochastic Local Operations and Classical Communication*). Introduit pour la première fois par Bennet *et al.* [33], et formalisé plus tard dans [87], le groupe SLOCC s'exprime mathématiquement comme le groupe des opérations locales inversibles.

Lorsque l'on s'intéresse aux états quantiques comme étant des vecteurs de l'espace de Hilbert $\mathcal{H}_n = \mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_n}$, un opérateur SLOCC se traduit mathématiquement comme le produit cartésien de matrices inversibles, modélisant une action réversible et indépendante pour chaque sous-espace de Hilbert associé à chaque particule (voir Equation 2.29),

$$G_{SLOCC} = \mathrm{GL}(d_1, \mathbb{C}) \times \mathrm{GL}(d_2, \mathbb{C}) \times \cdots \times \mathrm{GL}(d_n, \mathbb{C}) \ , \tag{2.29}$$

où $\mathrm{GL}(d, \mathbb{C})$ désigne le groupe général linéaire, ensemble des matrices inversibles de taille $d \times d$ à coefficients dans le corps des complexes $\mathbb{C}$.

Lorsque nous travaillons dans l'espace projectif $\mathbb{P}(\mathcal{H}_n)$ associé à l'espace de Hilbert $\mathcal{H}_n$, un opérateur SLOCC se traduit mathématiquement comme le produit cartésien de matrices inversibles de déterminant 1, modélisant une action réversible, indépendante pour chaque sous-espace de Hilbert associé à chaque particule, et préservant notamment les orientations et les transformations projectives (voir Equation 2.30),

$$G_{SLOCC} = \mathrm{SL}(d_1, \mathbb{C}) \times \mathrm{SL}(d_2, \mathbb{C}) \times \cdots \times \mathrm{SL}(d_n, \mathbb{C}) \ , \tag{2.30}$$

où $\mathrm{SL}(d, \mathbb{C})$ désigne le groupe spécial linéaire, ensemble des matrices inversibles de déterminant égal à 1 de taille $d \times d$ à coefficients dans le corps des complexes $\mathbb{C}$. Sauf précision de notre part, nous ferons référence à cette dernière définition du groupe SLOCC tout au long de ce manuscrit.

L'action du groupe SLOCC peut être vue comme similaire à l'action du groupe LOCC, si ce n'est que l'équivalence entre deux états n'est pas nécessairement déterministe. En effet, on introduit un aspect stochastique dans la correspondance entre les états, et la probabilité de succès d'une opération doit seulement être non nulle. De ce fait, les opérateurs SLOCC ne sont pas équivalents à des transformations LU. L'action d'un élément du groupe SLOCC sur un état quantique peut avoir l'effet d'augmenter ou de réduire le taux d'intrication (au sens de la mesure de l'intrication par exemple (voir Section 2.2.3)), mais ne peut pas créer de l'intrication (transformer un état séparable en état intriqué) ou complètement détruire de l'intrication entre particules, et ceci même en présence d'un processus stochastique. D'autre part, cet aspect non-déterministe des opérations locales, munies de communication classique, intéresse particulièrement les expérimentalistes [16].

La classification des états quantiques purs, sous l'action du groupe SLOCC a suscité beaucoup d'intérêt et généré beaucoup d'efforts au sein de la communauté scientifique. Dans certains cas, des résultats de géométrie algébrique, de théorie de la représentation ou de théorie des invariants, déjà établis par le passé, ont permis d'en déduire une classification pour certains systèmes quantiques multipartites [167, 152, 229, 130, 257, 266, 267, 155, 212, 201]. La classification de certains systèmes à quelques particules sous l'action du groupe est rappelée dans la prochaine sous-section (voir Section 2.2.2).

En outre, la LOCC-equivalence de deux états quantiques implique la SLOCC-équivalence de ces deux états, mais la réciproque n'est pas forcément vraie. Ainsi la classification des états sous l'action du groupe LOCC sera plus fine que la classification sous l'action du groupe SLOCC.

2.2.2 Classification sous SLOCC

Dans cette section nous nous proposons de rappeler les classifications connues sous SLOCC pour les systèmes purs à plusieurs qubits, en traitant le cas des 2-qubits, des 3-qubits et des 4-qubits.

Cas des 2-qubits

Le cas des systèmes à 2 particules à 2 états est historiquement celui qui a permis de définir le phénomène d'intrication. Dans ce cas, la classification est simple et binaire : un système à 2-qubits est soit séparable soit intriqué. Les représentants respectifs de ces deux classes d'équivalence peuvent être choisis comme étant l'état $|00\rangle$ et l'état $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Le second état est connu sous le nom d'état $|EPR\rangle$ ou d'état de Bell, en référence au paradoxe EPR et à l'inégalité de Bell [94, 28].

Dans le cas des systèmes purs à 2-qubits, déterminer à laquelle des deux classes appartient un état peut se faire de manière assez directe. En effet, si on considère un état $|\psi\rangle \in \mathcal{H}_2 = \mathbb{C}^2 \otimes \mathbb{C}^2$ tel que

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \ . \tag{2.31}$$

alors l'état est séparable si et seulement si $a_{00}a_{11} - a_{10}a_{01} = 0$. Si on représente le tenseur $|\psi\rangle$ sous la forme d'un vecteur multidimensionnel, c'est à dire ici une matrice 2×2, alors on a

$$|\psi\rangle \sim \begin{pmatrix} a_{00} & a_{10} \\ a_{10} & a_{11} \end{pmatrix} \ , \tag{2.32}$$

L'équation $a_{00}a_{11} - a_{10}a_{01} = 0$ permettant de distinguer les états séparables des états intriqués peut alors être interprétée de différentes manières. Elle est à la fois l'unique équation définissant la variété de Segre $X = \mathrm{Seg}(\mathbb{P}^1 \times \mathbb{P}^1)$ pour les 2-qubits, car elle est en effet le seul 2×2 mineur associé à la représentation matricielle de l'état $|\psi\rangle$. Cette équation est aussi le déterminant de la matrice, et par conséquent est l'équation définissant la variété duale X^*. On comprend alors que les états dégénérés correspondent dans ce cas exactement aux états séparables.

Cas des 3-qubits

Le cas des 3-qubits est le premier à illustrer l'existence d'états intriqués non-équivalents (les états $|GHZ\rangle$ et $|W\rangle$ par exemple, voir Table 2.1), comme cela a été publié la première fois par Dür *et al.* [87]. On dénombre six orbites sous l'action du groupe SLOCC pour les systèmes à 3-qubits. Du point de vue de la géométrie algébrique, la classification des systèmes à 3-qubits (voir Table 2.1) peut être décrite à l'aide notamment de la variété de Segre, la variété des tangentes et sécantes, et la variété duale [135]. Par ailleurs, une autre interprétation géométrique des classes d'intrication pour les systèmes à 3-qubits à été proposée par Levay dans [183].

Les états séparables correspondent, comme précédemment, aux tenseurs de la variété de Segre, donc aux tenseurs de rang 1, et sont des tenseurs dégénérés.

Les états bi-séparables correspondent aux systèmes quantiques qui peuvent se décomposer sur la forme de deux sous-systèmes indépendants : le premier sous-système est composé d'une particule, et le second est composé de deux particules intriquées. Ces tenseurs s'écrivent donc sous la forme du produit tensoriel d'un qubit et d'un état équivalent à un état EPR. Le rang de ces tenseurs est égal à 2, et ces derniers sont

Orbite	Formes normales	Classe	Rang	Δ_{222} de Cayley
$\mathcal{O}_6$	$\|000\rangle + \|111\rangle$	GHZ	2	$\neq 0$
$\mathcal{O}_5$	$\|001\rangle + \|010\rangle + \|100\rangle$	W	3	0
$\mathcal{O}_4$	$\|001\rangle + \|111\rangle$	Bi-Séparable C-AB	2	0
$\mathcal{O}_3$	$\|100\rangle + \|111\rangle$	Bi-Séparable A-BC	2	0
$\mathcal{O}_2$	$\|010\rangle + \|111\rangle$	Bi-Séparable B-CA	2	0
$\mathcal{O}_1$	$\|000\rangle$	Séparable	1	0

Table 2.1 – Classification de l'intrication sous SLOCC pour les systèmes à 3 qubits [135, 147].

considérés comme des états dégénérés, car annulant l'hyperdéterminant de Cayley Δ_{222} (définissant la variété duale pour les 3-qubits).

L'état $|W\rangle$ s'écrit comme la somme des états de base dont l'écriture binaire à une distance de Hamming avec l'écriture binaire de l'état $|000\rangle$ égale à 1. C'est un tenseur de rang 3, mais de rang de bord égal à 2 (voir Exemple 3) qui appartient géométriquement à la variété des tangentes [135], et est aussi un tenseur dégénéré.

Remarque 21. Comme évoqué précédemment, les variétés des tangentes sont des variétés auxiliaires intervenant notamment dans le problème de classification de l'intrication sous le groupe SLOCC, permettant une stratification de l'espace ambiant en termes de classes d'équivalences sous l'action du groupe SLOCC. En particulier, l'état $|W\rangle$ des 3-qubits appartient à la variété des tangentes $\tau\big(\mathrm{Seg}(\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1)\big)$, mais pas à la variété des sécantes $\sigma_2\big(\mathrm{Seg}(\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1)\big)=\mathbb{P}^7$ [135].

L'état $|GHZ\rangle$ est quant à lui le seul type d'intrication représenté par des tenseurs ne figurant pas sur la variété duale à la variété de Segre, et par conséquent n'annule pas l'hyperdéterminant de Cayley. Les états de type $|GHZ\rangle$ sont des tenseurs de rang 2, car ils sont les tenseurs génériques de la variété des sécantes $\sigma_2(X)$.

Du point de vue des variétés des sécantes, la première sécante remplit déjà tout l'espace, c'est à dire que $\sigma_2\big(\mathrm{Seg}(\mathbb{P}^1\times\mathbb{P}^1\times\mathbb{P}^1)\big)=\mathbb{P}^7=\mathbb{P}(\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2)$, et ses états généraux correspondent aux états de type $|GHZ\rangle$. Les sous-variétés incluses dans cette variété modélisent des états d'un type d'intrication différent, comme l'état $|W\rangle$ ou l'état bi-séparable, ce dernier pouvant être vu comme un état de la variété associée au produit $\mathbb{P}^1\times\sigma_2(\mathrm{Seg}(\mathbb{P}^1\times\mathbb{P}^1))$ [135].

Cas des 4-qubits

L'espace de Hilbert $\mathcal{H}_4=\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ pour les 4-qubits est connu pour contenir un nombre infini d'orbites sous l'action du groupe $G_{SLOCC}=\mathrm{GL}_2(\mathbb{C})\times\mathrm{GL}_2(\mathbb{C})\times\mathrm{GL}_2(\mathbb{C})\times\mathrm{GL}_2(\mathbb{C})$.

Néanmoins, en 2002, Verstraete et al. [262] propose une liste de neuf formes normales, définies par des paramètres, permettant de paramétriser toutes les orbites sous l'action du groupe SLOCC (en intégrant les permutations de qubits). Cette liste de

familles a par la suite été corrigée est republiée en 2006 par Chterental et Djokovic [72]. Nous utiliserons cette dernière tout au long de ce manuscrit afin de désigner les familles d'intrication correspondantes (voir Table 2.2).

$$G_{abcd} = \tfrac{a+d}{2}\big(|0000\rangle + |1111\rangle\big) + \tfrac{a-d}{2}\big(|0011\rangle + |1100\rangle\big) + \tfrac{b+c}{2}\big(|0101\rangle + |1010\rangle\big) + \tfrac{b-c}{2}\big(|0110\rangle + |1001\rangle\big)$$

$$L_{abc_2} = \tfrac{a+b}{2}\big(|0000\rangle + |1111\rangle\big) + \tfrac{a-b}{2}\big(|0011\rangle + |1100\rangle\big) + c\big(|0101\rangle + |1010\rangle\big) + |0110\rangle$$

$$L_{a_2b_2} = a\big(|0000\rangle + |1111\rangle\big) + b\big(|0101\rangle + |1010\rangle\big) + |0011\rangle + |0110\rangle$$

$$L_{ab_3} = a\big(|0000\rangle + |1111\rangle\big) + \tfrac{a+b}{2}\big(|0101\rangle + |1010\rangle\big) + \tfrac{a-b}{2}\big(|0110\rangle + |1001\rangle\big) + \tfrac{i}{\sqrt{2}}\big(|0001\rangle + |0010\rangle - |0111\rangle - |1011\rangle\big)$$

$$L_{a_4} = a\big(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\big) + i|0001\rangle + |0110\rangle - i|1011\rangle$$

$$L_{a_2 0_{3\oplus\overline{1}}} = a\big(|0000\rangle + |1111\rangle\big) + |0011\rangle + |0101\rangle + |0110\rangle$$

$$L_{0_{5\oplus\overline{3}}} = |0000\rangle + |0101\rangle + |1000\rangle + |1110\rangle$$

$$L_{0_{7\oplus\overline{1}}} = |0000\rangle + |1011\rangle + |1101\rangle + |1110\rangle$$

$$L_{0_{3\oplus\overline{1}}0_{3\oplus\overline{1}}} = |0000\rangle + |0111\rangle$$

TABLE 2.2 – Les 9 familles (corrigées) de Verstaete *et al.*

Nous définissons également un sous-ensemble de $\mathcal{H}_4$, appelé le cône nilpotent, défini comme l'ensemble des états annulant tous les polynômes invariants. En pratique, on définit la projectivisation $\mathcal{N}$ du cône nilpotent comme étant l'ensemble

$$\mathcal{N} = \{|\Psi\rangle \in \mathbb{P}(\mathcal{H}) \;/\; H(|\Psi\rangle) = L(|\Psi\rangle) = M(|\Psi\rangle) = D_{xy}(|\Psi\rangle) = 0\}\ . \tag{2.33}$$

Nous renvoyons le lecteur vers la Section 6.2.2 pour la définition d'un invariant et d'un covariant, et vers l'Annexe A.4 pour l'expression de ces invariants.

Le cône nilpotent renferme 31 orbites sous l'action du groupe SLOCC. Si on autorise l'action par permutation des 4-qubits (par le groupe symétrique $\mathcal{S}_4$), ces 31 orbites peuvent être réduites à 8 strates d'orbites non équivalentes notées $Gr_1, Gr_2, \ldots, Gr_8$, formant une chaîne d'inclusion (la fermeture des orbites de la strate Gr_{i+1} contient les orbites de Gr_i). En particulier, la strate Gr_1 ne contient qu'une seule orbite : celle des états séparables.

Pour permettre la distinction entre les différentes strates du cône nilpotent, un ensemble de polynômes définis comme somme ou produits de covariants peut être utilisé :

$$P_B = B_{2200} + B_{2020} + B_{2002} + B_{0220} + B_{0202} + B_{0022}, \tag{2.34}$$

$$P_C^1 = C_{3111} + C_{1311} + C_{1131} + C_{1113}, \tag{2.35}$$

$$P_C^2 = C_{3111} \cdot C_{1311} \cdot C_{1131} \cdot C_{1113}, \tag{2.36}$$

$$P_D^1 = D_{4000} + D_{0400} + D_{0040} + D_{0004}, \tag{2.37}$$

$$P_D^2 = D_{2200} + D_{2020} + D_{2002} + D_{0220} + D_{0202} + D_{0022}, \tag{2.38}$$

$$P_F = F_{2220}^1 + F_{2202}^1 + F_{2022}^1 + F_{0222}^1, \tag{2.39}$$

$$P_L = L_{6000} + L_{0600} + L_{0060} + L_{0006}\ . \tag{2.40}$$

On peut en effet déterminer à quelle strate appartient un état donné en évaluant le vecteur V défini dans l'Équation 2.41. Lorsque la valeur du polynôme est non nulle, on la remplace par la valeur 1 dans le vecteur d'évaluation. Ainsi, les éléments du vecteur V ne prendront que des valeurs binaires.

$$V = [A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F, P_L]\ . \tag{2.41}$$

À partir de la valeur de ce vecteur évaluation, on peut distinguer les différentes strates du cône nilpotent, ceci étant représenté dans la Table 2.3.

Strate	Forme normale	Vecteur V
Gr_8	$\|0001\rangle + \|0010\rangle + \|0100\rangle + \|1000\rangle + \|1100\rangle + \|1010\rangle + \|0110\rangle$	$[1,1,1,1,1,1,1,1]$
Gr_7	$\|0100\rangle + \|0001\rangle + \|1100\rangle + \|1010\rangle$	$[1,1,1,1,1,1,1,0]$
Gr_6	$\|0000\rangle + \|1000\rangle + \|0100\rangle + \|0010\rangle + \|0001\rangle + \|1001\rangle$	$[1,1,1,1,1,1,0,0]$
Gr_5	$\|0001\rangle + \|0010\rangle + \|0100\rangle + \|1000\rangle$	$[1,1,1,1,0,0,0,0]$
Gr_4	$\|0000\rangle + \|1110\rangle$	$[1,1,1,0,1,0,0,0]$
Gr_3	$\|0011\rangle + \|1001\rangle + \|1010\rangle$	$[1,1,1,0,0,0,0,0]$
Gr_2	$\|0000\rangle + \|0011\rangle$	$[1,1,0,0,0,0,0,0]$
Gr_1	$\|000\rangle$	$[1,0,0,0,0,0,0,0]$

Table 2.3 – Formes normales des strates du cône nilpotent pour les 4-qubits, et vecteurs d'évaluation des covariants correspondants [136].

En 2014 et 2017, Holweck *et al.* proposèrent un algorithme, basé sur le calcul de polynômes invariants sous l'action du groupe SLOCC, permettant de déterminer, pour un système à 4-qubits donné, la famille de Verstraete et al. correspondante, ainsi que la strate du cône nilpotent (dans le cas où l'état annule tous les invariants fondamentaux) [137, 138]. Ces algorithmes sont détaillés en Annexe A.4, et permettront notamment de mettre en évidence les familles d'intrication apparaissant au cours d'algorithmes quantiques dans les Chapitres 3 et 4. Ces algorithmes ont également récemment été utilisés pour étudier l'intrication des états à 4-qubits apparaissant dans des circuits quantiques composés de portes $c-Z$ et $SWAP$ [22].

2.2.3 Mesure de l'intrication

Une mesure de l'intrication a pour objectif de quantifier le taux d'intrication présent dans un système quantique. Pour être considérée comme une mesure de l'intrication, une mesure doit répondre à un certain nombre de critères du point de vue mathématique [260]. Une mesure de l'intrication :

- est une fonction à valeur dans $\mathbb{R}^+$,
- est invariante sous l'action d'opérations locales unitaires,
- n'augmente pas sous l'action du groupe G_{LOCC},
- est nulle pour les états séparables.

Une mesure de l'intrication qui diminue sous l'action du groupe G_{LOCC} est appelée *Entanglement Monotone*. On définit aussi la notion de *Entanglement Witness* (témoin d'intrication), qui n'est pas équivalente aux deux concepts précédents, et qui a pour but de pouvoir détecter l'intrication dans un système quantique.

On se propose à présent d'introduire les principales mesures de l'intrication utilisées dans le cadre de ce travail.

Mesure géométrique de l'intrication (MGI)

Une des mesures de l'intrication est celle connue sur le nom de *Geometric Measure of Entanglement* (GME). Introduite par [53] et [271], elle consiste à mesurer **la distance minimale** entre un état donné $|\psi\rangle \in \mathcal{H}_n$ et l'ensemble des états séparables. En pratique, cela revient à chercher l'état séparable $|\Phi\rangle$ (pas nécessairement unique) maximisant la quantité $|\langle\Phi|\psi\rangle|$. Cette mesure est directement adaptée à l'étude de l'intrication pour les systèmes à plusieurs particules. On définit alors la mesure géométrique de l'intrication E_g comme suit :

$$E_g(|\psi\rangle) = \min_{|\Phi\rangle\in S_n} -\log_2 |\langle\Phi|\psi\rangle|^2 = -\log_2 \max_{|\Phi\rangle\in S_n} |\langle\Phi|\psi\rangle|^2 \ , \tag{2.42}$$

avec S_n l'ensemble des états séparables pour les systèmes à n-qubits. Il existe, en outre, d'autres manières de définir la GME dans la littérature. La mesure groverienne de l'intrication, inspirée par l'algorithme de Grover (voir Section 1.2.1) et introduite par Biham *et al.* [38], notée E_G se définit comme suit pour un état $|\psi\rangle$ à n-qubits :

$$E_G(|\psi\rangle) = 1 - \max_{|\Phi\rangle\in S_n} |\langle\Phi|\psi\rangle|^2 \ . \tag{2.43}$$

On remarque que si $|\psi\rangle$ appartient à la variété des états séparables, la quantité $\max_{|\Phi\rangle\in S_n} |\langle\Phi|\psi\rangle|$ sera toujours égale à 1, et par conséquent $E_g(|\psi\rangle) = E_G(|\psi\rangle) = 0$.

L'implémentation de la MGI peut être vue comme un problème d'optimisation, dans la mesure où l'on recherche une approximation de l'état séparable le plus proche (ou le plus éloigné selon la définition adoptée) de l'état intriqué à mesurer. Teng propose une méthode efficace pour le calcul de la MGI en utilisant des méthodes de décompositions de tenseurs [255]. Dans le cas spécifique des tenseurs symétriques, Hübener *et al.* ont démontré que l'état séparable le plus proche de tout état symétrique multipartite est nécessairement lui même un état symétrique [142].

Polynômes de Mermin

L'inégalité de Bell a historiquement été mise en place pour remettre en question les différentes théories à variables cachées [28]. Plus précisément, l'inégalité de Bell permit de mettre en évidence les aspects stochastiques et probabilistes des corrélations lors de la mesure, prédites par la mécanique quantique, et non explicables dans le contexte d'un réalisme local comme celui proposé par Einstein, Podolski et Rosen [94]. De plus, ces inégalités se présentent comme de potentiels détecteurs d'intrication, comme l'est l'inégalité de Bell pour les états à 2-qubits [110]. La violation de ces inégalités révèle alors une présence de non-localité dans le système étudié, ce qui implique la présence d'intrication quantique.

Certains états sont donc amenés à violer ces inégalités associées à un protocole expérimental, réalisé concrètement pour la première fois par Aspect [14], et il peut alors être intéressant de pouvoir généraliser ces inégalités à des systèmes à n-qubits pour pouvoir en étudier l'intrication. Les polynômes mis en place par Mermin [188], permettent de définir des inégalités de type Bell, permettant d'étudier les corrélations entre un nombre arbitraire n de particules.

Comme cela est le cas dans la définition du protocole expérimental associé à la réalisation de l'inégalité de Bell, on définit deux dispositifs de mesure pour chaque particule du système quantique considéré. Ces derniers seront modélisés par des observables (voir Section 1.1.4), et on définira alors n couples d'observables notés A_i et ${A_i}'$, modélisant les deux bases de mesure pour chaque qubit. On rappelle ici que ces observables peuvent s'exprimer comme une combinaison linéaire normalisée des portes de Pauli, comme suit :

$$A_i = a_{i,X}X + a_{i,Y}Y + a_{i,Z}Z, \text{ avec } {a_{i,X}}^2 + {a_{i,Y}}^2 + {a_{i,Z}}^2 = 1 \ , \tag{2.44}$$

$${A_i}' = a'_{i,X}X + a'_{i,Y}Y + a'_{i,Z}Z, \text{ avec } (a'_{i,X})^2 + (a'_{i,Y})^2 + (a'_{i,Z})^2 = 1 \ . \tag{2.45}$$

Le polynôme de Mermin, noté M_n, peut en effet être défini de manière récursive [273], comme suit :

$$\begin{cases} M_1 = A_1, \\ M_n = \frac{1}{2}\Big(M_{n-1} \otimes (A_n + {A_n}') + {M_{n-1}}' \otimes (A_n - {A_n}')\Big) \end{cases} , \tag{2.46}$$

avec ${M_i}'$ s'exprimant comme l'observable M_i mais en remplaçant les observables avec apostrophe par des observables sans, et vice versa, ce qui nous donne :

$$\begin{cases} {M_1}' = {A_1}', \\ {M_n}' = \frac{1}{2}\Big({M_{n-1}}' \otimes ({A_n}' + A_n) + M_{n-1} \otimes ({A_n}' - A_n)\Big) \end{cases} . \tag{2.47}$$

Par ailleurs, il également possible de généraliser ces polynômes de Mermin à des systèmes quantiques dont les particules possèdent plus de deux états de base, comme cela est le cas pour les systèmes à plusieurs qutrits par exemple [6].

À titre d'exemple, nous nous proposons d'étudier les polynômes de Mermin dans le cas de systèmes 2-qubits. Dans le cas où $n = 2$, avec $|\psi\rangle \in \mathcal{H}_2$ nous obtenons alors le polynôme

$$M_2 = \frac{1}{2}\Big(M_1 \otimes (A_2 + A_2{}') + M_1{}' \otimes (A_2 - A_2{}') \Big) \ , \tag{2.48}$$

$$M_2 = \frac{1}{2}\Big(A_1 A_2 + A_1 A_2{}' + A_1{}' A_2 - A_1{}' A_2{}' \Big) \ , \tag{2.49}$$

qui correspond, à un facteur près, à l'opérateur de l'inégalité de CHSH utilisée pour prouver le théorème de Bell [74]. On notera l'évaluation de la valeur absolue de la valeur moyenne des résultats de la mesure par l'observable M_2, pour un état fixé $|\psi\rangle$, par :

$$\langle M_2 \rangle = |\langle \psi | M_2 | \psi \rangle| \ . \tag{2.50}$$

Le polynôme M_2 est alors paramétré par les observables $A_1, A_1{}', A_2, A_2{}'$. De manière générale, le polynôme de Mermin M_n est uniquement déterminé par les familles d'observables $\{A_i, A_i{}'\}_i$, eux même paramétrés par les différents coefficients $\{\ldots, a_{i,X}, a_{i,Y}, a_{i,Z}, \ldots\}$.

Si l'on cherche à évaluer le polynôme de Mermin pour l'état intriqué à 2-qubits $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, alors on obtient le polynôme C_{EPR} suivant :

$$\begin{aligned} C_{EPR} = a_{1,X}a_{2,X} - a_{1,Y}a_{2,Y} + a_{1,Z}a_{2,Z} \\ + a_{1,X}a'_{2,X} - a_{1,Y}a'_{2,Y} + a_{1,Z}a'_{2,Z} \\ + a'_{1,X}a_{2,X} - a'_{1,Y}a_{2,Y} + a'_{1,Z}a_{2,Z} \\ + a'_{1,X}a'_{2,X} - a'_{1,Y}a'_{2,Y} + a'_{1,Z}a'_{2,Z} \ . \end{aligned} \tag{2.51}$$

Chercher à maximiser la valeur absolue du polynôme $|C_{EPR}|$, c'est chercher à déterminer le jeu d'observables permettant une violation maximale des inégalités et donc une présence confirmée de l'intrication, et cela revient à trouver la valeur des coefficients maximisant cette quantité. On démontre qu'une solution possible, permettant d'atteindre la valeur maximale $|C_{EPR}| = \sqrt{2}$, est décrite par les paramètres suivants :

$$\begin{aligned} (a_{1,X}, a_{1,Y}, a_{1,Z}) &= (0, 0, 1), \\ (a'_{1,X}, a'_{1,Y}, a'_{1,Z}) &= (1, 0, 0), \\ (a_{2,X}, a_{2,Y}, a_{2,Z}) &= (\tfrac{1}{\sqrt{2}}, 0, \tfrac{1}{\sqrt{2}}), \\ (a'_{2,X}, a'_{2,Y}, a'_{2,Z}) &= (\tfrac{-1}{\sqrt{2}}, 0, \tfrac{1}{\sqrt{2}}), \end{aligned} \tag{2.52}$$

ce qui revient à choisir les observables comme étant égaux à

$$A_1 = Z, \ A_1{}' = X, \ A_2 = \frac{Z+X}{\sqrt{2}}, \ A_2{}' = \frac{Z-X}{\sqrt{2}} \ . \tag{2.53}$$

Sous les hypothèses du réalisme local, comme proposé en 1935 par Einstein *et al.* [94], en proposant de manière déterministe une valeur dans $\{-1, 1\}$ comme résultat de mesure associé à chaque observable, on démontre que la valeur associée au polynôme de Mermin est bornée par 1, et on notera $\langle M_n \rangle^{RL} \leq 1$ [76].

En revanche, du point de vue de la mécanique quantique, certains états intriqués, ne connaissant pas d'équivalents classiques, permettent d'atteindre des valeurs supérieures à 1, et donc de violer l'inégalité précédente. D'autre part, il a été

démontré que la valeur maximale possible dans l'évaluation du polynôme de Mermin est de $2^{\frac{n-1}{2}}$, avec n le nombre de qubits, et est atteinte pour tous les états $|GHZ_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right)$ généralisant l'état de Greenberger-Horne-Zeilinger pour les 3-qubits [76, 66]. On modélisera alors cette limite par l'inéquation $\langle M_n\rangle^{MQ} \leq 2^{\frac{n-1}{2}}$.

En revanche, si un état ne viole pas une inégalité, cela n'implique pas forcément une absence d'intrication. Dès lors, une manière d'utiliser les polynômes de Mermin est d'évaluer ces polynômes, pour diverses configurations d'observables, et de comparer la valeur obtenue, lors de l'évaluation du polynôme, à la limite classique (qui est fixée à 1, quelque soit le nombre de qubits n). Les polynômes permettraient donc d'apprécier (ou non) un degré de violation pour des états quantiques fixés. De plus, il pourra aussi être intéressant de rechercher quel peut être le jeu d'observable permettant de maximiser cette valeur absolue du polynôme, et donc d'en déduire la violation maximale possible pour un état, et cette fois ci de la comparer à la limite maximale de $2^{\frac{n-1}{2}}$.

Cette quantité maximale peut en fait aussi être utilisée pour détecter la présence d'intrication en observant une violation de l'inégalité classique, mais aussi pour caractériser certaines classes d'intrication sous l'équivalence LU. En effet, il a été démontré [81] que cette quantité maximale est invariante sous l'action du groupe LU. Cette propriété est celle exprimée dans la proposition suivante :

Proposition 2.2.1. *Soit $|\psi\rangle \in \mathcal{H}_n$ un état à n-qubits, et $\{A_i, A_i'\}_i$ les familles d'observables sur un qubit définissant le polynôme de Mermin M_n, comme décrit dans l'Équation 2.46. On définit alors la quantité $\mu(|\psi\rangle)$ comme étant :*

$$\mu(|\psi\rangle) = \max_{\{A_i, A_i'\}_i} |\langle\psi|M_n|\psi\rangle| \ . \tag{2.54}$$

Si les états $|\psi_1\rangle$ et $|\psi_2\rangle$ sont LU-équivalents, alors nous avons $\mu(|\psi_1\rangle) = \mu(|\psi_2\rangle)$. La fonction μ est donc invariante par transformation LU.

Démonstration. Soit $|\psi\rangle \in \mathcal{H}_n$ un état à n-qubits. Nous rappelons qu'un observable A sur un qubit, aux valeurs propres $\{-1, 1\}$ peut toujours être exprimé comme $A = a_X X + a_Y Y + a_Z Z$, avec $a_X, a_Y, a_Z \in \mathbb{R}$ et ${a_X}^2 + {a_Y}^2 + {a_Z}^2 = 1$. Pour l'action $g.A = g^\dagger A g$ sur A, par conjuguaison, avec $g \in U_2(\mathbb{C})$ une matrice unitaire, nous avons $g.A = \tilde{A} = \tilde{a_X} X + \tilde{a_Y} Y + \tilde{a_Z} Z$, avec $\tilde{a_X}, \tilde{a_Y}, \tilde{a_Z} \in \mathbb{R}$ et ${\tilde{a_X}}^2 + {\tilde{a_Y}}^2 + {\tilde{a_Z}}^2 = 1$. De ce fait, $\tilde{A}$ est aussi un observable sur un qubit, avec un spectre égal à $\{-1, 1\}$.

Soit $V = (a_{1,X}, a_{1,Y}, a_{1,Z}, \tilde{a_{1,X}}, \tilde{a_{1,Y}}, \tilde{a_{1,Z}}, \ldots, \tilde{a_{n,X}}, \tilde{a_{n,Y}}, \tilde{a_{n,Z}})$ un tuple de $6n$ paramètres définissant un polynôme de Mermin $M_n(V)$. Alors la quantité

$$\mu(|\psi\rangle) = \max_{V \in \mathbb{R}^{6n}, {a_{i,X}}^2 + {a_{i,Y}}^2 + {a_{i,Z}}^2 = 1, {\tilde{a_{i,X}}}^2 + {\tilde{a_{i,Y}}}^2 + {\tilde{a_{i,Z}}}^2 = 1} |\langle\psi|M_n(V)|\psi\rangle| \ , \tag{2.55}$$

existe, car c'est le maximum d'un polynôme de degré n à $6n$ variables (au plus), sous les contraintes de normalisation ${a_{i,X}}^2 + {a_{i,Y}}^2 + {a_{i,Z}}^2 = 1$ et ${\tilde{a_{i,X}}}^2 + {\tilde{a_{i,Y}}}^2 + {\tilde{a_{i,Z}}}^2 = 1$. Notons V' un tuple de paramètres maximisant le module de $\langle\psi|M_n(V)|\psi\rangle$, c'est à dire :

$$\mu(|\psi\rangle) = |\langle\psi|M_n(V')|\psi\rangle| \ . \tag{2.56}$$

Soit un état $|\varphi\rangle$ à n-qubits LU-équivalent à $|\psi\rangle$. Alors il existe $g = (g_1, \ldots, g_n) \in LU$, tel que $|\varphi\rangle = G|\psi\rangle$ avec $G = g_1 \otimes \cdots \otimes g_n$. Alors nous avons

$$\langle\psi|M_n(V')|\psi\rangle = \left(\langle\psi|G^\dagger\right) GM_n(V')G^\dagger\left(G|\psi\rangle\right) = \langle\varphi|M_n(V'')|\varphi\rangle \ , \tag{2.57}$$

pour un certain tuple de paramètres V''. Nous pouvons alors en déduire que

$$\mu(|\psi\rangle) \leq \mu(|\varphi\rangle) \ . \tag{2.58}$$

De plus, on peut remarquer que $|\psi\rangle = G^\dagger|\varphi\rangle$ est aussi vrai. Par un raisonnement similaire, on en déduit que $\mu(|\psi\rangle) \geq \mu(|\varphi\rangle)$, et on peut alors en conclure que $\mu(|\psi\rangle) = \mu(|\varphi\rangle)$.

□

De ce fait, il apparaît naturel de l'utiliser pour caractériser certaines classes d'intrication sous l'action du groupe LU, mais également comme mesure ou détecteur de violation et d'intrication [3, 7]. L'implémentation de cette mesure de violation implique l'implémentation de méthodes d'optimisation, et ceci est discuté indépendamment en Annexe A.8. Cette mesure sera notamment utilisée en Partie II pour étudier l'évolution de la violation de ces inégalités au cours d'algorithmes quantiques.

Invariants polynomiaux et algébriques

Certains polynômes et invariants, dont l'interprétation géométrique est parfois liée à la notion d'intrication, sont aussi mentionnés dans la littérature comme pouvant constituer des mesures de l'intrication lorsqu'ils sont évalués sur des états quantiques [5]. Cet aspect sera abordé notamment tout au long des prochains chapitres.

Un invariant est un polynôme donc l'évaluation reste inchangée sous une transformation (ou sous l'action d'un groupe) donnée. Dans notre cas, nous nous intéressons aux invariants sous l'action du groupe SLOCC. Parmi ces invariants nous pouvons citer l'hyperdéterminant, les invariants fondamentaux, le discriminant (pour les états symétriques) et l'hyperpfaffien (pour les états fermioniques). Ces polynômes s'annulent lorsqu'ils sont évalués sur des états séparables, et peuvent à la fois servir à mesurer l'intrication d'un point de vue quantitatif et qualitatif.

Enfin, nous pouvons également citer la notion de rang de tenseur comme une mesure algébrique de l'intrication, notion que nous exploitons tout au long de nos travaux.

Autres mesures

Pour les états bipartites, c'est à dire appartenant à un espace de Hilbert défini comme le produit tensoriel deux espaces de Hilbert, la décomposition de Schmidt peut être utilisée pour déterminer si l'état formé de ces deux parties est séparable ou non [216, 30]. Ce critère est d'ailleurs aussi applicable aux états mixtes (voir *PPT criterion* aussi [247, 64, 232, 30]). Une généralisation de cette décomposition peut aussi amener à quantifier le degré d'intrication [95].

La notion d'entropie, introduite notamment en théorie de l'information par Shannon [240], est également présente dans le domaine de l'information quantique et est

également liée à la notion d'intrication quantique [46, 141]. Différentes définitions existent lorsqu'elle est liée à un état quantique à plusieurs particules [31, 119]. Nous pouvons citer les plus connues dans la littérature : l'entropie de Von Neumann[4] [198], l'entropie de Rényi[5] [225], l'entropie de Tsallis[6] [259], etc.

Bien d'autres chercheurs et scientifiques se sont intéressés à la proposition et à la mise en place d'autres mesures de l'intrication, que ce soit pour des états purs ou mixtes. Nous pouvons citer ici une partie de ces travaux à titre informatif [285, 265, 214, 71, 258, 68, 104, 178, 30]

4. John von Neumann (1903 – 1957) est un mathématicien et physicien américano-hongrois. Il est connu pour ses contributions en mécanique quantique, en analyse fonctionnelle, en théorie des ensembles, en informatique, en sciences économiques et dans d'autres domaines des mathématiques et de la physique.

5. Alfréd Rényi (1921 – 1970) est un mathématicien hongrois, ayant apporté des contributions dans les domaines de la combinatoire, de la théorie des graphes et de la théorie des probabilités.

6. Constantino Tsallis (né en 1943) est un physicien grec naturalisé brésilien. Il est connu pour ses travaux en physique théorique et en statistiques.

Deuxième partie

L'Intrication Quantique dans les Algorithmes Quantiques

La discipline du calcul quantique, et les algorithmes associés, est de plus en plus considérée comme plus puissante et performante que son équivalent classique. Les travaux de Feyman [99] constituent un argument pionnier et de taille, mettant en avant le fait que la simulation de l'évolution d'un phénomène quantique général nécessite des ressources de calcul classique exponentiellement plus importantes que les ressources physiques nécessaires pour l'implémentation physique du phénomène ou processus quantique en lui même [154].

S'intéresser aux avantages, en termes de rapidité et de puissance de calcul, fournis par les algorithmes ou processus de calculs quantiques en comparaison avec l'informatique classique, c'est aussi caractériser et s'intéresser aux phénomènes non-classiques et à la nouvelle philosophie du calcul intervenant dans les algorithmes quantiques proposés dans la littérature. Parmi ces phénomènes, pressentis pour expliquer les gains en temps et ressources de calcul pour certains algorithmes quantiques, figure le phénomène d'intrication quantique.

Dans cette partie, nous nous focaliserons sur l'étude des deux algorithmes quantiques introduits au premier chapitre (voir Section 1.2), plus précisément celui de Grover et de Shor. Nous illustrerons notre étude par l'application concrète de ces algorithmes pour des cas précis de systèmes quantiques, parmi lesquels figurera le cas des 4-qubits. C'est dans cette mesure que nous introduisons tout d'abord les algorithmes et outils utilisés pour déterminer le type d'intrication (ou de famille associée) pour un état à 4-qubits donné. Nous nous intéressons ensuite à l'algorithme de Grover et étudions l'intrication des états générés par l'algorithme, en fonction de la taille du système et du nombre d'éléments marqués notamment. Nous clôturons cette partie par l'étude de l'intrication dans l'algorithme de Shor, notamment l'influence de la Transformée de Fourier Quantique sur l'intrication de registres quantiques ou d'états périodiques. Les études de ce chapitre sont à la fois axées sur un aspect quantitatif et qualitatif de l'intrication, et ce pour les deux algorithmes, en utilisant des outils originaux permettant de mettre en perspective les précédents résultats et travaux sur la question.

Chapitre 3

Algorithme de Grover et Intrication

"Search the whole world until you meet yourself", Marjory Sheba.

Dans ce chapitre, nous nous intéresserons à l'intrication dans l'algorithme de Grover. Le principe de l'algorithme et les notations adoptées ont été introduits en Section 1.2.1. Dans un premier temps, nous présenterons un état de l'art des études menées en ce qui concerne l'implication de l'intrication quantique dans l'algorithme de recherche de Grover. Dans un second temps, nous présenterons notre étude, d'un point de vue théorique et qualitatif, de l'intrication dans l'algorithme de Grover, en étudiant un certain nombre de cas où les types d'intrication générés par l'algorithme seront explicitement précisés. Nous proposerons enfin d'étudier l'évolution de l'intrication au cours de l'algorithme en utilisant des mesures numériques de l'intrication. Enfin, nous concluons cette section par une brève synthèse et discussion des résultats obtenus.

Nous présentons principalement dans ce chapitre nos travaux issus des articles [133, 147, 81]. Dans ces trois articles, nous avons étudié par avec co-auteurs la question de l'intrication dans l'algorithme de Grover. Dans le premier article [133], nous nous intéressons à la nature de l'intrication des états générés par l'algorithme de Grover en utilisant des outils provenant de la géométrie algébrique. Nous établissions un lien entre l'intrication des éléments générés par l'algorithme de Grover et certaines variétés algébriques auxiliaires construites à partir de la variété des états séparables. Une interprétation qualitative et géométrique des précédents travaux, comme ceux de Rossi *et al.* [226, 227], a pu être proposée. Certains cas ont été étudiés en détail comme celui des 3-qubits. Dans un second article [147], et dans le même esprit que notre précédent travail, nous étudions le cas des 4-qubits, en détaillant quels types d'intrication peuvent être générés à l'aide de l'algorithme de Grover, en fonction des éléments marqués. Dans un récent travail [81], nous nous sommes également intéressés à quantifier l'intrication au cours de l'algorithme de Grover en utilisant des mesures et détecteurs de l'intrication très peu investis précédemment dans la littérature, tout en reliant les résultats numériques obtenus aux résultats théoriques précédemment établis. Nous nous proposons de présenter conjointement ces travaux et de discuter les précédents travaux sur la question à la lumière de nos résultats.

3.1 État de l'art

L'algorithme de Grover est un des algorithmes quantiques les plus célèbres dans la littérature, notamment car il propose de meilleures performances, pour la recherche d'éléments dans une base de données, que ce qui est proposé en informatique classique. Bien que sa présence soit liée à l'implémentation de l'algorithme (en termes de choix de dimensions des systèmes quantiques), il a été prouvé que l'intrication quantique intervient tout au long des états de l'algorithme (dans sa version présentée en Chapitre 1). Néanmoins, son rôle et sa nature ne sont pas encore totalement cernés. Braunstein et Pati furent les premiers à démontrer la présence et la nécessité de l'intrication dans l'algorithme de Grover [45].

En 2002, Biham, Nielsen et Osborne [38] introduisent une mesure de l'intrication, plus précisément une *entanglement monotone*, dérivée de l'algorithme de Grover. À partir d'un état pur en entrée de l'algorithme, les auteurs étudient la maximisation P_{max} de la probabilité de succès de l'algorithme, et ce, sous l'action d'opérations locales unitaires. Les auteurs définissent alors ce que l'on appelle la Mesure Groverienne de l'Intrication (voir Section 2.2.3).

La même année, Forcer *et al.* [102] s'intéressent aux rôles de la superposition et de l'intrication quantique dans les calculs quantiques. Leur analyse est illustrée par une discussion autour d'une implémentation classique de l'algorithme de Grover. L'absence d'intrication multipartite implique une croissance exponentielle des ressources nécessaires à l'implémentation de tels algorithmes quantiques. Les auteurs concluent que l'intrication multipartite est la propriété clé des systèmes quantiques, fournissant une puissance remarquable aux ordinateurs quantiques.

Biham, Shapira and Shimoni ont analysé, en 2003, la dynamique de l'algorithme de Grover tout en initialisant l'algorithme avec un état pur $|\Psi\rangle$ arbitraire, au lieu de l'état de base $|0\ldots0\rangle$ [39]. Les auteurs ont montré que le meilleur moment pour effectuer la mesure est le même, pour les deux choix d'états initiaux, dans le cas où le nombre d'éléments marqués est le même. Biham *et al.* généralisent la Mesure Groverienne de l'Intrication à plusieurs éléments marqués. Selon les auteurs, tant que $|\mathcal{S}| << N$ (avec N la taille de la base de données) alors la mesure groverienne est indépendante du nombre d'éléments marqués $|\mathcal{S}|$.

En 2004, Orus et Latorre ont étudié le comportement de l'intrication lorsque la dimension du système augmente, dans une version adiabatique de l'algorithme de Grover [207], en précisant que l'entropie de Von Neumann reste une quantité bornée, et ce, indépendamment de la taille du système, et même au "point critique". Plus précisement, les auteurs stipulent que le maximum de l'entropie approche la valeur 1 à une vitesse proportionnelle à la racine carrée de la taille du système, ce qui est le facteur d'agrandissement typique de l'algorithme de Grover.

En 2005, Fang *et al.* [98] se sont attardés sur l'étude du degré d'intrication présent dans un registre à plusieurs qubits durant l'exécution de l'algorithme, sous le formalisme des matrices de densité. Les auteurs ont analysé les variations de la concurrence et de

l'entropie de Von Neumann pour les matrices de densité réduites à un ou deux qubits d'un registre à n-qubits. Cette analyse a été faite en fonction du nombre d'itérations et du nombre d'éléments marqués. Le calcul de la concurrence a montré que cette mesure peut être mise en relation avec la probabilité de succès de l'algorithme. De plus, Fang et ses collaborateurs ont observé que la concurrence atteint une valeur maximale approximativement à la moitié du nombre optimal d'itérations.

En 2008, Iwai *et al.* [146] ont publié un article portant sur la mesure de l'intrication du point de vue de la bipartition d'un système à n-qubits, mesure précédemment définie et étudiée du point de vue de la géométrie de Riemann dans un travail du premier auteur [145]. Ce dernier travail permit d'établir la distance séparant les états maximalement intriqués des états séparables. Dans le travail [146], les auteurs déterminent l'ensemble des états maximalement intriqués les plus proches d'un état séparable, comme on peut en rencontrer au début de l'algorithme de Grover. Ils apportent la confirmation que, même si l'état initial et les éléments marqués sont des états séparables, l'algorithme génère une séquence d'états intriqués.

En 2012, Wen et Cao ont tenté de décrire le comportement de l'intrication multipartite dans l'algorithme de Grover en se penchant sur une version adiabatique de l'algorithme de recherche [272]. L'entropie de Von Neumann a été calculée pour toutes les séparations bipartites possibles du système quantique. Ceci les mena à une nouvelle mesure de l'intrication, généralisant la mesure introduire par Meyer et Wallach en 2002 [189]. Ils démontrent l'existence et l'évolution de l'intrication tout au long du processus de recherche. Par ailleurs, la même évolution de l'intrication a été observée dans le cas bipartite et multipartite (début à zéro pour atteindre une valeur maximale au point critique, puis retour à la valeur zéro). Le comportement symétrique de l'intrication durant l'évolution adiabatique de l'algorithme est aussi mis en évidence dans ce travail. Nous pouvons aussi citer les travaux de Pati et Braunstein la même année [217].

Rossi *et al.* ont étudié en 2013 l'invariance du comportement de l'intrication par rapport à l'échelle du système pour l'algorithme de Grover [226]. Ils ont déterminé l'évolution quantitative de l'intrication des systèmes quantiques générés par l'algorithme de Grover, tout au long des étapes de calcul. Ils ont utilisé la Mesure Géométrique de l'Intrication comme mesure numérique. Les auteurs ont montré que l'intrication multipartite est toujours présente durant l'algorithme, et l'ont étudié en fonction du nombre d'itérations de l'algorithme, pour un nombre fixé de qubits. Ils ont trouvé que le maximum de l'intrication était atteint pour des itérations remarquables et précises en utilisant la GME, et ceci pour certaines valeurs spécifiques de $|\mathcal{S}|$.

La même année, Chakraborty *et al.* ont publié un article [61] dans la même philosophie que le travail de Rossi *et al.* [226]. La Mesure Géométrique de l'Intrication est utilisée pour quantifier et analyser l'intrication tout au long des itérations de l'algorithme. Les auteurs s'intéressent à comment l'intrication varie quand le nombre de qubits et d'éléments marqués augmente. Leur premier résultat est que le comportement de la valeur maximale de l'intrication est monotone en le nombre de qubits. Le second principal résultat est que, pour un nombre de qubits donné, un changement dans les éléments marqués implique un changement dans la quantité d'intrication.

Une année plus tard, Rossi *et al.* publièrent un nouvel article mettant en relation les états de Grover aux hypergraphes [227]. La GME est calculée en fonction du nombre de qubits, et en ne considérant que la première itération de l'algorithme de Grover. Pour différents cas étudiés, les courbes pour un et deux éléments recherchés montrent le même comportement : une décroissance exponentielle. Une association entre les états initiaux de l'algorithme et des hypergraphes est établie, fournissant une interprétation plus graphique, et permettant de mettre en évidence des propriétés d'intrication pour ces états, comme la biséparabilité ou la présence de *genuine entanglement*.

En 2015, Qu *et al.* [219] ont étudié l'intrication multipartite en utilisant le degré de séparabilité comme une mesure qualitative de l'intrication. D'autre part, les auteurs ont aussi utilisé une mesure quantitative de l'intrication introduite par Vidal [264], appelée le nombre de Schmidt (voir Section 2.2.3). Ces outils de mesure qualitatifs et quantitatifs leur ont permis d'étudier l'évolution de l'intrication dans l'algorithme de Grover. Leurs résultats, dépendant de l'étape de l'algorithme, confirment qu'après la première itération, des états "complètement" intriqués apparaissent dans l'algorithme.

Plus récemment, en 2016, Ye *et al.* [289] ont publié un travail traitant de l'influence des imperfections statiques sur l'intrication quantique et le *quantum discord*. La mesure de la concurrence est utilisée pour étudier le comportement de l'intrication. Les imperfections statiques peuvent rompre les corrélations quantiques selon les auteurs. En effet, pour chaque faible imperfection, l'intrication quantique présente un comportement périodique, alors que cette périodicité serait détruite en cas d'imperfection plus importante. Les auteurs confirment alors la propriété périodique de l'intrication au sein de l'algorithme de Grover. Nous pouvons aussi citer les travaux de Anand et Pati la même année [9].

Pan *et al.* ont également étudié en 2017 l'aspect invariant de la GME quant à la taille du système quantique [211]. À partir du travail de Rossi *et al.* [226], les auteurs ont montré que le comportement de l'intrication dans l'algorithme de Grover n'est pas toujours invariant par mise à l'échelle (nombre de qubits). Ils prouvent qu'après le "point critique", la GME n'est pas nécessairement *scale invariant*, et dépendra alors du nombre de qubits n et du nombre d'éléments marqués. Quelques exemples sont traités pour illustrer et confirmer leurs résultats, notamment lorsque les éléments marqués forment un état séparable, GHZ ou W.

On peut également mentionner les travaux assez récents de Nan et Wei [196] portant sur l'étude de l'évolution de la cohérence et de l'intrication durant l'algorithme, de Pan *et al.* [210] concernant l'influence de la porte d'Oracle et de Diffusion sur l'intrication en utilisant le GME, et de Fujikawa *et al.* [103].

3.2 Rang des tenseurs et variété des sécantes

Dans cette section, on se propose d'étudier géométriquement les tenseurs générés par l'algorithme Grover. Nous utilisons notamment la notion de rang pour caractériser les états générés par l'algorithme. Nous proposons par la suite une interprétation de

l'évolution de l'algorithme du point de vue de la variété des sécantes. Cela permit d'établir des résultats généraux sur la nature des états générés et le lieu du maximum de l'intrication au cours de l'algorithme de Grover.

3.2.1 Rang des états de Grover

Il convient tout d'abord de rappeler que l'algorithme de Grover débute par une initialisation des registres quantiques. L'état initial de l'algorithme de Grover est donc l'état parallélisé $|\Psi_0\rangle = |+\rangle^{\otimes n}$. Les amplitudes des éléments recherchés vont donc augmenter, tandis que les amplitudes des états de base restants vont diminuer (sans forcément atteindre la valeur 0).

On peut alors représenter l'état généré par l'algorithme de Grover $|\Psi_k\rangle$ à la k-ième itération (une itération correspondant à l'application de l'opérateur d'Oracle et de Diffusion), comme s'écrivant

$$|\Psi_k\rangle = \frac{\alpha_k}{|\mathcal{S}|} \sum_{\mathbf{x}\in\mathcal{S}} |\mathbf{x}\rangle + \beta_k |+\rangle^{\otimes n} \ , \tag{3.1}$$

avec α_k et β_k des nombres réels, vérifiant la relation de normalisation donnée par

$$|\mathcal{S}| \left(\frac{\beta_k}{\sqrt{N}} + \frac{\alpha_k}{|\mathcal{S}|} \right)^2 + (N - |\mathcal{S}|) \frac{{\beta_k}^2}{N} = 1 \ . \tag{3.2}$$

L'algorithme de Grover aura alors comme effet de faire décroître l'amplitude β_k vers 0 tout en augmentant α_k au plus proche de 1.

À partir de l'écriture de $|\Psi_k\rangle$ fournie en Équation 3.1, nous pouvons affirmer que le rang des états (intermédiaires) générés par l'algorithme de Grover est borné, pour $0 < k < k_{opt}$:

$$2 \leq \mathsf{Rang}(|\Psi_k\rangle) \leq |\mathcal{S}| + 1 \ . \tag{3.3}$$

La borne supérieure peut s'établir de manière assez directe. En effet, on remarque que dans l'Équation 3.1 l'état $|\Psi_k\rangle$ s'écrit comme la somme de $|\mathcal{S}|+1$ états séparables ($|\mathcal{S}|$ états recherchés et l'état parallélisé), et donc son rang est au plus égal à $|\mathcal{S}|+1$.

La borne inférieure est toujours assurée lorsque $\alpha_k \neq 0$ et $\beta_k \neq 0$, car on ne peut obtenir un état de rang 1 si ces deux coefficients sont non nuls. Le fait que $\alpha_k \neq 0$ est assuré par la convergence de l'algorithme. Si $\beta_k = 0$, alors la probabilité que les états de base composant l'écriture de $|\Psi_k\rangle$ appartiennent à $\mathcal{S}$ est égal à 1, ce qui signifie que $k = k_{opt}$. Or nous avons supposé $k < k_{opt}$. Ainsi on aura toujours $\alpha_k \neq 0$ et $\beta_k \neq 0$, et donc les tenseurs générés par l'algorithme de Grover seront au moins de rang 2, sous les conditions précédemment émises.

Ceci implique que dès la première itération de l'algorithme (sauf cas critique), l'algorithme de Grover génère des états de rang strictement supérieur à 1, et donc des états intriqués.

3.2.2 Grover et les variétés des sécantes

Ce résultat peut être précisé en termes de variétés algébriques, et plus précisément en termes de variétés des sécantes dans ce cas précis. On pose $|\mathcal{S}| = s$ pour plus de simplicité dans les notations.

Proposition 3.2.1. *Les états générés par l'algorithme de Grover correspondent à des points sur les variétés des sécantes, de la manière suivante :*

1. *Pour un seul état marqué, les états $|\Psi_k\rangle$ générés par l'algorithme de Grover pour $0 < k < k_{opt}$ sont des points généraux de la variété des sécantes $\sigma_2(X)$. En particulier, les états $|\Psi_k\rangle$ sont SLOCC équivalents à $|GHZ_n\rangle$,*
2. *Pour deux éléments marqués, si les éléments recherchés $|x_0\rangle$ et $|x_1\rangle$ sont tous à distance de Hamming maximale (dans leur écriture binaire), alors les états $|\Psi_k\rangle$ sont des points généraux de la variété des sécantes $\sigma_3(X)$.*

Remarque 22. Il est possible d'étendre cette proposition à plus d'éléments marqués. Si les éléments $|x_0\rangle, \ldots, |x_{s-1}\rangle$ de $\mathcal{S}$ sont tous à distance de Hamming maximale (dans leur écriture binaire), alors le plan $\mathbb{P}^s_{|x_0\rangle,\ldots,|x_{s-1}\rangle,|+^{\otimes n}\rangle}$ de dimension s engendré par les points $|x_0\rangle, \ldots, |x_{s-1}\rangle, |+\rangle^{\otimes n}$ de l'espace projectif est en position générale dans $\mathbb{P}(\mathcal{H}_n)$ et donc $|\Psi_k\rangle$ est un point général de la variété des sécantes $\sigma_{s+1}(X)$.

Ce résultat offre un nouvel angle d'approche pour l'étude de l'intrication dans l'algorithme de Grover, permettant de proposer une interprétation géométrique des précédents résultats numériques notamment.

3.2.3 Interprétation géométrique

Dans divers précédents travaux, la Mesure Groverienne/Géométrique de l'Intrication a été utilisée comme mesure de l'intrication pour étudier son évolution au cours de l'algorithme de Grover [38, 39, 226, 61, 227, 211, 210]. On se propose ici de se focaliser sur la Mesure Groverienne de l'Intrication (définie en Équation 2.43).

Dans le cas d'un seul élément marqué, l'évolution dans la MGI en fonction du nombre itérations k peut être décrite comme suit : elle débute à 0 pour $k = 0$, et croit ensuite jusqu'à atteindre son maximum pour $k \approx \frac{k_{opt}}{2}$, puis ensuite décroît jusqu'à 0 pour $k = k_{opt}$. Ce résultat est en effet représenté en Figure 1 de [226].

À la lumière des résultats des précédentes sous-sections, nous proposons une explication géométrique de ce comportement. La Proposition 3.2.1 peut être représentée sous la forme d'une figure géométrique (Figure 3.1). En effet, cela permet d'avoir une meilleure idée du comportement de la mesure de l'intrication : si $|x_0\rangle$ est l'état recherché, alors l'état de Grover $|\Psi_k\rangle$ peut être écrit comme

$$|\Psi_k\rangle = \alpha_k|x_0\rangle + \beta_k|+\rangle^{\otimes n} , \tag{3.4}$$

avec α_k et β_k des réels positifs, tels que pour $k \in [\![1, k_{opt}]\!]$, α_k augmente tandis que β_k diminue. De ce fait, l'état $|\Psi_k\rangle$ évolue au cours de l'algorithme sur la ligne sécante passant par les deux états séparables $|+\rangle^{\otimes n}$ et $|x_0\rangle$. Au début de l'algorithme, on se

trouve à l'état initial $|\Psi_0\rangle = |+\rangle^{\otimes n}$ et lorsque k atteint k_{opt} l'état de Grover est proche de l'état $|x_0\rangle$. Ceci indique que le maximum de la distance entre l'état de Grover et la variété des états séparables doit être atteint lorsque $|\Psi_k\rangle$ est proche du point milieu défini par $|+\rangle^{\otimes n}$ et $|x_0\rangle$.

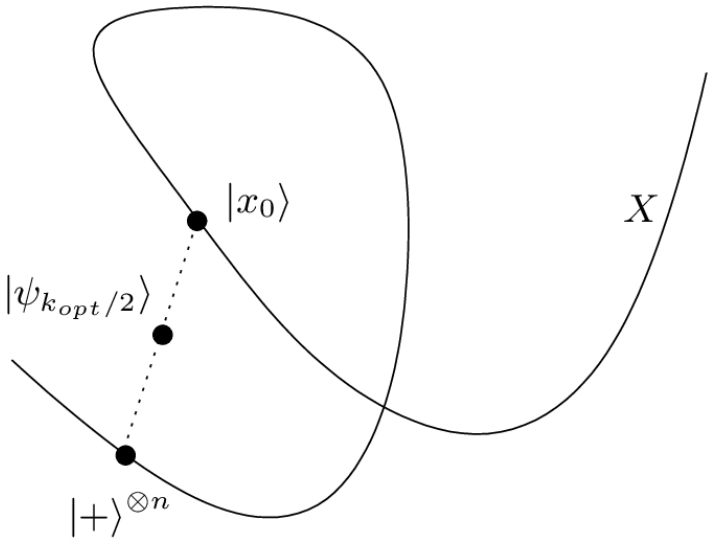


FIGURE 3.1 – Représentation graphique de la recherche d'un élément dans l'algorithme de Grover. L'évolution de l'algorithme est représentée comme un point se déplaçant sur une ligne sécante. La "courbe" X représente la variété des états séparables.

Dans le cas de deux éléments marqués $|x_0\rangle$ et $|x_1\rangle$, de distance de Hamming maximale pour leur écriture binaire, l'évolution dans la MGI en fonction du nombre itération k peut être décrite comme suit : elle débute à 0 pour $k = 0$, et croit ensuite jusqu'à atteindre son maximum pour $k \approx \frac{2k_{opt}}{3}$, puis ensuite décroît jusqu'à une valeur non nulle pour $k = k_{opt}$. Ce résultat est en effet représenté en Figure 2 de [226]. La raison pour laquelle la MGI n'est pas égale à 0 à la fin de l'algorithme est assez claire au vu des résultats précédents : lorsque k atteint l'itération optimale k_{opt}, l'état $|\Psi_k\rangle$ est proche d'être un point de la ligne sécante $\mathbb{P}^1_{|x_0\rangle,|x_1\rangle}$. De ce fait, $|\Psi_k\rangle$ n'est pas un point de X à la fin de l'algorithme. La représentation graphique des sécantes permet aussi de proposer une explication au fait que le maximum de l'intrication est atteint pour $k \approx \frac{2k_{opt}}{3}$ (voir Figure 3.2).

L'état de Grover $|\Psi_k\rangle$ évolue tout au long de l'algorithme sur le plan sécant $\mathbb{P}^2_{|x_0\rangle,|x_1\rangle,|+\rangle^{\otimes n}}$, en partant du point $|+\rangle^{\otimes n}$ pour arriver au milieu du segment joignant les points $|x_0\rangle$ et $|x_1\rangle$. Ainsi, on peut prévoir que la distance maximale entre l'état de Grover et la variété des états séparables est atteinte lorsque le point $|\Psi_k\rangle$ est proche du barycentre des trois points $|x_0\rangle$, $|x_1\rangle$ et $|+\rangle^{\otimes n}$.

Cette notion de barycentre, suggérée par les Figures 3.1 et 3.2, expliquant les résultats numériques des précédents travaux, peut être généralisée et précisée d'avantange.

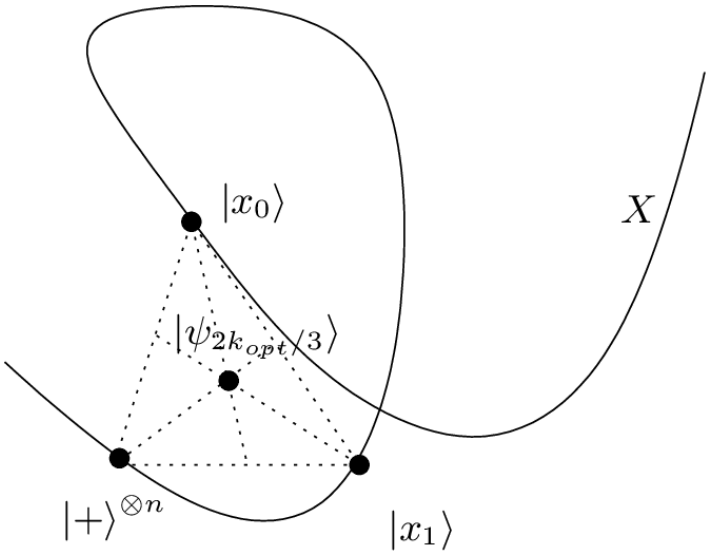


Figure 3.2 – Représentation graphique de la recherche de deux éléments orthogonaux dans l'algorithme de Grover. L'évolution de l'algorithme est représentée comme un point se déplaçant sur un plan sécant. La "courbe" X représente la variété des états séparables.

Théorème 3.2.1. *Soit $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$ l'espace de Hilbert des systèmes quantiques à n-d-dit (n particules à d états de base chacune). On note par $\mathcal{S}$ l'ensemble des éléments marqués, tous de distance de Hamming maximale, avec $|\mathcal{S}| \leq d$. Alors pour n grand, la mesure de l'intrication atteint son maximum pour $k \approx \frac{|\mathcal{S}|}{|\mathcal{S}|+1} k_{opt}$ avec $k_{opt} = \lfloor \frac{\pi}{4}\sqrt{\frac{d^n}{|\mathcal{S}|}} \rceil$.*

La preuve du Théorème 3.2.1 est accessible dans un de nos précédents travaux [133]. Ce théorème permet d'expliquer géométriquement l'évolution numérique observée à l'aide de différentes mesures de l'intrication.

Un autre résultat intéressant est mis en avant par les mêmes auteurs, représentant la mesure géométrique de l'intrication de l'état issu de la première itération de l'algorithme de Grover en fonction du nombre de qubits n, pour un et deux éléments marqués (Figure 1 de [227]), et peut également trouver une explication par des arguments géométriques. Dans les différents cas considérés, les courbes représentées ont le même comportement, à savoir une décroissance exponentielle.

En se replaçant dans notre contexte d'interprétation géométrique des états générés par l'algorithme de Grover, pour un ou deux éléments marqués, l'état $|\psi_1\rangle$ généré après la première itération (en excluant le cas critique) est respectivement un point général de la première sécante $\sigma_2(X)$ ou la seconde sécante $\sigma_3(X)$. Cependant, la dimension de ces variétés augmente linéairement en fonction de n, alors que la dimension de l'espace ambiant augmente exponentiellement. En effet, il est connu que

$$\dim(\sigma_k(X)) \leq k\dim(X) + k - 1 \ , \tag{3.5}$$

avec dans la plupart des cas l'égalité vérifiée. En particulier, dans notre cas $X = \underbrace{\mathbb{P}^1 \times \cdots \times \mathbb{P}^1}_{n \text{ times}}$, si $n > 2$ alors

$$\dim(\sigma_2(X)) = 2n + 1 \ . \tag{3.6}$$

La Dimension Relative de la première sécante, comparée à la dimension de l'espace ambiant (la dimension de l'espace projectif associé à l'espace de Hilbert $\mathcal{H}_n$) est alors donnée par

$$DR_{\sigma_2} : n \mapsto \frac{2n+1}{2^n - 1} \ . \tag{3.7}$$

Si on normalise cette fonction afin qu'elle soit égale à 1 pour $n = 1$, nous obtenons la Dimension Relative Normalisée de la première variété des sécantes :

$$DRN_{\sigma_2} : n \mapsto \frac{1}{3}\left(\frac{2n+1}{2^n - 1}\right) \ , \tag{3.8}$$

dont le comportement, représenté en Figure 3.3, est similaire à celui de la MGI en fonction de n obtenu pour l'état $|\psi_1\rangle$ dans [227].

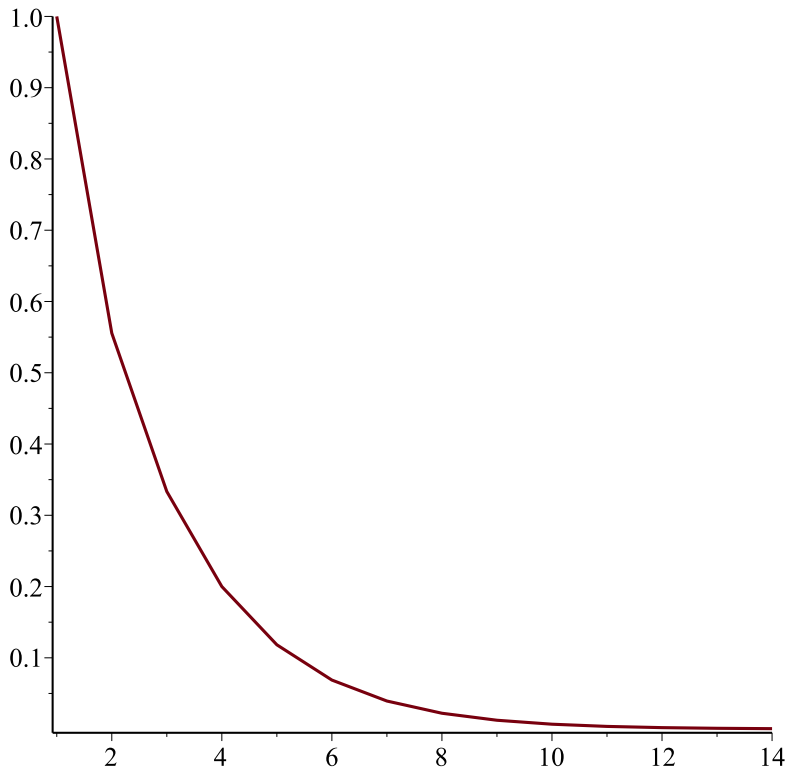


FIGURE 3.3 – Représentation graphique de l'évolution de la Dimension Relative Normalisée de la variété des sécantes $\sigma_2(X)$ en fonction du nombre de qubits.

La similarité de ces deux courbes peut être expliquée comme suit. Pour un état marqué, l'état $|\psi_1\rangle$ généré après la première itération de l'algorithme de Grover est toujours un point général de la variété des sécantes, tandis que la MGI mesure la distance de ce point à la variété des états séparables. Cependant, c'est une distance relative, dans la mesure où la MGI est toujours bornée par 1. Comme cela est représenté en Figure 3.3, plus la dimension de l'espace augmente, plus la dimension relative de la variété des sécantes décroît exponentiellement. La MGI est maximale pour les points généraux de l'espace ambiant. Ainsi, la distance (relative) de l'état $|\psi_1\rangle$ à la variété des états séparables décroît à la même vitesse que la dimension relative de la première sécante.

L'autre cas, tout aussi intéressant, est celui de deux éléments marqués. Pour deux éléments marqués, Rossi *et al.* [227] ont calculé la MGI de $|\psi_1\rangle$ en fonction du nombre de qubits, pour différents choix et configurations d'états marqués, plus précisément pour des éléments marqués ayant une distance de Hamming égale à 1, 2, 3 ou 4 (dans leur écriture binaire). Comme la distance de Hamming n'est pas maximale, les états en question ne sont pas des points génériques de la seconde variété des sécantes $\sigma_3(X)$. Par exemple, si la distance de Hamming est égale à 1, la somme des deux éléments marqués formera un état séparable, et de ce fait, l'état $|\psi_1\rangle$ appartiendra à la première variété des sécantes $\sigma_2(X)$.

Cependant, quelque soit la variété à laquelle appartient l'état $|\psi_1\rangle$, la dimension relative de la seconde variété des sécantes décroîtra aussi de manière exponentielle, car nous avons

$$\dim(\sigma_3(\mathbb{P}^1 \times \cdots \times \mathbb{P}^1)) \leq 3n + 2 \ . \tag{3.9}$$

Ainsi, le rapport entre la dimension des variétés des sécantes et la dimension de l'espace ambiant, fournit une explication aux comportements observés par Rossi *et al.* en ce qui concerne le comportement de la mesure géométrique de l'intrication lorsque la taille des systèmes quantiques augmente.

3.3 Étude de cas

Dans cette sous-section, nous étudions l'algorithme de Grover dans certains cas précis, lorsqu'il est appliqué à des systèmes quantiques de différentes tailles. Pour chaque cas, nous précisons les classes d'intrications atteintes, en fonction des éléments marqués durant l'algorithme. Nous tentons ensuite d'apporter une vision générale et une analyse de ces résultats. Pour cette étude, nous distinguerons différents cas d'application de l'algorithme de Grover, dépendants du nombre d'éléments recherchés :

- $|\mathcal{S}| < \dfrac{N}{4}$: le cas standard, le cas naturel d'application de l'algorithme de Grover,
- $|\mathcal{S}| = \dfrac{N}{4}$: le cas critique,
- $|\mathcal{S}| > \dfrac{N}{4}$: le cas exceptionnel.

Dans le cas critique, l'algorithme s'arrête après une seule itération, et l'état généré par l'algorithme est exactement la superposition des éléments recherchés.

3.3.1 Le cas $2 \times 2 \times 2$ (3-qubits)

On s'intéresse ici à l'application de l'algorithme de Grover aux systèmes à 3-qubits. On rappelle que la classification des systèmes à 3-qubits est précisée en Section 2.2.2, et nous utilisons l'algorithme présenté en Annexe A.1 pour déterminer la classe d'intrication associée à un état. Dans ce cas, $n = 3$, et donc l'algorithme de Grover recherche un ou plusieurs éléments dans une base de données à $N = 2^3 = 8$ éléments.

- Pour $|\mathcal{S}| = 1$, les états générés par l'algorithme de Grover appartiennent à l'orbite $\mathcal{O}_6$ (correspondant à $\sigma_2\big(\mathrm{Seg}(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)\big)$, comme attendu (voir Section 3.2).
- Pour $|\mathcal{S}| = 2$, qui est le cas critique pour les 3-qubits, les états générés par l'algorithme de Grover appartiennent aux orbites $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$, $\mathcal{O}_4$ et $\mathcal{O}_6$. Ce résultat pouvait être attendu compte tenu du fait que les formes normales de chacune de ces orbites peuvent s'écrire comme la somme de deux éléments de base (voir Section 3.5 pour plus de détails sur le cas critique).
- Pour $|\mathcal{S}| > 2$, les orbites $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$, $\mathcal{O}_4$et $\mathcal{O}_6$ sont atteintes.

On peut se limiter ici à l'étude des cas jusqu'à $|\mathcal{S}| \leq 4$, par argument de symétrie (en marquant plus de la moitié des éléments de la base, on génère des états équivalents et les mêmes orbites).

Par ailleurs, l'algorithme de Grover ne génère pas d'états appartenant à l'orbite $\mathcal{O}_5$ (l'orbite de $|W\rangle$), et ce quelque soit le nombre ou le choix des éléments marqués. Le Tableau 3.1 présente un exemple d'ensembles d'éléments marqués $\mathcal{S}$ pour chaque orbite atteinte, et pour différents nombres d'éléments marqués.

Orbite	Ensembles $\mathcal{S}$
$\mathcal{O}_6$	$\{\|000\rangle\}$, $\{\|000\rangle, \|111\rangle\}$, $\{\|000\rangle, \|001\rangle, \|010\rangle\}$, $\{\|000\rangle, \|001\rangle, \|010\rangle, \|100\rangle\}$
$\mathcal{O}_5$	—
$\mathcal{O}_4$	$\{\|000\rangle, \|110\rangle\}$, $\{\|000\rangle, \|010\rangle, \|100\rangle, \|111\rangle\}$
$\mathcal{O}_3$	$\{\|000\rangle, \|011\rangle\}$, $\{\|000\rangle, \|001\rangle, \|010\rangle, \|111\rangle\}$
$\mathcal{O}_2$	$\{\|000\rangle, \|101\rangle\}$, $\{\|000\rangle, \|001\rangle, \|100\rangle, \|111\rangle\}$
$\mathcal{O}_1$	$\{\|000\rangle, \|001\rangle\}$, $\{\|000\rangle, \|001\rangle, \|010\rangle, \|011\rangle\}$

TABLE 3.1 – Exemple d'ensembles d'éléments marqués $\mathcal{S}$ et les orbites atteintes correspondantes par l'algorithme de Grover dans le cas $2 \times 2 \times 2$.

3.3.2 Le cas $2 \times 2 \times 3$

On s'intéresse ici à l'application de l'algorithme de Grover aux systèmes quantiques de taille $2 \times 2 \times 3$. La classification de ces systèmes sous SLOCC amène à un nombre fini d'orbites [135], dont un représentant est présenté en Table 3.2 pour chacune de ces 8 orbites. Dans cette configuration, l'algorithme de Grover recherche un ou plusieurs éléments dans une base de données de $N = 2 \times 2 \times 3 = 12$ éléments. L'algorithme de classification utilisé est accessible en Annexe A.2.

- Pour $|\mathcal{S}| = 1$, les états générés par l'algorithme de Grover appartiennent à l'orbite $\mathcal{O}_6$, états génériques de la première variété des sécantes.

Orbite	Forme normale (représentant)
$\mathcal{O}_8$	$\|000\rangle + \|011\rangle + \|101\rangle + \|112\rangle$
$\mathcal{O}_7$	$\|000\rangle + \|011\rangle + \|102\rangle$
$\mathcal{O}_6$	$\|000\rangle + \|111\rangle$
$\mathcal{O}_5$	$\|000\rangle + \|011\rangle + \|101\rangle$
$\mathcal{O}_4$	$\|000\rangle + \|011\rangle$
$\mathcal{O}_3$	$\|000\rangle + \|101\rangle$
$\mathcal{O}_2$	$\|000\rangle + \|110\rangle$
$\mathcal{O}_1$	$\|000\rangle$

Table 3.2 – Orbites sous l'action du groupe SLOCC, et leurs représentants, pour les tenseurs de taille $2 \times 2 \times 3$ [135].

- Pour $|\mathcal{S}| = 2$, les orbites $\mathcal{O}_3$, $\mathcal{O}_4$, $\mathcal{O}_6$, $\mathcal{O}_7$ et $\mathcal{O}_8$ sont atteintes.
- Pour $|\mathcal{S}| = 3$, qui est le cas critique pour les états quantiques de taille $2 \times 2 \times 3$, les états générés par l'algorithme de Grover appartiennent aux orbites $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$, $\mathcal{O}_4$, $\mathcal{O}_5$, $\mathcal{O}_6$ et $\mathcal{O}_7$.
- Pour $|\mathcal{S}| = 4$ ou $|\mathcal{S}| = 6$, les orbites $\mathcal{O}_1$, $\mathcal{O}_3$, $\mathcal{O}_4$, $\mathcal{O}_6$, $\mathcal{O}_7$ et $\mathcal{O}_8$ sont atteintes.
- Pour $|\mathcal{S}| = 5$, les orbites $\mathcal{O}_6$, $\mathcal{O}_7$, et $\mathcal{O}_8$ sont atteintes.

On peut se limiter ici à l'étude des cas jusqu'à $|\mathcal{S}| \leq 6$, par argument de symétrie. Dans ce cas, en faisant varier les éléments marqués, l'algorithme de Grover génère des états de tous les types d'intrication. Le Tableau 3.3 présente un exemple d'ensembles d'éléments marqués $\mathcal{S}$ pour chaque orbite atteinte, et pour différents nombre d'éléments marqués.

Orbite	Ensembles $\mathcal{S}$
$\mathcal{O}_8$	$\{\|000\rangle, \|111\rangle\}$, $\{\|000\rangle, \|001\rangle, \|010\rangle, \|100\rangle\}$
$\mathcal{O}_7$	$\{\|000\rangle\|101\rangle\}$, $\{\|000\rangle, \|012\rangle, \|101\rangle\}$
$\mathcal{O}_6$	$\{\|000\rangle\}$, $\{\|000\rangle, \|110\rangle\}$
$\mathcal{O}_5$	$\{\|000\rangle, \|101\rangle, \|110\rangle\}$
$\mathcal{O}_4$	$\{\|000\rangle, \|100\rangle\}$, $\{\|000\rangle, \|001\rangle, \|010\rangle\}$
$\mathcal{O}_3$	$\{\|000\rangle, \|010\rangle\}$, $\{\|000\rangle, \|001\rangle, \|100\rangle\}$
$\mathcal{O}_2$	$\{\|000\rangle, \|010\rangle, \|100\rangle\}$
$\mathcal{O}_1$	$\{\|000\rangle, \|001\rangle, \|002\rangle\}$, $\{\|000\rangle, \|010\rangle, \|100\rangle, \|110\rangle\}$

Table 3.3 – Exemple d'ensembles d'éléments marqués $\mathcal{S}$ et les orbites atteintes correspondantes par l'algorithme de Grover dans le cas $2 \times 2 \times 3$.

3.3.3 Le cas $2 \times 3 \times 3$

Nous étudions dans cette sous-section l'application de l'algorithme de Grover appliqué aux systèmes quantiques de taille $2 \times 3 \times 3$. La classification de ces systèmes sous SLOCC amène à un nombre fini d'orbites [135], dont un représentant est présenté en Table 3.4 pour chacune de ces 17 orbites. Dans cette configuration, l'algorithme de Gro-

ver recherche un ou plusieurs éléments dans une base de données de $N = 2 \times 3 \times 3 = 18$ éléments. L'algorithme de classification utilisé est accessible en Annexe A.3.

Orbite	Forme normale (représentant)
$\mathcal{O}_{17}$	$\|000\rangle + \|011\rangle + \|100\rangle + \|122\rangle$
$\mathcal{O}_{16}$	$\|000\rangle + \|011\rangle + \|101\rangle + \|122\rangle$
$\mathcal{O}_{15}$	$\|000\rangle + \|011\rangle + \|022\rangle + \|101\rangle + \|112\rangle$
$\mathcal{O}_{14}$	$\|000\rangle + \|011\rangle + \|122\rangle$
$\mathcal{O}_{13}$	$\|000\rangle + \|011\rangle + \|022\rangle + \|101\rangle$
$\mathcal{O}_{12}$	$\|000\rangle + \|011\rangle + \|101\rangle + \|112\rangle$
$\mathcal{O}_{11}$	$\|000\rangle + \|011\rangle + \|121\rangle + \|102\rangle$
$\mathcal{O}_{10}$	$\|000\rangle + \|011\rangle + \|102\rangle$
$\mathcal{O}_{9}$	$\|000\rangle + \|011\rangle + \|022\rangle$
$\mathcal{O}_{8}$	$\|000\rangle + \|011\rangle + \|110\rangle + \|121\rangle$
$\mathcal{O}_{7}$	$\|000\rangle + \|011\rangle + \|120\rangle$
$\mathcal{O}_{6}$	$\|000\rangle + \|111\rangle$
$\mathcal{O}_{5}$	$\|000\rangle + \|011\rangle + \|101\rangle$
$\mathcal{O}_{4}$	$\|000\rangle + \|011\rangle$
$\mathcal{O}_{3}$	$\|000\rangle + \|101\rangle$
$\mathcal{O}_{2}$	$\|000\rangle + \|110\rangle$
$\mathcal{O}_{1}$	$\|000\rangle$

TABLE 3.4 – Orbites sous l'action du groupe SLOCC, et leurs représentants, pour les tenseurs de taille $2 \times 3 \times 3$ [135].

- Pour $|\mathcal{S}| = 1$, les états générés par l'algorithme de Grover appartiennent à l'orbite $\mathcal{O}_6$, états génériques de la première variété des sécantes.
- Pour $|\mathcal{S}| = 2$, les orbites $\mathcal{O}_4$, $\mathcal{O}_6$, $\mathcal{O}_7$, $\mathcal{O}_{10}$, $\mathcal{O}_{14}$ et $\mathcal{O}_{17}$ sont atteintes.
- Pour $|\mathcal{S}| = 3$, les orbites $\mathcal{O}_2$, $\mathcal{O}_3$, $\mathcal{O}_6$, $\mathcal{O}_7$, $\mathcal{O}_8$, $\mathcal{O}_{10}$, $\mathcal{O}_{12}$, $\mathcal{O}_{14}$, $\mathcal{O}_{16}$, et $\mathcal{O}_{17}$ sont atteintes.
- Pour $|\mathcal{S}| = 4$, les orbites $\mathcal{O}_4$, $\mathcal{O}_6$, $\mathcal{O}_7$, $\mathcal{O}_8$, $\mathcal{O}_9$, $\mathcal{O}_{10}$, $\mathcal{O}_{12}$, $\mathcal{O}_{14}$, $\mathcal{O}_{16}$, et $\mathcal{O}_{17}$ sont atteintes.
- Pour $|\mathcal{S}| = 5$ ou $|\mathcal{S}| = 7$, les orbites $\mathcal{O}_6$, $\mathcal{O}_7$, $\mathcal{O}_8$, $\mathcal{O}_{10}$, $\mathcal{O}_{11}$, $\mathcal{O}_{12}$, $\mathcal{O}_{13}$, $\mathcal{O}_{14}$, $\mathcal{O}_{16}$, et $\mathcal{O}_{17}$ sont atteintes.
- Pour $|\mathcal{S}| = 6$, les orbites $\mathcal{O}_1$, $\mathcal{O}_2$, $\mathcal{O}_3$, $\mathcal{O}_4$, $\mathcal{O}_6$, $\mathcal{O}_7$, $\mathcal{O}_8$, $\mathcal{O}_9$, $\mathcal{O}_{10}$, $\mathcal{O}_{11}$, $\mathcal{O}_{12}$, $\mathcal{O}_{14}$, $\mathcal{O}_{16}$, et $\mathcal{O}_{17}$ sont atteintes.
- Pour $|\mathcal{S}| = 8$, les orbites $\mathcal{O}_1$, $\mathcal{O}_6$, $\mathcal{O}_7$, $\mathcal{O}_8$, $\mathcal{O}_9$, $\mathcal{O}_{10}$, $\mathcal{O}_{11}$, $\mathcal{O}_{12}$, $\mathcal{O}_{13}$, $\mathcal{O}_{14}$, $\mathcal{O}_{16}$, et $\mathcal{O}_{17}$ sont atteintes.

L'algorithme de Grover ne génère pas d'états appartenant aux orbites $\mathcal{O}_5$ et $\mathcal{O}_{15}$, et ce, quelque soit le nombre ou le choix des éléments marqués. Le Tableau 3.5 présente un exemple d'ensembles d'éléments marqués $\mathcal{S}$ pour chaque orbite atteinte, et pour différents nombres d'éléments marqués.

3.3.4 Le cas $2 \times 2 \times 2 \times 2$ (4-qubits)

Notre dernier cas d'étude concerne l'application de l'algorithme de Grover appliqué aux systèmes à 4-qubits. On rappelle que la classification des systèmes à 4-qubits est

Orbite	Ensembles $\mathcal{S}$
$\mathcal{O}_{17}$	$\{\|000\rangle, \|111\rangle\}$, $\{\|000\rangle, \|001\rangle, \|110\rangle\}$
$\mathcal{O}_{16}$	$\{\|000\rangle, \|011\rangle, \|101\rangle\}$,$\{\|000\rangle, \|001\rangle, \|010\rangle, \|100\rangle\}$
$\mathcal{O}_{15}$	—
$\mathcal{O}_{14}$	$\{\|000\rangle, \|011\rangle\}$, $\{\|000\rangle, \|001\rangle, \|010\rangle\}$
$\mathcal{O}_{13}$	$\{\|000\rangle, \|001\rangle, \|010\rangle, \|101\rangle, \|110\rangle\}$
$\mathcal{O}_{12}$	$\{\|000\rangle, \|010\rangle, \|121\rangle\}$, $\{\|000\rangle, \|001\rangle, \|110\rangle, \|120\rangle\}$
$\mathcal{O}_{11}$	$\{\|000\rangle, \|001\rangle, \|002\rangle, \|010\rangle, \|111\rangle\}$
$\mathcal{O}_{10}$	$\{\|000\rangle, \|101\rangle\}$, $\{\|000\rangle, \|001\rangle, \|100\rangle\}$
$\mathcal{O}_{9}$	$\{\|000\rangle, \|011\rangle, \|100\rangle, \|111\rangle\}$
$\mathcal{O}_{8}$	$\{\|000\rangle, \|001\rangle, \|112\rangle\}$, $\{\|000\rangle, \|001\rangle, \|012\rangle, \|102\rangle\}$
$\mathcal{O}_{7}$	$\{\|000\rangle, \|110\rangle\}$, $\{\|000\rangle, \|001\rangle, \|012\rangle\}$
$\mathcal{O}_{6}$	$\{\|000\rangle\}$, $\{\|000\rangle, \|001\rangle\}$
$\mathcal{O}_{5}$	—
$\mathcal{O}_{4}$	$\{\|000\rangle, \|100\rangle\}$,$\{\|000\rangle, \|001\rangle, \|100\rangle, \|101\rangle\}$
$\mathcal{O}_{3}$	$\{\|000\rangle, \|010\rangle, \|020\rangle\}$
$\mathcal{O}_{2}$	$\{\|000\rangle, \|001\rangle, \|002\rangle\}$
$\mathcal{O}_{1}$	$\{\|000\rangle, \|001\rangle, \|002\rangle, \|100\rangle, \|101\rangle, \|102\rangle\}$

Table 3.5 – Exemple d'ensembless d'éléments marqués $\mathcal{S}$ et les orbites atteintes correspondantes par l'algorithme de Grover dans le cas $2 \times 3 \times 3$.

précisée en Section 2.2.2. Dans notre cas $n = 4$, et l'algorithme de Grover recherche donc un ou plusieurs éléments dans une base de données à $N = 2^4 = 16$ éléments.

- **Cas standard ($|\mathcal{S}| < \frac{N}{4}$) :**
  - Pour $|\mathcal{S}| = 1$, on atteint toujours la sous-famille G_{00cc}, comme prévu.
  - Pour $|\mathcal{S}| = 2$, les états générés par l'algorithme de Grover appartiennent à G_{abc0}, L_{00c_2}, L_{ab0_2}, Gr_8 et Gr_4.
  - Pour $|\mathcal{S}| = 3$, on peut atteindre les sous-familles G_{abc0}, L_{00c_2}, L_{aa0_2}, $L_{0_2b_2}$ et $L_{a_20_{3\oplus\bar{1}}}$.
- **Cas critique ($|\mathcal{S}| = \frac{N}{4}$) :** Pour $|\mathcal{S}| = 4$, qui est le cas critique (toutes les amplitudes sont envoyées sur 0, sauf pour les états marqués, et l'algorithme converge après une itération), on peut atteindre toutes les familles ou strates associées à tous les états qui peuvent être écrits sous la forme d'une somme de 4 états de base : G_{00cc}, G_{a000}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{a00_2}, $L_{0_2b_2}$, et de la strate Gr_8 à la strate Gr_1.
- **Cas exceptionnel ($|\mathcal{S}| > \frac{N}{4}$) :**
  - Pour $|\mathcal{S}| = 5$, les sous-familles G_{abc0}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{ab0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$ et $L_{a_20_{3\oplus\bar{1}}}$ peuvent être obtenues à l'aide de l'algorithme de Grover.
  - Pour $|\mathcal{S}| = 6$, l'algorithme de Grover peut générer des états qui appartiennent à G_{abcd}, G_{abc0}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{ab0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$, L_{a_4}, $L_{a_20_{3\oplus\bar{1}}}$, Gr_8 et Gr_4.
  - Pour $|\mathcal{S}| = 7$, nous pouvons obtenir les familles suivantes : G_{abcd}, G_{abc0}, G_{00cc}, G_{ab00}, L_{00c_2}, L_{aa0_2}, L_{ab0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$, $L_{a_20_{3\oplus\bar{1}}}$.
  - For $|\mathcal{S}| = 8$, les états générés appartiennent à G_{abc0}, G_{00cc}, G_{ab00}, L_{00c_2}, L_{aa0_2}, $L_{a_2b_2}$, $L_{0_2b_2}$, $L_{a_20_{3\oplus\bar{1}}}$, Gr_8, Gr_7, Gr_4, Gr_2 and Gr_1.

On se limitera ici à l'étude des cas jusqu'à $|\mathcal{S}| \leq 8$, par argument de symétrie. Nous

tenons à préciser ici que l'état $|W_4\rangle$ (correspondant à la strate Gr_5) n'est pas atteint par les états générés par l'algorithme de Grover, sauf dans le cas critique. Les autres strates du cône nilpotent qui ne sont pas atteintes sont les strates Gr_6 et Gr_3. De plus, on remarque que les familles et sous-familles associées L_{abc_2}, L_{ab_3}, L_{0b_3} et L_{a0_3} ne sont pas générées par l'algorithme de Grover, quelque soit la combinaison d'éléments marqués choisie. Le Tableau 3.6 présente un exemple d'ensembles d'éléments marqués $\mathcal{S}$ pour chaque famille, sous famille ou strate nilpotente atteinte, et pour différents nombres d'éléments marqués.

Famille ou strate	Ensembles $\mathcal{S}$
G_{abcd}	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0101\rangle, \|1010\rangle, \|1111\rangle\}$
G_{abc0}	$\{\|0000\rangle, \|1111\rangle\}$
G_{00cc}	$\{\|0000\rangle\}$
G_{a000}	$\{\|0000\rangle, \|0011\rangle, \|1100\rangle, \|1111\rangle\}$
G_{ab00}	$\{\|0000\rangle, \|0011\rangle, \|1101\rangle, \|1110\rangle\}$
L_{abc_2}	—
L_{00c_2}	$\{\|0000\rangle, \|0011\rangle\}$
L_{aa0_2}	$\{\|0000\rangle, \|0101\rangle\}$
L_{a00_2}	$\{\|0000\rangle, \|0110\rangle, \|1001\rangle, \|1111\rangle\}$
L_{ab0_2}	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0101\rangle, \|1010\rangle\}$
$L_{a_2b_2}$	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0100\rangle, \|1001\rangle\}$
$L_{0_2b_2}$	$\{\|0000\rangle, \|0001\rangle, \|0110\rangle\}$
L_{ab_3}	—
L_{0b_3}	—
L_{a0_3}	—
L_{a_4}	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0101\rangle, \|0110\rangle, \|1101\rangle\}$
$L_{a_20_{3\oplus\bar{1}}}$	$\{\|0000\rangle, \|0001\rangle, \|1110\rangle\}$
Gr_8	$\{\|0000\rangle, \|0111\rangle\}$
Gr_7	$\{\|0000\rangle, \|0001\rangle, \|0110\rangle, \|1011\rangle\}$
Gr_6	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|1100\rangle\}$
Gr_5	$\{\|0000\rangle, \|0011\rangle, \|0101\rangle, \|1001\rangle\}$
Gr_4	$\{\|0000\rangle, \|0001\rangle\}$
Gr_3	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0100\rangle\}$
Gr_2	$\{\|0000\rangle, \|0001\rangle, \|0110\rangle, \|0111\rangle\}$
Gr_1	$\{\|0000\rangle, \|0001\rangle, \|0010\rangle, \|0011\rangle\}$

TABLE 3.6 – Exemple d'ensembles d'éléments marqués $\mathcal{S}$ et les familles ou strates atteintes correspondantes par l'algorithme de Grover dans le cas des 4-qubits.

3.4 Étude quantitative

Dans cette sous-section, on se propose d'étudier l'intrication d'un point de vue quantitatif, en observant l'évolution de certaines mesures de l'intrication ou de non-localité (voir Section 2.2.3) tout au long de l'algorithme de Grover. Nous comparons également nos résultats obtenus par rapport aux précédentes études menées sur l'évolution de la quantité d'intrication au cours de l'algorithme (voir Section précédente 3.1).

Les résultats présentés dans cette sous-section proviennent majoritairement de travaux déjà publiés dans un journal international [133, 147, 81]. Dans ces travaux nous choisissons d'utiliser l'hyperdéterminant comme une mesure potentielle de l'intrication, ainsi que d'évaluer les polynômes de Mermin afin de pouvoir détecter ou quantifier l'intrication ou la non-localité pour un état quantique, notamment pour les états à 4-qubits. Nous utilisons principalement l'algorithme de promenade aléatoire pour les optimisations numériques (voir Annexe A.8).

3.4.1 Évaluation de Mermin

Dans un premier temps, on se propose d'utiliser les polynômes de Mermin afin de mesurer ou de quantifier l'intrication à travers l'observation du degré de violation des inégalités de Mermin. La définition des polynômes de Mermin et la façon dont ils peuvent être utilisés pour détecter ou quantifier l'intrication est donnée en Chapitre 2 Section 2.2.3.

Nous rappelons que nous notons A_i un observable sur un qubit, pouvant toujours être défini comme une combinaison des matrices de Pauli [81] à savoir $A_i = a_{i,1}X + a_{i,2}Y + a_{i,3}Z$, avec la condition de normalisation usuelle ${a_{i,1}}^2 + {a_{i,2}}^2 + {a_{i,3}}^2 = 1$.

Nous nous plaçons ici dans le contexte usuel d'application de l'algorithme de Grover, c'est à dire que le nombre d'éléments marqués est égal à 1, et on notera $\mathcal{S} = \{|x_0\rangle\}$. De plus, nous adoptons une approche particulière pour l'évaluation des polynômes de Mermin. Nous évaluons les polynômes de Mermin en utilisant les mêmes paramètres, et donc en considérant le même dispositif de mesure ou les mêmes observables, et ce de manière identique pour tous les états générés par l'algorithme de Grover. Par ailleurs, nous considérons les 2 mêmes observables A_1 et A_2 pour toutes les particules, restreignant les paramètres définissant le polynôme de Mermin au nombre de 6, regroupés dans le vecteur noté $V = (a_{1,1}, a_{1,2}, a_{1,3}, a_{2,1}, a_{2,2}, a_{2,3})$.

Ces paramètres choisis correspondent aux coefficients, définissant les 2 observables A_1 et A_2, qui maximisent le polynôme de Mermin pour l'état $|\Psi_{ent}\rangle = \frac{1}{K}\left(|x_0\rangle + |+\rangle^{\otimes n}\right)$, avec K le coefficient de normalisation adéquat. En effet, ce choix d'état $|\Psi_{ent}\rangle$ intervient en cohérence avec l'interprétation géométrique des états générés par l'algorithme de Grover (voir Section 3.2). Le maximum de l'intrication dans l'algorithme de Grover étant observé à mi-chemin entre la première itération et l'itération optimale, l'état de Grover $\left|\psi_{k_{opt}/2}\right\rangle$ sera d'autant plus proche de l'état $|\Psi_{ent}\rangle$ à mesure que n augmente.

Par ailleurs, l'état $|\Psi_{ent}\rangle$ de rang 2 est défini comme la superposition équilibrée des états $|x_0\rangle$ et $|+\rangle^{\otimes n}$. L'état $|+\rangle^{\otimes n}$ fait intervenir l'état $|x_0\rangle$ dans son écriture, et la projection $\langle x_0|+\rangle^{\otimes n}$ tend vers 0 lorsque n tend vers l'infini. Ceci suggère qu'asymptotiquement, l'état $|\Psi_{ent}\rangle$ se comporterait comme l'état $|GHZ_n\rangle$, pour n grand. Cette observation doit être mise en relation avec le fait que les états de type $|GHZ_n\rangle$ sont ceux qui maximisent la violation des inégalités définies par les polynômes de Mermin [188, 76, 6].

Pour la mise en place pratique des calculs, nous choisissons de considérer l'état $|0\rangle^{\otimes n}$ comme l'élément recherché lors de l'exécution de l'algorithme de Grover. Dans ce cas, l'optimisation des paramètres liés aux observables permettant de maximiser la valeur du polynôme de Mermin semble donner un vecteur V_{opt} arborant toujours la même forme symétrique, à savoir un vecteur de la forme $V_{opt} = (a_{1,1}, a_{1,2}, a_{1,1}, a_{2,1}, a_{2,2}, a_{2,1})$, sous les notations précédentes.

Exemple 6. Lorsque l'élément $|00000000\rangle$ est recherché, la valeur maximale $\mu_8(|\Psi_{ent}\rangle)$ du polynôme de Mermin pour l'état $|\Psi_{ent}\rangle$ est obtenue, par optimisation numérique, pour le jeu de paramètres

$$V_{opt,8} = (-0.18885, -0.15053, -0.18885, -0.50674, 0.62644, -0.50674) \ .$$

Le vecteur $V_{opt,8}$ est ensuite utilisé pour évaluer le polynôme de Mermin pour les états à 8-qubits générés par l'algorithme de Grover. ♢

Ainsi, pour chaque état généré par l'algorithme de Grover pour les itérations $k \in [\![0, k_{opt}]\!]$, on évalue le polynôme de Mermin sur l'état correspondant, en ayant préalablement déterminé les coefficients optimisés V_{opt} pour n fixé. Ceci est ensuite répété pour différentes tailles de systèmes à n-qubits, plus précisément entre 4 et 12 qubits. C'est notamment le fait de fixer les paramètres du polynôme de Mermin afin de maximiser ce dernier pour l'état $|\Psi_{ent}\rangle$ qui permet de réduire les ressources nécessaires au calcul de l'évaluation de Mermin pour les états de Grover. L'ensemble des résultats est représenté, sous la forme d'un graphique annoté, en Figure 3.4.

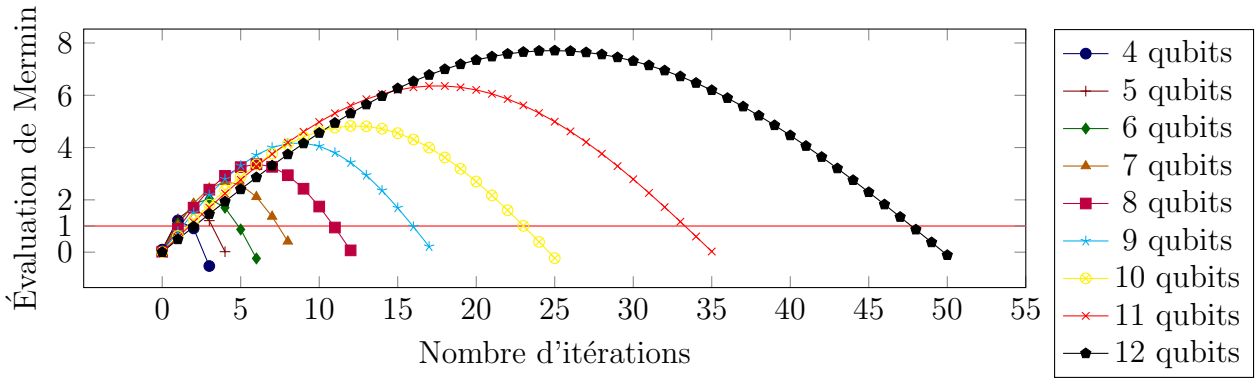


FIGURE 3.4 – Degré de violation des inégalités de Mermin tout au long de l'exécution de l'algorithme de Grover pour $4 \leq n \leq 12$ qubits [81].

Remarque 23. Pour chaque valeur de n, nous observons une violation de la borne classique, impliquant la présence de non-localité dans les états générés par l'algorithme de Grover. Ceci contraste notamment avec la conclusion des travaux de Batle *et al.* [23]. De plus, on observe un comportement du degré de violation des inégalités Mermin assez similaire à celui de la mesure géométrique de l'intrication.

3.4.2 L'hyperdéterminant $2 \times 2 \times 2 \times 2$

L'hyperdéterminant peut aussi être évalué pour mesurer la quantité d'intrication présente pour les états générés par l'algorithme de Grover. L'évaluation de cette mesure n'est pertinente que pour les états non-dégénérés, c'est-à-dire les états en dehors de la variété duale X^*.

On trace en Figure 3.5 et 3.6 les courbes représentant l'évolution de la valeur absolue de l'hyperdéterminant pour deux ensembles d'éléments marqués différents, permettant à l'algorithme de Grover de générer des états n'annulant pas l'hyperdéterminant (et rendant donc pertinent les courbes).

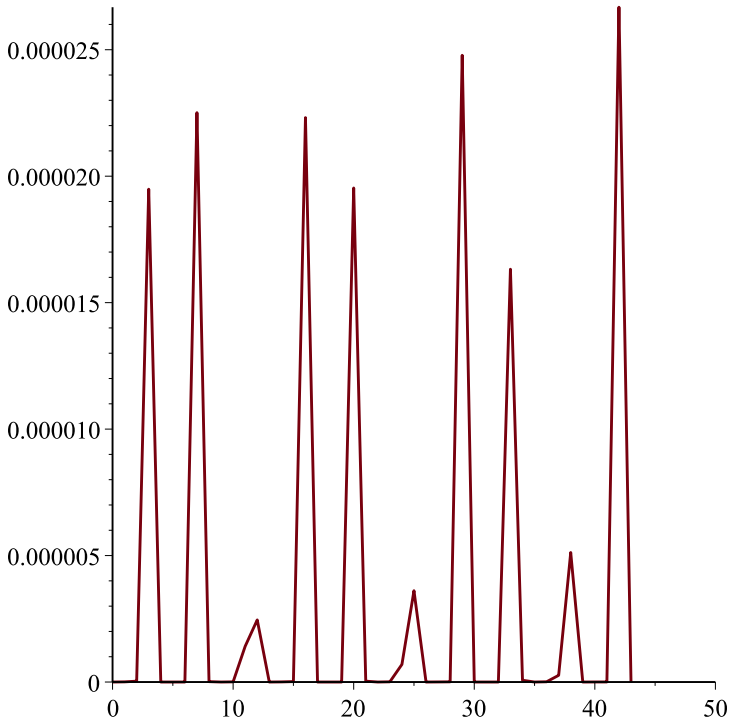


Figure 3.5 – Évolution de la valeur absolue de l'hyperdéterminant pour les 4-qubits en fonction du nombre d'itérations dans l'algorithme de Grover, pour l'ensemble d'éléments marqués $\mathcal{S} = \{|0000\rangle, |1111\rangle\}$. Les états générés appartiennent à la famille G_{abc0}.

Nous choisissons de tracer cette évolution sur un nombre d'itérations supérieur à celui d'une application normale de l'algorithme de Grover, afin de mettre notamment en évidence l'aspect périodique de l'évolution de l'intrication au cours de l'algorithme de Grover, et ce déplacement de va et vient sur la droite projective entre l'état $|+\rangle^{\otimes n}$ et l'état $\frac{1}{\sqrt{|\mathcal{S}|}}(|x_0\rangle + \cdots + |x_{s-1}\rangle)$. On remarque également l'existence de pics de valeurs à certaines itérations, correspondant aux itérations proches de $\frac{|\mathcal{S}|k_{opt}}{|\mathcal{S}|+1}$.

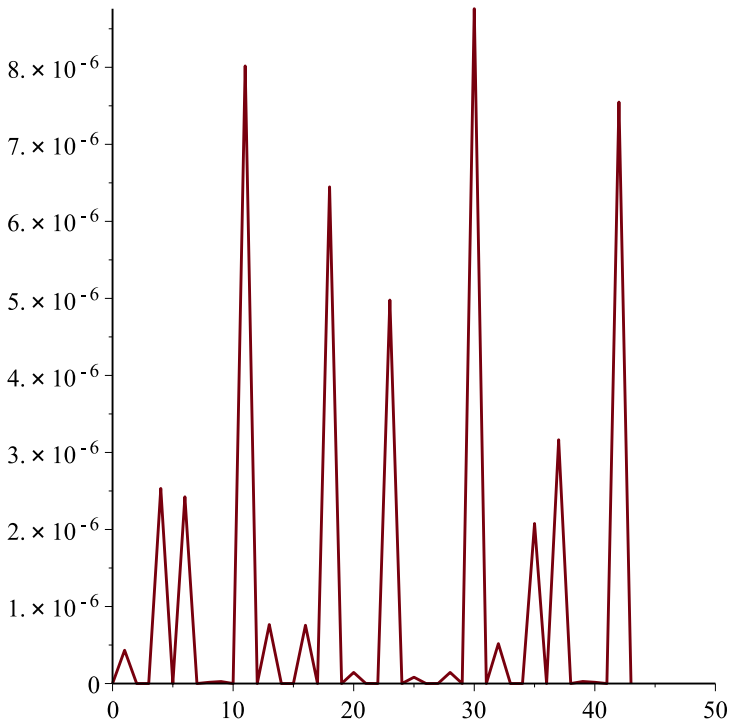


FIGURE 3.6 – Évolution de la valeur absolue de l'hyperdéterminant pour les 4-qubits en fonction du nombre d'itérations dans l'algorithme de Grover, pour l'ensemble d'éléments marqués $\mathcal{S} = \{|0000\rangle, |0001\rangle, |0010\rangle, |0101\rangle, |1010\rangle, |1111\rangle\}$. Les états générés appartiennent à la famille G_{abcd}.

3.5 Synthèse et discussions

Les résultats issus de l'étude quantitative de l'algorithme de Grover, en utilisant les polynômes de Mermin d'une part, permettent de mettre en évidence l'émergence de l'aspect non-local des états générés par l'algorithme de Grover, et donc la présence effective d'intrication dans ce processus de calcul quantique. De plus, l'interprétation géométrique et l'étude de la classe d'intrication des états générés par l'algorithme de Grover montre également que ce ne sont pas des états séparables. Ceci vient alors encore apporter une confirmation de ce résultat bien connu [45, 146, 219].

La présence d'un point pivot, d'un point critique pour l'intrication [207], est aussi confirmée et mise en avant par nos travaux. En termes de mesure de l'intrication, nous observons ce point critique remarquable (maximum) dans la courbe d'évolution de l'intrication. Nous donnons aussi une interprétation géométrique de ce point en terme de barycentre des états marqués et de l'état initial. De plus, ceci est également confirmé d'un point de vue quantitatif [272, 226] pour les évolutions de l'hyperdéterminant ou de l'évaluation de Mermin, et est expliqué par le déplacement des points de Grover sur la variété des sécantes.

L'invariance de ce comportement de l'intrication, lorsque la dimension de l'espace

augmente, est aussi observée dans nos travaux. En effet, de manière qualitative, nous pouvons expliquer ce comportement quelque soit le nombre de qubit, en traduisant l'évolution dans l'algorithme comme un déplacement sur des variétés algébriques. De plus, nous observons pour les tracés de l'évolution de Mermin pour les différents nombres de qubits, que le comportement est toujours le même. Ceci vient confirmer les résultats établis par [226, 61, 211].

Pour un nombre fixé de qubits, il a été affirmé qu'un changement dans le nombre d'éléments marqués implique un changement dans la quantité d'intrication [61]. Ceci peut être expliqué d'un point de vue théorique car un changement dans le nombre ou le choix des éléments marqués implique un changement de la structre de l'enveloppe convexe ce qui implique nécessairement une modification de la distance à la variété des états séparables, et donc un changement dans la MGI. De plus, changer les éléments marqués, c'est changer de sécante sur laquelle on se déplace tout au long de l'algorithme, et c'est aussi changer l'état final à l'itération optimale, ce qui modifiera la quantité d'intrication en fonction de l'état final. Aussi, nous avons pu détailler les différents classes d'intrication pouvant être atteintes pour différentes configurations d'états marqués, ce qui confirme qu'il y a aussi un changement de type d'intrication. Enfin, les courbes de l'hyperdéterminant pour deux ensembles d'états marqués montrent un comportement différent de l'intrication, et une périodicité différente pour l'intrication.

La décroissance exponentielle observée pour la mesure géométrique de l'intrication [227], lorsque le nombre de qubits n augmente, est aussi expliquées à l'aide de notre interprétation en termes de variétés de sécantes, notamment en considérant le rapport de la dimension de la variété des sécantes et de l'espace ambiant, impliquant une modification de la distance à la variété des états séparables.

D'autre part, l'aspect périodique de l'intrication, mis en avant dans un travail de Ye *et al.* [289], est aussi observé lors de l'étude de l'évolution de la valeur absolue de l'hyperdéterminant pour le cas des 4-qubits.

Dans le cas critique de l'application de l'algorithme de Grover, lorsque $|\mathcal{S}| = \frac{N}{4}$ et lorsque la taille de la base de données N est divisible par 4, l'algorithme se termine en effet au bout d'une seule itération (et c'est pourquoi le cas est qualifié de critique, car c'est un cas exceptionnel) et l'état généré est exactement une superposition des états recherchés. Les amplitudes des états non-recherchés sont éliminées après seulement l'application d'une porte d'Oracle et d'une porte de Diffusion. Ainsi, tout état pouvant s'écrire comme la somme de $\frac{N}{4}$ (lorsque 4 divise N) éléments de la base canonique représente une orbite (strate ou famille d'orbites), sous l'action du groupe SLOCC, qui peut être atteinte par l'algorithme de Grover [133, 147]. D'un point de vue pratique, l'algorithme de Grover peut alors servir à générer des points de certaines orbites, notamment des points génériques de la variété des sécantes $\sigma_{\frac{N}{4}}(X)$.

Enfin, lors de l'étude des classes d'intrication atteintes par l'algorithme de Grover, notamment pour les cas considérés, il est apparu que certaines classes d'intrication n'étaient jamais générées par l'algorithme de Grover, ou seulement dans le cas critique. Le fait que l'état $|W\rangle$ ne soit pas généré dans le cas des 3-qubits est intéressant, et

implique que l'algorithme de Grover ne peut générer des points lisses de la variété des tangentes $\tau(X)$. Ceci est d'autant plus intéressant que la notion de variété tangente semble aussi toujours intervenir pour les états n'étant pas générés par l'algorithme de Grover dans les autres exemples étudiés. En effet, dans le cas $2 \times 3 \times 3$ ce sont les orbites $\mathcal{O}_5$ et $\mathcal{O}_{15}$ qui ne sont pas atteintes par l'algorithme. Or l'orbite $\mathcal{O}_5$ correspond à la variété des tangentes $\tau(X)$ et l'orbite $\mathcal{O}_{15}$ à la variété $T(X, \tau(X))$. Dans le cas des 4-qubits, les familles L_{abc_2} et L_{ab_3} ne sont pas atteintes pas l'algorithme, et ces familles correspondent respectivement aux variétés X^* et $\tau(X)^*$. Les strates Gr_5, Gr_6 et Gr_3 ne sont atteintes que dans le cas critique, et correspondent respectivement aux variétés $\tau(X)$, $Osc_3(X)$ et $\mathbb{P}_1 \times \tau(X)$ (dont la définition fait intervenir la notion de tangente). Cette observation pourrait donner une interprétation géométrique pour qualifier les états ne pouvant pas être générés par l'algorithme.

3.6 Perspectives

Une première manière de poursuivre ce travail est d'étudier les états générés par l'algorithme pour d'autres dimensions des systèmes quantiques. Par exemple, il est possible d'étudier le cas des 3-qutrits, où une classification sous forme de familles existe aussi (voir Section 5.3.1). On peut également envisager d'étudier le cas des 5-qubits, ou de dimensions supérieures. Malgré le fait qu'une classification complète n'existe pas, des outils partiels comme ceux proposés en Chapitre 5 et 7 pourraient être envisagés.

Ces études pourraient permettre d'avoir une vision plus globale de l'intrication intervenant dans l'algorithme de Grover, dans l'optique de pouvoir généraliser à des dimensions supérieures certaines observations ou résultats mis en évidence dans ce chapitre. D'une part, ceci permettrait de prévoir quel type d'intrication peut être généré par l'algorithme de Grover, en fonction du nombre de qubits et de la nature des éléments marqués. Cela peut permettre aussi de prévoir pour quelle itération l'état généré par l'algorithme atteint le maximum possible de l'intrication, en fonction du nombre de qubits et des éléments marqués.

D'autre part, ceci peut également fournir des informations sur les états et les types d'intrication que l'algorithme de Grover ne peut générer. En effet, il serait intéressant d'étudier plus en profondeur le lien entre les classes d'intrication non-atteintes par l'algorithme de Grover, ou seulement atteintes dans le cas critique, et les variétés des tangentes associées. Enfin, une réflexion plus profonde sur la nature des états intriqués mis en œuvre dans l'algorithme (et ceux non-atteints) et le gain en complexité des algorithmes quantiques pourrait être menée à partir de ces observations et résultats.

Chapitre 4

Algorithme de Shor et Intrication

"A classical computation is like a solo voice — one line of pure tones succeeding each other. A quantum computation is like a symphony — many lines of tones interfering with one another", Seth Lloyd.

Dans ce chapitre, nous nous intéressons à l'algorithme de Shor, et comment l'intrication s'y manifeste. Plus précisément, nous étudions la "partie quantique" de l'algorithme de Shor, c'est à dire l'algorithme de recherche de la période (voir Section 1.2.2 pour une introduction à l'algorithme de Shor). Nous présentons tout d'abord les précédents travaux sur cette question puis, comme cela a été fait pour l'algorithme de Grover (voir Chapitre 3), nous tentons de qualifier et de quantifier l'intrication au sein de l'algorithme de recherche de la période. L'ensemble des résultats présentés dans ce chapitre ont été publiés dans les articles suivants [147, 81].

4.1 État de l'art

Au début des années 2000, Jozsa *et al.* ont suggéré que l'intrication quantique joue un rôle majeur dans l'efficacité des calculs quantiques [96, 154]. Il a été en effet prouvé que l'intrication quantique est bien présente dans l'algorithme de Shor, que ce soit du point de vue théorique [213, 154, 242, 156, 194] ou expérimental [166, 175].

La majorité des études en rapport avec l'intrication et l'algorithme de Shor portent sur l'intrication entre les deux registres quantiques de l'algorithme. En 2001, Parker et Planio [213] ont regardé l'intrication bipartite moyenne, en utilisant la négativité logarithmique comme mesure de l'intrication, à chaque étape de l'algorithme. Les états de l'algorithme sont définis par les opérations *controlled-*U_α (impliqué dans l'opération d'exponentiation modulaire). Les auteurs ont prouvé que l'intrication existe dans l'algorithme et que la quantité d'intrication augmente vers la fin de l'algorithme. Ils ont aussi démontré que si l'on cherche à réduire l'intrication en introduisant des états plus mixtes dans le qubit de contrôle, alors on réduit l'efficacité des calculs.

Un an plus tard, Jozsa et Linden publièrent un article portant sur le rôle de l'intrication dans l'accélération des calculs quantiques [154]. Ils y discutent les différences entre le calcul classique et quantique, et de la possibilité de simuler classiquement et

de manière efficace un calcul quantique. En particulier, il a été affirmé que si on ne peut pas classiquement simuler de manière efficace, et en un temps polynomial, un algorithme quantique, alors l'intrication quantique est présente dans ce même algorithme quantique. C'est le cas de l'algorithme de Shor, et la présence d'intrication est prouvée dans ce travail en considérant des états à "progression arithmétique" (équivalents aux états périodiques), et en considérant le fait que ces états ne sont pas p-bloqués.

En 2004, Orus et Latorre [207] ont étudié le comportement de l'intrication dans l'algorithme de Shor lors d'un changement d'échelle, prouvant analytiquement la nécessité d'utiliser une quantité exponentiellement grande d'intrication entre les deux registres, après l'étape d'exponentiation modulaire. Ceci implique l'impossibilité d'une simulation classique efficace en utilisant le protocole proposé par Vidal [264].

En 2005, Shimoni *et al.* ont utilisé la Mesure Groverienne de l'Intrication pour caractériser les états quantiques générés par l'algorithme de Shor [242]. À chaque étape de la Transformée de Fourier Quantique (après chaque porte *controlled-*R_k, la porte d'Hadamard n'affectant pas l'intrication), ils évaluent la Mesure Groverienne de l'Intrication, et ceci pour des états quantiques généraux ou pour les états périodiques de l'algorithme de Shor. Pour des états factorisés aléatoires, les auteurs démontrent que l'intrication reste la même après la plupart des étapes, mais que pour certaines portes *controlled-*R_k précises le taux d'intrication augmente significativement. Pour les états périodiques, leurs résultats avancent que l'intrication ne change essentiellement pas, et que les variations observées pour un nombre de qubits n petit deviennent négligeables quand n augmente.

Kendon et Munro ont publié en 2006 dans un article intitulé "*Entanglement and its role in Shor's algorithm*" [156], où ils s'intéressent à l'intrication impliquée dans l'algorithme de Shor en décomposant la porte U_f et en considérant la TFQ^{-1} comme une seule porte. Ils se focalisent tout d'abord sur l'intrication entre le premier et le second registre, et dans un second temps étudient l'intrication dans le premier registre. Une étude quantitative de l'intrication est effectuée dans cet article, et quelques mesures de l'intrication comme l'entropie des sous-systèmes (*entropy of subsystems* entre les deux registres), la négativité ou bien l'*entanglement of formation* (pour le premier registre) sont utilisées. Selon les auteurs, après l'exponentiation modulaire, l'intrication entre les deux registres ne peut augmenter durant l'application de Transformée de Fourier Quantique inverse. De plus, toujours selon les auteurs, l'intrication dans le premier registre ne peut qu'être généré ou déplacée, mais pas diminuée. Les auteurs font aussi remarquer que plus la période r est proche d'une puissance de 2, plus la valeur de la différence dans l'entropie moyenne ΔE_1 avant et après la TFQ^{-1} devient faible. Lorsque r est une puissance de 2, alors TFQ^{-1} implique que $\Delta E_1 = 0$ dans tout les cas.

En 2007, certaines expériences pratiques de l'algorithme de Shor ont pu être implémentées. Lanyon *et al.* [166] ont implémenté une version compilée de l'algorithme de Shor en utilisant des systèmes photoniques. Ils ont prouvé l'existence de l'intrication au cours de l'algorithme par tomographie des états quantiques, et que l'intrication est impliquée dans les opérations arithmétiques. La même année, Lu *et al.* [175] implémentent l'algorithme de factorisation de Shor en utilisant aussi des photons pour

modéliser les qubits. L'expérience est mise en place pour des 4-qubits photoniques, et l'intrication *genuine* est détectée durant l'algorithme, entre le premier et le second registre.

Trois ans plus tard, Most, Shimoni et Biham ont publié un travail en rapport avec l'intrication des états périodique, la Transformée de Fourier Quantique et l'algorithme de Shor [194]. Ils mettent en évidence l'importance et le rôle des états périodiques durant l'algorithme. Ils analysent aussi l'intrication des états périodiques en regardant comment ces états sont affectés par la Transformée de Fourier Quantique. Quelques approximations sont utilisées pour évaluer la mesure Groverienne de l'intrication pour les états périodiques. Selon les auteurs, la Transformée de Fourier Quantique ne change pas l'intrication des états périodiques, pour un nombre suffisamment grand de qubits. Nous pouvons également mentionner certains récents travaux portant sur une problématique plus ou moins similaire [93, 80, 60].

Tout ces travaux ont principalement étudié l'intrication en utilisant des mesures diverses de l'intrication, menant à une étude quantitative de l'intrication. Cela permit de donner une première vision globale concernant l'évolution de l'intrication durant l'algorithme. Dans les sections suivantes, nous présentons une étude quantitative de l'intrication en utilisant des mesures originales de l'intrication et en comparant nos résultats à ceux de la littérature. D'autre part, nous étudions également de manière plus qualitative l'intrication, en déterminant quelles sont les classes d'intrication présentes et comment elles évoluent après application de la TFQ, tentant de donner une interprétation géométrique ou des éléments de réflexion afin de compléter les précédents résultats de la littérature.

4.2 Intrication des états périodiques

Les états périodiques sont des états générés durant la première partie de l'algorithme de Shor, et sont les états sur lesquels la Transformée de Fourier Quantique sera appliquée. Par ailleurs, ces états jouent également un rôle important dans d'autres algorithmes quantiques faisant intervenir cette même transformée [194].

L'intrication est un des candidats proposés pour expliquer l'avantage que propose les algorithmes quantiques face aux performances des algorithmes classiques. L'étude de l'intrication des états périodiques devient donc indispensable pour comprendre dans quelle mesure ce phénomène apparaît et intervient tout au long de l'algorithme.

Dans cette sous-section, nous nous intéressons à l'intrication des états périodiques en tant que tels, c'est à dire avant l'application de la Transformée de Fourier Quantique. En effet, comme nous le verrons plus tard dans cette section, l'intrication des états périodiques avant l'application de la TFQ jouera un rôle prépondérant en ce qui concerne le type ou la quantité d'intrication après la TFQ. Nous étudions de manière exhaustive les classes d'intrication associées aux états périodiques pour les systèmes à 3-qubits et 4-qubits, et proposons un certain nombre de généralisation et de règles concernant le type d'intrication, en fonction du shift et de la période des états périodiques, à partir des patterns observés.

4.2.1 Cas des 3-qubits

Dans cette sous-section, nous étudions le type d'intrication associé à l'ensemble des états périodiques pour les systèmes à 3-qubits. Les notations utilisées ici font référence à la classification des 3-qubits présentée en Section 2.2.2. Pour chaque valeur du shift l et de la période r, nous déterminons l'orbite sous SLOCC de l'état périodique associé. Nous utilisons ici l'algorithme de classification des 3-qubits présenté en Annexe A.1. Tous les résultats obtenus sont regroupés dans la Table 4.1.

r \ l	0	1	2	3	4	5	6	7
1	$\mathcal{O}_1$	$\mathcal{O}_6$	$\mathcal{O}_4$	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$
2	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_4$	$\mathcal{O}_4$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
3	$\mathcal{O}_5$	$\mathcal{O}_5$	$\mathcal{O}_6$	$\mathcal{O}_2$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
4	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
5	$\mathcal{O}_2$	$\mathcal{O}_6$	$\mathcal{O}_2$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
6	$\mathcal{O}_4$	$\mathcal{O}_4$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
7	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$

Table 4.1 – Orbites sous SLOCC pour les états à 3-qubits periodiques, en fonction du shift l et de la période r.

En observant sur ce tableau la répartition des orbites en fonction du shift et de la période, nous pouvons établir les observations suivantes :

- Lorsque $l = 0$ et que la période prend les valeurs $r = 1$, $r = 2$ et $r = 4$, alors l'état est séparable,
- Lorsque $r = 4$, alors l'état appartient toujours à l'orbite $\mathcal{O}_1$ (état séparable),
- Tous les états présents sur l'anti-diagonale définie de $\{l = 1, r = 7\}$ à $\{l = 7, r = 1\}$, et tous les états dans la partie inférieure droite sous cette anti-diagonale appartiennent à l'orbite $\mathcal{O}_1$ (états séparables),
- Si la période prend les valeurs $r = 1$, $r = 2$, et $r = 4$, et si le shift $0 \leq l \leq r - 1$ ou $4 \leq l \leq r + 3$, alors l'état est séparable,
- Lorsque $\{l = 1, r = 1\}$, et lorsque $\{l = 0, r = 7\}$, $\{l = 1, r = 5\}$, $\{l = 2, r = 3\}$, et $\{l = 3, r = 1\}$ (anti-diagonale où l'on monte de 2 cases vers le haut quand on avance d'une case vers la droite) les états périodiques correspondants appartiennent à l'orbite $\mathcal{O}_6$, qui est l'orbite de l'état $|GHZ\rangle$,
- L'orbite $\mathcal{O}_5$ n'est atteinte que lorsque $\{l = 0, r = 3\}$ et $\{l = 1, r = 3\}$.

Une partie de ces observations peut être prévue de par l'écriture des états périodiques dans la base canonique. En effet, l'état $\left|\Psi^3_{0,7}\right\rangle$ correspond exactement à l'écriture de l'état $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, tout comme l'écriture de l'état $\left|\Psi^3_{1,2}\right\rangle$ permet de conclure que c'est un état séparable :

$$\left|\Psi^3_{1,2}\right\rangle = \frac{1}{2}\left(|001\rangle + |011\rangle + |101\rangle + |111\rangle\right) = |+\rangle^{\otimes 2}|1\rangle \ . \tag{4.1}$$

Un grande majorité de ces observations de placement des classes d'intrication sur la table en deux dimension apparaissent également lorsqu'on augmente le nombre de

qubits, et c'est notamment le cas pour les systèmes à 4-qubits. Ceci est en effet l'objet de la sous-section suivante.

4.2.2 Cas des 4-qubits

Dans cette sous-section, nous étudions le type d'intrication associé à l'ensemble des états périodiques pour les systèmes à 4-qubits. Les notations utilisées ici font référence à la classification des 4-qubits rappelée en Section 2.2.2. Pour chaque valeur du shift l et de la période r, nous déterminons la (sous) famille de Verstraete *et al.* associée ou la strate du cône nilpotent associée à l'état périodique correspondant. Tous les résultats obtenus sont regroupés dans la Table 4.2. Pour obtenir celle-ci, nous utilisons l'algorithme présenté en Annexe A.4 et déterminons la classe d'intrication pour tous les 15×15 états périodiques.

On observe alors que :

- Lorsque $l = 0$ et que la période prend les valeurs $r = 1$, $r = 2$, $r = 4$ et $r = 8$, alors l'état est séparable,
- Lorsque $r = 8$, alors l'état appartient toujours à l'orbite Gr_1 (état séparable),
- Tous les états présents sur l'anti-diagonale définie de $\{l = 1, r = 15\}$ à $\{l = 15, r = 1\}$, et tous les états dans la partie inférieure droite sous cette anti-diagonale appartiennent à l'orbite Gr_1 (états séparables),
- Si la période prend les valeurs $r = 1$, $r = 2$, $r = 4$ et $r = 8$, si le shift $0 \leq l \leq r - 1$ ou $8 \leq l \leq r + 7$, alors l'état est séparable,
- Lorsque $\{l = 1, r = 1\}$, $\{l = 7, r = 1\}$, et lorsque $\{l = 0, r = 15\}$, $\{l = 1, r = 13\}$, $\{l = 2, r = 11\}$, $\{l = 3, r = 9\}$ et $\{l = 4, r = 7\}$ (presque une moitié d'anti-diagonale) les états périodiques appartiennent à la sous-famille G_{00cc}, qui contient l'orbite de l'état $|GHZ_4\rangle$.

Nous remarquons que les observations effectuées à la sous-section précédente sont également présentes de manière équivalente pour le cas des 4-qubits. Nous proposons alors de généraliser et de formaliser ces observations aux états périodiques à n-qubits dans la sous-section suivante.

4.2.3 Cas général

Dans cette sous-section nous généralisons les observations, dans le cas des 3 et 4-qubits, concernant le type d'intrication en fonction des valeurs du shift et de la période pour les états périodiques. Nous tentons pour chaque proposition d'apporter la preuve correspondante, permettant de mettre en évidence l'aspect séparable ou non d'un état périodique, et en fournissant dans certains cas l'écriture explicite simplifiée ou factorisée d'un état périodique (afin de permettre l'identification directe du rang ou de la classe d'intrication).

Proposition 4.2.1. *Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits. Si le shift $l = 0$ et la période $r = 2^s$ divise $N = 2^n$ alors $\left|\Psi^n_{0,r}\right\rangle$ est un état séparable, et on peut l'écrire $\left|\Psi^n_{0,r}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |0\rangle^{\otimes s}$.*

l / r	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Gr_1	G_{00cc}	Gr_4	L_{00c_2}	Gr_2	L_{00c_2}	Gr_4	G_{00cc}	Gr_1	Gr_4	Gr_2	Gr_4	Gr_1	Gr_2	Gr_1	Gr_1
2	Gr_1	Gr_1	Gr_4	Gr_4	Gr_2	Gr_2	Gr_4	Gr_4	Gr_1	Gr_1	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1
3	$G_{aa(-2a)0}$	G_{abc0}	G_{abc0}	L_{a00_2}	Gr_8	Gr_8	L_{aa0_2}	Gr_6	Gr_3	Gr_3	Gr_4	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1
4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
5	G_{a000}	Gr_6	Gr_6	Gr_6	Gr_6	L_{aa0_2}	Gr_4	Gr_4	Gr_2	Gr_4	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
6	Gr_3	Gr_3	Gr_3	Gr_3	Gr_4	Gr_4	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
7	Gr_6	Gr_6	Gr_4	Gr_2	G_{00cc}	Gr_2	Gr_4	Gr_2	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
8	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
9	Gr_2	Gr_4	Gr_2	G_{00cc}	Gr_2	Gr_4	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
10	Gr_2	Gr_2	Gr_4	Gr_4	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
11	Gr_4	Gr_4	G_{00cc}	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
12	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
13	Gr_4	G_{00cc}	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
14	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
15	G_{00cc}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1

Table 4.2 – Familles de Verstraete *et al.* et strates du cône nilpotent pour les états à 4-qubits periodiques, en fonction du shift l et de la période r.

Démonstration. Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits, et soit $N = 2^n$. On suppose que le shift $l = 0$, et que la période divise N. Alors il existe un entier p tel que $r \times p = N$, et donc il existe $(s, q) \in \mathbb{N}^2$ tel que $r = 2^s$ et $p = 2^q$. On rappele que $\left|\Psi^n_{0,r}\right\rangle$ peut être exprimé comme

$$\left|\Psi^n_{0,r}\right\rangle = \frac{1}{\sqrt{A}} \sum_{i=0}^{A-1} |0 + ir\rangle, \quad \text{avec } A = \left\lceil \frac{N-0}{r} \right\rceil = p \ , \tag{4.2}$$

alors

$$\left|\Psi^n_{0,r}\right\rangle = \frac{1}{\sqrt{p}} \big(|0\rangle + |r\rangle + |2r\rangle + \cdots + |(p-1)r\rangle \big) \ . \tag{4.3}$$

Lorsque la période r est égale à N, on obtient $A = \left\lceil \frac{N-0}{r} \right\rceil = 1$ état de base dans l'écriture de $\left|\Psi^n_{0,r}\right\rangle$, qui est en effet $|0 \ldots 0\rangle$ en notation binaire. L'état est donc séparable et on a $\left|\Psi^n_{0,r}\right\rangle = |+\rangle^{\otimes(n-n)} \otimes |0\rangle^{\otimes n} = |0\rangle^{\otimes n}$. De plus, si la période r est égale à 1, alors nous avons tous les $A = \left\lceil \frac{N-0}{r} \right\rceil = N$ états de base dans l'écriture de l'état périodique, et on récupère l'état complètement parallélisé comme attendu : $\left|\Psi^n_{0,r}\right\rangle = |+\rangle^{\otimes(n-0)} \otimes |0\rangle^{\otimes 0} = |+\rangle^{\otimes n}$.

On s'intéresse maintenant au cas où $1 < r < N$, c'est à dire lorsque $2 \leq r \leq \frac{N}{2}$. L'état périodique associé est une somme de p états de base, et p est pair, alors on pourra toujours séparer en deux parties l'écriture de l'état périodique :

$$\left|\Psi^n_{0,r}\right\rangle = \frac{1}{\sqrt{p}} \big(\underbrace{|0\rangle + |r\rangle + |2r\rangle + \cdots + \left|\big(\tfrac{p}{2} - 1\big)r\right\rangle}_{\frac{p}{2} \text{ termes}} + \underbrace{\left|\tfrac{p}{2}r\right\rangle + \cdots + |(p-1)r\rangle}_{\frac{p}{2} \text{ termes}} \big) \ . \tag{4.4}$$

On peut aisément voir que nous avons toujours les états $|0\rangle$ et $\left|\frac{p}{2}r\right\rangle = \left|\frac{N}{2}\right\rangle$ dans les parties de l'état périodique, et ces états de base peuvent être respectivement écrits en notation binaire sous la forme $|00 \ldots 0\rangle$ et $|10 \ldots 0\rangle$. Ainsi, en fonction de la période r, il restera (ou pas) d'autres termes dans chaque partie, mais nous pouvons toujours ré-écrire l'état périodique comme suit :

$$\begin{aligned} \left|\Psi^n_{0,r}\right\rangle = \tfrac{1}{\sqrt{p}} \big(& \underbrace{|0\rangle + |r\rangle + |2r\rangle + \cdots + \left|\big(\tfrac{p}{2} - 1\big)r\right\rangle}_{\frac{p}{2} \text{ termes}} \\ & + \underbrace{\left|\frac{N}{2} + 0\right\rangle + \left|\frac{N}{2} + r\right\rangle + \left|\frac{N}{2} + 2r\right\rangle + \cdots + \left|\frac{N}{2} + \big(\tfrac{p}{2} - 1\big)r\right\rangle}_{\frac{p}{2} \text{ termes}} \big) \ . \end{aligned} \tag{4.5}$$

De ce fait, l'état périodique peut être exprimé comme

$$\left|\Psi^n_{0,r}\right\rangle = |+\rangle \otimes \frac{1}{\sqrt{2^{q-1}}} \left(|0\rangle + |r\rangle + |2r\rangle + \cdots + \left|\big(\tfrac{p}{2} - 1\big)r\right\rangle \right) = |+\rangle \otimes \left|\Psi^{n-1}_{0,r}\right\rangle \ . \tag{4.6}$$

À présent, si l'on considère l'état $\left|\Psi_{0,r}^{n-1}\right\rangle$, on peut répéter le même processus jusqu'à ce qu'il ne reste qu'un seul état dans la décomposition en somme de l'état périodique. Ce cas arrive lorsque $A = 1$, c'est à dire lorsque le nombre de qubits de l'état périodique considéré (le facteur droit du produit tensoriel dans l'Équation (4.6)) est égal à s. Ce processus est donc répété $q = n - s$ fois, et au final, on récupère l'état séparable :

$$\left|\Psi_{0,r}^{n}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |0\rangle^{\otimes s} \ . \tag{4.7}$$

□

Proposition 4.2.2. *Soit $\left|\Psi_{l,r}^{n}\right\rangle$ un état périodique à n-qubits. Si la période r est égale à $\frac{N}{2} = 2^{n-1}$ alors, pour toutes les valeurs possibles du shift l, $\left|\Psi_{l,r}^{n}\right\rangle$ est un état séparable.*

Démonstration. Soit $\left|\Psi_{l,r}^{n}\right\rangle$ un état périodique à n-qubits, et soit $N = 2^n$. On suppose que la période r est égale à $\frac{N}{2}$. L'état périodique ne contient alors que $A = \left\lceil \frac{N-l}{\frac{N}{2}} \right\rceil$ états de base dans son écriture. Si le shift satisfait la condition $0 \leq l < \frac{N}{2}$ alors il y a aura $A = 2$ éléments, sinon si $\frac{N}{2} \leq l < N$ alors n'y aura que $A = 1$ seul élément.

Dans le second cas, le seul élément dans l'état périodique sera $|l\rangle$ et donc il est clair que l'état périodique est séparable. Dans le premier cas, on peut ré-écrire l'état périodique sous la forme :

$$\left|\Psi_{l,\frac{N}{2}}^{n}\right\rangle = \frac{1}{\sqrt{2}}\left(|l\rangle + \left|l + \frac{N}{2}\right\rangle\right) = |+\rangle \otimes |l\rangle \ , \tag{4.8}$$

qui est en effet aussi un état séparable.

□

Proposition 4.2.3. *Soit $\left|\Psi_{l,r}^{n}\right\rangle$ un état périodique à n-qubits, et soit $N = 2^n$. Si $l + r \geq N$ alors $\left|\Psi_{l,r}^{n}\right\rangle$ est séparable.*

Démonstration. Du fait que $l + r \geq N \iff 1 \geq \frac{N-l}{r}$, on peut en déduire que le nombre d'états de base nécessaires pour écrire $\left|\Psi_{l,r}^{n}\right\rangle$ sera égal à $A = \left\lceil \frac{N-l}{r} \right\rceil = 1$, ce qui implique que l'état est séparable. □

Proposition 4.2.4. *Soit $\left|\Psi_{l,r}^{n}\right\rangle$ un état périodique à n-qubits. Si la période $r = 2^s$ divise $N = 2^n$ alors pour toutes les valeurs du shift, respectivement $l \in [\![0, 2^s - 1]\!]$ ou $l \in [\![\frac{N}{2}, \frac{N}{2} + 2^s - 1]\!]$, l'état $\left|\Psi_{l,2^s}^{n}\right\rangle$ est un état séparable, et il s'écrit respectivement $\left|\Psi_{l,2^s}^{n}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |l\rangle^{[s]}$ ou $\left|\Psi_{l,2^s}^{n}\right\rangle = |1\rangle \otimes |+\rangle^{\otimes(n-s-1)} \otimes |l\rangle^{[s]}$ (avec $|l\rangle^{[s]}$ l'état $|l\rangle$ écrit en notation binaire à l'aide de s bits).*

Démonstration. Soit $\left|\Psi_{l,r}^{n}\right\rangle$ un état périodique à n-qubits, et soit $N = 2^n$. On suppose que la période r divise N. Alors il existe un entier p tel que $r \times p = N$, et donc il existe $(s, q) \in \mathbb{N}^2$ tels que $r = 2^s$ et $p = 2^q$. De ce fait r est une puissance de 2.

Il en résulte que la notation binaire de r est composée d'un unique digit à '1', et de $n-1$ digits à '0'. Il est connu que pour $r = 2^s$, le digit '1' se trouve à la s-ième position. Ainsi, tous les multiples de r, qui sont en fait une somme du même nombre binaire r,

peuvent être écrits avec des '0' et des '1' à gauche du s-ième digit, et uniquement des '0' a droite du s-ième digit (si on suppose que le bit de poids fort est placé à gauche).

On s'intéresse tout d'abord au premier cas, lorsque $l \in [\![0, 2^s - 1]\!]$. En supposant que le shift satisfasse la condition $0 \leq l < r = 2^s$, on peut démontrer que le nombre de termes dans l'écriture de $\left|\Psi^n_{l,r}\right\rangle$ est toujours égal à $A = \left\lceil \frac{N-l}{r} \right\rceil = p = 2^q$, et l'état périodique correspondant s'écrit :

$$\left|\Psi^n_{l,r}\right\rangle = \frac{1}{\sqrt{p}}\big(|l\rangle + |l+r\rangle + |l+2r\rangle + \cdots + |l+(p-1)r\rangle\big) \ . \tag{4.9}$$

En sachant que $l < r$, et en sachant que r et tout ses multiples ne contiennent que des '0' à droite du s-ième digit '1' (dans l'écriture binaire de r), on sait que l'on peut factoriser, par la notation binaire de l sur s digits, la somme des états de base définissant $\left|\Psi^n_{l,r}\right\rangle$. Ceci aura pour effet de retirer les s bits de poids faible dans la notation binaire de r et ses multiples, ce qui nous amène à l'expression suivante :

$$\left|\Psi^n_{l,r}\right\rangle = \frac{1}{\sqrt{p}}\big(|0\rangle + |1\rangle + |2\rangle + \cdots + |(p-1)\rangle\big)^{[n-s]} \otimes |l\rangle^{[s]} \ . \tag{4.10}$$

Le facteur de gauche de ce produit tensoriel est en effet l'état $|+\rangle^{\otimes(n-s)}$, et on peut alors conclure que si r divise N, et si $l \in [\![0, 2^s - 1]\!]$, alors on récupère un état séparable de la forme :

$$\left|\Psi^n_{l,r}\right\rangle = |+\rangle^{\otimes(n-s)} \otimes |l\rangle^{[s]} \ . \tag{4.11}$$

On s'intéresse à présent au second cas, c'est à dire lorsque $l \in [\![\frac{N}{2}, \frac{N}{2} + 2^s - 1]\!]$, qui est assez similaire au premier cas si ce n'est que l'on ajoute $\frac{N}{2}$ à la valeur du shift. Cependant, on sait que $\frac{N}{2}$ est aussi une puissance de 2, et dans notre cas cela correspond à l'état $|10\ldots0\rangle$ en notation binaire, lorsque l'on travaille avec n qubits. Ce digit '1' sera alors présent dans chaque état de base composant l'état périodique et on peut alors définir $l' = l - \frac{N}{2}$ tel que :

$$\left|\Psi^n_{l,r}\right\rangle = \frac{1}{\sqrt{\frac{p}{2}}}\Big(|l\rangle + |l+r\rangle + |l+2r\rangle + \cdots + \Big|l + \big(\frac{p}{2} - 1\big)r\Big\rangle\Big), \tag{4.12}$$

$$\left|\Psi^n_{l,r}\right\rangle = \frac{1}{\sqrt{\frac{p}{2}}}\ |1\rangle \otimes \Big(|l'\rangle + |l'+r\rangle + |l'+2r\rangle + \cdots + \Big|l' + \big(\frac{p}{2} - 1\big)r\Big\rangle\Big) \ . \tag{4.13}$$

Le facteur de droite du produit tensoriel, avec le facteur de normalisation $\frac{1}{\sqrt{\frac{p}{2}}}$, et en effet un état périodique de shift $l' \in [\![0, 2^s - 1]\!]$ et de période $r = 2^s$ pour $(n-1)$-qubits. En réutilisant le résultat issu du premier cas, on peut conclure que cet état est séparable et on peut exprimer l'état périodique global $\left|\Psi^n_{l,r}\right\rangle$ comme étant égal à :

$$\left|\Psi^n_{l,r}\right\rangle = |1\rangle \otimes |+\rangle^{\otimes(n-s-1)} \otimes \left|l - \frac{N}{2}\right\rangle^{[s]} \ . \tag{4.14}$$

□

Proposition 4.2.5. *Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits, et soit $N = 2^n$. Alors il y a au moins $\left\lfloor \frac{N-2}{3} \right\rfloor + 3$ paires (l, r) définissant des états périodiques SLOCC équivalents à $|GHZ_n\rangle$, et on peut distinguer les 3 différents cas suivants :*

- *le cas où $l = 1$ et $r = 1$,*
- *le cas où $l = \frac{N}{2} - 1$ et $r = 1$,*
- *et les $\left\lfloor \frac{N-2}{3} \right\rfloor + 1$ autres états sur l'anti-diagonale définie par la relation $2l + r = N - 1$.*

Démonstration. Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits, et soit $N = 2^n$.

Dans le premier cas, le shift est $l = 1$ et la période $r = 1$, on obtient l'état périodique suivant :

$$\left|\Psi^n_{1,1}\right\rangle = \frac{1}{\sqrt{N-1}} \sum_{x=1}^{N-1} |x\rangle = \frac{\sqrt{N}}{\sqrt{N-1}} |+\rangle^{\otimes n} - \frac{1}{\sqrt{N-1}} |0\rangle^{\otimes n} \ . \tag{4.15}$$

Cet état est un état (générique) de rang 2, appartenant aux points lisses de la variété des sécantes $\sigma_2(X)$, et en particulier est SLOCC équivalent à l'état $|GHZ_n\rangle$.

Dans le second cas, le shift est $l = \frac{N}{2} - 1$ et la période $r = 1$. En remarquant que $\left|\frac{N}{2}\right\rangle = |10 \dots 0\rangle$, et donc que $\left|\frac{N}{2} - 1\right\rangle = |01 \dots 1\rangle$, on obtient l'état périodique

$$\begin{aligned} \left|\Psi^n_{\frac{N}{2}-1,1}\right\rangle = \frac{1}{\sqrt{\frac{N}{2}+1}} \sum_{x=\frac{N}{2}-1}^{N-1} |x\rangle = \frac{1}{\sqrt{\frac{N}{2}+1}} \Big(& |011 \dots 1\rangle + |100 \dots 0\rangle \\ & + |10 \dots 01\rangle + \dots + |111 \dots 1\rangle \Big) \ , \end{aligned} \tag{4.16}$$

qui peut aussi être exprimé comme

$$\left|\Psi^n_{\frac{N}{2}-1,1}\right\rangle = \frac{1}{\sqrt{\frac{N}{2}+1}} \Big(|011 \dots 1\rangle + \sqrt{\frac{N}{2}} |1\rangle \otimes |+\rangle^{\otimes n-1} \Big) \ , \tag{4.17}$$

et cet état est aussi SLOCC équivalent à $|GHZ_n\rangle$.

Pour le troisième cas, nous nous intéressons à l'anti-diagonale dont le "point de départ" est l'état définit par $\{l = 0, r = N - 1\}$ et progressant vers le haut et la droite du tableau en ajoutant un au shift l (déplacement d'une case vers la droite) et en retirant 2 à la période r (déplacement de 2 cases vers le haut). Cette anti-diagonale est alors définie par les équations suivantes :

$$\begin{cases} l = k \\ r = N - 1 - 2k \end{cases} \quad \text{with } k \in [\![0, \frac{N}{2} - 1]\!] \ . \tag{4.18}$$

Nous avons déjà démontré que l'état tout en haut à droite de cette anti-diagonale $\{l = \frac{N}{2} - 1, r = 1\}$ est SLOCC équivalent à $|GHZ_n\rangle$, et on peut facilement prouver que l'état tout en bas à gauche de l'anti-diagonale $\{l = 0, r = N - 1\}$ est en fait la

définition de l'état GHZ généralisé $|GHZ_n\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\big)$. La partie intéressante est de déterminer ce qu'il se passe au milieu de l'anti-diagonale.

En effet, on peut déduire à partir des équations de l'anti-diagonale que les états appartenant à celle-ci vérifient $2l + r = N - 1$. De plus, nous savons que l'état en bas à gauche de l'anti-diagonale $\{l = 0, r = N - 1\}$ ne possède que 2 états de base dans son écriture. Par conséquent, on peut remarquer que si un état périodique ne possède que deux états de base dans son écriture, alors il satisfait la condition de l'anti-diagonale $2l + r = N - 1$, et donc l'état est SLOCC équivalent à l'état $|GHZ_n\rangle$. En effet, cet état périodique que l'on va noter $|\Psi\rangle$ ne possède que 2 états de base et peut être écrit

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|l\rangle + |l + r\rangle\big) \ . \tag{4.19}$$

Par ailleurs, nous rappelons que le shift l et la période r doivent satisfaire la condition $2l + r = l + (l + r) = N - 1$. Si on travaille en notation binaire, et en notant que $N-1 = 2^n-1$ est toujours écrit avec uniquement des digits '1' dans sa notation binaire, on peut en conclure que les deux nombres binaires l et $l+r$ sont des compléments (par rapport à $N = 2^n$). Ainsi, l'état $|\Psi\rangle$ est par définition équivalent à l'état $|GHZ_n\rangle$.

On peut se demander : combien d'états satisfont ces conditions pour les états périodiques ? Afin d'apporter une réponse, on s'intéresse à la condition en prêtant attention au nombre d'états de base dans les états périodiques considérés. Nous devons avoir $A = \left\lceil \frac{N-l}{r} \right\rceil = 2$ états de base dans l'écriture de l'état périodique, ce qui est équivalent à l'inéquation

$$1 < \frac{N - l}{r} \leq 2 \ . \tag{4.20}$$

Si on substitue à présent l et r par les équations définissant l'anti-diagonale, alors on obtient l'inéquation suivante :

$$1 < \frac{N - k}{N - 1 - 2k} \leq 2 \ . \tag{4.21}$$

En résolvant l'inéquation en k et en oubliant l'opération d'arrondissement, on obtient le résultat suivant :

$$-1 < k \leq \frac{N - 2}{3} \ . \tag{4.22}$$

En replaçant notre inéquation dans le contexte des nombres entiers, alors nous avons prouvé que pour $k \in [\![0, \left\lfloor \frac{N-2}{3} \right\rfloor]\!]$ l'état périodique défini par $l = k$ et $r = N - 1 - 2k$ ne possède que deux états de base dans son écriture.

Enfin, le nombre d'états équivalents à $|GHZ_n\rangle$ sur l'anti-diagonale est égal à $\left\lfloor \frac{N-2}{3} \right\rfloor + 1$, sans comptabiliser le cas où $\{l = \frac{N}{2} - 1, r = 1\}$. En d'autres termes, de l'état $\{l = 0, r = N - 1\}$ à l'état $\{l = \left\lfloor \frac{N-2}{3} \right\rfloor, r = N - 1 - 2\left\lfloor \frac{N-2}{3} \right\rfloor\}$, tous les états sur l'anti-diagonale précédemment définie sont SLOCC équivalents à $|GHZ_n\rangle$.

□

Ces résultats généraux concernant la nature de l'intrication de certains états périodiques précis permet de déterminer rapidement dans certains cas la présence ou non d'intrication dans ces systèmes quantiques pouvant apparaître après la mesure du second registre dans l'algorithme de recherche de la période dans l'algorithme de Shor.

4.3 Transformée de Fourier Quantique et Intrication

La Transformée de Fourier Quantique est une porte quantique constituant un élément clé dans l'algorithme de Shor, et plus particulièrement dans l'algorithme de recherche de la période. Elle est utilisée pour mettre en évidence la période associée aux états du second registre, issus de la mesure du premier registre, afin de faciliter la détermination de l'ordre de la fonction définissant le problème de factorisation (voir Sections 1.2.2 et 1.2.2).

L'influence de la Transformée de Fourier Quantique sur l'intrication des registres quantiques n'est pas totalement comprise et cernée, que ce soit au niveau de la variation de la quantité d'intrication (via des mesures de l'intrication comme la MGI) ou au niveau des changements de classes d'intrication induits par l'application de cette transformée.

À partir des travaux précédents, notamment ceux de Most *et al.* [194], nous tentons d'apporter des éléments de réflexion et de réponses à partir notamment des outils, précédemment utilisés, issus de la géométrie algébrique. Dans un premier temps, nous étudions l'influence de la Transformée de Fourier Quantique sur les états périodiques. Nous évaluons les polynômes de Mermin ainsi que l'hyperdéterminant afin de mesurer et d'observer l'évolution de l'intrication. Nous utilisons aussi les outils théoriques mentionnés pour déterminer les classes d'intrication caractérisant les états périodiques après l'application de la TFQ. Enfin, nous posons et étudions certaines questions liées à l'influence de la TFQ sur l'intrication des registres quantiques, en dehors du contexte de l'algorithme de Shor.

4.3.1 Application de la TFQ sur les états périodiques – Étude qualitative

Dans cette sous-section nous nous intéressons à l'étude des classes d'intrication atteintes par les états périodiques après l'application de la Transformée de Fourier Quantique. Comme cela a été fait précédemment, nous étudions en détail le cas des 3-qubits et des 4-qubits, et tentons par la suite de proposer quelques généralisations des similarités observées.

Dans un premier temps, nous nous intéressons aux systèmes à 3-qubits. Nous menons une étude exhaustive en considérant toutes les combinaisons possibles de shift l et de période r.

r \ l	0	1	2	3	4	5	6	7
1	$\mathcal{O}_1$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_1$
2	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$
3	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
4	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
5	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
6	$\mathcal{O}_3$	$\mathcal{O}_3$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$
7	$\mathcal{O}_6$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$	$\mathcal{O}_1$

TABLE 4.3 – Orbites SLOCC des états à 3-qubit résultant de l'application de la TFQ sur des états périodiques en fonction de leur shift l et de la période r.

À partir des résultats présentés en Table 4.3, nous pouvons extraire les propriétés suivantes pour les états périodiques à 3-qubits après l'application de la Transformée de Fourier Quantique :

- Lorsque $r = 4$, l'état correspond toujours à l'orbite $\mathcal{O}_1$ (séparable),
- Pour tous les états ayant un shift l et une période r satisfaisant la condition $l + r \geq 8$ (c'est à dire que l'on se trouve sur ou en dessous de l'anti-diagonale de $\{l = 1, r = 7\}$ à $\{l = 7, r = 1\}$), ils appartiennent à l'orbite $\mathcal{O}_1$ du cône nilpotent, et sont donc des états séparables,
- Si la période prend les valeurs $r = 1$, $r = 2$, et $r = 4$, et si le shift vérifie $0 \leq l \leq r - 1$, alors l'état est un état séparable,
- Si la période prend les valeurs $r = 1$, et $r = 2$, et si le shift vérifie $4 \leq l \leq r + 3$, alors l'état n'est pas séparable,
- Si la période est égale à $r = 2$, alors si le shift vérifie $2 \leq l \leq 5$, alors l'état appartient à l'orbite $\mathcal{O}_3$, et donc l'état n'est pas séparable.

Nous nous intéressons à présent aux systèmes à 4-qubits. Comme précédemment, nous menons une étude exhaustive en considérant toutes les combinaisons possibles de shift l et de période r. À partir des résultats présentés en Table 4.4, nous pouvons extraire les propriétés suivantes pour les états périodiques à 4-qubits après l'application de la Transformée de Fourier Quantique :

- Lorsque $r = 8$, l'état correspond toujours à l'orbite Gr_1 (séparable),
- Pour tous les états ayant un shift l et une période r satisfaisant la condition $l + r \geq 16$ (c'est à dire que l'on se trouve sur ou en dessous de l'anti-diagonale de $\{l = 1, r = 15\}$ à $\{l = 15, r = 1\}$), ils appartiennent à l'orbite Gr_1 du cône nilpotent, et sont donc des états séparables,
- Si la période prend les valeurs $r = 1$, $r = 2$, $r = 4$ et $r = 8$, et si le shift vérifie $0 \leq l \leq r - 1$, alors l'état est un état séparable,
- Si la période prend les valeurs $r = 1$, $r = 2$, et $r = 4$, et si le shift vérifie $8 \leq l \leq r + 7$, alors l'état n'est pas séparable,
- Si la période est égale à $r = 2$, alors si le shift vérifie $2 \leq l \leq 13$, alors l'état appartient à la strate Gr_4, et donc l'état n'est pas séparable.

Ces observations sur les états générés après l'application de la Transformée de Fou-

l / r	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Gr_1	G_{00cc}	G_{abc0}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	Gr_1
2	Gr_1	Gr_1	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_1	Gr_1
3	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1
4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1
5	G_{abcd}	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
6	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
7	$L_{a_20_{3\oplus\bar{1}}}$	$L_{a_20_{3\oplus\bar{1}}}$	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
8	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
9	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
10	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
11	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
12	Gr_2	Gr_2	Gr_2	Gr_2	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
13	L_{00c_2}	L_{00c_2}	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
14	Gr_4	Gr_4	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1
15	L_{00c_2}	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1	Gr_1

Table 4.4 – Familles de Verstraete *et al.* et strates du cône nilpotent des états à 4-qubits obtenus après l'application de la TFQ sur des états périodiques en fonction de leur shift l et de la période r.

rier Quantique sur des états périodiques particuliers (de par leurs valeurs de période et de shift) sont à la fois présentes dans le cas des 3-qubits et des 4-qubits. On peut alors espérer voir ces résultats se généraliser à n'importe quel système périodique à n-qubits. Néanmoins, nous n'avons pas été en mesure de poursuivre ce travail pour proposer une preuve de la validité de ces résultats aux dimensions supérieures.

Nous nous proposons alors de formuler explicitement la généralisation de ces observations sous la forme de questionss. Pour l'une d'entre elles, nous proposons néanmoins une démonstration faisant appel à une des propriétés fondamentales de la TFQ.

Question 24. Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits avec un shift l et une période r, et soit $N = 2^n$. Si $r = \frac{N}{2}$, alors quelque soit la valeur du shift l, l'état obtenu après l'application de la TFQ à l'état $\left|\Psi^n_{l,r}\right\rangle$ est-il toujours séparable ?

Question 25. Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits avec un shift l et une période r, et soit $N = 2^n$. Si $r = 2^k$ avec $k \in [\![0, n-1]\!]$, et si le shift vérifie $0 \leq l \leq r-1$, alors l'état obtenu après l'application de la TFQ à l'état $\left|\Psi^n_{l,r}\right\rangle$ est-il séparable ?

Question 26. Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits avec un shift l et une période r, et soit $N = 2^n$. Si $r = 2^k$ avec $k \in [\![0, n-2]\!]$, et si le shift vérifie $\frac{N}{2} \leq l \leq \frac{N}{2} + r - 1$, alors l'état obtenu après l'application de la TFQ à l'état $\left|\Psi^n_{l,r}\right\rangle$ est-il non-séparable ?

Question 27. Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits avec un shift l et une période r, et soit $N = 2^n$. Si $r = 2$ et si le shift vérifie $2 \leq l \leq \frac{N}{2} - 3$, alors l'état obtenu après l'application de la TFQ à l'état $\left|\Psi^n_{l,r}\right\rangle$ est-il équivalent à l'état biséparable $|0\rangle \otimes |GHZ_{n-1}\rangle$, par action du groupe SLOCC ou par permutation des qubits ?

Proposition 4.3.1. *Soit $\left|\Psi^n_{l,r}\right\rangle$ un état périodique à n-qubits avec un shift l et une période r, et soit $N = 2^n$. Alors après l'application de la TFQ, tous les états sur ou en dessous de l'anti-diagonale définie de la case $\{l = 1, r = N-1\}$ à $\{l = N-1, r = 1\}$ sont séparables.*

Démonstration. Nous avons démontré à la Proposition 4.2.3 que le nombre d'états dans l'écriture des états périodiques $\left|\Psi^n_{l,r}\right\rangle$ avec $l + r \geq N$ (en dessous ou sur l'anti-diagonale) est égal à $A = 1$, et donc ils sont des états de la base canonique. En utilisant la Remarque 28, nous pouvons conclure qu'après application de la TFQ, nous récupérons toujours un état factorisé (séparable). □

Nous espérons que cette étude et ces observations concernant l'influence de la TFQ sur l'intrication des états périodiques permettront de mieux comprendre ou de simplifier l'étude de l'intrication dans l'algorithme de Shor ou de recherche de la période.

4.3.2 Application de la TFQ sur les états périodiques – Étude quantitative

Nous nous intéressons dans cette sous-section uniquement au cas des 4-qubits. Nous désignerons alors les états périodiques $\left|\Psi^4_{l,r}\right\rangle$ par le couple (l, r) pour plus de commodité. Le circuit explicite de la Transformée de Fourier Quantique pour les 4-qubits est représenté en Figure 4.1.

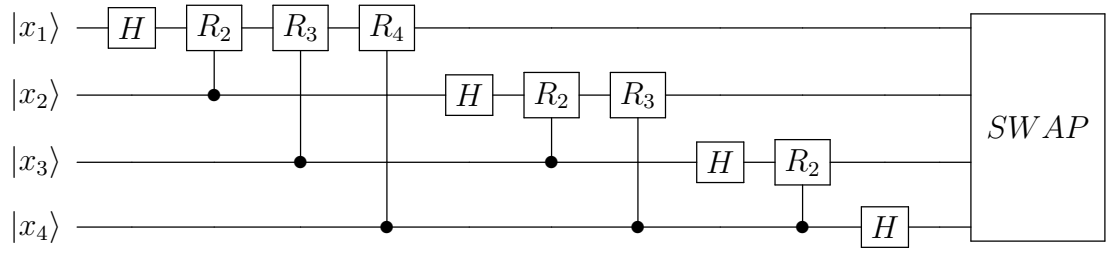


Figure 4.1 – Les 11 portes quantiques composant le circuit quantique pour la Transformée de Fourier Quantique à 4-qubits.

Comme suggéré en Section 2.2.3, les polynômes invariants peuvent être utilisés comme des mesures potentielles de l'intrication. Nous utilisons tout d'abord l'hyperdéterminant $|Det_{2222}|$ associé aux 4-qubits comme une mesure quantitative de l'intrication, et calculant la quantité d'intrication d'un état périodique en entrée, et ce après chaque porte quantique composant la Transformée de Fourier Quantique. Nous nous restreignons ici uniquement au cas des états périodiques.

Lorsque l'on observe la valeur absolue de l'hyperdéterminant Det_{2222} après chaque porte unitaire composant la TFQ, nous pouvons distinguer 3 différents comportements pour le cas des 4-qubits :

- **Cas 1 :** La valeur de l'hyperdéterminant est non nulle pour l'état périodique initial, et ne s'annule ni pendant ni après l'application de la TFQ,
- **Cas 2 :** La valeur de l'hyperdéterminant est nulle pour l'état périodique initial, et ensuite devient non-nulle après une étape précise de la TFQ, puis enfin ne s'annule plus en passant par les portes suivantes,
- **Cas 3 :** La valeur de l'hyperdéterminant est toujours égale à 0, avant, pendant et après l'application de la TFQ.

Le premier cas n'apparaît que lorsque les états $(1,3)$ et $(2,3)$ sont en entrée. Dans les deux cas, l'état périodique en entrée correspond à la famille G_{abc0}, qui effectivement n'annule pas l'hyperdéterminant. Après l'application de la TFQ sur ces états, on retrouve un état appartenant à la famille générique G_{abcd}. On représente en Figure 4.2 l'évolution de $|Det_{2222}|$ tout au long des états composant la TFQ, dont l'axe de abscisses représente l'index de la porte quantique appliquée. Par exemple, à l'index 0, on a l'état périodique initial ; à l'index 1, on applique la porte d'Hadamard sur l'état initial ; à l'index 3, on récupère l'état résultant de l'application de la première porte d'Hadamard, de la première porte $c-R_2$ et de la première porte $c-R_3$ à l'état périodique initial ; et ainsi de suite. Nous observons dans ce cas une décroissance globale de la valeur absolue de l'hyperdéterminant tout en se déplaçant vers une famille plus générique.

Le second cas intervient pour les couples $(l,r) \in \mathcal{S}_2$, avec $\mathcal{S}_2$ l'ensemble défini comme suit :

$$\begin{aligned}\mathcal{S}_2 = \{&(0,3),(0,5),(2,1),(3,1),(3,3),(4,1),(4,3),(5,1),(5,3),\\ &(6,1),(6,3),(7,1),(9,1),(10,1),(11,1),(12,1)\}\ .\end{aligned} \tag{4.23}$$

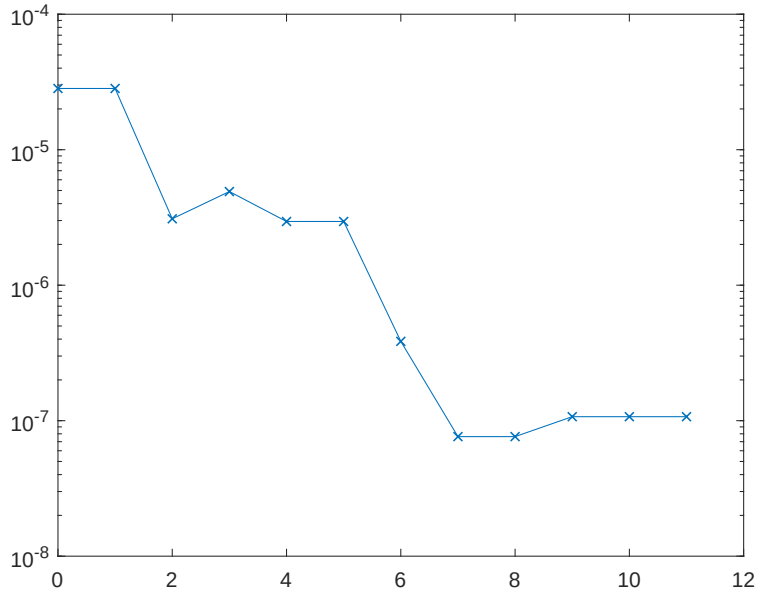


FIGURE 4.2 – Évolution de la valeur absolue de l'hyperdéterminant tout au long des portes composant la TFQ, pour l'état périodique défini par $(l, r) = (1, 3)$.

Dans le second cas, les états périodiques initiaux sont des points de la variété duale X^*, car annulant l'hyperdéterminant. Ensuite, en fonction du couple (l, r) considéré, la valeur de l'hyperdéterminant devient non-nulle après une des portes $c - R_k$. Nous pouvons distinguer différents comportements en ce qui concerne l'évolution de la quantité $|Det_{2222}|$ tout au long de la TFQ, et ceci est représenté en Figure 4.3.

Dans le troisième cas, lorsque la valeur de l'hyperdéterminant est toujours nulle, ceci arrive pour tous les couples restant $(l, r) \notin \mathcal{S}_2 \cup \{(1, 3), (2, 3)\}$. Ceci implique que les états concernés restent toujours dans la variété duale tout au long de l'application de la TFQ, mais cela ne signifie pas que la TFQ ne modifie par la classe d'intrication de ces états, impliquant éventuellement un changement d'orbite au sein des états dégénérés.

Il est intéressant ici de remarquer que la valeur de l'hyperdéterminant ne change pas après l'application des portes d'Hadamard (portes d'index 1, 5, 8 et 10), ainsi que pour la porte Swap, comme cela pouvait être attendu. En effet l'hyperdéterminant est invariant par opération unitaire locale et permutation des qubits. Il en résulte que les changements dans la valeur de l'hyperdéterminant sont uniquement dus à l'application des portes $c - R_k$, et ces opérateurs sont donc responsables de la génération ou de la modification de l'intrication par la Transformée de Fourier Quantique.

De plus, pour la plupart des états à 4-qubits (92,5%), il est important de préciser que l'on se trouve dans le troisième cas, et donc que l'hyperdéterminant en tant que mesure ne change pas après et durant la TFQ (en restant notamment à 0), et cette observation peut être mise en relation avec ce qui a été précisé par Shimoni *et al.* dans [242], où il est remarqué que la mesure Groverienne de l'intrication n'est que légèrement affectée

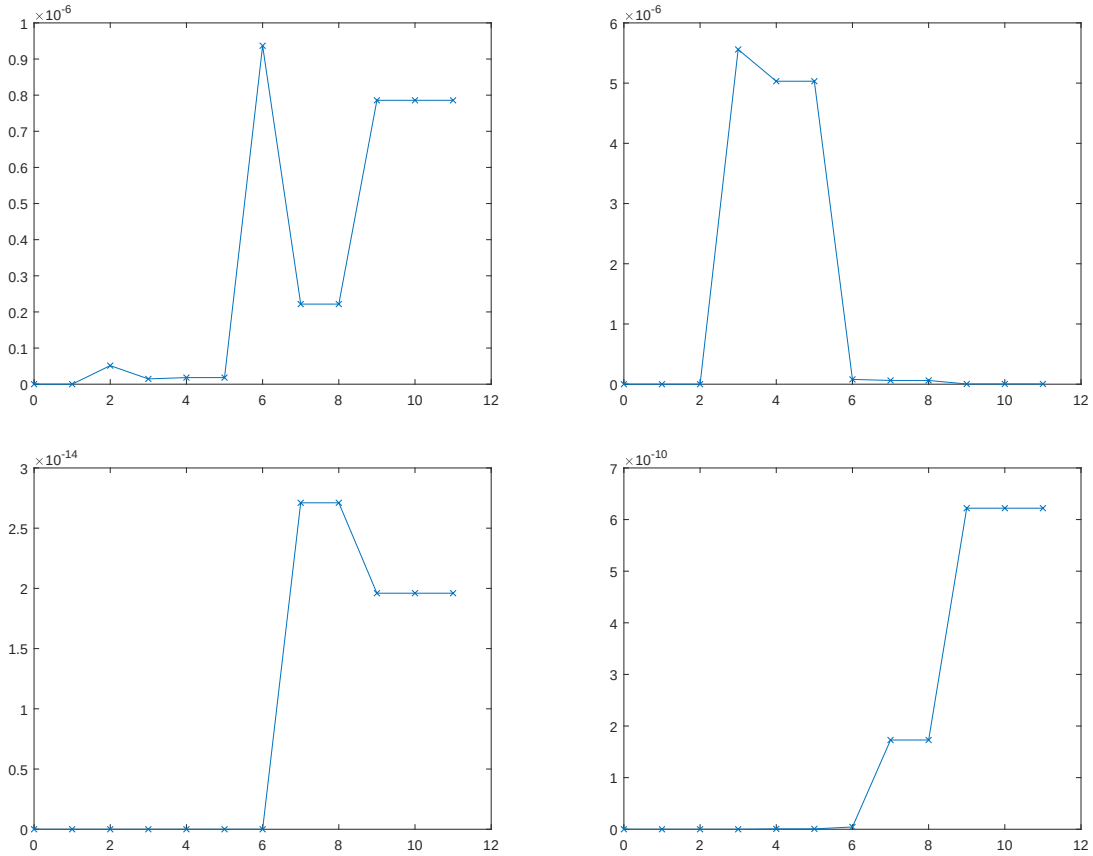


Figure 4.3 – Évolution de la valeur absolue de l'hyperdéterminant tout au long des portes composant la TFQ, pour les états périodiques définis par $(l, r) = (0, 3)$ (haut gauche), $(l, r) = (5, 3)$ (haut droit), $(l, r) = (11, 1)$ (bas gauche) et $(l, r) = (9, 1)$ (bas droit).

par la TFQ. Dans ce sens, la mesure Groverienne détecte ici la présence d'intrication, mais pas nécessairement les changements de classe d'intrication. Ceci est notamment nuancé et discuté en Section 4.3.3.

Enfin, il peut être intéressant aussi de relever le fait que l'hyperdéterminant est toujours nul et ne change jamais de valeur durant la TFQ, pour tous les couples (l, r) lorsque r est une puissance de 2, comme cela a déjà été mentionné par Kendon et Munro [156]. Cependant, nous pouvons tout de même observer un changement qualitatif de l'intrication, comme cela a pu être mis en avant dans les sous-sections précédentes. Nous observons également que la valeur de l'hyperdéterminant ne varie et ne change que pour certaines valeurs de la période, qui sont $r = 1$, $r = 3$ et $r = 5$.

Nous décidons à présent d'adopter une autre approche pour mesurer la quantité d'intrication et son évolution tout au long de la TFQ. Les polynômes de Mermin, précédemment utilisés pour étudier l'intrication dans l'algorithme de Grover, constituent une manière de mesurer l'aspect non-local de systèmes quantiques. Malgré le fait

que les deux approches soient différentes, l'hyperdéterminant étant défini de manière algébrique tandis que l'évaluation de Mermin est basée sur la notation d'observable, ces deux mesures peuvent présenter un comportement similaire en ce qui concerne l'évolution de l'intrication pour certains états périodiques tout au long de la TFQ (voir Figure 4.4).

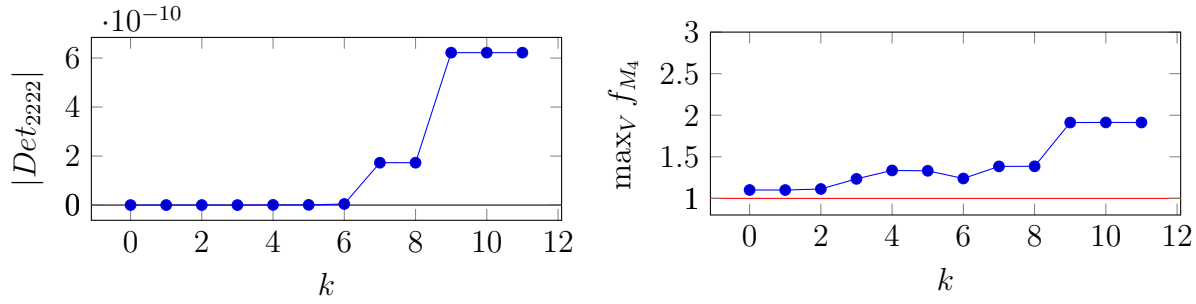
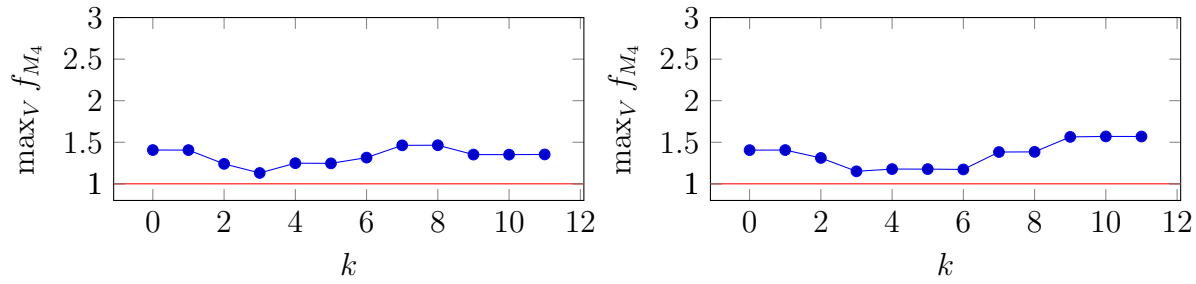


FIGURE 4.4 – Comparaison de l'évaluation de l'intrication au cours de la Transformée de Fourier Quantique pour l'état périodique $(l, r) = (9, 1)$, en utilisant l'hyperdéterminant (courbe de gauche) et l'évaluation de Mermin (courbe de gauche).

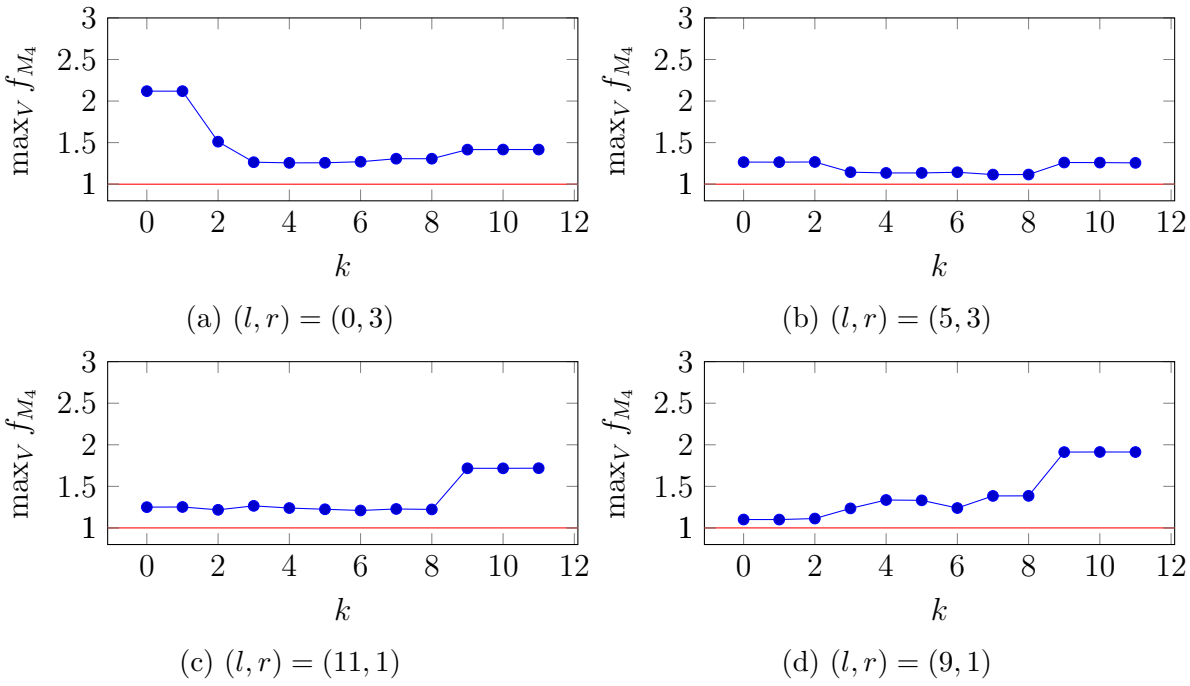
Nous reprenons les 3 comportements différents observés pour l'évolution de l'hyperdéterminant et proposons d'observer comment réagit l'évaluation de Mermin dans ces cas là. Tout d'abord, les états correspondant aux Cas 1 et 2 violent la limite classique durant l'application de la TFQ. Les courbes correspondantes sont représentées en Figure 4.5 pour le Cas 1, et en Figure 4.6 pour le Cas 2.



(a) $(l, r) = (1, 3)$ (b) $(l, r) = (2, 3)$

FIGURE 4.5 – Évolution de la valeur maximale du polynôme de Mermin pour les états périodiques $(1, 3)$ (sous-figure (a) à gauche) et $(2, 3)$ (sous-figure (b) à droite) en fonction des étapes de la TFQ. Les états périodiques correspondent au Cas 1 du comportement de l'hyperdéterminant.

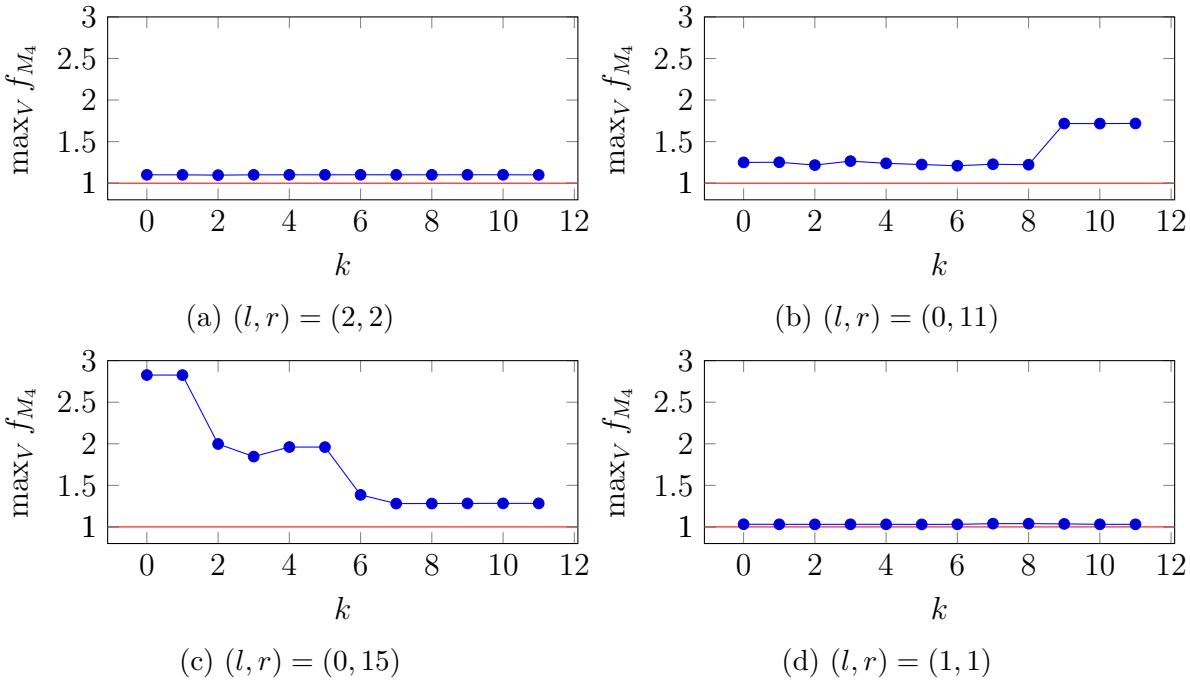
Seulement certains états correspondant au Cas 3 produisent des courbes à valeur constante, avec certaines d'entre elles égales à la limite classique de 1 (elles ne seront pas représentées). C'est notamment le cas pour l'état périodique correspondant à $(l, r) = (2, 4)$ qui demeure séparable durant tout le processus. Les courbes correspondantes sont représentées en Figure 4.7 pour le Cas 3.



(a) $(l, r) = (0, 3)$ (b) $(l, r) = (5, 3)$

(c) $(l, r) = (11, 1)$ (d) $(l, r) = (9, 1)$

Figure 4.6 – Évolution de la valeur maximale du polynôme de Mermin pour les états périodiques correspondant au Cas 2 du comportement de l'hyperdéterminant (le couple (l, r) est renseigner en sous-titre de chaque sous-figure), en fonction des étapes de la TFQ.



(a) $(l, r) = (2, 2)$ (b) $(l, r) = (0, 11)$

(c) $(l, r) = (0, 15)$ (d) $(l, r) = (1, 1)$

Figure 4.7 – Évolution de la valeur maximale du polynôme de Mermin pour les états périodiques correspondant au Cas 3 du comportement de l'hyperdéterminant (le couple (l, r) est renseigner en sous-titre de chaque sous-figure), en fonction des étapes de la TFQ.

Il pourrait être intéressant d'affiner et de prolonger cette étude, en étudiant de manière plus étroite le lien entre l'évolution de l'intrication en terme de mesure et les changements de classe d'intrication induits par la TFQ. Par exemple, les états périodiques définis par $(l, r) = (2, 2)$ et $(l, r) = (0, 11)$ sont SLOCC équivalents (avant la TFQ, voir Table 4.2) et appartiennent tout deux à la strate Gr_4. En revanche, ces deux états présentent des comportements différents en termes d'évolution de l'évaluation de Mermin durant la TFQ (voir Figure 4.7 (a) et (b)). Plus précisément, la valeur de l'évaluation de Mermin pour l'état $(l, r) = (2, 2)$ semble stagner tout au long de la TFQ, tandis que l'évaluation pour l'état $(l, r) = (0, 11)$ connaît une augmentation après un certaine porte $c - R_k$. Ceci doit aussi être mis en perspective avec le fait que la classe d'intrication de l'état $(l, r) = (2, 2)$ n'est pas modifiée par application de la TFQ, tandis que l'état $(l, r) = (0, 11)$ arrive dans une famille plus générique et n'est plus dans le cône nilpotent à la fin de l'application de la TFQ. Cette relation entre le changement de classe et la variation des différentes mesures de l'intrication mériterait alors plus d'attention pour comprendre plus en détail l'influence de la TFQ et de la classe d'intrication en entrée sur l'intrication des états au milieu et à la fin de l'algorithme.

De manière similaire, un autre exemple d'états correspondants au Cas 3 est celui des deux états périodiques définis par $(l, r) = (0, 15)$ et $(l, r) = (1, 1)$. Le lecteur pourra s'assurer que ces deux états sont SLOCC équivalents, plus précisément SLOCC équivalents à $|GHZ_4\rangle$, avant l'application de la TFQ. Ceci est d'autant plus clair pour l'état $\left|\Psi^4_{0,15}\right\rangle = |GHZ_4\rangle$ qui atteint la valeur maximale possible pour l'évaluation de Mermin avant la TFQ, qui est pour rappel de $2\sqrt{2}$. Cette valeur est revanche très loin de la valeur obtenue pour l'état définit par $(l, r) = (1, 1)$, où son évaluation de Mermin reste assez proche de la limite classique, et ce pour toutes les étapes de la TFQ. En effet, cet état s'exprime initialement comme

$$\left|\Psi^4_{1,1}\right\rangle = \frac{\sqrt{16}}{\sqrt{15}}\left(|++++\rangle - \frac{1}{\sqrt{16}}|0000\rangle\right) , \tag{4.24}$$

qui est un état appartenant à la variété des sécantes $\sigma_2(X)$. C'est état est donc aussi SLOCC équivalent à $|GHZ_4\rangle$ mais est néanmoins plus proche de la variété des états séparables au sens de la mesure géométrique de l'intrication. De ce fait, ce constat peut expliquer la différence d'évolution des courbes correspondant à ces deux états (Figure 4.7 (c) et (d)), et permet aussi de rappeler que l'évaluation de Mermin n'est pas nécessairement SLOCC invariante, mais dépend du représentant choisi, à une opération unitaire près.

Nous espérons que ces observations permettrons une étude plus approndie du lien entre mesure de l'intrication et classes d'intrication sous SLOCC et LOCC , pour les états périodiques intervenant au sein de l'algorithme de Shor.

4.3.3 Linear Shift Invariant property

Une des propriétés intéressantes de la Transformée de Fourier Quantique, souvent rappelée dans le contexte de l'algorithme de Shor, est celle de *Linear Shift Invariance*. Il est connu que si un état à n-qubits présente une écriture périodique avec un certain shift, alors après l'application de la TFQ on récupérera un état sans shift (un état quantique

dont l'écriture commence avec l'état de base $|00\dots0\rangle$) avec un certain comportement périodique directement lié à la précédente période et au nombre d'éléments de base $N = 2^n$ [200].

Dans leur travaux datant de 2010, Most *et al.* ont étudié cette propriété afin de proposer une approximation de la description d'un état périodique après l'application de la Transformée de Fourier Quantique. Nous proposons ci-dessous une traduction (de nos soins) du passage concerné dans leur article [194] :

"Par analogie avec la Transformée de Fourier Discrète (DFT), la TFQ est utilisée afin de révéler les périodicités de l'état en entrée. En particulier, les amplitudes de l'état $\left|\Psi^n_{l,r}\right\rangle$ *forment une suite périodique, et lorsque la DFT est appliquée sur cette dernière, la suite résultante peut être approchée par une suite périodique de même nature, qui est telle que les indices des termes non nuls forment une suite arithmétique. Dans cette suite résultante, la raison est égale à* N/r*, le terme initial est zero, et des phases additionnelles sont ajoutées. [...] Comme l'application de la TFQ sur un état quantique est équivalente à l'application de la DFT sur ses amplitudes, l'action de la TFQ sur les états périodiques peut être approximativement décrite comme :* $\left|\Psi^n_{l,r}\right\rangle \xrightarrow{TFQ} \left|\Psi^n_{0,2^n/r}\right\rangle$*."*

Cette approximation peut s'avérer utile pour estimer en pratique des mesures de l'intrication après application de la QFT, comme cela est proposé dans [194]. Cependant, il apparaît que cette approximation ne préserve pas la nature de l'intrication de l'état périodique après TFQ, en termes d'orbites sous l'action du groupe SLOCC, pour une nombre faible de qubits. En effet, l'étude d'un exemple simple, dans le cas des 3-qubits, peut illustrer cette observation. Soit l'état périodique suivant :

$$\left|\Psi^3_{5,1}\right\rangle = \frac{1}{\sqrt{3}}\big(|101\rangle + |110\rangle + |111\rangle\big) = \frac{1}{\sqrt{3}}|1\rangle \otimes \Big(|01\rangle + |10\rangle + |11\rangle\Big) \ . \tag{4.25}$$

Cet état biséparable appartient clairement à l'orbite $\mathcal{O}_3$ de la classification des 3-qubits. Lorsque l'on applique la TFQ à cet état, on obtient l'état $|\Psi^*\rangle$:

$$|\Psi^*\rangle = QFT\left|\Psi^3_{5,1}\right\rangle \ . \tag{4.26}$$

Cet état présente également des propriétés périodiques intéressantes, mais appartient cependant à l'orbite $\mathcal{O}_6$.

En revanche, si l'on se penche sur l'état périodique approximant l'application de la TFQ sur $\left|\Psi^3_{0,8}\right\rangle$, c'est à dire l'état de shift $l = 0$ et de période $\frac{N}{r} = \frac{8}{1} = 8$, on obtient l'état $|000\rangle$ qui est un état séparable, et n'est pas SLOCC équivalent à l'état $|\Psi^*\rangle$. Ainsi, d'un point de vue qualitatif, l'approximation utilisée dans [194] ne permet pas de rendre compte du changement dans la nature de l'intrication des états périodiques.

D'autre part, d'un point de vue quantitatif, un certain nombre d'éléments peuvent être relevés pour cet exemple. Tout d'abord, l'état initial $\left|\Psi^3_{5,1}\right\rangle$ considéré appartient à la variété duale de la variété de Segre, et annule donc l'hyperdéterminant. La Transformée de Fourier Quantique, dans ce cas, implique un changement dans la valeur de l'hyperdéterminant car elle génère un état non-dégénéré. En revanche, si l'on considère l'état issu de l'approximation, il annule l'hyperdéterminant, ce qui marque un premier point de différence avec l'état théoriquement attendu.

Du point de vue de la Mesure Géométrique de l'Intrication (MGI), dans sa définition Groverienne, l'application de la TFQ à l'état $\left|\Psi^3_{5,1}\right\rangle$ implique un changement dans la MGI, plus précisément une augmentation. En revanche la MGI associée à l'état $\left|\Psi^3_{0,8}\right\rangle$ est nulle car c'est un état séparable.

Dans cette mesure, l'approximation introduite dans [194] ne permet pas de rendre compte des mêmes propriétés liées à l'intrication que celles du véritable état issu de la TFQ, que ce soit d'un point de vue qualitatif ou quantitatif.

État	Orbite	E_G	$\lvert Det_{222}\rvert$
$\left\lvert\Psi^3_{5,1}\right\rangle$	$\mathcal{O}_3$	0.127322	0
$\lvert\Psi^*\rangle$	$\mathcal{O}_6$	0.578616	0.042893
$\left\lvert\Psi^3_{0,8}\right\rangle$	$\mathcal{O}_1$	0	0

TABLE 4.5 – Récapitulatif des classes et mesures d'intrication pour l'exemple considéré.

Toutes ces informations sont regroupées dans la Table 4.5. L'exemple traité dans le cas des 3-qubits permet de se rendre compte des aspects non pris en compte par l'approximation proposée. Il est peut être possible, asymptotiquement, que si le nombre de particules augmente, l'approximation devient plus précise. En revanche, elle ne permet pas de tenir compte du réel effet de la TFQ sur l'intrication des états à faible nombre de particules.

4.3.4 La Transformée de Fourier Quantique et le groupe SLOCC

Une autre propriété intéressante de la Transformée de Fourier Quantique, généralement utile dans le contexte du calcul quantique, est le fait que la TFQ envoie l'état de base $|0\rangle^{\otimes n}$ sur l'état complètement parallélisé $|+\rangle^{\otimes n}$. Cette propriété peut en effet peut être généralisée à tout état de la base de calcul.

Remarque 28. Si l'on applique la Transformée de Fourier Quantique sur un des états de la base de calcul (base canonique), alors on obtient un état qui est séparable. Nous pouvons directement déduire ce résultat à partir de la représentation factorisée rappelée en Equation (5.4) de la Section II.6 du livre [200]. En effet, pour un état de base $|j_1 j_2 \dots j_n\rangle$, on obtient l'état factorisé $\frac{1}{\sqrt{2^n}}(|0\rangle + e^{2i\pi 0\cdot j_n}|1\rangle)\cdot(|0\rangle + e^{2i\pi 0\cdot j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2i\pi 0\cdot j_1 j_2 \dots j_n}|1\rangle)$ après l'application de la Transformée de Fourier Quantique.

Cette propriété est aussi reliée au problème de classification de l'intrication après l'application de la TFQ. En effet, on peut en déduire que tout état de base reste dans la variété des états séparables après l'application de la Transformée de Fourier Quantique. Cependant, ceci n'est pas vrai pour tous les états séparables, comme ceci peut être observé par exemple dans les Tables 4.2 et 4.4, et plus loin dans cette section.

En effet, ces tables montrent que la TFQ peut transformer des états séparables en états intriqués et peut changer la nature de l'intrication. On se propose de considérer un autre exemple simple et clair pour le cas des 3-qubits, et d'appliquer la TFQ à l'état $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$. Nous savons que l'état $|W\rangle$ appartient à la variété des tangentes et correspond à l'orbite $\mathcal{O}_5$ pour les 3-qubits. Après application de la TFQ nous obtenons l'état suivant :

$$TFQ|W\rangle = \frac{1}{\sqrt{8}}\frac{1}{\sqrt{3}}\Big(3|000\rangle + (\omega+\omega^2+\omega^4)|001\rangle + \omega^2|010\rangle + (\omega^3+\omega^6+\omega^4)|011\rangle \\ +|100\rangle + (\omega^5+\omega^2+\omega^4)|101\rangle + \omega^6|110\rangle + (\omega^7+\omega^6+\omega^4)|111\rangle\Big)\ , \tag{4.27}$$

avec $\omega = e^{\frac{2i\pi}{8}}$.

Si l'on évalue l'hyperdéterminant de Cayley pour cet état résultant de la TFQ appliquée à $|W\rangle$, on obtient une valeur égale à $\dfrac{-i}{36}$, ce qui signifie que cet état appartient à l'orbite $\mathcal{O}_6$, et est donc équivalent à l'état $|GHZ\rangle$. On observe alors une modification de la classe d'intrication par application de la Transformée de Fourier Quantique.

De ce fait, il peut être intéressant d'étudier de plus près dans quelle mesure on peut passer d'un type d'intrication à un autre par application de la TFQ, et de manière générale d'étudier quelles peuvent être les classes d'équivalence liées à l'action du groupe SLOCC$\cup\{TFQ, TFQ^{-1}\}$ ou SLOCC$\cup\{H, c-R_k, SWAP\}$ (où $c-R_k$ désigne la porte *controlled-*R_k définissant la TFQ). Il peut également s'avérer intéressant d'étudier l'intrication générée par les circuits composés des portes H, $SWAP$ et $c-R_k$, comme cela a pu être étudié par Bataille et Luque [22] pour le cas des portes $c-Z$ et $SWAP$, afin de comprendre plus en profondeur l'influence de telles portes (contrôlées) sur l'intrication des états générés.

En guise de premier cas d'étude dans cette direction, nous proposons de nous pencher sur le cas des états à 2-qubits et 3-qubits. Dans le cas des 2-qubits, on constate qu'il n'existe qu'une seule orbite sous l'action du groupe que l'on notera $G' =$ SLOCC $\cup$ $\{TFQ, TFQ^{-1}\}$. En effet, si l'on considère l'état $|\Psi_1\rangle$ défini par

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |01\rangle\Big)\ , \tag{4.28}$$

si on lui applique la TFQ, on obtient l'état intriqué $|\Psi_2\rangle$.

$$|\Psi_2\rangle = \frac{1}{2\sqrt{2}}\Big(2|00\rangle + (1+i)|01\rangle + (1-i)|11\rangle\Big)\ . \tag{4.29}$$

Nous savons que pour les systèmes à 2-qubits, il n'existe que deux classes d'intrication sous SLOCC : séparable ou intriqué (EPR). Etant donné que nous pouvons passer de l'état séparable $|\Psi_1\rangle$ à l'état intriqué $|\Psi_2\rangle$, alors il n'existe qu'une seule orbite sous l'action du groupe G'.

Pour étudier ce qu'il se passe pour le cas des 3-qubits, on définit un certain nombre d'états à 3-qubits auxquels nous appliquons la TFQ. :

$$|\Phi_1\rangle = \frac{1}{\sqrt{3}}\Big(|001\rangle + |010\rangle + |100\rangle\Big) \in \mathcal{O}_5, \tag{4.30}$$

$$|\Phi_2\rangle = TFQ|\Phi_1\rangle, \quad |\Phi_3\rangle = TFQ|\Phi_2\rangle, \tag{4.31}$$

$$|\Phi_3\rangle = \frac{1}{\sqrt{3}}\Big(|100\rangle + |110\rangle + |111\rangle\Big) \in \mathcal{O}_3, \tag{4.32}$$

$$|\Phi_4\rangle = \frac{1}{\sqrt{2}}\Big(|110\rangle + |111\rangle\Big) \in \mathcal{O}_4, \tag{4.33}$$

$$|\Phi_5\rangle = TFQ|\Phi_4\rangle, \tag{4.34}$$

$$|\Phi_6\rangle = \frac{1}{\sqrt{2}}\Big(|101\rangle + |111\rangle\Big) \in \mathcal{O}_1, \tag{4.35}$$

$$|\Phi_7\rangle = TFQ|\Phi_6\rangle, \tag{4.36}$$

$$|\Phi_8\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |101\rangle\Big) \in \mathcal{O}_2, \tag{4.37}$$

$$|\Phi_9\rangle = TFQ|\Phi_8\rangle \ . \tag{4.38}$$

En observant la Figure 4.8 regroupant l'ensemble des passages possibles entre les états précédemment définis, nous pouvons nous assurer que, en partant d'un état particulier $|\Phi_i\rangle$, nous pouvons atteindre n'importe quel état dans n'importe quelle orbite, en appliquant une succession d'opérations SLOCC et/ou de TFQ (ou son inverse).

Nous pouvons ainsi conclure qu'il n'existe qu'une unique orbite sous l'action du groupe G', dans les cas des 2-qubits et des 3-qubits. Il peut apparaître difficile d'étudier le cas des 4-qubits, le nombre d'orbites sous l'action du groupe SLOCC étant infini. En revanche, une première étude peut être menée en considérant à la place les familles et sous familles de Verstraete *et al.*, ainsi que les strates du cône nilpotent. Les résultats présentés en Table 4.2 et 4.4 peuvent également être utilisés pour déterminer des états équivalents sous l'action de la TFQ (et son inverse), mais qui ne sont pas équivalents sous l'action du groupe SLOCC.

4.4 Perspectives

Dans cette section nous proposons quelques idées et perspectives pour poursuivre le travail autour de l'algorithme de Shor présenté dans ce chapitre.

Tout d'abord, il serait intéressant d'étudier l'intrication qui apparait à d'autres endroits de l'algorithme. Par exemple, on pourrait étudier l'intrication entre les deux registres quantiques durant l'algorithme de recherche de la période. Aussi, on pourrait étudier l'intrication générée par la porte U_f (exponentiation modulaire), et comment l'intrication évolue tout au long de l'application de cette porte.

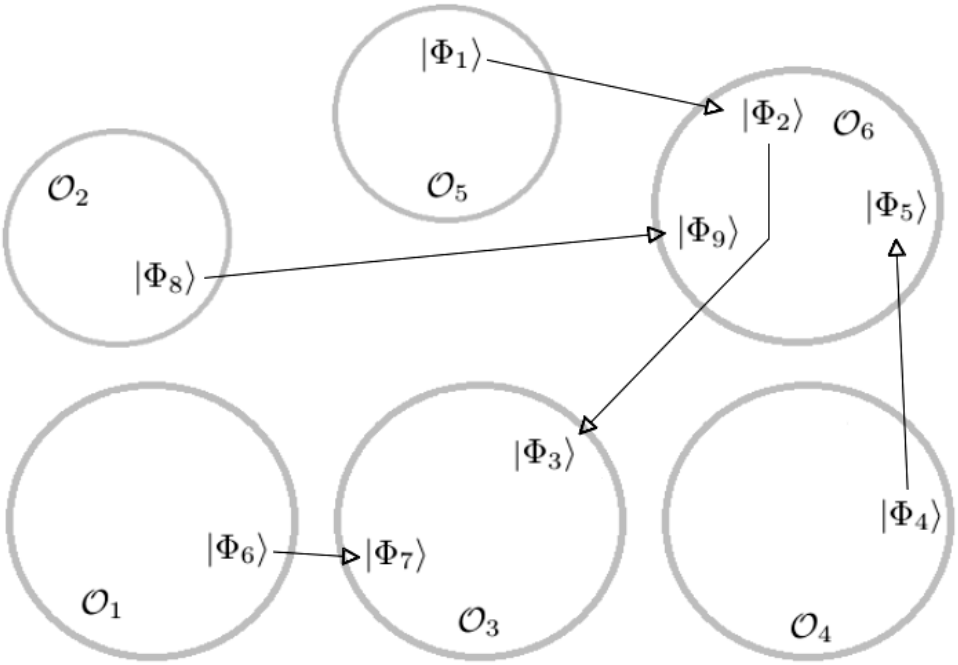


Figure 4.8 – Représentation des passages possibles entre les classes d'équivalence du groupe SLOCC, par action du groupe SLOCC et de la Transformée de Fourier Quantique. Les états quantiques regroupés dans le même cercle gris appartiennent à la même orbite SLOCC. Les flèches à tête blanche correspondent à l'application de la Transformée de Fourier Quantique. L'état le plus proche de la tête de la flèche est l'état résultat de la TFQ appliquée à l'état à la racine de la flèche.

Notre étude qualitative de l'algorithme concernait les états quantiques à trois ou quatre particules, et cela a permis d'avoir une première idée des classes d'intrication potentiellement impliquées dans l'algorithme. En revanche, il pourrait être plus intéressant (mais plus difficile) de considérer des cas où la taille des entiers à factoriser permet à l'algorithme de Shor de montrer en pratique son efficacité (par rapport aux algorithmes classiques) et de voir si l'intrication change (qualitativement ou quantitativement) dans ce cas.

En ce qui concerne les états périodiques, on pourrait continuer à établir des résultats généraux sur la classe d'intrication des états périodiques avant et après l'application de la TFQ, en fonction du shift et de la période. On peut également étudier plus précisément quels sont les états périodiques qui sont générés par l'algorithme de recherche de la période (après la mesure du second registre).

Aussi, durant cette thèse, nous n'avons considéré que des états périodiques aux coefficients réels positif et équilibrés. Il serait intéressant d'étudier l'influence de l'introduction de phases ou de coefficients, rompant l'équilibre dans l'expression des états périodiques, sur la classe d'intrication. Ceci pourrait éventuellement permettre de se rapprocher de la forme des états périodiques générés par l'algorithme de recherche de la période.

Comprendre plus en profondeur comment la TFQ crée ou modifie qualitativement et quantitativement l'intrication dans les états quantiques constitue également une perspective intéressante. On pourrait envisager tout d'abord une étude des circuits composés de portes H, $c\text{-}R_k$ et $SWAP$, dans le même esprit que l'étude menée par [22]. Enfin, on peut également poursuivre le travail sur l'étude des orbites sous l'action conjointe du groupe SLOCC et de la TFQ, et d'étudier si l'on peut toujours passer d'une classe d'intrication à une autre par cette action.

Troisième partie

La Géométrie Algébrique Au Service De l'Intrication Quantique

Dans la partie précédente, nous nous sommes principalement attardés à l'application d'outils déjà existants pour l'étude de l'intrication dans les algorithmes quantiques. Dans cette partie, en exploitant toujours la relation profonde entre l'intrication et la géométrie algébrique, nous tentons d'apporter des outils originaux afin de caractériser et d'étudier différemment ou de manière plus efficace l'intrication.

Dans le premier chapitre, nous utilisons les singularités simples des hypersurfaces comme invariants SLOCC pour caractériser l'intrication quantique. Nous nous intéressons au cas des systèmes à 3-qutrits et associons à chaque état une hypersurface, issue d'une construction originale de [137]. En étudiant les singularités de cette hypersurface, nous sommes en mesure de distinguer différentes classes d'intrication, et de ré-interpréter la classification des 3-qutrits.

Dans le second chapitre, nous nous intéressons aux états maximalement intriqués. Nous étudions les états maximalement intriqués du point de vue de différentes mesures algébriques et géométriques de l'intrication. De plus, nous considérons différents systèmes quantiques, notamment les états symétriques et fermioniques.

Enfin, dans le troisième chapitre, nous tentons de mettre en place des classifieurs de l'intrication par des méthodes d'apprentissage machine. En utilisant une approche par apprentissage supervisé, nous construisons des réseaux de neurones pour reconnaître l'appartenance ou non d'un point à une variété algébrique. Nous étudions trois différentes variétés liées à la notion d'intrication, et présentons des exemples d'application pour la classification de l'intrication sous l'action du groupe SLOCC.

Chapitre 5

Intrication et Singularités des Hypersurfaces

"Physicists explain creation by telling us that the universe began with the Big Bang, an intense energy singularity that continued expanding. But pray, please do explain who created the singularity ?", Ashwin Sanghi.

La variété duale associée à la variété de Segre définit les états dégénérés, les états non-génériques de l'espace projectif associé à l'espace de Hilbert. Comme établi précédemment, cette variété est définie par un unique polynôme, qui est l'hyperdéterminant. Cet objet trouve un lien étroit avec la notion d'intrication, que ce soit sur le plan qualitatif ou quantitatif. D'un point de qualitatif, les points singuliers associés à l'hyperdéterminant, et leurs types de singularité, définissent des classes d'intrication différentes, et il pourrait être intéressant d'étudier ce polynôme sous cet angle.

Dans ce chapitre, nous utilisons la théorie de singularités pour étudier les classes d'intrication des systèmes à 3-qutrits sous l'action du groupe SLOCC. L'idée développée ici est d'étudier les singularités des hypersurfaces associées à des états quantiques pour en tirer une information sur la classe d'intrication de ces états. Cette construction a été développée pour la première fois en 2014 par Holweck *et al.* [137], inspirée par une construction de Knop [161] et sera illustrée dans ce chapitre uniquement dans le cas des 3-qutrits, présentant principalement le travail mené dans [131].

5.1 Idée principale et construction géométrique

Un système à 3-qutrits est un système quantique composé de trois particules, disposant chacune de trois états de base. De ce fait un état à 3-qutrits $|\psi\rangle$ sera considéré comme un tenseur de l'espace de Hilbert associé $\mathcal{H}_{333} = \mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$, et pourra toujours être écrit comme

$$|\psi\rangle = \sum_{i,j,k \in [\![0,2]\!]} a_{ijk} |ijk\rangle \text{ avec } a_{ijk} \in \mathbb{C} \ . \tag{5.1}$$

On rappelle que X désigne la variété des états séparables, c'est à dire l'unique orbite fermée pour l'action de $G_{SLOCC} = \mathrm{SL}_3(\mathbb{C}) \times \mathrm{SL}_3(\mathbb{C}) \times \mathrm{SL}_3(\mathbb{C})$ sur $\mathbb{P}(H_{333})$, dont un

représentant est l'état $|000\rangle$. On peut paramétrer l'orbite X en utilisant le plongement de Segre (comme discuté Section 2.1.3) de trois plans projectifs :

$$\begin{array}{rccc} \text{Seg} : & \mathbb{P}^2 \times \mathbb{P}^2 \times \mathbb{P}^2 & \to & \mathbb{P}^{26} = \mathbb{P}(\mathcal{H}_{333}) \\ & ([x_0 : x_1 : x_2], [y_0 : y_1 : y_2], [z_0 : z_1 : z_2]) & \mapsto & [x_0y_0z_0 : \ldots : W_J : \ldots : x_2y_2z_2] \end{array}, \tag{5.2}$$

où $W_J = x_iy_jz_k$ pour $J = (i, j, k) \in [\![0, 2]\!]^3$. Les monômes, représentant chaque coordonnée dans $\mathbb{P}^{26}$, sont ordonnés selon la valeur de leurs indices en base 3, de telle sorte que $W_{J_1} < W_{J_2}$ si et seulement si $9i_1 + 3j_1 + k_1 \leq 9i_2 + 3j_2 + k_2$.

Une notion importante dans ce chapitre est celle d'hyperplan. À chaque système quantique modélisé par l'état $|\varphi\rangle$, on peut associer une forme linéaire sur l'espace de Hilbert $\mathcal{H}$ associé, que l'on notera $\langle\varphi|$, à l'aide du produit hermitien associé à l'espace de Hilbert. On définit alors l'hyperplan $H_\varphi \subset \mathbb{P}(\mathcal{H})$ comme le lieu des zéros de la forme linéaire $\langle\varphi|$, c'est à dire l'ensemble des états $|\psi\rangle \in \mathbb{P}(\mathcal{H})$ tels que $\langle\varphi|\psi\rangle = 0$.

À partir de l'hyperplan H_φ associé à un état $|\varphi\rangle$, on peut construire l'intersection $H_\varphi \cap X$, qui est la restriction de l'hyperplan aux états séparables. En d'autres termes, cette section $H_\varphi \cap X$ est l'ensemble des états séparables annulant la forme linéaire $\langle\varphi|$. En notant $\langle\varphi| = \sum_{i,j,k\in[\![0,2]\!]} h_{ijk}\langle ijk|$ la forme linéaire définissant l'hyperplan H_φ, la section hyperplane $H_\varphi \cap X$ sera, conformément au plongement de Segre (voir Équation 5.2), l'hypersurface X_φ de X définie par l'équation

$$\big\langle\varphi|\text{Seg}(\mathbb{P}^2 \times \mathbb{P}^2 \times \mathbb{P}^2)\big\rangle = \sum_{i,j,k\in[\![0,2]\!]} h_{ijk}x_iy_jz_k = 0 \text{ avec } h_{ijk} \in \mathbb{C} \ . \tag{5.3}$$

L'hypersurface X_φ, ainsi définie, peut présenter des singularités ou être lisse. Comme la variété X des états séparables est SLOCC-homogène, les types de singularité de l'hypersurface associée à $|\varphi\rangle$ et à $g|\varphi\rangle$ sont les mêmes, et ce, pour tout $g \in G_{SLOCC}$. En d'autres termes, le type de singularité de l'hypersurface X_φ est invariant sous l'action du groupe SLOCC. Toute quantité invariante sous l'action du groupe SLOCC peut en effet être utilisée pour caractériser les différentes orbites. Il devient alors intéressant d'étudier les classes d'intrication et de les caractériser à l'aide des singularités des hypersurfaces correspondantes.

En particulier, comme les états d'une même orbite sous l'action du groupe SLOCC doivent définir le même type de singularité d'hypersurface, si deux états sont associés à deux types de singularités différents, alors on peut conclure que ces états n'appartiennent pas à la même orbite, et donc qu'ils définissent deux types d'intrication distincts. En revanche, deux états définissant le même type de singularité ne sont pas nécessairement SLOCC équivalents. Plusieurs orbites peuvent en effet définir des hypersurfaces partageant le même type de singularité.

Dans les sections suivantes, nous définissons la notion de singularité simple, la classification de Arnold associée et comment déterminer le type de singularité en pratique. Nous nous focalisons ensuite sur le cas des sytèmes à 3-qutrits, en rappelant tout d'abord la classification des orbites sous l'action du groupe SLOCC dans le cas des 3-qutrits. Nous caractérisons ensuite chaque orbite par le biais du type de singularité associé.

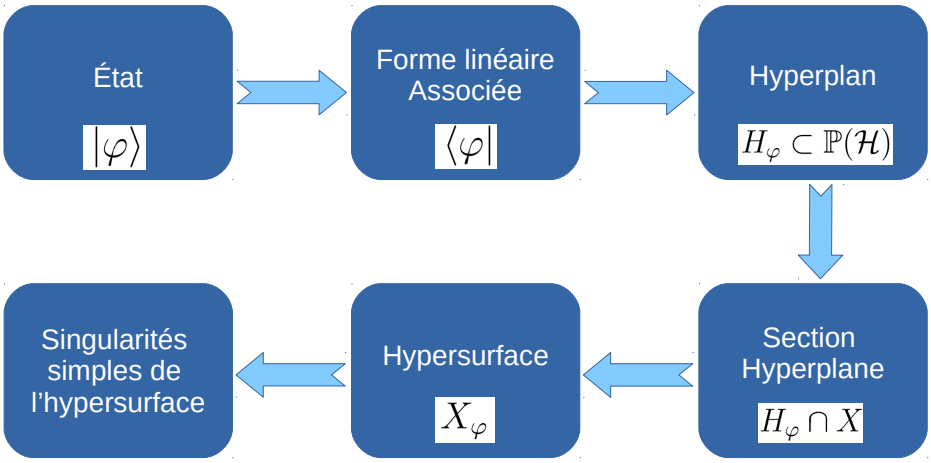


FIGURE 5.1 – Construction géométrique SLOCC invariante associant une singularité à un état quantique [137].

Nous rappelons enfin l'existence d'un lien entre ces derniers résultats et ce qui concerne le lieu singulier de la variété duale.

5.2 Les singularités simples

Dans cette section, nous introduisons tout d'abord la notion de singularité simple de fonctions complexes, notamment en rappelant la classification d'Arnold [11, 12]. Cette manière de caractériser les singularités simples permet naturellement l'implémentation pratique de critères pour identifier le type de singularité, que nous présenteront en deuxième partie de section.

5.2.1 La classification d'Arnold

La variété de Segre $X = \mathrm{Seg}(\mathbb{P}^{d-1} \times \cdots \times \mathbb{P}^{d-1}) \subset \mathbb{P}^{d^n-1}$ des n-dits est une variété algébrique rationnelle (elle est équivalente à un produit d'espaces projectifs par une application birationnelle [248]). De ce fait, les hypersurfaces X_φ seront définies par des polynômes homogènes à coefficients complexes. La classification est établie pour un cas plus général d'applications (ou germes d'applications) holomorphes $f : \mathbb{C}^n \to \mathbb{C}$.

On rappelle qu'une fonction holomorphe est une fonction à valeurs complexes, définie et dérivable sur l'ensemble (ou un sous-ensemble) des complexes. La notion de germe renvoie à des propriétés locales d'un objet mathématique, et permet notamment l'étude locale d'une fonction en termes de continuité ou de dérivabilité.

Définition 29. Un point $x \in \mathbb{C}^n$ est appelé *point critique* d'une fonction holomorphe f si à ce point x les dérivées de la fonction f sont égales à zéro.

Définition 30. Un point critique est dit *non-dégénéré* ou *point critique de Morse* si et seulement si la dérivée seconde partielle de la fonction en ce point est une forme quadratique non-dégénérée, c'est à dire si et seulement si la matrice Hessienne de f, au point critique, est de rang maximal.

Définition 31. Le *corang* d'un point critique d'une fonction est la dimension du noyau de la dérivée seconde au point critique.

On considère à présent l'ensemble $\mathcal{O}_n$ des germes de fonctions au point $0 \in \mathbb{C}^n$. Soit $\mathcal{D}_n$, le groupe des germes de l'application biholomorphe $g : (\mathbb{C}^n, 0) \to (\mathbb{C}^n, 0)$. Ce groupe agit sur l'espace $\mathcal{O}_n$ par la règle $g(f) = f \circ g^{-1}$, avec $f \in \mathcal{O}_n$ et $g \in \mathcal{D}_n$. Les orbites pour cette action seront alors exactement les classes d'équivalences des germes de fonctions.

Définition 32. Deux germes de fonctions au point 0 sont dit *équivalents* si l'on peut passer d'une fonction à une autre par un changement de coordonnées biholomorphe, laissant le point 0 invariant.

Ces premières définitions nous permettent à présent d'introduire la notion de singularité.

Définition 33. Deux points critiques sont dit *équivalents* si les germes de fonction les définissant sont équivalents. La classe d'équivalence d'un germe de fonction à un point critique est appelée *singularité*.

Remarque 34. À partir de cette définition, il vient que le corang d'un point critique est un invariant de la classe d'équivalence définie par la singularité. De ce fait, une singularité sera dite de type Morse (aussi appelée non-dégénérée ou quadratique) si et seulement si son corang est égal à 0.

Définition 35. Deux germes de fonction $f : (\mathbb{C}^n, 0) \to (\mathbb{C}, 0)$ et $h : (\mathbb{C}^m, 0) \to (\mathbb{C}, 0)$, avec $n \leq m$, sont *équivalents en stabilité* si ces fonctions deviennent équivalentes après l'addition d'une forme quadratique non-dégénérée en des variables supplémentaires :

$$f(x_1, \ldots, x_n) + {x_{n+1}}^2 + \cdots + {x_m}^2 \sim h(y_1, \ldots, y_m) \ . \tag{5.4}$$

Cette définition nous permet de comparer les dégénérescences des points critiques des fonctions dépendant d'un nombre de variables différent. Ajouter des termes quadratiques de rang maximal dépendant de nouvelles variables n'affecte pas la classification du type de singularité.

Il existe aussi un autre invariant des singularités pouvant être utile pour distinguer différents types de singularité ayant le même corang. Cet invariant est le nombre de Milnor, aussi appelé la multiplicité du point critique, et est défini en introduisant le quotient suivant :

Définition 36. L'*algèbre locale $\mathcal{Q}_f$ de la singularité de f*, est définie comme le quotient de l'algèbre des germes de fonction par l'idéal du gradient de f :

$$\mathcal{Q}_f = \mathcal{O}_n / \mathbf{I}_{\nabla_f} \ , \text{ avec } \mathbf{I}_{\nabla_f} = \mathcal{O}_n \langle f_1, \ldots, f_n \rangle \ . \tag{5.5}$$

l'idéal du gradient généré par les dérivées partielles $f_i = \partial f / \partial x_i$ de la fonction f.

Définition 37. La multiplicité d'un point critique, c'est à dire le nombre de Milnor μ d'une singularité d'un germe $(f, 0)$, est égale à la dimension de l'algèbre locale de $(f, 0)$,

$$\mu = \dim_{\mathbb{C}} (\mathcal{Q}_f) = \dim_{\mathbb{C}} \left(\mathcal{O}_n / \mathbf{I}_{\nabla_f} \right) \ . \tag{5.6}$$

Il est intéressant de préciser ici qu'un point critique sera dit *isolé* si et seulement si $\mu < \infty$. D'autre part, les singularités simples ont été définies par Arnold comme étant les classes de singularités qui sont stables, au sens définit ci-dessous :

Définition 38. Une singularité $(f, 0)$ est dite simple si et seulement si une perturbation (suffisamment) faible de la singularité génère uniquement un nombre fini de classes non-équivalentes.

Remarque 39. On remarque, à partir de cette définition, qu'une singularité $(f, 0)$ de type Morse est simple ssi toute fonction $f + \varepsilon h$ (pour ε petit) est soit non-singulière ou soit de matrice Hessienne de rang maximal.

Dans sa classification des singularités simples [12], Arnold a prouvé qu'être une singularité simple est équivalent à une des conditions suivantes :

- $\mu < \infty$,
- $\mathsf{corang}\left(\frac{\partial^2 f}{\partial x_i \partial x_j}(x_0)\right) \leq 2$,
- $\mathsf{corang}\left(\frac{\partial^2 f}{\partial x_i \partial x_j}(x_0)\right) = 2$, et le terme cubique dans les directions dégénérées de la matrice Hessienne est non nul,
- $\mathsf{corang}\left(\frac{\partial^2 f}{\partial x_i \partial x_j}(x_0)\right) = 2$, et le terme cubique dans les directions dégénérées de la matrice Hessienne est un cube, et $\mu < 9$.

À l'aide de ces conditions, Arnold a pu obtenir une classification des singularités simples en 5 différents types, deux séries infinies A_n et D_n, et trois exceptionnelles E_6, E_7 et E_8, permettant d'établir la classification des singularité simples présentée en Table 5.1.

$A_n, n \geq 1$	$D_n, n \geq 4$	E_6	E_7	E_8
x^{n+1}	$x^2y + y^{n-1}$	$x^3 + y^4$	$x^3 + xy^3$	$x^3 + y^5$

TABLE 5.1 – Formes normales associées aux singularités simples. Le nombre de Milnor est noté n ici.

Remarque 40. Un germe de fonction $(f, 0)$ avec une singularité simple est équivalent en stabilité à une des formes normales de la Table 5.1.

Remarque 41. En reprenant les notations de la Table 5.1, la singularité de type Morse correspond aux singularités simples de type A_1.

À partir de ces définitions et de la classification introduite par Arnold, nous expliquons dans la prochaine sous-section comment procéder en pratique au calcul et à la détermination du type de singularité associé à une hypersurface.

5.2.2 Calcul du type de singularité

Dans cette sous-section, on s'intéresse à la détermination effective du type de singularité par le calcul, à partir des éléments théoriques définis à la sous-section précédente.

Nous utilisons principalement le logiciel de calcul formel Maple 17 [1] et le programme Singular 3.1.6. [84] afin de réaliser ces calculs.

Comme précisé précédemment, tout système quantique à 3-qutrits $|\varphi\rangle$ définit une unique forme linéaire $\langle\varphi|$, définissant elle même un hyperplan H_φ. En intersectant cet hyperplan avec la variété des états séparables, on obtient l'hypersurface X_φ définie par un polynôme homogène P défini sur $\mathbb{P}^2 \times \mathbb{P}^2 \times \mathbb{P}^2$, par plongement de Segre (voir Équation 5.3), dépendant des coefficients définissant l'état $|\varphi\rangle$.

On étudie ensuite ce polynôme dans différentes *cartes*, en fixant une des trois variables x_i à 1, une des trois variables y_j à 1 et une des trois autres variables z_k à 1. L'étude de P dans une carte précise redéfinit son écriture, que l'on notera P_{ijk} (dans la carte $[i, j, k]$) défini sur $\mathbb{C}^6$, et on recherche ensuite les éventuels points critiques de cette hypersurface, en recherchant les points $\mathbf{x}$ tels que $P_{ijk}(\mathbf{x}) = 0$ et $\nabla P_{ijk}(\mathbf{x}) = 0$ (toutes les dérivées partielles s'annulent). L'étude de ce polynôme dans chaque carte possible permettra de mettre en évidence les multiplicités des types de singularité rencontrés. Aussi, si un polynôme ne présente aucune singularité dans aucune carte, alors la section hyperplane ne présente aucune singularité et est lisse.

Dans cette étude, nous nous intéressons uniquement aux singularités simples et isolées. Toute singularité non-isolée sera considérée comme telle, et nous ne cherchons pas à différencier les singularités non-isolées entre elles. Dans notre cas, on considérera qu'une solution $\mathbf{x}$ de $P_{ijk}(\mathbf{x}) = 0$ et $\nabla P_{ijk}(\mathbf{x}) = 0$ est isolée si et seulement si les valeurs des variables x_i, y_j et z_k définissant la solution $\mathbf{x}$ sont indépendantes entre elles. Par exemple, une solution du type $\{x_1 = z_1, y_0 = 0, y_1 = \frac{1}{z_1}, z_0 = 0, z_1 = z_1\}$ dans la carte $[2, 2, 2]$ sera considérée comme non-isolée.

Si le point singulier est un point isolé, on calcule ensuite le corang de la matrice Hessienne du polynôme P_{ijk}. Pour rappel, la matrice Hessienne $H(f)$ d'une fonction f dépendant des variables $(x_1, \ldots, x_n)$ est la matrice des dérivées partielles de f, de telle sorte que le coefficient d'indice i, j vérifie $H_{ij}(f) = \dfrac{\partial^2 f}{\partial x_i \partial x_j}$. Comme rappelé en Remarque 39, si le corang de la matrice Hessienne est égal à 0 (et donc le rang est maximal) alors la singularité est de type A_1 (de type Morse). Si le corang de la matrice Hessienne est égal à 1, alors la singularité est de type A_n avec $n \geq 2$. Enfin, si le corang est égal à 2, la singularité peut être de type D_n avec $n \geq 4$, de type E_6, de type E_7 ou de type E_8. Si le corang est supérieur à 2, alors la singularité n'est plus une singularité simple.

Enfin, le calcul effectif de la multiplicité de la singularité μ (nombre de Milnor) se fait à l'aide du logiciel Singular, et permet de déterminer n lorsque le corang est égal à 1 ou 2, permettant notamment de différencier (dans la plupart des cas) entre les singularités de même corang. Toutes ces étapes de calcul sont résumées de manière succincte et simplifiée dans l'Algorithme 2.

Algorithme 2 SingularType

Require: Y un vecteur de taille 27, représentant l'état à 3 qutrits
Ensure: Le type de singularité simple de Y

• Définition du polynôme $P(x_0, x_1, x_2, y_0, \ldots, z_2)$ de l'hypersurface de l'état considéré
for chaque carte [i,j,k] avec (i,j,k)=0..2 **do**

• Restriction du polynôme P en substituant $x_i = y_j = z_k = 1$

• Détermination de(s) point(s) singulier(s) isolé(s) éventuel(s) de l'hypersurface ($P_{ijk} = 0$ et $\nabla P_{ijk} = 0$, et solutions indépendantes pour être isolé)

• Si le point est isolé, on calcule le corang de la matrice Hessienne :

Type	A_1	$A_{n>1}$	$D_{n\geq 4}$	E_6	E_7	E_8
Corang	0	1	2	2	2	2

• Si besoin, on calcule le nombre de Milnor μ qui est la multiplicité de la singularité, permettant de les distinguer (partiellement, voir Remarque 42).
end for

Remarque 42. L'Algorithme 2 n'est à priori pas suffisant pour traiter tous les cas, car il faudrait analyser la forme cubique dans les directions dégénérées. Il s'avère que dans notre cas d'étude, les types de singularité obtenus ne le nécessitaient pas.

On se propose à présent d'étudier deux exemples pratiques et de déterminer le type de singularité associé.

Exemple 7. Soit $H_{\varphi_1} \in \mathbb{P}({\mathcal{H}_{333}}^*)$ un hyperplan associé à la forme linéaire $\langle\varphi_1| = \langle 000| + \langle 111| + \langle 222|$. La section hyperplane $H_{\varphi_1} \cap X$ est tangente à $|A\rangle = |021\rangle$. En effet, un vecteur tangent de X à $|A\rangle$ est de la forme $|t_1\rangle = \alpha|121\rangle + \beta|221\rangle + \delta|001\rangle + \sigma|011\rangle + \lambda|020\rangle + \epsilon|022\rangle$, et on peut aisément vérifier que $\langle\varphi_1|t_1\rangle = 0$. La fonction définissant $H_{\varphi_1} \cap X$ correspond à la restriction de la forme linéaire à X (la variété des états séparables), et peut être exprimée comme :

$$f_1(x_0, x_1, x_2, y_0, y_1, y_2, z_0, z_1, z_2) = x_0y_0z_0 + x_1y_1z_1 + x_2y_2z_2 \ . \tag{5.7}$$

De plus, f_1 peut être écrite dans la carte $[0, 2, 1]$, correspondant à $x_0 = y_2 = z_1 = 1$, comme un polynôme homogène à 6 variables :

$$f_1(x_1, x_2, y_0, y_1, z_0, z_2) = y_0z_0 + x_1y_1 + x_2z_2 \ . \tag{5.8}$$

Nous cherchons ensuite les points singuliers de ce polynôme, en résolvant les deux équations $f_1(x_1, x_2, y_0, y_1, z_0, z_2) = 0$ et $\nabla f_1(x_1, x_2, y_0, y_1, z_0, z_2) = 0$. Ceci revient à résoudre les équations suivantes :

$$y_0z_0 + x_1y_1 + x_2z_2 = 0, y_1 = 0, z_2 = 0 \ , \tag{5.9}$$

$$z_0 = 0, x_1 = 0, y_0 = 0, x_2 = 0 \ . \tag{5.10}$$

Nous trouvons une solution unique qui est $x_1 = x_2 = y_0 = y_1 = z_0 = z_2 = 0$, correspondant au point $|A\rangle = |021\rangle$ dans cette carte. La matrice Hessienne de f_1, au point $x = |A\rangle$, est

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} ,$$

qui est de rang 6, c'est-à-dire de rang maximal. On peut alors conclure que le point $|A\rangle = |021\rangle$ de l'hypersurface $H_{\varphi_1} \cap X$ est un point singulier isolé de type A_1.

♢

Exemple 8. Soit $H_{\varphi_2} \in \mathbb{P}(\mathcal{H}_{333}{}^*)$ un hyperplan associé à la forme linéaire $\langle\varphi_2| = \langle 012| + \langle 021| + \langle 102| + \langle 110| + \langle 111| + \langle 200|$. La section hyperplane $H_{\varphi_2} \cap X$ est tangente à $|B\rangle = |222\rangle$. En effet, un vecteur tangent de X à $|B\rangle$ est de la forme $|t_2\rangle = \alpha|022\rangle + \beta|122\rangle + \delta|202\rangle + \sigma|212\rangle + \lambda|220\rangle + \epsilon|221\rangle$, et on peut aisément vérifier que $\langle\varphi_1|t_2\rangle = 0$. La fonction définissant $H_{\varphi_2} \cap X$correspond à la restriction de la forme linéaire à X (la variété des états séparables), et peut être exprimée comme :

$$f_2(x_0, x_1, x_2, y_0, y_1, y_2, z_0, z_1, z_2) = x_0y_1z_2 + x_0y_2z_1 + x_1y_0z_2 + x_1y_1z_0 + x_1y_1z_1 + x_2y_0z_0 \ . \tag{5.11}$$

De plus, f_2 peut être écrite dans la carte $[2, 2, 2]$, correspondant à $x_2 = y_2 = z_2 = 1$, comme un polynôme non-homogène à 6 variables :

$$f_2(x_0, x_1, y_0, y_1, z_0, z_1) = x_0y_1 + x_0z_1 + x_1y_0 + x_1y_1z_0 + x_1y_1z_1 + y_0z_0 \ . \tag{5.12}$$

Nous cherchons ensuite les points singuliers de ce polynôme, en résolvant les deux équations $f_2(x_0, x_1, y_0, y_1, z_0, z_1) = 0$ et $\nabla f_2(x_0, x_1, y_0, y_1, z_0, z_1) = 0$. Ceci revient à résoudre les équations suivantes :

$$x_0y_1 + x_0z_1 + x_1y_0 + x_1y_1z_0 + x_1y_1z_1 + y_0z_0 = 0, y_1 + z_1 = 0 \ , \tag{5.13}$$

$$y_0 + y_1z_0 + y_1z_1 = 0, x_1 + z_0 = 0, x_0 + x_1z_0 + x_1z_1 = 0 \ , \tag{5.14}$$

$$x_1y_1 + y_0 = 0, x_0 + x_1y_1 = 0 \ . \tag{5.15}$$

Nous trouvons une solution unique qui est $x_0 = x_1 = y_0 = y_1 = z_0 = z_1 = 0$, correspondant au point $|B\rangle = |222\rangle$ dans cette carte. La matrice Hessienne de f_2, au point $x = |B\rangle$, est

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} ,$$

qui est de rang 4, et donc de corang 2. On peut vérifier, en utilisant un logiciel de calcul formel comme Singular, que le nombre de Milnor de cette singularité d'hypersurface est $\mu = 4$. On peut alors conclure que le point $|B\rangle = |222\rangle$ de l'hypersurface $H_{\varphi_2} \cap X$ est un point singulier isolé de type D_4.

♢

5.3 Classification des 3-qutrits et singularités simples

Dans cette section nous nous intéressons au problème de classification des états à 3-qutrits sous l'action du groupe SLOCC, du point de vue des singularités simples associées à chaque orbite. Nous rappelons tout d'abord la classification des 3-qutrits sous SLOCC et les différentes familles d'orbites connues. Nous présentons ensuite les résultats de nos calculs et les singularités associées à chaque orbite. Enfin, nous réinterprétons ces derniers résultats du point de vue de lieux singuliers de la variété duale et des perturbations de la stabilité des états et des singularités associées. Ceci nous permet de proposer une stratification de l'espace de Hilbert en termes de singularités de la variété duale.

5.3.1 Classification des matrices $3 \times 3 \times 3$ et familles de Nurmiev

En 2000, Nurmiev a présenté une classification des matrices de taille $3 \times 3 \times 3$ dans $\mathbb{C}$, sous l'action du groupe $G_{SLOCC} = \mathrm{SL}_3(\mathbb{C}) \times \mathrm{SL}_3(\mathbb{C}) \times \mathrm{SL}_3(\mathbb{C})$ [201].

Tout tenseur $|\psi\rangle$ de taille $3 \times 3 \times 3$ peut s'écrire de manière unique sous la forme $|T\rangle = |S\rangle + |N\rangle$, où $|S\rangle$ est semi-simple, et où $|N\rangle$ est nilpotent. Un tenseur de taille $3 \times 3 \times 3$ est dit semi-simple si son orbite sous SLOCC est fermée, et est dit nilpotent si la fermeture de son orbite sous SLOCC contient le tenseur nul [50].

Nurmiev a démontré que tout tenseur semi-simple est SLOCC-équivalent à un tenseur de la forme

$$|S\rangle = aX_1 + bX_2 + cX_3 \ , \tag{5.16}$$

avec

$$X_1 = |000\rangle + |111\rangle + |222\rangle, \quad X_2 = |012\rangle + |120\rangle + |201\rangle, \quad X_3 = |021\rangle + |102\rangle + |210\rangle \ . \tag{5.17}$$

La variété des états nilpotents coïncide avec le cône nilpotent, qui est la variété où tous les invariants s'annulent [195, 49, 50].

Par ailleurs, selon Nurmiev [201], les orbites sous l'action du groupe SLOCC de l'espace de Hilbert $\mathcal{H}_{333}$ des 3-qutrits consiste en 5 familles : 4 familles dépendent de paramètres et une en est indépendante (c'est le cône nilpotent). Les formes normales correspondant à chaque famille sont connues et décrites dans [201]. Chaque famille est une combinaison linéaire des trois vecteurs X_1, X_2 et X_3, plus un partie nilpotente. Les coefficients complexes a, b et c associés à ces vecteurs doivent vérifier un ensemble de conditions, listées comme suit :

- première famille F_1 : $abc \neq 0$, $(a^3 + b^3 + c^3)^3 - (3abc)^3 \neq 0$,
- deuxième famille F_2 : $b\,(a^3 + b^3) \neq 0$, $c = 0$,
- troisième famille F_3 : $a \neq 0$, $b = c = 0$,
- quatrième famille F_4 : $c = -b \neq 0$, $a = 0$.

La cinquième famille de la classification de Nurmiev ne dépend d'aucun paramètre est appelée le cône nilpotent, et ne contient que des orbites nilpotentes (pas de partie semi-simple). Géométriquement, le cône nilpotent $\mathcal{N} \subset \mathbb{P}^{26}$ est une variété de dimension 23, définie comme les points annulant les 3 générateurs de l'algèbre des polynômes SLOCC-invariants de $\mathcal{H}_{333}$ [51].

Les listes des formes linéaires associées aux formes normales de chaque famille ou strate du cône nilpotent sont regroupées en Table 5.2 et 5.3. Dans la sous-section suivante, pour chaque famille de Nurmiev ou orbite du cône nilpotent, nous calculons la section hyperplane correspondante et nous étudions le type de singularité associé (comme cela est explicité dans la Section 5.2.2).

5.3.2 Singularités simples et systèmes à 3-qutrits

L'étude des singularités simples associées aux hypersurfaces définies par les systèmes à 3-qutrits nous permet d'établir le théorème suivant :

Théorème 5.3.1. *Soit $H_\varphi \cap X$ une section hyperplane singulière (non lisse) de la variété algébrique des états séparables pour les systèmes à 3-qutrits, c'est à dire $X = \mathrm{Seg}(\mathbb{P}^2 \times \mathbb{P}^2 \times \mathbb{P}^2) \subset \mathbb{P}^{26}$, définie par un état quantique pur $|\varphi\rangle \in \mathbb{P}(\mathcal{H}_{333}) = \mathbb{P}^{26}$. Alors $H_\varphi \cap X$ n'admet que des singularités simples ou non-isolées. De plus, si x est un point singulier isolé de $H_\varphi \cap X$, alors son type de singularité est soit A_1, A_2, A_3 ou D_4.*

Afin de prouver ce théorème, le calcul du type de singularité pour chacune des sections $H_\varphi \cap X$ est nécessaire. Ceci est effectué pour toutes les formes normales proposées par Nurmiev. Pour chaque famille et sous -famille, nous calculons le type de singularité associé. Certaines familles dépendent de paramètres. Nous calculerons alors les types de singularité en considérant ces coefficients a, b et c comme étant génériques, puis en les introduisant comme des variables supplémentaires lors de la recherche de points singuliers (tout en précisant les contraintes imposées par la définition de chaque famille, voir Section 5.3.1).

Les résultats obtenus à l'issue de ces calculs prouvent le Théorème 5.3.1, à savoir que seulement les types de singularité A_1, A_2, A_3 et D_4 sont atteints. L'ensemble des résultats est rassemblé en Table 5.2 et 5.3.

5.3.3 Structure en oignon et lieu singulier de la variété duale

En reprenant les notations de la Table 5.2, la famille $F_{1,1}$ est la forme générique d'un état semi-simple, et ces états sont les plus stables, au sens où perturber l'état par l'action $|F_{1,1}\rangle \rightsquigarrow |F_{1,1}\rangle + \varepsilon|\psi\rangle$ ne modifiera pas l'appartenance de l'état à la famille $F_{1,1}$. Du point de vue de notre construction, cela se traduit par le fait que l'intersection $H_{F_{1,1}} \cap X$ est une hypersurface lisse, et qu'une petite perturbation de celle-ci donnera également une hypersurface lisse.

Ensuite, les hypersurfaces ne possédant que des singularités simples sont les hypersurfaces les plus stables après les hypersurfaces lisses. Conformément à la définition

Orbites	**Hyperplan associé**	**Paramètres**	**Type de singularité**
$F_{1,1}$	$aX_1{}^\dagger + bX_2{}^\dagger + cX_3{}^\dagger$	a,b,c génériques	Section lisse
$F_{2,1}$	$aX_1{}^\dagger + bX_2{}^\dagger + \langle 021| + \langle 102|$	a,b génériques $a = 0$	A_1 $3A_1$
$F_{2,2}$	$aX_1{}^\dagger + bX_2{}^\dagger + \langle 021|$	a,b génériques $a = 0$	$2A_1$ $3A_1$
$F_{2,3}$	$aX_1{}^\dagger + bX_2{}^\dagger + \langle 201|$	a,b génériques $a = 0$	$3A_1$ $3A_1$
$F_{3,1}$	$aX_1{}^\dagger + \langle 012| + \langle 021| + \langle 102| + \langle 120|$	a générique	$2A_1$
$F_{3,2}$	$aX_1{}^\dagger + \langle 012| + \langle 021| + \langle 102|$	a générique	$3A_1$
$F_{3,3}$	$aX_1{}^\dagger + \langle 012| + \langle 021| + \langle 120|$	a générique	$3A_1$
$F_{3,4}$	$aX_1{}^\dagger + \langle 012| + \langle 021|$	a générique	$4A_1$
$F_{3,5}$	$aX_1{}^\dagger + \langle 012| + \langle 120|$	a générique	$4A_1$
$F_{3,6}$	$aX_1{}^\dagger + \langle 021| + \langle 102|$	a générique	$4A_1$
$F_{3,7}$	$aX_1{}^\dagger + \langle 012|$	a générique	$5A_1$
$F_{3,8}$	$aX_1{}^\dagger + \langle 021|$	a générique	$5A_1$
$F_{3,9}$	$aX_1{}^\dagger$	a générique	$6A_1$
$F_{4,1}$	$b(X_2{}^\dagger - X_3{}^\dagger) + \langle 002| + \langle 020| + \langle 111| + \langle 200|$	b générique	A_2
$F_{4,2}$	$b(X_2{}^\dagger - X_3{}^\dagger) + \langle 002| + \langle 011| + \langle 020|$ $+\langle 101| + \langle 110| + \langle 200|$	b générique	A_3
$F_{4,3}$	$b(X_2{}^\dagger - X_3{}^\dagger) + \langle 000| + \langle 111|$	b générique	D_4
$F_{4,4}$	$b(X_2{}^\dagger - X_3{}^\dagger) + \langle 001| + \langle 010| + \langle 100| + \langle 200|$	b générique	Non-isolée
$F_{4,5}$	$b(X_2{}^\dagger - X_3{}^\dagger) + \langle 000|$	b générique	Non-isolée
$F_{4,6}$	$b(X_2{}^\dagger - X_3{}^\dagger)$	b générique	Non-isolée

TABLE 5.2 – Hyperplans et types de singularité des hypersurfaces X_φ correspondantes pour un $|\varphi\rangle$ dépendant de paramètres.

d'une singularité simple par Arnold, la connaissance du type de singularité d'une hypersurface X_φ fournit une information sur les déformations possibles de cette singularité, par une petite perturbation. En particulier, une telle déformation de la singularité D_4 produit des singularités de type A_3, A_2 et A_1, comme résumé dans le diagramme d'adjacence suivant :

$$A_1 \leftarrow A_2 \leftarrow A_3 \leftarrow D_4 \ . \tag{5.18}$$

Ceci nous permet d'établir que les états équivalents à la forme normale correspondant à la famille $F_{4,3}$ (singularité de type D_4) peuvent, sous l'action d'une petite perturbation, amener à des états du type $F_{4,2}$ (singularité de type A_3), $F_{4,1}$ (singularité de type A_2), $F_{2,1}$ (singularité de type A_1) ou $F_{1,1}$ (section lisse). Il en va de même pour l'orbite N_2 (singularité de type D_4) du cône nilpotent qui peut produire un état de l'orbite N_1 (singularité de type A_3) après une légère perturbation. Ceci nous permet entre autres de hiérarchiser les différentes familles et orbites, en observant les familles ou orbites pouvant être générées par perturbation d'une forme normale donnée.

Orbite	**Hyperplan associé**	**Type singularité**
N_1	$\langle 012\vert + \langle 021\vert + \langle 102\vert + \langle 111\vert + \langle 120\vert + \langle 200\vert$	A_3
N_2	$\langle 012\vert + \langle 021\vert + \langle 102\vert + \langle 110\vert + \langle 111\vert + \langle 200\vert$	D_4
N_3	$\langle 002\vert + \langle 011\vert + \langle 020\vert + \langle 111\vert + \langle 120\vert + \langle 200\vert$	Non-isolée
N_4	$\langle 002\vert + \langle 011\vert + \langle 101\vert + \langle 110\vert + \langle 220\vert$	Non-isolée
N_5	$\langle 002\vert + \langle 020\vert + \langle 021\vert + \langle 110\vert + \langle 201\vert$	Non-isolée
N_6	$\langle 002\vert + \langle 011\vert + \langle 101\vert + \langle 120\vert + \langle 210\vert$	Non-isolée
N_7	$\langle 002\vert + \langle 011\vert + \langle 020\vert + \langle 101\vert + \langle 210\vert$	Non-isolée
N_8	$\langle 002\vert + \langle 020\vert + \langle 111\vert + \langle 200\vert$	Non-isolée
N_9	$\langle 000\vert + \langle 011\vert + \langle 111\vert + \langle 122\vert$	Non-isolée
N_{10}	$\langle 002\vert + \langle 011\vert + \langle 020\vert + \langle 101\vert + \langle 110\vert + \langle 200\vert$	Non-isolée
N_{11}	$\langle 002\vert + \langle 020\vert + \langle 101\vert + \langle 210\vert$	Non-isolée
N_{12}	$\langle 002\vert + \langle 020\vert + \langle 100\vert + \langle 111\vert$	Non-isolée
N_{13}	$\langle 002\vert + \langle 011\vert + \langle 020\vert + \langle 101\vert + \langle 110\vert$	Non-isolée
N_{14}	$\langle 002\vert + \langle 010\vert + \langle 021\vert + \langle 100\vert + \langle 201\vert$	Non-isolée
N_{15}	$\langle 011\vert + \langle 022\vert + \langle 100\vert$	Non-isolée
N_{16}	$\langle 002\vert + \langle 011\vert + \langle 020\vert + \langle 100\vert$	Non-isolée
N_{17}	$\langle 001\vert + \langle 010\vert + \langle 102\vert + \langle 120\vert$	Non-isolée
N_{18}	$\langle 000\vert + \langle 011\vert + \langle 101\vert + \langle 112\vert$	Non-isolée
N_{19}	$\langle 002\vert + \langle 010\vert + \langle 101\vert$	Non-isolée
N_{20}	$\langle 000\vert + \langle 111\vert$	Non-isolée
N_{21}	$\langle 001\vert + \langle 010\vert + \langle 100\vert$	Non-isolée
N_{22}	$\langle 000\vert + \langle 011\vert + \langle 022\vert$	Non-isolée
N_{23}	$\langle 000\vert + \langle 011\vert$	Non-isolée
N_{24}	$\langle 000\vert$	Non-isolée

Table 5.3 – Hyperplans et types de singularité des hypersurfaces X_φ correspondantes pour $|\varphi\rangle$ dans le cône nilpotent des états à 3-qutrits. L'orbite triviale (vecteur nul) est omise.

D'autre part, l'étude du type de singularité des hypersurfaces X_φ peut aussi être interprétée en termes de lieu singulier de la variété duale X^* (voir Section 2.1.8). La variété duale est généralement une hypersurface, invariante sous l'action du groupe SLOCC, et est définie par une équation polynomiale appelée hyperdéterminant. L'hypersurface associée est singulière et de codimension 1. Par définition (voir Section 2.1.8), la variété X^* paramétrise les sections hyperplanes singulières de X. Ainsi, H est un hyperplan n'appartenant pas à la variété duale X^* si et seulement si l'intersection $H \cap X$ est lisse et ne présente aucune singularité [137]. Dans le cas des 3-qutrits, les points n'appartenant pas à la variété duale sont équivalents à la famille $F_{1,1}$. Cet invariant permet donc d'identifier les états les plus génériques, aussi appelés non-dégénérés.

Cela constitue donc un moyen pratique de vérifier si un état $|\varphi\rangle$ appartient ou non à la variété duale, en construisant l'hypersurface X_φ associée, et en observant si elle est lisse ou si elle présente des singularités. Cette observation constitue de ce fait une solution intéressante pour évaluer la nullité de l'hyperdéterminant pour un état

donné, notamment lorsque l'expression de l'hyperdéterminant n'est pas connue. Ceci sera notamment utilisé au Chapitre 7 pour vérifier la validité du classifieur associé aux états non-dégénérés pour le cas des 5-qubits.

L'hyperdéterminant (en particulier celui de taille $3 \times 3 \times 3$ dans le cas des 3-qutrits) peut être utilisé pour décrire les classes d'intrication en étudiant le lieu singulier de l'hypersurface définie par ce polynôme. En effet, les points lisses de l'hypersurface représentant la variété duale correspondent à des sections hyperplanes avec un unique point singulier de type A_1 (Morse). Dans le cas des 3-qutrits, ces points lisses de la variété duale correspondent aux états génériques de la famille $F_{2,1}$. Il a été par ailleurs prouvé (avec l'exception du cas des 3-qubits) que le lieu singulier de la variété duale est de codimension 1 dans la variété duale. Ainsi l'étude de la variété duale X^*, et du lieu singulier de la variété duale X^*_{sing}, peut amener à une classification originale des états quantiques [274].

Le lieu singulier de la variété duale X^*_{sing} regroupe deux types de points singuliers

$$X^*_{sing} = X^*_{node} \cup X^*_{cusp} \ . \tag{5.19}$$

Les points de type *node* correspondent aux sections hyperplanes ayant plusieurs (plus que un) points singuliers isolés. Les points de type *cusp* correspondent aux sections hyperplanes ayant un point singulier qui n'est pas de type A_1. Ces notions liées aux singularités des hyperdéterminants, et donc de la variété duale, ont été étudiées par Weyman et Zelevinksy [274], et ont été utilisées plus tard dans le contexte de l'étude de l'intrication par Miyake [190].

De plus, on peut distinguer différents type de singularité *node* ou *cusp* en observant la multiplicité des points singuliers de la section hyperplane associée : cette multiplicité est égale à la somme des nombres de Milnor de tous les points singuliers isolés [85, 215]. À partir des résultats obtenus à la Section 5.3.2, nous pouvons établir, à titre d'exemple, que l'état $|F_{3,6}\rangle$ appartient à $X^*_{node,4}$, tandis que l'état $|N_1\rangle$ appartient à $X^*_{cusp,3}$.

De ce fait, nos résultats présentés en Section 5.3.2 pour le cas des 3-qutrits nous permettent de décrire la stratification induite par les points singuliers de la variété duale X^*. Cette stratification de l'espace de Hilbert $\mathcal{H}_{333}$ par des variétés invariantes sous l'action du groupe SLOCC peut être représentée sous la forme d'un diagramme en structure d'oignon (voir Figure 5.2), dans l'esprit de la structure en oignon proposée par Miyake pour la classification des systèmes à 3-qubits [190].

Cette construction peut alors se montrer intéressante dans le contexte de la classification des états intriqués sous l'action du groupe SLOCC, proposant une approche originale pour distinguer ou hiérarchiser différents types d'intrication.

5.4 Perspectives

Dans cette section nous proposons quelques idées et perspectives pour poursuivre le travail autour de l'algorithme de Shor présenté dans ce chapitre.

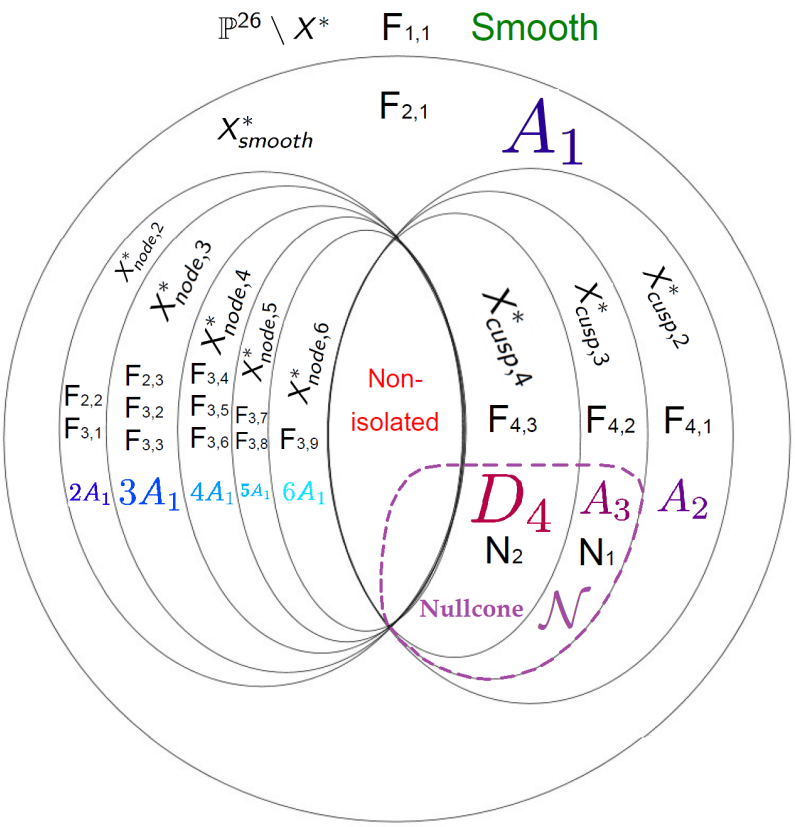


Figure 5.2 – Structure en oignon de l'espace de Hilbert $\mathcal{H}_{333}$ associé aux 3-qutrits [131].

Tout d'abord, une poursuite de ce travail pourrait s'intéresser à d'autres cas d'études. Par exemple, on peut étudier les singularités associées aux états fermioniques $(3, 9)$ et $(4, 8)$ (voir chapitre suivant). De plus, on peut également s'intéresser à des états spécifiques et les caractériser par rapport à leurs singularités (états liés aux graphes ou hypergraphes, les classifications des états symétriques, certains formes connues pour des états à 5-qubits, etc.).

Aussi, il est possible d'aller plus loin dans la description des états en étudiant les singularités non-isolées des hypersurfaces. Ceci permettrait d'affiner la classification et le diagramme en oignon pour les 3-qutrits et 4-qubits par exemple.

Chapitre 6

États maximalement intriqués

"The chief purpose of a union is to maximize the income of its members", Timothy Noah.

L'étude et la compréhension des états multipartites hautement intriqués se révèle importante dans le contexte du traitement de l'information quantique et du calcul quantique. En effet, les états maximalement intriqués s'avèrent cruciaux dans l'implémentation de réseaux quantiques, dans le domaine MBQC (measurement based quantum computer) [223], dans les codes correcteurs d'erreurs quantiques et dans des protocoles de communication quantique [75, 233, 112].

Pour les systèmes bipartites ou multipartite à deux ou trois particules, la question des états maximalement intriqués a été étudiée sous différents angles [97]. La question devient plus difficile dans le cas multipartite, et c'est pourquoi nous proposons d'étudier cette question du point de vue des mesures algébriques de l'intrication, et de comparer nos résultats lorsque d'autres existent.

Dans cette section, nous cherchons à maximiser certaines mesures de l'intrication, dont l'évaluation de polynômes invariants ou mesure géométrique de l'intrication. L'hyperdéterminant, polynôme définissant la variété duale des états séparables, est utilisé non pas comme marqueur qualitatif de l'intrication, mais comme mesure quantitative de l'intrication. Ce polynôme peut aussi être défini pour les états symétriques et fermioniques, et nous nous proposons alors de maximiser sa valeur absolue afin de proposer de nouveaux états maximalement intriqués, ou de retrouver des états déjà proposés comme étant maximalement intriqués par rapport à d'autre mesures de l'intrication.

Nous utilisons principalement l'algorithme de promenade aléatoire pour les optimisation numériques, et nous confirmons parfois les résultats en utilisant l'algorithme de gradient ou l'optimisation par essaim particulaire (voir Annexe A.8).

6.1 Maximum de l'hyperdéterminant

Dans cette section, nous nous intéressons à deux cas de systèmes multipartites du point de vue de l'hyperdéterminant : celui des 4-qubits et des 3-qutrits. Le premier cas a

été assez bien étudié dans la littérature, tandis que pour le second nous ne connaissons pas de candidat maximisant Det_{333}.

6.1.1 Cas des 4-qubits

Dans cette section nous proposons une nouvelle expression d'état réel maximisant l'hyperdéterminant des 4-qubits, et présentons également la méthode associée. Nous rappelons tout d'abord brièvement les précédents travaux, puis nous présentons notre approche ainsi que le résultat obtenu.

Précédents travaux

Higushi et Sudbey on décrit en 2000 [129] un état pur $|HS\rangle$ (voir Équation 6.1) à 4-qubits, dont la matrice de densité réduite de chaque qubit est maximalement mélangée. De plus, cet état maximise également l'intrication moyenne (au sens de l'entropie de Von Neumann) pour toutes bipartitions en systèmes à 2-qubits

$$|HS\rangle = \frac{1}{\sqrt{6}}\left(|0011\rangle + |1100\rangle + \omega\left(|0101\rangle + |1010\rangle\right) + \omega^2\left(|0110\rangle + |1001\rangle\right)\right) \ , \tag{6.1}$$

avec $\omega = e^{\frac{2i\pi}{3}}$.

En 2006, Yeo et Chua ont démontré qu'il était possible de procéder à une téléportation quantique d'un système à 2-qubits quelconque, et proposèrent également une extension du protocole de *dense coding* [290]. Pour ce faire, ils ont introduit ce qu'ils appellent un *genuine* état intriqué à quatre parties, noté $|YC\rangle$, et défini par

$$|YC\rangle = \frac{1}{\sqrt{8}}\left(|0000\rangle - |0011\rangle - |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle\right) \ . \tag{6.2}$$

Par ailleurs, Briegel et Raussendorf ont présenté trois états $|C_1\rangle$, $|C_2\rangle$ et $|C_3\rangle$ appelés *cluster states* [52], reconnus pour posséder la propriété que l'entropie de Von Neumann est maximale pour deux des trois possibles bipartitions. L'entropie moyenne sur toutes les bipartitions reste néanmoins inférieure à celle de l'état $|HS\rangle$. Ces états décrits en Équation 6.3, maximisent également la α-entropie de Rényi pour $\alpha \geq 2$.

$$\begin{aligned} |C_1\rangle &= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle\right) \ , \\ |C_2\rangle &= \frac{1}{2}\left(|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle\right) \ , \\ |C_3\rangle &= \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle - |1111\rangle\right) \ . \end{aligned} \tag{6.3}$$

En 2010, dans une conjecture assez connue de Gour et Wallach [113], prouvée par la suite dans [65], deux états $|L\rangle$ et $|M\rangle$ sont proposés comme maximisant l'α-entropie de Tsallis (respectivement pour tout $\alpha > 2$ et $0 < \alpha < 2$). De plus, l'état $|L\rangle$ maximise la valeur absolue de l'hyperdéterminant des 4-qubits, tandis que l'état $|M\rangle$ maximise l'entropie d'intrication [129] :

$$|L\rangle = \frac{1}{\sqrt{3}}\left(|u_0\rangle + \omega|u_1\rangle + \omega^2|u_2\rangle\right) \ , \tag{6.4}$$

$$|M\rangle = \frac{i}{\sqrt{2}}|u_0\rangle + \frac{1}{\sqrt{6}}\left(|u_1\rangle + |u_2\rangle + |u_3\rangle\right) \ , \tag{6.5}$$

avec $\omega = e^{\frac{2i\pi}{3}}$ et

$$\begin{aligned}
|u_0\rangle &= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right) \ , \\
|u_1\rangle &= \frac{1}{2}\left(|0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle\right) \ , \\
|u_2\rangle &= \frac{1}{2}\left(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle\right) \ , \\
|u_3\rangle &= \frac{1}{2}\left(|0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle\right) \ .
\end{aligned} \tag{6.6}$$

Dans les travaux présentés dans sa thèse [5], Alsina présente également un état symétrique $|HD\rangle$ maximisant l'hyperdéterminant des 4-qubits, s'exprimant comme suit :

$$|HD\rangle = \frac{1}{\sqrt{6}}\Big(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle + \sqrt{2}|1111\rangle\Big) \ . \tag{6.7}$$

À l'exception des états $|L\rangle$ et $|HD\rangle$, tous les autres états présentés comme maximalement intriqués annulent l'hyperdéterminant. Nous pouvons également citer les travaux suivants en lien avec la question des états à 4-qubits maximalement intriqués [54, 208, 42, 287, 29, 221, 97, 251].

Approche pour les réels

Dans cette section, nous présentons une approche de détermination d'un état maximalement intriqué du point de vue de l'hyperdéterminant (comme mesure de l'intrication), en ne considérant que les états à coefficients réels. Notre approche combine recherche et optimisation numérique de l'hyperdéterminant, avec une recherche analytique d'une expression exacte de l'état.

La valeur absolue de l'hyperdéterminant constitue une mesure de l'intrication, comme cela a été discuté tout au long de ce manuscrit, et pour le cas des 4-qubits, la valeur maximale est de $\frac{1}{19683} \approx 0.00005080526343$.

Il est connu que l'hyperdéterminant s'annule pour les états dégénérés, les états de la variété duale de Segre. On cherchera alors un candidat parmi les familles d'états non-dégénérés, et n'annulant donc pas l'hyperdéterminant. Or il s'avère que la seule famille pour laquelle l'hyperdéterminant n'est pas nul, est la famille des états les plus génériques, c'est-à-dire la famille G_{abcd}.

Pour rappel, la famille G_{abcd} s'exprime comme :

$$\begin{aligned}
G_{abcd}\colon\ & \frac{a+d}{2}\big(|0000\rangle + |1111\rangle\big) + \frac{a-d}{2}\big(|0011\rangle + |1100\rangle\big) + \\
& \frac{b+c}{2}\big(|0101\rangle + |1010\rangle\big) + \frac{b-c}{2}\big(|0110\rangle + |1001\rangle\big) \ ,
\end{aligned} \tag{6.8}$$

et on peut également l'exprimer sous la forme d'un vecteur ligne :

$$G_{abcd}: \left(\frac{a+d}{2}, 0, 0, \frac{a-d}{2}, 0, \frac{b+c}{2}, \frac{b-c}{2}, 0, 0, \frac{b-c}{2}, \frac{b+c}{2}, 0, \frac{a-d}{2}, 0, 0, \frac{a+d}{2}\right) . \tag{6.9}$$

Lorsque les paramètres a, b, c et d appartiennent aux complexes, alors il est possible d'atteindre le maximum de l'hyperdéterminant, par optimisation numérique ou en considérant l'état $|HS\rangle$ par exemple. En revanche, en se restreignant à des coefficients réels, nos calculs d'optimisation suggèrent qu'il n'est pas possible d'atteindre le maximum de l'hyperdéterminant. La valeur de $|Det_{2222}|$ maximale possible pour la forme G_{abcd}, avec $a, b, c, d \in \mathbb{R}$ est d'environ $3,34898 \times 10^{-7}$.

Nous choisissons alors d'élargir la définition de la famille G_{abcd} en ajoutant des états de base dans l'écriture, et en s'inspirant de la symétrie des coefficients dans l'écriture en vecteur ligne (voir Equation 6.9). Nous définissons alors la forme $G_{abcdefgh}$ comme suit :

$$G_{abcdefgh}: \frac{1}{\sqrt{2}}(a, b, c, d, e, f, g, h, h, g, f, e, d, c, b, a) , \tag{6.10}$$

avec $a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2 = 1$. Nous pouvons alors obtenir alors une valeur maximale de $|Det_{2222}|$ en optimisant numériquement les 8 coefficients. Un exemple de jeu de coefficients (a, b, c, d, e, f, g, h) pour $G_{abcdefgh}$ maximisant $|Det_{2222}|$ est :

$$(0.35355, 0.2041, -0.2041, -0.35355, 0.6124, -0.35355, 0.35355, 0.2041) . \tag{6.11}$$

Ici, la recherche numérique permet à la fois d'établir avec une grande probabilité l'existence d'un état réel de la forme $G_{abcdefgh}$ maximisant $|Det_{2222}|$, mais également de pouvoir opérer un certain nombre de simplifications dans la définition de la forme générale, en observant les coefficients pouvant être égaux (à un signe près).

En observant les similitudes dans les coefficients, nous arrivons à réduire le nombre de paramètres jusqu'à 3, et nous définissons alors une nouvelle forme G_{ABC} telle que :

$$G_{ABC}: \frac{1}{\sqrt{2}}\left(\frac{A}{\sqrt{3}}, \frac{-C}{2}, \frac{C}{2}, B, \frac{-C}{2}, \frac{A}{\sqrt{3}}, \frac{-A}{\sqrt{3}}, \frac{C}{2}, \frac{C}{2}, \frac{-A}{\sqrt{3}}, \frac{A}{\sqrt{3}}, \frac{-C}{2}, B, \frac{C}{2}, \frac{-C}{2}, \frac{A}{\sqrt{3}}\right) . \tag{6.12}$$

Nous vérifions une nouvelle fois par optimisation numérique qu'il est possible de maximiser $|Det_{2222}|$ à partir de la forme G_{ABC} restreinte aux réels. Notre objectif à présent est de déterminer une expression exacte d'un état réel maximisant $|Det_{2222}|$ en partant de la forme simplifiée G_{ABC}.

Une condition nécessaire (mais non-suffisante) à la maximisation d'une fonction polynomiale est l'annulation des dérivées partielles du polynôme. On se propose alors de résoudre analytiquement le système formé par les équations des dérivées partielles de l'hyperdéterminant Det_{2222}. Nous réduisons le nombre de paramètres à 2 en fixant $A = \sqrt{1 - B^2 - C^2}$, par condition de normalisation. Nous noterons alors la forme simplifiée G_{BC}.

L'évaluation de l'hyperdéterminant sur la forme G_{BC} donne l'expression suivante :

$$Det_{2222}(G_{BC}) = \frac{1}{725594112}\left(2\sqrt{3}\sqrt{-B^2-C^2+1}B+2B^2+5C^2-2\right)^6 \left(B\sqrt{3}-2\sqrt{3}C-3\sqrt{-B^2-C^2+1}\right)\left(B\sqrt{3}+2\sqrt{3}C-3\sqrt{-B^2-C^2+1}\right) \left(2B^2\sqrt{3}+\sqrt{3}C^2+6\sqrt{-B^2-C^2+1}B\right)^2\left(B\sqrt{3}+\sqrt{-B^2-C^2+1}\right)^6 . \quad (6.13)$$

Nous dérivons cette expression par rapport à B et C, ce qui nous donne deux polynômes en deux variables, et nous cherchons les solutions qui annulent ces deux polynômes simultanément. À l'aide du logiciel de calcul Maple, nous arrivons à déterminer un ensemble de solutions, et, pour chaque solution réelle, la forme ainsi définie est utilisée pour évaluer l'hyperdéterminant jusqu'à trouver la valeur maximale (à un signe près), qui dans notre cas est connue.

Nous présentons une solution possible dans la proposition suivante.

Proposition 6.1.1. *Soient $|v_1\rangle$, $|v_2\rangle$ et $|v_3\rangle$ trois vecteurs de $\mathcal{H}_4 = \mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ tels que :*

$$|v_1\rangle = \frac{1}{\sqrt{6}}\left(|0000\rangle+|0101\rangle-|0110\rangle-|1001\rangle+|1010\rangle+|1111\rangle\right) ,$$

$$|v_2\rangle = \frac{1}{\sqrt{2}}\left(|0011\rangle+|1100\rangle\right) ,$$

$$|v_3\rangle = \frac{1}{\sqrt{8}}\left(-|0001\rangle+|0010\rangle-|0100\rangle+|0111\rangle+|1000\rangle-|1011\rangle+|1101\rangle-|1110\rangle\right) .$$

Alors, le maximum de l'hyperdéterminant $|Det_{2222}|$ est atteint pour l'état réel à 4-qubits $|M_{2222}\rangle \in \mathcal{H}_4$, défini par :

$$|M_{2222}\rangle = A|v_1\rangle + B|v_2\rangle + C|v_3\rangle , \quad (6.14)$$

avec

$$A = \frac{1}{\sqrt{8}} , \quad B = \frac{\sqrt{6}}{4} , \quad C = \frac{1}{\sqrt{2}} .$$

6.1.2 Cas des 3-qutrits

Dans cette section nous proposons une expression d'état réel maximisant l'hyperdéterminant des 3-qutrits. Dans le chapitre précédent, nous avons étudié les singularités des hypersurfaces liées aux 3-qutrits, et avons discuté la relation avec les singularités de la variété duale. Nous cherchons à présent à déterminer un état maximalement intriqué parmi les états non-dénégérés (présentant donc une section hyperplane lisse).

Il existe assez peu de travaux concernant la recherche d'états maximalement intriqués pour les 3-qutrits. De manière non-exhaustive, nous pouvons citer les travaux de Enriquez *et al.* [97] et de Hebenstreit *et al.* [126].

Proposition d'un état maximalement intriqué

Dans cette sous-section nous présentons un candidat d'état à 3-qutrits maximalement intriqué du point de vue de l'hyperdéterminant. L'objectif est de proposer une expression exacte de cet état, en suivant la même approche que celle utilisée pour le cas des 4-qubits (voir Section 6.1.1).

Nous cherchons donc à nous limiter à l'étude des états non-dégénérés, qui n'annulent pas l'hyperdéterminant. Comme rappelé en Chapitre 5 et dans [50], un vecteur $|\psi_s\rangle$ non-dégénéré de $\mathcal{H}_{333}$, correspondant à la première famille de Nurmiev $F_{1,1}$, peut être exprimé comme la combinaison des trois tenseurs semi-simples

$$|\psi_s\rangle = A|v_1\rangle + B|v_2\rangle + C|v_3\rangle \ , \tag{6.15}$$

$$|\psi_s\rangle : (A, B, C) \ , \tag{6.16}$$

avec $|A|^2 + |B|^2 + |C|^2 = 1$ et

$$\begin{aligned} |v_1\rangle &= \frac{1}{\sqrt{3}} \left(|000\rangle + |111\rangle + |222\rangle\right) \ , \\ |v_2\rangle &= \frac{1}{\sqrt{3}} \left(|012\rangle + |120\rangle + |201\rangle\right) \ , \\ |v_3\rangle &= \frac{1}{\sqrt{3}} \left(|021\rangle + |102\rangle + |210\rangle\right) \ . \end{aligned} \tag{6.17}$$

À partir de l'expression donnée en [50], et pour les états de la forme $|\psi_s\rangle$, l'hyperdéterminant Det_{333} associé aux états à 3-qubits s'exprime comme suit :

$$\begin{aligned} Det_{333}(|\psi_s\rangle) = -\tfrac{4}{387420489}\, A^3B^3C^3 \left(A+B+C\right)^3 \times \\ \left(A^2 + 2\,AB - AC + B^2 - BC + C^2\right)^3 \left(A^2 - AB + 2\,AC + B^2 - BC + C^2\right)^3 \\ \left(A^2 - AB - AC + B^2 + 2\,BC + C^2\right)^3 \left(A^2 - AB - AC + B^2 - BC + C^2\right)^3 \ . \end{aligned} \tag{6.18}$$

Notre objectif est de maximiser la valeur absolue de ce polynôme, en fonction des trois paramètres A, B et C. Nous utilisons l'algorithme d'optimisation numérique de la marche aléatoire afin de nous guider. Après une optimisation sur les complexes, puis sur les réels, il apparaît que la valeur maximale potentielle de $|Det_{333}|$ peut être atteinte en se restreignant à des paramètres dans $\mathbb{R}$. À titre d'exemple voici deux états $|\psi_{s_1}\rangle$ et $|\psi_{s_2}\rangle$ atteignant la valeur numérique, supposée maximale, d'environ $6,907059 \times 10^{-7}$, s'exprimant comme :

$$|\psi_{s_1}\rangle : (-0.4597089177, 0.6279551660, 0.6279649847) \ , \tag{6.19}$$

$$\begin{aligned} |\psi_{s_2}\rangle = (0.4187234964 + 0.1897453668i, -0.5719715278 - 0.2591902230i, \\ -0.5719688559 - 0.2592064016i) \ . \end{aligned} \tag{6.20}$$

Se restreindre aux réels permet de réduire le nombre de paramètres à considérer (trois au lieu de six), pour déterminer l'expression exacte d'un état maximisant l'hyperdéterminant. De plus, et de la même manière que les recherches numériques ont permis de réduire les paramètres pour les 4-qubits, dans le cas des 3-qubits nous avons également observé des relations entre les coefficients A, B et C, et ceci de manière

systématique (au terme de chaque optimisation). Nous nous restreignons donc au cas $B = C$, ce qui réduit l'étude à 2 paramètres. Comme A et B sont des réels, et qu'ils doivent vérifier la condition de normalisation $A^2 + 2B^2 = 1$, on peut encore réduire le nombre de paramètres, en posant $A = -\sqrt{1 - 2B^2}$.

On substitue ensuite A et C par leur expression en fonction de B dans l'hyperdéterminant Det_{333}, et on le dérive par rapport à la variable B. On cherche ensuite les solutions réelles qui annulent la dérivée, et pour chaque solution trouvée, on évalue la valeur absolue de l'hyperdéterminant, jusqu'à trouver la valeur maximale établie numériquement. Ceci nous permet de trouver une valeur de B permettant d'atteindre cette valeur, et donc d'en déduire les valeurs de A et C permettant de définir cet état. Nous présentons ce résultat dans la Proposition 6.1.2.

Proposition 6.1.2. *Soient $|v_1\rangle$, $|v_2\rangle$ et $|v_3\rangle$ trois vecteurs de $\mathcal{H}_{333} = \mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ tels que :*

$$|v_1\rangle = \frac{1}{\sqrt{3}} \left(|000\rangle + |111\rangle + |222\rangle\right) \ ,$$

$$|v_2\rangle = \frac{1}{\sqrt{3}} \left(|012\rangle + |120\rangle + |201\rangle\right) \ ,$$

$$|v_3\rangle = \frac{1}{\sqrt{3}} \left(|021\rangle + |102\rangle + |210\rangle\right) \ .$$

Alors, un maximum local de l'hyperdéterminant $|Det_{333}|$, dont la valeur exacte est $\frac{\sqrt{3}}{2507653251072}$, est atteint pour l'état réel à 3-qutrits $|M_{333}\rangle \in \mathcal{H}_{333}$, défini par :

$$|M_{333}\rangle = A|v_1\rangle + B|v_2\rangle + B|v_3\rangle \ ,$$

avec

$$A = -\frac{1}{6}\sqrt{18 - 6\sqrt{3}} \ , \quad B = \frac{1}{6}\sqrt{9 + 3\sqrt{3}} \ .$$

Au vu des optimisations numériques que nous avons pu lancer, nous pensons que cet état $|M_{333}\rangle$ est très probablement celui pour lequel on atteint le maximum global de la valeur absolue de l'hyperdéterminant.

6.2 États symétriques maximalement intriqués

Nous nous intéresserons aux états symétriques maximalement intriqués dans cette section. Guidés par les travaux de Aulbach (voir sous-section suivante), nous évaluons les invariants algébriques associés aux tenseurs symétriques sur les états proposés dans la littréature, et proposons également des états maximisant la valeur absolue de ces polynômes. Nous étudions les systèmes de quatre à douze qubits, ainsi que le cas des 20-qubits.

Nous avons introduit la notion d'état symétrique en Chapitre 1 Section 1.3.2, et il peut être intéressant pour le lecteur de préter attention à cette section avant d'entamer la lecture de celle-ci. De même, nous avons présenté le lien entre états symétrique séparables et variété de Veronese en Chapitre 2 Section 2.1.4.

De manière générale dans cette section, on exprimera un état symétrique $|\psi\rangle$ à n-qubits dans la base de Dicke (voir Équation 1.60) par

$$|\psi\rangle = \sum_{k=0}^{n} a_k |D_k\rangle \ . \tag{6.21}$$

6.2.1 Précédents travaux

Dans sa thèse, ainsi que dans des travaux publiés dans divers articles [17, 18, 16], Aulbach utilise la représentation de Majorana des états symétriques pour déterminer des états maximalement intriqués au sens de la mesure géométrique de l'intrication. Ceci implique de déterminer la répartition des points sur la sphère de Bloch, et ceci lié à un problème appelé problème de Majorana. Dans certains cas, la disposition de ces points définie par les solides platoniciens est utilisée pour définir des états symétriques. Notre travail se place dans la continuité du travail développé par Aulbach.

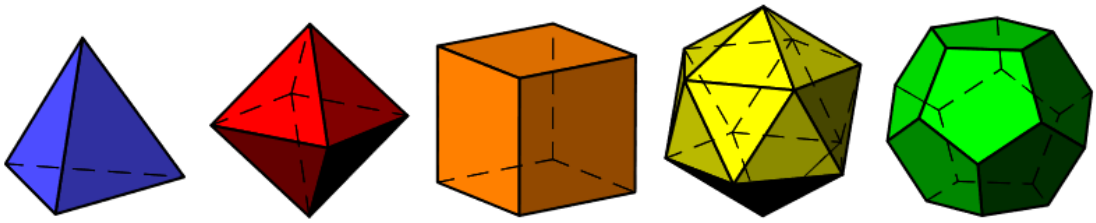


Figure 6.1 – Représentation des cinq solides platoniciens de gauche à droite : tétraèdre ($n = 4$), octaèdre ($n = 6$), cube ($n = 8$), icosaèdre ($n = 12$) et dodécaèdre ($n = 20$) [18].

D'autre part, Enriquez *et al.* [97] répertorient différents états symétriques comme candidats à la maximisation de l'intrication. Ces états sont notamment des systèmes à 4-qubits, 5-qubits, 3-qutrits et 4-qutrits.

6.2.2 Formes binaires et covariants associés

Les formes binaires sont un sujet d'étude qui ont intéressé les chercheurs en théorie classique des invariants, depuis plusieurs années déjà, pour lequel une large littérature à été produite. Deux ouvrages de référence dans ce domaine sont celui de Olver [205] et celui de Kung et Rota [162], et ce sont ceux qui nous serviront de référence principale.

La théorie classique des invariants de formes binaires a pour but de déterminer des polynômes invariants et covariants d'une forme binaire, à des fins de classification. Nous rappelons qu'un polynôme covariant est un polynôme défini par les coefficients de la forme binaire et des variables auxiliaires x et y, tel qu'il reste invariant pour l'action de $\mathrm{SL}_2(\mathbb{C})$ sur les coefficients et les variables [179].

Plus précisément, une forme binaire f est un polynôme homogène de degré n en x et y tel que :

$$f(x,y) = \sum_{k=0}^{n} \binom{n}{k} a_k x^{n-k} y^k \ . \tag{6.22}$$

Si on définit l'image de f par tout élément $g \in \mathrm{SL}_2(\mathbb{C})$ comme étant la forme binaire $\tilde{f}$, définie par :

$$\tilde{f}(\tilde{x},\tilde{y}) = \sum_{k=0}^{n} \binom{n}{k} a_k \left(\alpha\tilde{x} + \beta\tilde{y}\right)^{n-k} \left(\gamma\tilde{x} + \delta\tilde{y}\right)^k = \sum_{k=0}^{n} \binom{n}{k} b_k \tilde{x}^{n-k}\tilde{y}^k \ , \tag{6.23}$$

alors tout polynôme P est un polynôme covariant si, et seulement si, on a

$$P(a_0,\ldots,a_k,x,y) = P(b_0,\ldots,b_k,\tilde{x},\tilde{y}) \ . \tag{6.24}$$

L'exemple de covariant le plus simple est la forme binaire elle même. Un polynôme covariant ne faisant pas apparaître les variables x et y est appelé polynôme invariant.

En guise d'exemple, nous pouvons étudier le cas où $n = 4$. Dans ce cas, bien connu dans la littérature, l'anneau des polynômes invariants des formes binaires quartiques est généré par deux polynômes I_2 et I_3. On notera alors

$$\mathbb{C}[\mathrm{Sym}^4\mathbb{C}^{*2}]^{\mathrm{SL}_2\mathbb{C}} = \mathbb{C}[I_2, I_3] \ , \tag{6.25}$$

avec,

$$I_2 = a_0a_4 - a_1a_3 + \frac{{a_2}^2}{2} \ , \tag{6.26}$$

$$I_3 = \begin{vmatrix} a_0 & \frac{a_1}{2} & \frac{a_2}{\sqrt{6}} \\ \frac{a_1}{2} & \frac{a_2}{\sqrt{6}} & \frac{a_3}{2} \\ \frac{a_2}{\sqrt{6}} & \frac{a_3}{2} & a_4 \end{vmatrix} . \tag{6.27}$$

Dans ce cas, le discriminant Δ_4 des formes binaires quartiques peut être exprimé comme étant égal à :

$$\Delta_4 = \left(I_2\right)^3 - 27\left(I_3\right)^2 \ . \tag{6.28}$$

La classification des polynômes quartiques binaires fait aussi appel aux covariants $Hess(f)$ et $T(f)$, et ceux-ci permettent à l'aide des invariants de classifier les quartiques selon la multiplicité et le nombre de racines (comme cela est fait dans l'algorithme de classification des 4-qubits, voir Annexe A.4). La classification des quartiques [205] et les valeurs des covariants associées sont regroupées en Table 6.1.

Les formes binaires trouvent un lien direct avec les états symétriques multi-qubits (le lien est d'autant plus évident en considérant le polynôme de Majorana), et de ce fait la classification de ces formes binaires sous SLOCC nous amène à une classification de l'intrication des états symétriques (voir Figure 6.2 pour un exemple pour les 4-qubits). Ceci est notamment l'objet de travaux et d'un article en cours de développement. Les invariants associés à ces formes binaires trouvent également un sens du point de vue de la géométrie algébrique, et cela est l'objet de notre sous-section suivante.

Forme canonique f	Covariants	Racines
$x^4 + \lambda x^2y^2 + y^4$	$\lambda \neq \pm 2, \Delta_4 \neq 0$	4 racines simples
$x^2(x^2 + y^2)$	$\Delta_4 = 0, T(f) \neq 0$	une racine double
x^2y^2	$\Delta_4 = T(f) = 0, I_2 \neq 0$	deux racines doubles
x^3y	$I_2 = I_3 = 0, Hess(f) \neq 0$	une racine triple
x^4	$Hess(f) = 0, f \neq 0$	une racine quadruple
0	$f = 0$	

Table 6.1 – Classification des formes quartiques binaires [205].

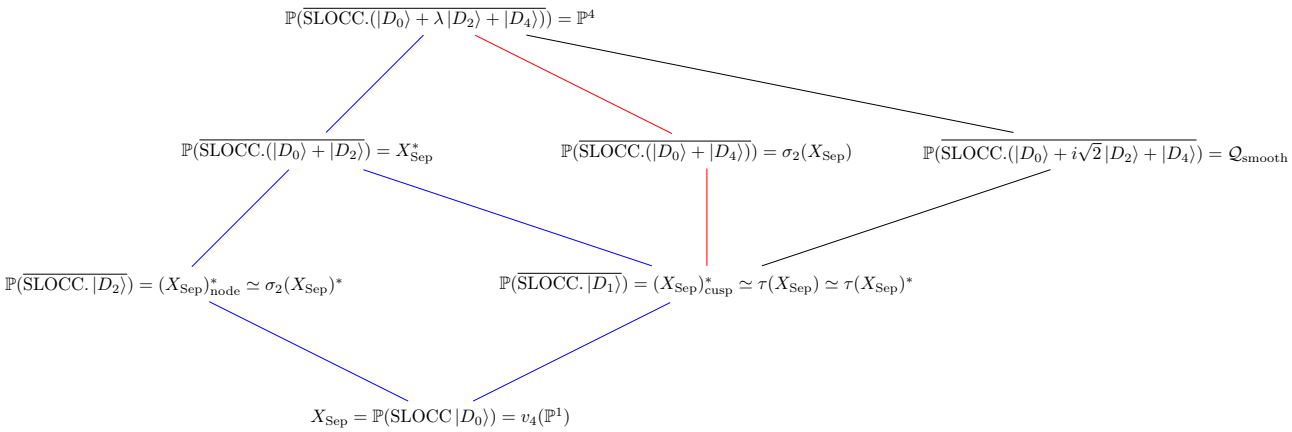


Figure 6.2 – Classification sous SLOCC des états symétriques pour le cas des 4-qubits.

6.2.3 Invariants des états symétriques comme mesures de l'intrication

Il existe des polynômes invariants associés aux états symétriques, définissant eux même des formes binaires. Les invariants I_2 etI_3, ainsi que le discriminant Δ_4 sont des exemples d'invariants associés aux états à 4-qubits symétriques. Ces invariants peuvent être généralisés à des dimensions supérieures.

Le discriminant, noté Δ_n, est un polynôme invariant sous l'action du groupe SLOCC. La variété duale à la variété de Veronese est définie par l'annulation du discriminant. Ce polynôme peut être défini pour tous les systèmes symétriques à n-qubits, et sa valeur absolue sera utilisée comme mesure de l'intrication, de manière analogue à l'hyperdéterminant (ces deux polynômes étant directement liés).

Dans le cas où $n = 2k$ est pair, il existe un invariant de degré 2, noté I_2 (généralisant la notation pour les 4-qubits), appelé *quadrinvariant*, s'exprimant comme :

$$I_2(|\psi\rangle) = \sum_{i=0}^{n} (-1)^i a_i a_{n-i} \ . \tag{6.29}$$

De plus, l'invariant I_3 peut également être généralisé. Lorsque $n = 2k$, on peut définir le *catalecticant*, polynôme invariant noté I_{k+1} tel que

$$I_{k+1}(|\psi\rangle) = \begin{vmatrix} a_0 & a_1/\sqrt{\binom{n}{1}} & \dots & a_k/\sqrt{\binom{n}{k}} \\ a_1/\sqrt{\binom{n}{1}} & a_2/\sqrt{\binom{n}{2}} & \dots & a_{k+1}/\sqrt{\binom{n}{k+1}} \\ a_2/\sqrt{\binom{n}{2}} & a_3/\sqrt{\binom{n}{3}} & \dots & a_{k+2}/\sqrt{\binom{n}{k+2}} \\ \vdots & \vdots & \dots & \vdots \\ a_k/\sqrt{\binom{n}{k}} & a_{k+1}/\sqrt{\binom{n}{k+1}} & \dots & a_n \end{vmatrix} . \tag{6.30}$$

Le catalecticant I_{k+1} est interprété géométriquement comme le polynôme définissant la k-ième variété des sécantes $\sigma_k\left(\nu_n(\mathbb{P}^1)\right)$ associée à la variété de Veronese $\nu_n(\mathbb{P}^1)$ des n-qubits symétriques.

Nous chercherons à maximiser et évaluer ces invariants en valeur absolue, les considérant comme mesures algébriques de l'intrication, pour qualifier les états publiés par Aulbach et pouvoir également proposer de nouveaux candidats pour la maximisation de l'intrication.

6.2.4 Étude de cas

Dans cette sous-section, nous étudions les états symétriques à n-qubits proposés par Aulbach [16], pour différentes valeurs de n. Nous proposons également des états maximisant les invariants liés aux états symétriques, et comparons ces états aux états précédents du point de vue de la valeur de la MGI et des invariants.

Nous optimisons la valeur absolue du discriminant ainsi que les invariants (pour les cas où n est pair), à la fois pour des coefficients réels et complexes. Lorsque le maximum de ces invariants est atteint par un état déjà proposé par Aulbach, alors nous ne proposons pas de nouvel état et renseignons seulement quel état maximise quelle quantité. Lorsque nous avons trouvé un état atteignant des valeurs plus intéressantes nous le proposons. Si nous ne proposons qu'un tenseur symétrique à coefficients réels, c'est que la recherche sur les complexes n'apporte pas de résultat supplémentaire. Si nous proposons un état à coefficients complexes, c'est que nous obtenons de meilleurs résultats pour cet état (et ne renseignons donc pas les états réels obtenus).

4-qubits

Le *Tetrahedron state*, noté $|\Psi_4\rangle$, est un état issu de la configuration en tétraèdre des points sur la sphère de Majorana. Cet état défini à partir d'un solide platonicien est celui qui maximise la valeur absolue du discriminant Δ_4. Il est également proposé par Aulbach comme étant l'état maximalement intriqué au sens de la mesure géométrique de l'intrication. Aussi, il maximise la valeur absolue de l'invariant I_3. En revanche, il annule l'invariant I_2.

$$|\Psi_4\rangle = \frac{1}{\sqrt{3}}\left(|D_0\rangle + \sqrt{2}|D_3\rangle\right) . \tag{6.31}$$

Nous proposons alors un état maximisant l'invariant I_2, que l'on notera $\left|M_4^{I_2}\right\rangle$. Cet état ne maximise pas les autres mesures, mais atteint la moitié de la valeur maximale

pour le discriminant Δ_4.

$$\left|M_4^{I_2}\right\rangle = \sum_{k=0}^{4} a_k |D_k\rangle \ , \tag{6.32}$$

avec ,

$$\begin{aligned} a_0 \approx 0.2508956376 + 0.09070126553i,\ a_1 \approx 0.2670784937 - 0.5786744308i, \\ a_2 \approx -0.06133783029 + 0.2036694216i,\ a_3 \approx -0.09691598770 + 0.6299308152i, \\ a_4 \approx -0.2592667786 - 0.06293867312i \ . \end{aligned} \tag{6.33}$$

Tous les résultats sont regroupés en Table 6.2.

État	$\lvert\Delta_4\rvert$	$\lvert I_2\rvert$	$\lvert I_3\rvert$	E_g
$\lvert\Psi_4\rangle$	1024	0	0,0962250449	$\log_2(3) \approx 1.584962500$
$\left\lvert M_4^{I_2}\right\rangle$	512	2	0.000001394	0.9999796162

Table 6.2 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 4-qubits symétriques.

5-qubits

Le *Square Pyramid state* $|\Psi_5\rangle$, proposé par Aulbach comme état maximalement intriqué pour les 5-qubits symétriques, présente une MGI conjecturée comme étant maximale. Néanmoins, cet état ne maximise pas le discriminant $|\Delta_5|$.

$$|\Psi_5\rangle = \frac{|D_0\rangle + |D_4\rangle}{\sqrt{1+A^2}}, \quad \text{avec } A \approx 1.531538191 \ . \tag{6.34}$$

En revanche, c'est le *Triagonal bipyramid state* $|\psi_5\rangle$ qui maximise le discriminant, mais en contre-partie présente une MGI inférieure à celle de $|\Psi_5\rangle$.

$$|\psi_5\rangle = \frac{1}{\sqrt{2}} \left(|D_1\rangle + |D_4\rangle\right) \ . \tag{6.35}$$

Il nous est apparu que tous les états maximisant la valeur absolue du discriminant présentent la même valeur de MGI que l'état $|\psi_5\rangle$. De plus, à l'issue de nos recherches numériques, il semble ne pas exister d'état maximisant à la fois les deux mesures. Tous les résultats sont regroupés en Table 6.3.

État	$\lvert\Delta_5\rvert$	E_g
$\lvert\Psi_5\rangle$	1.203132030×10^5	1.742268948
$\lvert\psi_5\rangle$	1.318359375×10^5	1.678071904

Table 6.3 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 5-qubits symétriques.

6-qubits

Dans le cas des 6 qubits, le solide platonicien correspondant à l'octaèdre régulier définit un état $|\Psi_6\rangle$, appelé *octahedron state* par Aulbach, constituant l'unique solution aux problèmes de Thomson et de Tóth. En plus de résoudre le problème de Marojana pour 6-qubits [16], cet état maximise tous les invariants des tenseurs symétriques à 6-qubits, à savoir : la valeur absolue du discriminant Δ_6, la valeur absolue de l'invariant I_2 et la valeur absolue de l'invariant I_4.

$$|\Psi_6\rangle = \frac{1}{\sqrt{2}}\left(|D_1\rangle + |D_5\rangle\right) \ . \tag{6.36}$$

De plus, tous les états maximisant un des invariants (états déterminés numériquement), semblent systématiquement maximiser les deux autres invariants, tout en présentant une valeur de la MGI égale à celle de l'état $|\Psi_6\rangle$. Nous présentons les valeurs exactes en Table 6.4.

État	$\lvert\Delta_6\rvert$	$\lvert I_2\rvert$	$\lvert I_4\rvert$	E_g
$\lvert\Psi_6\rangle$	80621568	1	$\frac{1}{144} \approx 0.00694$	$\log_2(\frac{9}{2}) \approx 2.169925$

TABLE 6.4 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 6-qubits symétriques.

7-qubits

L'état $\left|\psi_7^{\text{Tó}}\right\rangle$ présenté par Aulbach est l'état solution au problème de Tóth, mais ne maximise ni la mesure géométrique de l'intrication ni la valeur absolue du discriminant.

$$\left|\psi_7^{\text{Tó}}\right\rangle = \alpha|D_0\rangle - \beta|D_3\rangle - \gamma|D_6\rangle \ , \tag{6.37}$$

avec,

$$\alpha \approx 0.295510, \ \beta \approx 0.602458, \ \gamma \approx 0.741430 \ . \tag{6.38}$$

D'autre part, le *Pentagonal Dipyramid state*, noté $|\Psi_7\rangle$, présente une valeur de MGI bien plus grande (potentiellement maximale), et maximise aussi la valeur absolue du discriminant.

$$|\Psi_7\rangle = \frac{1}{\sqrt{2}}\left(|D_1\rangle + |D_6\rangle\right) \ . \tag{6.39}$$

Dans le cas des 7-qubits, une corrélation est systématiquement observée entre la maximisation (potentielle) de la MGI et de la valeur absolue du discriminant. Tous les résultats sont regroupés en Table 6.5.

8-qubits

Le *Regular Cube state*, noté $|\psi_8^c\rangle$, est un solide platonicien et est l'état qui maximise l'invariant $|I_2|$. Tous les états maximisant cet invariant (trouvés numériquement) présentent les mêmes valeurs pour la MGI et tous les autres invariants que l'état $|\psi_8^c\rangle$. En revanche, cet état ne maximise pas le discriminant et l'invariant $|I_5|$, ni la MGI.

État	$\lvert\Delta_7\rvert$	E_g
$\lvert\psi_7^{\text{Tó}}\rangle$	$1.774279622 \times 10^{10}$	1.692798
$\lvert\Psi_7\rangle$	$9.654915737 \times 10^{10}$	2.298691396

Table 6.5 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 7-qubits symétriques.

$$|\psi_8^c\rangle = \frac{1}{2\sqrt{6}}\left(\sqrt{5}|D_0\rangle + \sqrt{14}|D_4\rangle + \sqrt{5}|D_8\rangle\right) . \tag{6.40}$$

L'état $|\Psi_8\rangle$, nommé *Asymmetric Pentagonal Dipyramid state* par Aulbach, est celui qui maximise la mesure géométrique de l'intrication. Cet état annule le discriminant, et annule l'invariant I_2 également. De plus, il ne maximise par l'invariant I_5.

$$|\Psi_8\rangle = \alpha|D_1\rangle + \beta|D_6\rangle , \tag{6.41}$$

avec ,

$$\alpha \approx 0.671588032,\ \beta \approx 0.740924770 . \tag{6.42}$$

L'état $|\Psi_8^a\rangle$ appelé *Maximally Entangled Antiprism state* ne maximise aucun des invariants, et ne maximise pas non plus la MGI. En revanche, lorsqu'on évalue la valeur absolue de l'invariant I_5, on atteint une valeur très proche du maximum.

$$|\Psi_8^a\rangle = \frac{|D_0\rangle + A|D_4\rangle - |D_8\rangle}{\sqrt{2+A^2}},\ A = 1.847592 . \tag{6.43}$$

Les états $\left|\psi_8^{\text{Th}}\right\rangle$ et $\left|\psi_8^{\text{Tó}}\right\rangle$ désignent respectivement les états solutions au problèmes de Thomson et Tóth pour les 8-qubits. Leur expression n'étant pas donnée par Aulbach, nous ne pouvons évaluer les invariants pour ces états, mais la valeur de la MGI est fournie, nous les utilisons donc à des fins de comparaison.

L'état $\left|M_8^{\Delta}\right\rangle$ est celui qui maximise la valeur absolue du discriminant. La valeur de la MGI est surpérieure aux états solutions des problèmes de Thomson et Tóth, mais reste inférieure à celle des trois premiers états présentés dans cette section. Cet état ne maximise pas I_2, mais présente une valeur assez proche du maximum pour l'invariant I_5.

$$\left|M_8^{\Delta}\right\rangle = \sum_{k=0}^{8} a_k|D_k\rangle , \tag{6.44}$$

avec ,

$$\begin{aligned} a_0 \approx 0.4114878254,\ a_1 \approx 0.1688959820,\ a_2 \approx 0.2944907798,\\ a_3 \approx -0.4149640033,\ a_4 \approx 0.2782623034,\ a_5 \approx 0.4628387130,\\ a_6 \approx 0.1293370123,\ a_7 \approx 0.2802238915,\ a_8 \approx -0.3953844931 . \end{aligned} \tag{6.45}$$

Enfin, après optimisation sur les complexes de l'invariant $|I_5|$, nous obtenons l'état $\left|M_8^{I_5}\right\rangle$ qui maximise l'invariant. Cependant, il ne maximise pas la valeur absolue du discriminant, ni de I_2, ni de la MGI.

$$\left|M_8^{I_5}\right\rangle = \sum_{k=0}^{8} b_k |D_k\rangle \ , \tag{6.46}$$

avec ,

$$\begin{aligned} b_0 \approx -0.2893248984 - 0.04211482037i,\ b_1 \approx 0.3845108489 + 0.008581859818i, \\ b_2 \approx 0.2495947516 + 0.1026688600i,\ b_3 \approx 0.3847336846 - 0.2212385794i, \\ b_4 \approx -0.01555897955 + 0.06124221024i,\ b_5 \approx -0.03200009998 + 0.3501447109i, \\ b_6 \approx -0.03240731033 - 0.4676685377i,\ b_7 \approx 0.1012411063 - 0.1488502853i, \\ b_8 \approx -0.1750153953 - 0.2938904319i \ . \end{aligned} \tag{6.47}$$

Tous les résultats sont regroupés en Table 6.6.

État	$\lvert\Delta_8\rvert$	$\lvert I_2\rvert$	$\lvert I_5\rvert$	E_g
$\lvert\psi_8^c\rangle$	$3.976821570 \times 10^{14}$	1	0.0001521451549	2.263034406
$\lvert\Psi_8\rangle$	0	0	0.0001547751396	2.445210155
$\lvert\Psi_8^a\rangle$	$4.392369364 \times 10^{14}$	0.2611196229	0.0001656284628	2.436587205
$\left\lvert\psi_8^{\text{Th}}\right\rangle$	?	?	?	2.084181498
$\left\lvert\psi_8^{\text{Tó}}\right\rangle$	?	?	?	1.711525327
$\left\lvert M_8^{\Delta}\right\rangle$	$4.720704891 \times 10^{14}$	0.1176806458	0.0001630388050	2.180671949
$\left\lvert M_8^{I_5}\right\rangle$	$4.499195566 \times 10^{14}$	0.2352913838	0.0001657652540	2.387041658

TABLE 6.6 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 8-qubits symétriques.

9-qubits

L'état $|\psi_9\rangle$ nommé *Triaugmented Triangular Prism state* a une valeur de la MGI qui n'est pas maximale. L'évaluation de la valeur absolue du discriminant pour cet état n'est pas maximale, mais elle se rapproche sensiblement du maximum conjecturé.

$$|\psi_9\rangle = \frac{|D_0\rangle - A\left(|D_3\rangle + |D_6\rangle\right) + |D_9\rangle}{\sqrt{2+2A^2}}, \text{ avec } A = \frac{1+8\sqrt{2}}{2\sqrt{21}} \ . \tag{6.48}$$

Les états $\left|\psi_9^{\text{Tó}}\right\rangle$ et $\left|\psi_9^{\text{Th}}\right\rangle$ sont respectivement des états solutions aux problèmes de Tóth et Thomson. La MGI associée à ces états est renseignée par Aulbach (et n'est pas intéressante comparée aux autres états présentés), mais pas leur expression.

L'état conjecturé maximalement intriqué par Aulbach est l'état $|\Psi_9\rangle$, qui semble maximiser la MGI, mais annulant le discriminant :

$$|\Psi_9\rangle = \frac{1}{\sqrt{2}}\left(|D_2\rangle + |D_7\rangle\right) \ . \tag{6.49}$$

D'autre part, après recherche numérique (sur les réels et complexes), nous proposons un état $\left|M_9^{\Delta}\right\rangle$ présentant une valeur du discriminant supérieure à tous les autres états

(et conjecturée comme étant maximale). Néanmoins pour les états maximisant $|\Delta_9|$, la MGI n'est, quant à elle, pas maximale. La valeur de la MGI pour l'état $\left|M_9^{\Delta}\right\rangle$ est en effet inférieure à celle des états $|\psi_9\rangle$ et $|\Psi_9\rangle$, mais reste tout de même supérieure à celle des états $\left|\psi_9^{\text{Tó}}\right\rangle$ et $\left|\psi_9^{\text{Th}}\right\rangle$.

$$\left|M_9^{\Delta}\right\rangle = \sum_{k=0}^{9} a_k |D_k\rangle \ , \tag{6.50}$$

avec ,

$$\begin{aligned} a_0 \approx -0.02545949738,\ a_1 \approx 0.5980327618,\ a_2 \approx 0.0271815356, \\ a_3 \approx 0.1489917661,\ a_4 \approx -0.1467454621,\ a_5 \approx 0.1254195894, \\ a_6 \approx 0.6618843307,\ a_7 \approx -0.06623252399, \\ a_8 \approx 0.03231183422,\ a_9 \approx -0.3714636942 \ . \end{aligned} \tag{6.51}$$

Tous les résultats sont regroupés en Table 6.7.

État	$\lvert\Delta_9\rvert$	E_g
$\lvert\psi_9\rangle$	6.434502×10^{18}	2.488046183
$\left\lvert\psi_9^{\text{Tó}}\right\rangle$	?	2.150714397
$\left\lvert\psi_9^{\text{Th}}\right\rangle$	?	2.434192780
$\lvert\Psi_9\rangle$	0	2.553960277
$\left\lvert M_9^{\Delta}\right\rangle$	$6.456659659 \times 10^{18}$	2.446117463

Table 6.7 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 9-qubits symétriques.

10-qubits

L'état $\left|\psi_{10}^{\text{Th}}\right\rangle$, résolvant le problème de Thomson, est défini par le *Gyroelongated Square Bipyarmid state*, et permet d'atteindre une valeur de la MGI proche du maximum. Un légère modification de la latitude des points de Majorana ont permis à Albauch de déterminer un état conjecturé comme étant maximalement intriqué, noté $|\Psi_{10}\rangle$, et possède la valeur de MGI la plus élevée parmi tous les états présentés dans cette section. L'état $\left|\psi_{10}^{\text{Tó}}\right\rangle$ solution du problème de Tóth est également présenté, mais ne présente pas de MGI intéressante. Pour ces trois états, l'expression dans la base de Dicke ne nous est pas connue, et ne permet donc pas l'évaluation des invariants.

Le *Maximally Positive state* est l'état symétrique positif proposé comme maximalement intriqué, et est noté $|\Psi_{10}^{\text{pos}}\rangle$. Pour cet état, la MGI n'est pas maximale, mais n'est pas très éloignée du maximum trouvé par Aulbach. De la même manière, la valeur absolue du discriminant et de I_6 n'est pas maximale, mais se rapproche de la valeur maximale trouvée après optimisation. En revanche, l'état annule l'invariant I_2.

$$|\Psi_{10}^{\text{pos}}\rangle = \alpha|D_0\rangle + \beta|D_4\rangle + \gamma|D_9\rangle \ , \tag{6.52}$$

avec,

$$\alpha \approx 0.395053091,\ \beta \approx 0.678420822;\ ,\ \gamma \approx 0.619417665 \ . \tag{6.53}$$

D'autre part, l'état $|\psi_{10}^{\text{pos}}\rangle$, qualifié de *Rotationally Symmetric to the Maximally Positive state*, est en effet défini comme symétrique à l'état $|\Psi_{10}^{\text{pos}}\rangle$, et possède une MGI légèrement inférieure à cet état. Cependant, cet état annule la valeur absolue du discriminant, mais maximise la valeur absolue de l'invariant I_2. Enfin, la valeur obtenue pour l'invariant I_6 n'est pas intéressante, lorsqu'elle est comparée à la valeur maximale.

$$|\psi_{10}^{\text{pos}}\rangle = \frac{1}{\sqrt{2}}\left(|D_2\rangle + |D_8\rangle\right) \ . \tag{6.54}$$

De plus, après une recherche numérique, nous proposons un état réel $\left|M_{10}^{\Delta}\right\rangle$ maximisant le discriminant. La MGI obtenue pour cet état est très proche de la valeur maximale. Elle est aussi supérieure à la MGI de l'état $\left|\psi_{10}^{\text{Th}}\right\rangle$. La valeur absolue de I_5 se rapproche sensiblement de la valeur maximale, tandis que la valeur de l'invariant I_2 n'est pas maximale.

$$\left|M_{10}^{\Delta}\right\rangle = \sum_{k=0}^{10} a_k |D_k\rangle \ , \tag{6.55}$$

avec ,

$$\begin{aligned} a_0 \approx 0.2323571768 + 0.1364747379i,\ a_1 \approx -0.08278980820 + 0.3089726145i,\\ a_2 \approx 0.4126253099 - 0.08632416017i,\ a_3 \approx 0.09119013158 - 0.03072904886i,\\ a_4 \approx -0.2543943260 + 0.1850526626i,\ a_5 \approx -0.2199500353 + 0.1198756628i,\\ a_6 \approx -0.2049516503 - 0.3805495544i,\ a_7 \approx -0.2590746280 + 0.3357172208i,\\ a_8 \approx -0.1549402140 + 0.04954393637i,\ a_9 \approx -0.05993323393 - 0.01010714449i,\\ a_{10} \approx 0.2529007257 - 0.2822984972i \ . \end{aligned} \tag{6.56}$$

Un des états maximisant la valeur absolue de l'invariant I_6 est l'état $\left|M_{10}^{I_6}\right\rangle$, défini ci-dessous. Il possède une valeur absolue du discriminant proche de la valeur maximale et supérieure à celle de l'état $|\Psi_{10}^{\text{pos}}\rangle$. La mesure géométrique de l'intrication de cet état est supérieure à celle des états $|\Psi_{10}^{\text{pos}}\rangle$ et $|\psi_{10}^{\text{pos}}\rangle$ en étant assez proche de la valeur maximale, mais inférieure à la valeur de MGI pour les états $\left|\psi_{10}^{\text{Th}}\right\rangle$ et $|\Psi_{10}\rangle$.

$$\left|M_{10}^{I_6}\right\rangle = \sum_{k=0}^{10} b_k |D_k\rangle \ , \tag{6.57}$$

avec ,

$$\begin{aligned} b_0 \approx 0.3171250394,\ b_1 \approx 0.1772167737,\ b_2 \approx -0.4787182647,\\ b_3 \approx -0.008253575939,\ b_4 \approx -0.2677664075,\ b_5 \approx -0.2524604762,\\ b_6 \approx -0.2537012052,\ b_7 \approx 0.5372491380,\ b_8 \approx 0.02451776893,\\ b_9 \approx 0.06625974693,\ b_{10} \approx 0.3812598508 \ . \end{aligned} \tag{6.58}$$

Tous les résultats sont regroupés en Table 6.8.

État	$\lvert\Delta_{10}\rvert$	$\lvert I_2\rvert$	$\lvert I_6\rvert$	E_g
$\lvert\psi_{10}^{\text{Th}}\rangle$	?	?	?	2.731632770
$\lvert\Psi_{10}\rangle$	?	?	?	2.737432003
$\lvert\psi_{10}^{\text{Tó}}\rangle$	?	?	?	1.958874344
$\lvert\Psi_{10}^{\text{pos}}\rangle$	$2.390216719 \times 10^{23}$	0	0.000001555217741	2.679763091
$\lvert\psi_{10}^{\text{pos}}\rangle$	0	1	0.000001371742112	2.678071905
$\lvert M_{10}^{\Delta}\rangle$	$2.578708780 \times 10^{23}$	0.2068976588	0.000001585909110	2.736670775
$\lvert M_{10}^{I_6}\rangle$	$2.531244978 \times 10^{23}$	0.2758526873	0.000001596424019	2.720835818

Table 6.8 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 10-qubits symétriques.

11-qubits

L'expression de l'état $\lvert\psi_{11}^{\text{Th}}\rangle$, solution au problème de Thomson, n'est pas explictement donnée par Aulbach. Cependant, l'expression de l'état $\lvert\psi_{11}^{\text{Tó}}\rangle$, solution au problème de Tóth est donnée mais la MGI associée est assez faible.

$$\lvert\psi_{11}^{\text{Tó}}\rangle = \frac{\sqrt{462}}{25}|D_0\rangle + \frac{11}{25}|D_5\rangle - \frac{\sqrt{42}}{25}|D_{10}\rangle \ . \tag{6.59}$$

En reprenant les mêmes vecteurs de base que l'état solution du problème de Tóth, et en optimisant les amplitudes de probabilité, Aulbach propose un état $|\Psi_{11}\rangle$ comme étant potentiellement maximalement intriqué. Cet état est celui qui a la plus grande MGI parmi les états proposés par Aulbach, les états maximisant le discriminant ayant une MGI bien inférieure. De plus, la valeur du discriminant pour l'état $|\Psi_{11}\rangle$ est inférieure à tous les autres états proposés :

$$|\Psi_{11}\rangle = \alpha|D_0\rangle + \beta|D_5\rangle - \gamma|D_{10}\rangle \ . \tag{6.60}$$

avec,

$$\alpha \approx 0.376611967,\ \beta \approx 0.715661256,\ \gamma \approx 0.588211181 \ . \tag{6.61}$$

D'autre part, l'état positif symétrique maximalement intriqué $|\Psi_{11}^{\text{pos}}\rangle$ déterminé numériquement par Aulbach, présente la même valeur absolue du discriminant que l'état de Tóth $\lvert\psi_{11}^{\text{Tó}}\rangle$. Il possède aussi une MGI assez proche de la MGI maximale potentielle, également supérieure à celle des états maximisant le discriminant.

$$|\Psi_{11}^{\text{pos}}\rangle = \alpha|D_1\rangle + \beta|D_5\rangle - \gamma|D_{10}\rangle \ . \tag{6.62}$$

avec,

$$\alpha \approx 0.550982113,\ \beta \approx 0.578058577,\ \gamma \approx 0.601886195 \ . \tag{6.63}$$

Enfin, nous proposons un état $\lvert M_{11}^{\Delta}\rangle$ maximisant la valeur absolue du discriminant après optimisation numérique pour des coefficients complexes. La valeur de la MGI n'est pas maximale, mais reste tout de même supérieure à celle de l'état $\lvert\psi_{11}^{\text{Tó}}\rangle$.

$$\lvert M_{11}^{\Delta}\rangle = \sum_{k=0}^{11} a_k|D_k\rangle \ , \tag{6.64}$$

avec ,

$$\begin{aligned} a_0 \approx -0.1349724068 + 0.2808519945i,\ a_1 \approx -0.04226554075 - 0.1182755877i, \\ a_2 \approx 0.2484586088 + 0.2880580792i,\ a_3 \approx 0.3788092524 - 0.1228068108i, \\ a_4 \approx 0.03137996622 + 0.1319071999i,\ a_5 \approx -0.2528424418 + 0.1083668311i, \\ a_6 \approx 0.1150089949 - 0.01598674178i,\ a_7 \approx 0.1895403275 + 0.2495940741i, \\ a_8 \approx -0.3309058181 + 0.1065237926i,\ a_9 \approx -0.01634886892 + 0.3813881798i, \\ a_{10} \approx -0.04175683331 - 0.06665883136i,\ a_{11} \approx 0.1741480562 - 0.02738520897i\ . \end{aligned} \tag{6.65}$$

Tous les résultats sont regroupés en Table 6.9.

État	$\lvert\Delta_{11}\rvert$	E_g
$\lvert\psi_{11}^{\text{Th}}\rangle$	?	2.482570
$\lvert\psi_{11}^{\text{Tó}}\rangle$	$9.394400141 \times 10^{27}$	0.435963338
$\lvert\Psi_{11}\rangle$	$6.841164175 \times 10^{25}$	2.817698505
$\lvert\Psi_{11}^{\text{pos}}\rangle$	$9.394400141 \times 10^{27}$	2.773622669
$\lvert M_{11}^{\Delta}\rangle$	$2.487249584 \times 10^{28}$	2.585125923

TABLE 6.9 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 11-qubits symétriques.

12-qubits

L'état $|\Psi_{12}\rangle$, appelé *Icosahedron state*, est issu du solide platonicien qu'est l'icosaèdre et constitue une solution aux problèmes de Tóth et Thomson. Cet état maximise la mesure géométrique de l'intrication, et maximise aussi la valeur absolue des invariants I_2 et I_7. En revanche, la valeur maximale du discriminant n'est pas atteinte.

$$|\Psi_{12}\rangle = \frac{1}{5}\left(\sqrt{7}|D_1\rangle - \sqrt{11}|D_6\rangle - \sqrt{7}|D_{11}\rangle\right)\ . \tag{6.66}$$

L'état symétrique positif $|\Psi_{12}^{\text{pos}}\rangle$ est proposé comme état maximalement intriqué (parmi tous les états positifs). Il présente une MGI légèrement inférieure à celle de l'*Icosahedron state*. Il ne maximise aucun des invariants, mais la valeur absolue de I_7 associée s'approche du maximum.

$$|\Psi_{12}^{\text{pos}}\rangle = \alpha|D_1\rangle + \beta|D_6\rangle + \alpha|D_{11}\rangle\ , \tag{6.67}$$

avec,

$$\alpha \approx 0.555046977,\ \beta \approx 0.619552827\ . \tag{6.68}$$

Enfin, un qui maximise la valeur absolue du discriminant est l'état $\lvert M_{12}^{\Delta}\rangle$. Cet état maximise également les invariants I_2 et I_7, et maximise aussi la MGI (atteignant la même valeur que l'état $|\Psi_{12}\rangle$).

$$\lvert M_{12}^{\Delta}\rangle = \sum_{k=0}^{12} a_k|D_k\rangle\ , \tag{6.69}$$

avec ,

$$\begin{aligned} a_0 \approx -0.03072652071 + 0.3088934983i,\ a_1 \approx -0.1539068313 + 0.08559489458i,\\ a_2 \approx 0.1944951782 + 0.1806169414i,\ a_3 \approx -0.1221557503 - 0.3572299861i,\\ a_4 \approx -0.006152485729 - 0.2591535581i,\ a_5 \approx 0.2732385278 - 0.04759548299i,\\ a_6 \approx -0.1302972739 - 0.1185283549i,\ a_7 \approx 0.02159386768 - 0.2765468353i,\\ a_8 \approx -0.2585585423 + 0.01835428213i,\ a_9 \approx 0.3671759544 + 0.08791194249i,\\ a_{10} \approx 0.1981132071 + 0.1766040590i,\ a_{11} \approx -0.07067753030 + 0.1612797770i,\\ a_{12} \approx 0.3046176995 - 0.05978759503i\ . \end{aligned} \tag{6.70}$$

Tous les résultats sont regroupés en Table 6.10.

État	$\lvert\Delta_{12}\rvert$	$\lvert I_2\rvert$	$\lvert I_7\rvert$	E_g
$\lvert\Psi_{12}\rangle$	$6.203331354 \times 10^{33}$	1	$5.890775571 \times 10^{-9}$	3.117457579
$\lvert\Psi_{12}^{\text{pos}}\rangle$	$3.641674830 \times 10^{33}$	0.2323085880	$5.401494287 \times 10^{-9}$	2.993524699
$\lvert M_{12}^{\Delta}\rangle$	$1.137091783 \times 10^{34}$	1	$5.890775599 \times 10^{-9}$	3.117486134

Table 6.10 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 12-qubits symétriques.

20-qubits

Le *Dodecahedron state*, état associé au solide platonicien, noté $|\psi_{20}\rangle$, est un état qui maximise l'invariant I_2. Sa mesure géométrique de l'intrication est moins intéressante que celle des états présentés par la suite. Cet état ne maximise pas le discriminant, et de même pour l'invariant I_{11}.

$$|\psi_{20}\rangle = \frac{1}{25\sqrt{3}}\left(\sqrt{187}|D_0\rangle + \sqrt{627}|D_5\rangle + \sqrt{247}|D_{10}\rangle - \sqrt{627}|D_{15}\rangle + \sqrt{187}|D_{20}\rangle\right)\ . \tag{6.71}$$

Les états $\left|\psi_{20}^{\text{Tó}}\right\rangle$ et $\left|\psi_{20}^{\text{Th}}\right\rangle$ sont les solutions au problème de Tóth et Thomson pour les 20-qubits. Il présentent une mesure géométrique supérieure à celle du *Dodecahedron state*, Celle associée à l'état solution du problème de Thomson étant supérieure aux deux autres.

Nous proposons l'état complexe $\left|M_{20}^{\Delta}\right\rangle$ comme maximisant le discriminant Δ_{20}. Cet état possède une MGI supérieure aux états proposés par Aulbach, mais ne maximise par les autres invariants.

$$\left|M_{20}^{\Delta}\right\rangle = \sum_{k=0}^{20} a_k|D_k\rangle\ , \tag{6.72}$$

avec ,

$$\begin{aligned}
a_0 &\approx 0.1508641395 - 0.2074592909i,\ a_1 \approx -0.04348719410 + 0.05982718075i,\\
a_2 &\approx -0.007215973384 + 0.01018331119i,\ a_3 \approx 0.2671186080 - 0.3675908755i,\\
a_4 &\approx 0.04884246537 - 0.06740783303i,\ a_5 \approx 0.1025546157 - 0.1407846500i,\\
a_6 &\approx -0.1111399563 + 0.1530330791i,\ a_7 \approx 0.05898217121 - 0.08123870400i,\\
a_8 &\approx 0.01138613101 - 0.01572548933i,\ a_9 \approx -0.1201082924 + 0.1652831727i,\\
a_{10} &\approx 0.09707842232 - 0.1333469530i,\ a_{11} \approx 0.2956313325 - 0.4068348128i,\\
a_{12} &\approx -0.001836433624 + 0.002485727944i,\ a_{13} \approx 0.1070201504 - 0.1470580227i,\\
a_{14} &\approx -0.04267018825 + 0.05866007755i,\ a_{15} \approx 0.05673273351 - 0.07825275364i,\\
a_{16} &\approx -0.1247405028 + 0.1715558232i,\ a_{17} \approx 0.04571334774 - 0.06300088062i,\\
a_{18} &\approx 0.2460595051 - 0.3385117982i,\ a_{19} \approx -0.002568387640 + 0.003655240308i,\\
a_{20} &\approx 0.1216970965 - 0.1674325506i\ .
\end{aligned} \tag{6.73}$$

L'état $\left|M_{20}^{I_2}\right\rangle$ est un des états qui maximise l'invariant I_2. Il diffère de l'état $|\psi_{20}\rangle$ dans la mesure où il présente une valeur supérieure pour le discriminant et la MGI. Pour ce qui concerne l'invariant I_{11}, c'est l'état $|\psi_{20}\rangle$ qui est plus intéressant.

$$\left|M_{20}^{I_2}\right\rangle = \sum_{k=0}^{20} b_k |D_k\rangle\ , \tag{6.74}$$

avec ,

$$\begin{aligned}
b_0 &\approx 0.2420694911,\ b_1 \approx -0.03523089732,\ b_2 \approx 0.09359104644,\\
b_3 &\approx 0.4688617634,\ b_4 \approx -0.1135820404,\ b_5 \approx 0.008395418393,\\
b_6 &\approx -0.1685464469,\ b_7 \approx -0.08433351912,\ b_8 \approx 0.0009289274410,\\
b_9 &\approx -0.2409269148,\ b_{10} \approx -0.4583265955,\ b_{11} \approx 0.2409195653,\\
b_{12} &\approx 0.0009261549026,\ b_{13} \approx 0.08433730090,\ b_{14} \approx -0.1685470447,\\
b_{15} &\approx -0.008399826346,\ b_{16} \approx -0.1135829952,\ b_{17} \approx -0.4688713935,\\
b_{18} &\approx 0.09359058740,\ b_{19} \approx 0.03521551515,\ b_{20} \approx 0.2420616475\ .
\end{aligned} \tag{6.75}$$

Enfin, nous proposons aussi l'état $\left|M_{20}^{I_{11}}\right\rangle$ comme candidat à l'état qui maximise l'invariant I_{11}. Cet état à la particularité d'avoir une MGI supérieure à tous les états présentés précédemment, et suggère que l'on pourrait éventuellement atteindre une valeur de MGI encore plus grande, en cherchant d'autres états qui maximisent l'invariant I_{11}.

$$\left|M_{20}^{I_{11}}\right\rangle = \sum_{k=0}^{20} c_k |D_k\rangle\ , \tag{6.76}$$

avec ,

$$\begin{aligned}
c_0 &\approx 0.04672174113 - 0.2523322314i,\ c_1 \approx -0.05069006573 + 0.04775699387i,\\
c_2 &\approx -0.04718394150 + 0.1021861476i,\ c_3 \approx -0.1590231434 + .3848619055i,\\
c_4 &\approx -0.02902596854 - 0.1569313402i,\ c_5 \approx -0.07696456685 + 0.07224485275i,\\
c_6 &\approx -0.09376435062 + 0.2035585893i,\ c_7 \approx 0.07806916194 + 0.06366061380i,\\
c_8 &\approx -0.04759595305 + 0.006445863013i,\ c_9 \approx 0.05301678648 - 0.1016543395i,\\
c_{10} &\approx 0.03609247219 - 0.4913401650i,\ c_{11} \approx 0.1184721897 + 0.1269084191i,\\
c_{12} &\approx -0.009108493287 - 0.006036402071i,\ c_{13} \approx 0.1803612698 - 0.08976913083i,\\
c_{14} &\approx -0.04430825373 - 0.1748209208i,\ c_{15} \approx -0.03003595026 + 0.04460972146i,\\
c_{16} &\approx -0.1138802790 - 0.04440768458i,\ c_{17} \approx -0.4070270968 - 0.1002096450i,\\
c_{18} &\approx 0.1547528831 - 0.01637363064i,\ c_{19} \approx 0.05633196292 - 0.03447193714i,\\
c_{20} &\approx 0.1099938346 - 0.2246437635i\ .
\end{aligned} \tag{6.77}$$

Tous les résultats sont regroupés en Table 6.11.

État	$\lvert\Delta_{20}\rvert$	$\lvert I_2\rvert$	$\lvert I_{11}\rvert$	E_g
$\lvert\psi_{20}\rangle$	$2.690718856 \times 10^{90}$	1	$1.739064106 \times 10^{-23}$	3.325780420
$\lvert\psi_{20}^{\text{Tó}}\rangle$	?	?	?	3.327075
$\lvert\psi_{20}^{\text{Th}}\rangle$	?	?	?	3.418012
$\lvert M_{20}^{\Delta}\rangle$	$1.061217213 \times 10^{96}$	0.1788691429	$2.229358366 \times 10^{-23}$	3.427028693
$\lvert M_{20}^{I_2}\rangle$	$2.040771647 \times 10^{94}$	1	$8.586804141 \times 10^{-28}$	3.492765025
$\lvert M_{20}^{I_{11}}\rangle$	$2.088432427 \times 10^{94}$	0.6189929947	$3.537212104 \times 10^{-23}$	3.613963543

Table 6.11 – Évaluation des mesures algébriques et géométriques de l'intrication pour les différents états maximalement intriqués, dans le cas des 20-qubits symétriques.

6.3 États fermioniques maximalement intriqués

Dans cette section, nous nous intéressons à la question du maximum de l'intrication pour les états fermioniques. Ces états fermioniques correspondent mathématiquement aux tenseurs antisymétriques, et les états séparables peuvent être vus comme des points de la variété Grassmannienne. Nous renvoyons le lecteur vers la Section 2.1.5.

Nous utiliserons la notation tensorielle pour désigner les vecteurs de la base canonique. Ainsi $e_1 \sim |0\rangle$ et $e_k \sim |k-1\rangle$. De plus, nous utiliserons parfois une notation raccourcie e_{ijk} pour désigner le produit externe $e_i \wedge e_j \wedge e_k$. Nous rappelons qu'un état fermionique à k particules et n états de base est un vecteur $|\psi\rangle$ normalisé de $\bigwedge^k \mathbb{C}^n$, donc l'écriture générale est donnée par

$$|\psi\rangle = \sum_{1\leq i_1,\dots,i_k\leq n} a_{i_1,\dots,i_k}\ e_{i_1} \wedge \cdots \wedge e_{i_k}\ , \tag{6.78}$$

avec $(e_i)_{1\leq i\leq n}$ une base orthonormée de $\mathbb{C}^n$, et les amplitudes complexes $a_{i_1,\dots,i_k}$ vérifiant $\sum_{1\leq i_1,\dots,i_k\leq n} |a_{i_1,\dots,i_k}|^2 = 1$.

Nous présenterons tout d'abord l'hyperpfaffien, analogue de l'hyperdéterminant pour les tenseurs antisymétriques, qui sera utilisé comme mesure de l'intrication. Nous verrons ensuite comment définir la mesure géométrique de l'intrication pour les états fermioniques, et le lien qu'elle entretient avec le rang antisymétrique. Enfin, nous traiterons un certain nombre de cas d'étude, et présenterons de nouveaux candidats pour des états maximalement intriqués.

6.3.1 L'hyperdéterminant pour les états fermioniques

Comme rappelé en Section 2.1.8, et tout au long de ce manuscrit, si X est une variété projective, alors on note X^* la variété duale, qui est définie par le lieu d'annulation de l'hyperdéterminant.

Dans le cas où X est définie comme la variété de Segre, alors la variété duale est définie par l'hyperdéterminant usuel, introduit par Cayley au milieu du 19$^{\text{ème}}$ siècle. Dans le cas où X est définie comme étant la variété de Veronese, alors comme rappelé en section précédente, la variété duale est définie par le discriminant.

Dans cette section, nous nous intéressons aux états à k fermions à n états, c'est à dire aux états appartenant à l'espace de Hilbert $\mathcal{H}_{k,n} = \bigwedge^k \mathbb{C}^n$, espace des k tenseurs antisymétriques de $\mathbb{C}^n$. Si l'on définit $X = G(k,n) \subset \mathbb{P}(\mathcal{H}_{k,n})$ comme étant la variété Grassmannienne modélisant les états fermioniques séparables, alors la variété duale X^* est définie par le polynôme appelé *Hyperpfaffien* de format (k,n), et sera noté $\Delta_{k,n}$.

Remarque 43. L'hyperpfaffien est une généralisation aux dimensions supérieures du *Pfaffien* (correspondant au cas $(k,n) = (2,2k)$), polynôme (de degré k) directement lié au déterminant des matrices antisymétriques.

Un aspect important dans le cadre de l'étude de l'intrication sous SLOCC est que les hyperpfaffiens sont justement des polynômes invariants sous l'action de ce groupe, notamment par construction, et du fait que la variété $G(k,n)$ définit une orbite sous l'action du groupe.

Exemple 9. Prenons l'exemple des systèmes à 3 fermions, où chaque fermion possède 6 états de base. Dans ce cas, un état fermionique $|\psi\rangle \in \bigwedge^3 \mathbb{C}^6$ est un tenseur antisymétrique normalisé s'exprimant comme

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{1\leq i,j,k\leq 6} p_{i,j,k}\ e_i \wedge e_j \wedge e_k\ ,$$

avec N la constante de normalisation. L'anneau des polynômes invariants $\mathbb{C}[\bigwedge^3 \mathbb{C}^6]^{\text{SLOCC}}$ est généré par l'hyperpfaffien $\Delta_{3,6}$. Ce polynôme est défini de manière unique, à une constante multiplicative près, et peut être exprimé explicitement comme :

$$\Delta_{3,6}(\psi) =$$
$$4(p_{123}{}^2p_{456}{}^2+p_{124}{}^2p_{356}{}^2+p_{125}{}^2p_{346}{}^2+p_{345}{}^2p_{126}{}^2+p_{134}{}^2p_{256}{}^2+p_{135}{}^2p_{246}{}^2+p_{245}{}^2p_{136}{}^2+p_{145}{}^2p_{236}{}^2+p_{235}{}^2p_{146}{}^2+p_{234}{}^2p_{156}{}^2$$
$$+4(p_{123}p_{145}p_{246}p_{356}-p_{123}p_{145}p_{346}p_{256}-p_{123}p_{245}p_{146}p_{356}+p_{123}p_{345}p_{146}p_{256}+p_{123}p_{245}p_{346}p_{156}-p_{123}p_{345}p_{246}p_{156}$$
$$+p_{124}p_{135}p_{236}p_{456}+p_{124}p_{135}p_{346}p_{256}-p_{124}p_{235}p_{136}p_{456}-p_{124}p_{345}p_{136}p_{256}-p_{124}p_{235}p_{346}p_{156}+p_{124}p_{345}p_{236}p_{156}$$
$$-p_{134}p_{125}p_{236}p_{456}+p_{134}p_{125}p_{246}p_{356}+p_{234}p_{125}p_{136}p_{456}+p_{125}p_{345}p_{136}p_{246}-p_{234}p_{125}p_{146}p_{356}-p_{125}p_{345}p_{236}p_{146}$$
$$+p_{134}p_{235}p_{126}p_{456}-p_{134}p_{245}p_{126}p_{356}-p_{234}p_{135}p_{126}p_{456}+p_{135}p_{245}p_{126}p_{346}+p_{234}p_{145}p_{126}p_{356}-p_{235}p_{145}p_{126}p_{346}$$
$$+p_{134}p_{235}p_{246}p_{156}-p_{134}p_{245}p_{236}p_{156}+p_{234}p_{135}p_{146}p_{256}+p_{135}p_{245}p_{236}p_{146}-p_{234}p_{145}p_{136}p_{256}+p_{235}p_{145}p_{136}p_{246})$$
$$+2(-p_{123}p_{124}p_{356}p_{456}+p_{123}p_{125}p_{346}p_{456}-p_{123}p_{345}p_{126}p_{456}+p_{123}p_{134}p_{256}p_{456}-p_{123}p_{135}p_{246}p_{456}+p_{123}p_{245}p_{136}p_{456}$$
$$-p_{123}p_{145}p_{236}p_{456}+p_{123}p_{235}p_{146}p_{456}-p_{123}p_{234}p_{156}p_{456}-p_{124}p_{125}p_{346}p_{356}+p_{124}p_{345}p_{126}p_{356}-p_{124}p_{134}p_{256}p_{356}$$
$$-p_{124}p_{135}p_{246}p_{356}+p_{124}p_{245}p_{136}p_{356}-p_{124}p_{145}p_{236}p_{356}+p_{124}p_{235}p_{146}p_{356}+p_{124}p_{234}p_{156}p_{356}-p_{125}p_{345}p_{126}p_{346}$$
$$-p_{134}p_{125}p_{346}p_{256}-p_{125}p_{135}p_{246}p_{346}-p_{125}p_{245}p_{136}p_{346}+p_{125}p_{145}p_{236}p_{346}+p_{125}p_{235}p_{146}p_{346}+p_{234}p_{125}p_{346}p_{156}$$
$$+p_{134}p_{345}p_{126}p_{256}-p_{135}p_{345}p_{126}p_{246}-p_{245}p_{345}p_{126}p_{136}+p_{145}p_{345}p_{126}p_{236}+p_{235}p_{345}p_{126}p_{146}-p_{234}p_{345}p_{126}p_{156}$$
$$-p_{134}p_{135}p_{246}p_{256}+p_{134}p_{245}p_{136}p_{256}+p_{134}p_{145}p_{236}p_{256}-p_{134}p_{235}p_{146}p_{256}-p_{134}p_{234}p_{156}p_{256}-p_{135}p_{245}p_{136}p_{246}$$
$$-p_{135}p_{145}p_{236}p_{246}-p_{135}p_{235}p_{146}p_{246}-p_{234}p_{135}p_{246}p_{156}-p_{145}p_{245}p_{136}p_{236}-p_{235}p_{245}p_{136}p_{146}+p_{234}p_{245}p_{136}p_{156}$$
$$-p_{235}p_{145}p_{236}p_{146}+p_{234}p_{145}p_{236}p_{156}-p_{234}p_{235}p_{146}p_{156})).$$

♢

6.3.2 Mesure géométrique de l'intrication pour les états fermioniques

Dans cette section, nous nous intéressons à la mesure géométrique de l'intrication pour les états fermioniques. Nous discuterons alors deux approches possibles, et nous nous arrêterons sur une définition acceptable de cette mesure. Nous étudierons ensuite le lien entre mesure géométrique pour les fermions et rang des tenseurs antisymétriques.

Définition pour les états fermioniques

Comme rappelé en Section 2.2.3, une manière de mesurer le degré d'intrication d'un état pur est de considérer la distance à l'état séparable le plus proche. Nous adopterons ici la version Groverienne E_G de la mesure de l'intrication rappelée en Équation 2.43.

Premièrement, en remarquant que $\bigwedge^k \mathbb{C}^n$ est inclus dans $(\mathbb{C}^n)^{\otimes k}$, on peut alors considérer un état fermionique $|\psi\rangle \in \bigwedge^k \mathbb{C}^n$ comme un état pur dans $(\mathbb{C}^n)^{\otimes k}$. On peut alors utiliser la mesure géométrique E_G des états purs pour évaluer la distance de l'état $|\psi\rangle$ à l'état séparable de $(\mathbb{C}^n)^{\otimes k}$ le plus proche. Des exemples d'évaluation de la MGI pour des tenseurs antisymétriques sont accessibles dans [271].

Cette première définition présente néanmoins certains inconvénients, dont notamment le fait que la MGI est égale à $E_G(|\psi\rangle) = 1 - \frac{1}{k!}$ pour les états $|\psi\rangle = e_1 \wedge \cdots \wedge e_k$ de rang antisymétrique égal à 1. Cette quantité tend vers 1 lorsque k croit, ce qui nous laisse entendre qu'une autre définition de la MGI est nécessaire.

Une seconde possibilité est de définir la mesure géométrique non pas comme une distance par rapport aux états séparables de $\mathbb{C}^n \otimes \cdots \otimes \mathbb{C}^n$, mais plutôt comme une distance par rapport aux états fermioniques de rang antisymétrique égal à 1, c'est à dire par rapport aux états séparables de la variété $G(k,n)$. Ceci nous amène donc à définir ce qu'on appellera la *Mesure Géométrique Grassmannienne de l'Intrication* (MGGI) :

Définition 44. Soit $|\psi\rangle \in \bigwedge^k \mathbb{C}^n \subset (\mathbb{C}^n)^{\otimes k}$ un état fermionique de k particules à n états de base. On définit la Mesure Géométrique Grassmannienne de l'Intrication (MGGI) de l'état $|\psi\rangle$, notée $E_{GG}(|\psi\rangle)$, comme étant la quantité suivante :

$$E_{GG}(|\psi\rangle) = 1 - \max_{|\varphi\rangle \in G(k,n)} |\langle\psi|\varphi\rangle|^2 \ .$$

Comme cela sera discuté en sous-section 6.3.3, cette définition de la mesure géométrique de l'intrication pour les états fermioniques présente des résultats similaires à la mesure géométrique de l'intrication lorsqu'on les évalue sur des états définis de manière analogue.

Lien avec le rang de tenseur

La définition du rang antisymétrique étant rappelée en Section 2.1.6, nous établissons une relation d'inégalité entre la Mesure Géométrique Grassmannienne de l'Intrication et la rang antisymétrique dans la proposition suivante :

Proposition 6.3.1. *Soit $|\psi\rangle \in \bigwedge^k \mathbb{C}^n$ un vecteur unitaire de rang antisymétrique r, tel que $|\psi\rangle = \sum_{i=1}^r a_i |\varphi_i\rangle$, avec les $|\varphi_i\rangle$ des tenseurs de rang 1 (appartenant donc à $G(k,n)$) et avec $\langle\varphi_i|\varphi_j\rangle = 0$ pour $i \neq j$. Alors le rang antisymétrique r et la Mesure Géométrique Grassmannienne de l'Intrication sont reliés par la relation suivante :*

$$\frac{1}{1 - E_{GG}(|\psi\rangle)} \leq r \ .$$

Démonstration. Soit $|\psi\rangle$ un tenseur antisymétrique de rang antisymétrique r correspondant à un état fermionique dans $\bigwedge^k \mathbb{C}^n$, tel que

$$|\psi\rangle = \sum_{i=1}^{r} a_i |\varphi_i\rangle \ ,$$

avec $\forall i \ |\varphi_i\rangle \in G(k,n)$, et $\langle\varphi_i|\varphi_j\rangle = 0$ pour $i \neq j$, et avec a_i les amplitudes complexes vérifiant $\sum_{i=1}^r |a_i|^2 = 1$. Comme les états $|\varphi_i\rangle$ sont orthogonaux, alors on a $\langle\psi|\varphi_i\rangle = a_i$. De ce fait, nous obtenons l'inégalité suivante :

$$|a_i|^2 \leq \max_{|\delta\rangle \in G(k,n)} |\langle\psi|\delta\rangle|^2 \ ,$$

ce qui revient à dire que

$$|a_i|^2 \leq 1 - E_{GG}(\psi) \ .$$

En réutilisant ce résultat et en sommant les probabilités de mesure, on en arrive à l'inégalité suivante :

$$\sum_{i=1}^{r} |a_i|^2 = 1 \leq \sum_{i=1}^{r} 1 - E_{GG}(\psi) = r\,(1 - E_{GG}(\psi)) \ .$$

On en déduit alors directement l'inégalité apparaissant dans la proposition. □

Ce résultat est déjà connu dans le cadre des systèmes à plusieurs qubits, et provient de la relation entre l'entropie de Rényi et l'entropie d'Hartley, et des inégalités associées [97].

Exemple 10. Dans [13][Exemple 22], les auteurs ont démontré que le rang du tenseur antisymétrique $T = e_1 \wedge e_2 \wedge e_3 + e_1 \wedge e_4 \wedge e_5 + e_2 \wedge e_4 \wedge e_6 \in \bigwedge^3 \mathbb{C}^6$ est égal à 3, par des arguments géométriques. La Proposition 6.3.1 nous permet de retrouver ce résultat. En effet, si on considère un état fermionique normalisé $|\psi\rangle$ colinéaire à T, alors $E_{GG}(|\psi\rangle) = 5/9$ et donc $r \geq 3$. Compte tenu de l'écriture du tenseur, nous pouvons également établir que le rang antisymétrique vérifie $r \leq 3$. De ce fait, on conclut que $r = 3$. ♢

6.3.3 Étude de cas

Dans cette sous-section, nous étudions pour différents cas, différentes valeurs de (k, n) pour les états de $\bigwedge^k \mathbb{C}^n$, la maximisation de l'hyperpfafiien et des invariants fondamentaux (lorsque leur expression est unique), et une tentative de maximisation de la mesure géométrique grassmannienne de l'intrication.

Cas $k = 3$, $n = 6$

Le premier cas est celui des états fermioniques de $\bigwedge^3 \mathbb{C}^6$. Nous nous intéressons tout d'abord à l'intrication de ces états du point de vue de la MGGI. La classification de l'intrication des états à 3-qubits présente certaines similarités avec celle des états de $\bigwedge^3 \mathbb{C}^6$, et à titre d'exemple, on peut aisément vérifier que :

$$E_G\left(|GHZ\rangle\right) = \frac{1}{2}, \quad E_G\left(|W\rangle\right) = \frac{5}{9}\,. \tag{6.79}$$

De manière assez analogue, l'évaluation de la MGGI sur les états remarquables de la classification des états fermioniques de $\bigwedge^3 \mathbb{C}^6$ est présentée ci-dessous en Table 6.12.

D'autre part, lorsque l'hyperpfaffien (voir Exemple 9) est considéré comme mesure de l'intrication, l'état maximisant celle-ci est l'état $\left|GHZ^f\right\rangle$ pour lequel $|\Delta_{3,6}(\left|GHZ^f\right\rangle)| = 1$.

Type d'état	État	$\lvert\Delta_{3,6}\rvert$	MGGI	Rang_{ASym}
Séparable	$e_1 \wedge e_2 \wedge e_3$	0	0	1
Biséparable	$e_1 \wedge (e_2 \wedge e_3 + e_4 \wedge e_5)$	0	1/2	2
W^f	$e_4 \wedge e_2 \wedge e_3 + e_1 \wedge e_5 \wedge e_3 + e_1 \wedge e_2 \wedge e_6$	0	5/9	3
GHZ^f	$e_1 \wedge e_2 \wedge e_3 + e_4 \wedge e_5 \wedge e_6$	1	1/2	2

Table 6.12 – Intrication des états fermioniques pour le cas $(k, n) = (3, 6)$ du point de vue de l'hyperpfiaffien, de la MGGI et du rang.

Cas $k = 3$, $n = 7$

Dans le cas où $(k, n) = (3, 7)$, l'hyperpfaffien $\Delta_{3,7}$ est également générateur de tous les invariants fondamentaux. La structure des orbites des états de $\bigwedge^3 \mathbb{C}^7$ est connue dans la littérature mathématique [118] et en information quantique [231]. Pour chaque représentant de chaque orbite, nous évaluons l'hyperpfaffien, la MGGI et le rang. Nous regroupons ces informations dans la Table 6.13.

Dans ce cas, c'est l'état associé à la dernière orbite qui maximise la valeur de la MGGI. Cet état est également l'état de rang maximal dans la classification.

Cas $k = 3$, $n = 8$

Dans le cas où $(k, n) = (3, 8)$, l'hyperpfaffien $\Delta_{3,8}$ est également générateur de tous les invariants fondamentaux. La structure des orbites des états de $\bigwedge^3 \mathbb{C}^8$ est aussi connue dans la littérature [118, 231]. Pour chaque représentant de chaque orbite, nous évaluons

Orbite	État	$\lvert\Delta_{3,7}\rvert$	MGGI	Rang_{ASym}
II	e_{123} (Séparable)	0	0	1
III	$e_{123}+e_{145}$ (Biséparable)	0	1/2	2
IV	$e_{456}+e_{147}+e_{257}$ (W)	0	5/9	3
V	$e_{123}+e_{456}$ (GHZ)	0	1/2	2
VI	$e_{147}+e_{257}+e_{367}$	0	2/3	3
VII	$e_{456}+e_{147}+e_{257}+e_{367}$	0	2/3	3
VIII	$e_{123}+e_{456}+e_{147}$	0	2/3	3
IX	$e_{123}+e_{456}+e_{147}+e_{257}$ (GHZ_3)	0	5/8	3
X	$e_{123}+e_{456}+e_{147}+e_{257}+e_{367}$	$\neq 0$	7/10	4

TABLE 6.13 – Intrication des états fermioniques pour le cas $(k,n)=(3,7)$ du point de vue de l'hyperpfiaffien, de la MGGI et du rang.

l'hyperpfaffien, la MGGI et le rang. Nous regroupons ces informations dans la Table 6.14.

Orbite	État	$\lvert\Delta_{3,8}\rvert$	MGGI	Rang_{ASym}
II	e_{123} (Séparable)	0	0	1
III	$e_{123}+e_{145}$ (Biséparable)	0	1/2	2
IV	$e_{456}+e_{147}+e_{257}$ (W)	0	5/9	3
V	$e_{123}+e_{456}$ (GHZ)	0	1/2	2
VI	$e_{147}+e_{257}+e_{367}$	0	2/3	3
VII	$e_{456}+e_{147}+e_{257}+e_{367}$	0	2/3	3
VIII	$e_{123}+e_{456}+e_{147}$	0	2/3	3
IX	$e_{123}+e_{456}+e_{147}+e_{257}$ (GHZ_3)	0	5/8	3
X	$e_{123}+e_{456}+e_{147}+e_{257}+e_{367}$	0	7/10	4
XI	$e_{127}+e_{138}+e_{146}+e_{235}$	0	2/3	4
XII	$e_{128}+e_{137}+e_{146}+e_{236}+e_{245}$	0	7/10	4
XIII	$e_{135}+e_{246}+e_{147}+e_{238}$	0	3/4	4
XIV	$e_{138}+e_{147}+e_{156}+e_{235}+e_{246}$	0	0.6748495	4
XV	$e_{128}+e_{137}+e_{146}+e_{247}+e_{256}+e_{345}$	0	0.7239023	5
XVI	$e_{156}+e_{178}+e_{234}$	0	2/3	3
XVII	$e_{158}+e_{167}+e_{234}+e_{256}$	0	2/3	4
XVIII	$e_{148}+e_{157}+e_{236}+e_{245}+e_{347}$	0	7/10	4
XIX	$e_{134}+e_{234}+e_{156}+e_{278}$	0	1/2	3
XX	$e_{137}+e_{237}+e_{256}+e_{148}+e_{345}$	0	6/10	4
XXI	$e_{138}+e_{147}+e_{245}+e_{267}+e_{356}$	0	7/10	4
XXII	$e_{128}+e_{147}+e_{236}+e_{257}+e_{358}+e_{456}$	0	0.7073452	4
XXIII	$e_{124}+e_{134}+e_{256}+e_{378}+e_{157}+e_{468}$	$\neq 0$	2/3	4

TABLE 6.14 – Intrication des états fermioniques pour le cas $(k,n)=(3,8)$ du point de vue de l'hyperpfiaffien, de la MGGI et du rang.

Dans ce cas, les états qui n'annulent pas l'hyperpfaffien sont des états équivalents au représentant de la dernière orbite XXIII. D'autre part, le représentant de l'orbite XV est celui qui présente la plus grande MGGI, et présente aussi la plus haute valeur de rang antisymétrique.

Cas $k = 3$, $n = 9$

Dans le cas des 3-fermions à 9 états, l'anneau des polynômes invariants est généré par 4 polynômes linéairement indépendants de degré 12, 18, 24 et 30. En d'autres termes nous avons $\mathbb{C}[\bigwedge^3\mathbb{C}^9]^{\mathrm{SLOCC}} = \mathbb{C}[I_{12}, I_{18}, I_{24}, I_{30}]$.

Tout état $|\psi\rangle$ de $\bigwedge^3\mathbb{C}^9$ peut être décomposé comme la somme d'un état semi-simple et d'un état nilpotent, tel que $|\psi\rangle = |\psi_S\rangle + |\psi_N\rangle$. Les états semi-simples génériques de $\bigwedge^3\mathbb{C}^9$ peuvent être exprimés comme une combinaison linéaire de 4 états générateurs :

$$|\psi_S\rangle = z_1|p_1\rangle + z_2|p_2\rangle + z_3|p_3\rangle + z_4|p_4\rangle \ , \tag{6.80}$$

avec

$$\begin{aligned}
|p_1\rangle &= e_1 \wedge e_2 \wedge e_3 + e_4 \wedge e_5 \wedge e_6 + e_7 \wedge e_8 \wedge e_9 \ , \\
|p_2\rangle &= e_1 \wedge e_4 \wedge e_7 + e_2 \wedge e_5 \wedge e_8 + e_3 \wedge e_6 \wedge e_9 \ , \\
|p_3\rangle &= e_1 \wedge e_5 \wedge e_9 + e_2 \wedge e_6 \wedge e_7 + e_3 \wedge e_4 \wedge e_8 \ , \\
|p_4\rangle &= e_1 \wedge e_6 \wedge e_8 + e_2 \wedge e_4 \wedge e_9 + e_3 \wedge e_5 \wedge e_7 \ .
\end{aligned} \tag{6.81}$$

et

$$|z_1|^2 + |z_2|^2 + |z_3|^2 + |z_4|^2 = 1 \ . \tag{6.82}$$

L'hyperpfaffien $\Delta_{3,9}$ s'annule sur les éléments nilpotents, et il suffit alors de se restreindre aux états semi-simples génériques, comme exprimé en Équation 6.91, pour déterminer des états fermioniques maximisant l'hyperpfaffien.

Cet hyperpfaffien $\Delta_{3,9}$ ont été récemment calculé sous forme explicite par Holweck et Oeding dans [139]. L'expression de cet hyperdéterminant évalué sur les éléments semi-simples est $\Delta_{3,9}(|\psi_S\rangle) = h^3$ avec

$$\begin{aligned}
h = {} & z_1z_2z_3z_4(z_1+z_2-z_3)(z_1+z_3-z_4)(z_1-z_2+z_4)(z_2+z_3+z_4) \\
& (z_1^2 - z_1z_2 + z_2^2 + z_1z_3 - 2z_2z_3 + z_3^2)(z_1^2 + z_1z_2 + z_2^2 - z_1z_4 - 2z_2z_4 + z_4^2) \\
& (z_1^2 - z_1z_3 + z_3^2 + z_1z_4 - 2z_3z_4 + z_4^2)(z_2^2 - z_2z_3 + z_3^2 - z_2z_4 + 2z_3z_4 + z_4^2) \\
& (z_1^2 - 2z_1z_2 + z_2^2 - z_1z_4 + z_2z_4 + z_4^2)(z_1^2 - z_1z_2 + z_2^2 - 2z_1z_3 + z_2z_3 + z_3^2) \\
& (z_1^2 - z_1z_2 + z_2^2 + z_1z_3 + z_2z_3 + z_3^2)(z_1^2 + z_1z_2 + z_2^2 - z_1z_4 + z_2z_4 + z_4^2) \\
& (z_1^2 + z_1z_2 + z_2^2 + 2z_1z_4 + z_2z_4 + z_4^2)(z_1^2 + 2z_1z_2 + z_2^2 + z_1z_3 + z_2z_3 + z_3^2) \\
& (z_1^2 - z_1z_3 + z_3^2 - 2z_1z_4 + z_3z_4 + z_4^2)(z_1^2 - z_1z_3 + z_3^2 + z_1z_4 + z_3z_4 + z_4^2) \\
& (z_1^2 + 2z_1z_3 + z_3^2 + z_1z_4 + z_3z_4 + z_4^2)(z_2^2 - z_2z_3 + z_3^2 - z_2z_4 - z_3z_4 + z_4^2) \\
& (z_2^2 - z_2z_3 + z_3^2 + 2z_2z_4 - z_3z_4 + z_4^2)(z_2^2 + 2z_2z_3 + z_3^2 - z_2z_4 - z_3z_4 + z_4^2) \ .
\end{aligned} \tag{6.83}$$

Nous maximisons ensuite cette quantité par recherche numérique et nous proposons l'état $\left|M^{\Delta}_{3,9}\right\rangle$ comme état maximisant l'hyperpfaffien, exprimé comme suit :

$$\left|M^{\Delta}_{3,9}\right\rangle = \frac{1}{\sqrt{3}}\big(\alpha_1|p_1\rangle + \alpha_2|p_2\rangle + \alpha_3\left(|p_3\rangle + |p_4\rangle\right)\big) \ , \tag{6.84}$$

avec

$$\alpha_1 = 0.7767649052, \quad \alpha_2 = 0.3802944266, \quad \alpha_3 = 0.3549735421 \ . \tag{6.85}$$

Nous nous proposons également de maximiser les invariants fondamentaux afin de proposer des états maximalement intriqués en ce sens. Les invariants de degré 24 et 30 n'étant pas définis de manière unique, nous choisissons de nous restreindre aux deux invariants I_{12} et I_{18} comme mesure algébrique de l'intrication. Leur expression, lorsqu'ils sont évalués sur les éléments semi-simples, est donnée dans les équations suivantes.

$$\begin{aligned} I_{12}(|\psi_S\rangle) = {} & z_1^{12} + \big(22z_2^6 + (-220z_3^3 - 220z_4^3)z_2^3 + 22z_3^6 - 220z_4^3z_3^3 + 22z_4^6\big)z_1^6 \\ & + \big((-220z_3^3 + 220z_4^3)z_2^6 + (220z_3^6 - 220z_4^6)z_2^3 - 220z_3^6z_4^3 + 220z_3^3z_4^6\big)z_1^3 + z_2^{12} \\ & + (22z_3^6 + 220z_3^3z_4^3 + 22z_4^6)z_2^6 + (220z_3^6z_4^3 + 220z_3^3z_4^6)z_2^3 + z_3^{12} + 22z_3^6z_4^6 + z_4^{12} \ . \end{aligned} \tag{6.86}$$

$$\begin{aligned} I_{18}(|\psi_S\rangle) = {} & z_1^{18} + \big(- 17z_2^6 + (170z_3^3 + 170z_4^3)z_2^3 - 17z_3^6 + 170z_4^3z_3^3 - 17z_4^6\big)z_1^{12} \\ & + \big((1870z_3^3 - 1870z_4^3)z_2^6 + (-1870z_3^6 + 1870z_4^6)z_2^3 + 1870z_3^6z_4^3 - 1870z_3^3z_4^6\big)z_1^9 \\ & + \big(- 17z_2^{12} + (1870z_3^3 + 1870z_4^3)z_2^9 + (-7854z_3^6 - 7854z_4^6)z_2^6 + (1870z_3^9 + 1870z_4^9)z_2^3 \\ & \quad -17z_3^{12} + 1870z_3^9z_4^3 - 7854z_3^6z_4^6 + 1870z_3^3z_4^9 - 17z_4^{12}\big)z_1^6 - 17z_3^6z_4^{12} \\ & + \big((170z_3^3 - 170z_4^3)z_2^{12} + (-1870z_3^6 + 1870z_4^6)z_2^9 + (1870z_3^9 - 1870z_4^9)z_2^6 \\ & + (-170z_3^{12} + 170z_4^{12})z_2^3 + 170z_3^{12}z_4^3 - 1870z_3^9z_4^6 + 1870z_3^6z_4^9 - 170z_3^3z_4^{12}\big)z_1^3 \\ & + z_2^{18} + (-17z_3^6 - 170z_3^3z_4^3 - 17z_4^6)z_2^{12} + (-1870z_3^6z_4^3 - 1870z_3^3z_4^6)z_2^9 \\ & + (-17z_3^{12} - 1870z_3^9z_4^3 - 7854z_3^6z_4^6 - 1870z_3^3z_4^9 - 17z_4^{12})z_2^6 - 17z_3^{12}z_4^6 \\ & + (-170z_3^{12}z_4^3 - 1870z_3^9z_4^6 - 1870z_3^6z_4^9 - 170z_3^3z_4^{12})z_2^3 + z_3^{18} + z_4^{18} \ . \end{aligned} \tag{6.87}$$

En maximisant la valeur absolue de ces deux invariants fondamentaux, nous obtenons un autre état candidat comme état maximalement intriqué :

$$\big|M_{3,9}^{I_{12}}\big\rangle = \big|M_{3,9}^{I_{18}}\big\rangle = \frac{1}{\sqrt{3}}|p_1\rangle \ . \tag{6.88}$$

Enfin, en recherchant un état maximisant la Mesure Géométrique Grassmannienne de l'Intrication parmi les états semi-simples de la forme $|\psi_S\rangle$, nous proposons un état candidat, que nous notons $\big|M_{3,9}^{\mathrm{MGGI}}\big\rangle$, exprimé comme suit

$$\big|M_{3,9}^{\mathrm{MGGI}}\big\rangle = \frac{1}{\sqrt{3}}\big(\alpha_1(|p_1\rangle + |p_2\rangle - |p_3\rangle) + \alpha_2|p_4\rangle\big) \ , \tag{6.89}$$

avec

$$\alpha_1 \approx -0.3708072875, \quad \alpha_2 \approx -0.7664893123 \ . \tag{6.90}$$

États	$\lvert\Delta_{3,9}\rvert$	$\lvert I_{12}\rvert$	$\lvert I_{18}\rvert$	MGGI	Rang_{ASym}
$\big\lvert M_{3,9}^{\Delta}\big\rangle$	$5.006756885 \times 10^{-14}$	0.00023110204	$1.266305139 \times 10^{-6}$	0.7988788	≥ 5
$\big\lvert M_{3,9}^{I_{12}}\big\rangle$	0	0.0013717421	$5.080526343 \times 10^{-5}$	2/3	3
$\big\lvert M_{3,9}^{\mathrm{MGGI}}\big\rangle$	0	0.00036635565	$2.036095010 \times 10^{-6}$	0.804163492	≥ 6

TABLE 6.15 – Comparaison des mesures numériques (algébriques et géométriques) pour les états fermioniques maximalement intriqués, dans le cas $(k, n) = (3, 9)$.

Cas $k = 4$, $n = 8$

Ce cas présent partage des similarités avec le cas précédent. En effet, dans le cas des 4-fermions à 8 états, l'anneau des polynômes invariants est généré par 7 polynômes linéairement indépendants de degré 2, 6, 8, 10, 12, 14 et 18. En d'autres termes nous avons $\mathbb{C}[\bigwedge^4\mathbb{C}^8]^{\mathrm{SLOCC}} = \mathbb{C}[I_2, I_6, I_8, I_{10}, I_{12}, I_{14}, I_{18}]$.

De la même manière que pour le cas précédent, tout état $|\psi\rangle$ de $\bigwedge^4\mathbb{C}^8$ peut être décomposé comme la somme d'un état semi-simple et d'un état nilpotent, tel que $|\psi\rangle = |\psi_S\rangle + |\psi_N\rangle$. Les états semi-simples génériques de $\bigwedge^4\mathbb{C}^8$ peuvent être exprimés comme une combinaison linéaire de 7 états générateurs :

$$|\psi_S\rangle = y_1|p_1\rangle + y_2|p_2\rangle + y_3|p_3\rangle + y_4|p_4\rangle + y_5|p_5\rangle + y_6|p_6\rangle + y_7|p_7\rangle \ , \tag{6.91}$$

avec

$$\begin{aligned}
|p_1\rangle &= e_1 \wedge e_2 \wedge e_3 \wedge e_4 + e_5 \wedge e_6 \wedge e_7 \wedge e_8 \ , \\
|p_2\rangle &= e_1 \wedge e_3 \wedge e_5 \wedge e_6 + e_6 \wedge e_8 \wedge e_2 \wedge e_4 \ , \\
|p_3\rangle &= e_1 \wedge e_5 \wedge e_6 \wedge e_2 + e_8 \wedge e_4 \wedge e_3 \wedge e_7 \ , \\
|p_4\rangle &= e_1 \wedge e_6 \wedge e_8 \wedge e_3 + e_4 \wedge e_7 \wedge e_5 \wedge e_2 \ , \\
|p_5\rangle &= e_1 \wedge e_8 \wedge e_4 \wedge e_5 + e_7 \wedge e_2 \wedge e_6 \wedge e_3 \ , \\
|p_6\rangle &= e_1 \wedge e_4 \wedge e_7 \wedge e_6 + e_2 \wedge e_3 \wedge e_8 \wedge e_5 \ , \\
|p_7\rangle &= e_1 \wedge e_7 \wedge e_2 \wedge e_8 + e_3 \wedge e_5 \wedge e_4 \wedge e_6 \ .
\end{aligned} \tag{6.92}$$

et

$$|y_1|^2 + |y_2|^2 + |y_3|^2 + |y_4|^2 + |y_5|^2 + |y_6|^2 + |y_7|^2 = 1 \ . \tag{6.93}$$

L'hyperpfaffian $\Delta_{4,8}$ définissant l'équation de la variété duale de $G(4,8)$ peut être défini de manière unique (à une constante multiplicative près). Son expression, lorsqu'elle est évaluée sur les états semi-simples, est établie dans [139], et nous avons $\Delta_{4,8}(|\psi_S\rangle) = h^2$ avec

$$\begin{aligned}
h = {} & (y_1 + y_2 + y_3 + y_6)(y_1 + y_2 + y_3 - y_6)(y_1 + y_2 - y_3 + y_6)(y_1 + y_2 - y_3 - y_6) \\
& (y_1 - y_2 + y_3 + y_6)(y_1 - y_2 + y_3 - y_6)(y_1 - y_2 - y_3 + y_6)(y_1 - y_2 - y_3 - y_6) \\
& (y_1 + y_3 + y_4 + y_5)(y_1 + y_3 + y_4 - y_5)(y_1 + y_3 - y_4 + y_5)(y_1 + y_3 - y_4 - y_5) \\
& (y_1 - y_3 + y_4 + y_5)(y_1 - y_3 + y_4 - y_5)(y_1 - y_3 - y_4 + y_5)(y_1 - y_3 - y_4 - y_5) \\
& (y_1 + y_2 + y_5 + y_7)(y_1 + y_2 + y_5 - y_7)(y_1 + y_2 - y_5 + y_7)(y_1 + y_2 - y_5 - y_7) \\
& (y_1 - y_2 + y_5 + y_7)(y_1 - y_2 + y_5 - y_7)(y_1 - y_2 - y_5 + y_7)(y_1 - y_2 - y_5 - y_7) \\
& (y_1 + y_4 + y_6 + y_7)(y_1 + y_4 + y_6 - y_7)(y_1 + y_4 - y_6 + y_7)(y_1 + y_4 - y_6 - y_7) \\
& (y_1 - y_4 + y_6 + y_7)(y_1 - y_4 + y_6 - y_7)(y_1 - y_4 - y_6 + y_7)(y_1 - y_4 - y_6 - y_7) \\
& (y_2 + y_3 + y_4 + y_7)(y_2 + y_3 + y_4 - y_7)(y_2 + y_3 - y_4 + y_7)(y_2 + y_3 - y_4 - y_7) \\
& (y_2 - y_3 + y_4 + y_7)(y_2 - y_3 + y_4 - y_7)(y_2 - y_3 - y_4 + y_7)(y_2 - y_3 - y_4 - y_7) \\
& (y_2 + y_4 + y_5 + y_6)(y_2 + y_4 + y_5 - y_6)(y_2 + y_4 - y_5 + y_6)(y_2 + y_4 - y_5 - y_6) \\
& (y_2 - y_4 + y_5 + y_6)(y_2 - y_4 + y_5 - y_6)(y_2 - y_4 - y_5 + y_6)(y_2 - y_4 - y_5 - y_6) \\
& (y_3 + y_5 + y_6 + y_7)(y_3 + y_5 + y_6 - y_7)(y_3 + y_5 - y_6 + y_7)(y_3 + y_5 - y_6 - y_7) \\
& (y_3 - y_5 + y_6 + y_7)(y_3 - y_5 + y_6 - y_7)(y_3 - y_5 - y_6 + y_7)(y_3 - y_5 - y_6 - y_7) \\
& \times y_1 y_2 y_3 y_4 y_5 y_6 y_7 \ .
\end{aligned} \tag{6.94}$$

Nous maximisons ensuite cette quantité (en valeur absolue) par recherche numérique et nous proposons l'état $\left|M_{4,8}^{\Delta}\right\rangle$ comme état maximisant l'hyperpfaffien, exprimé comme suit :

$$\left|M_{4,8}^{\Delta}\right\rangle = \frac{1}{\sqrt{2}}\big(\alpha_1|p_1\rangle + \alpha_2|p_2\rangle + \alpha_3|p_3\rangle + \alpha_4|p_4\rangle + \alpha_5|p_5\rangle + \alpha_6|p_6\rangle + \alpha_7|p_7\rangle\big) \ , \tag{6.95}$$

avec ,

$$\begin{aligned} \alpha_1 \approx -0.3564913724 - 0.1989369517i,\ \alpha_2 \approx 0.3986132399 - 0.2379732935i,\\ \alpha_3 \approx 0.1054323755 + 0.1219883503i,\ \alpha_4 \approx -0.1568134594 + 0.1355347505i,\\ \alpha_5 \approx -0.2931832323 + 0.3599485127i,\ \alpha_6 \approx 0.2669584458 + 0.3088755866i,\\ \alpha_7 \approx -0.1452208681 - 0.3815462436i \ . \end{aligned} \tag{6.96}$$

En ce qui concerne les invariants fondamentaux, dans ce cas seulement l'invariant I_2 de degré 2 est défini de manière unique, et son expression est donnée comme suit, lorsqu'il est évalué sur les états semi-simples :

$$I_2(|\psi_S\rangle) = y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 + y_6^2 + y_7^2 \ . \tag{6.97}$$

En maximisant la valeur absolue de cet invariant fondamental, nous obtenons un autre état candidat comme état maximalement intriqué :

$$\left|M_{4,8}^{I_2}\right\rangle = \frac{1}{\sqrt{3}}|p_1\rangle \ . \tag{6.98}$$

Enfin, en ce qui concerne la maximisation de la MGGI, après une recherche aléatoire, nous n'avons pas trouvé d'état fermionique présentant une MGGI supérieure à celle de l'état maximisant l'hyperpfaffien. Tous les résultats sont regroupés dans la Table 6.16.

États	$\lvert\Delta_{4,8}\rvert$	$\lvert I_2\rvert$	MGGI	Rang_{ASym}
$\lvert M_{4,8}\rangle$	$2.644439239 \times 10^{-24}$	0.000003556	0.821903148	≥ 6
$\left\lvert M_{4,8}^{I_2}\right\rangle$	0	0.5	0.5	2

TABLE 6.16 – Comparaison des mesures numériques (algébriques et géométriques) pour les états fermioniques maximalement intriqués, dans le cas $(k, n) = (4, 8)$.

6.4 États aléatoires et hyperdéterminants

Dans cette section, nous tentons de présenter la répartition des valeurs de l'hyperdéterminant obtenues à partir d'états générés aléatoirement. Nous procédons dans le même esprit que Alsina dans sa thèse [5], en générant un nombre conséquent d'états aléatoires, puis en les ordonnant dans un ordre croissant pour obtenir une représentation graphique.

Nous reprenons les cas précédemment étudiés dans ce chapitre, et évaluons les différentes valeurs des hyperdéterminants, discriminants et hyperpfaffiens sur des états aléatoirement générés. Nous présentons certaines courbes générées, puis discutons ces résultats en Section 6.5.2. Nous générons 2000 tenseurs aléatoires : 10000 sont des tenseurs réels, et 10000 sont des tenseurs à coefficients complexes.

6.4.1 Hyperdéterminant des 4-qubits

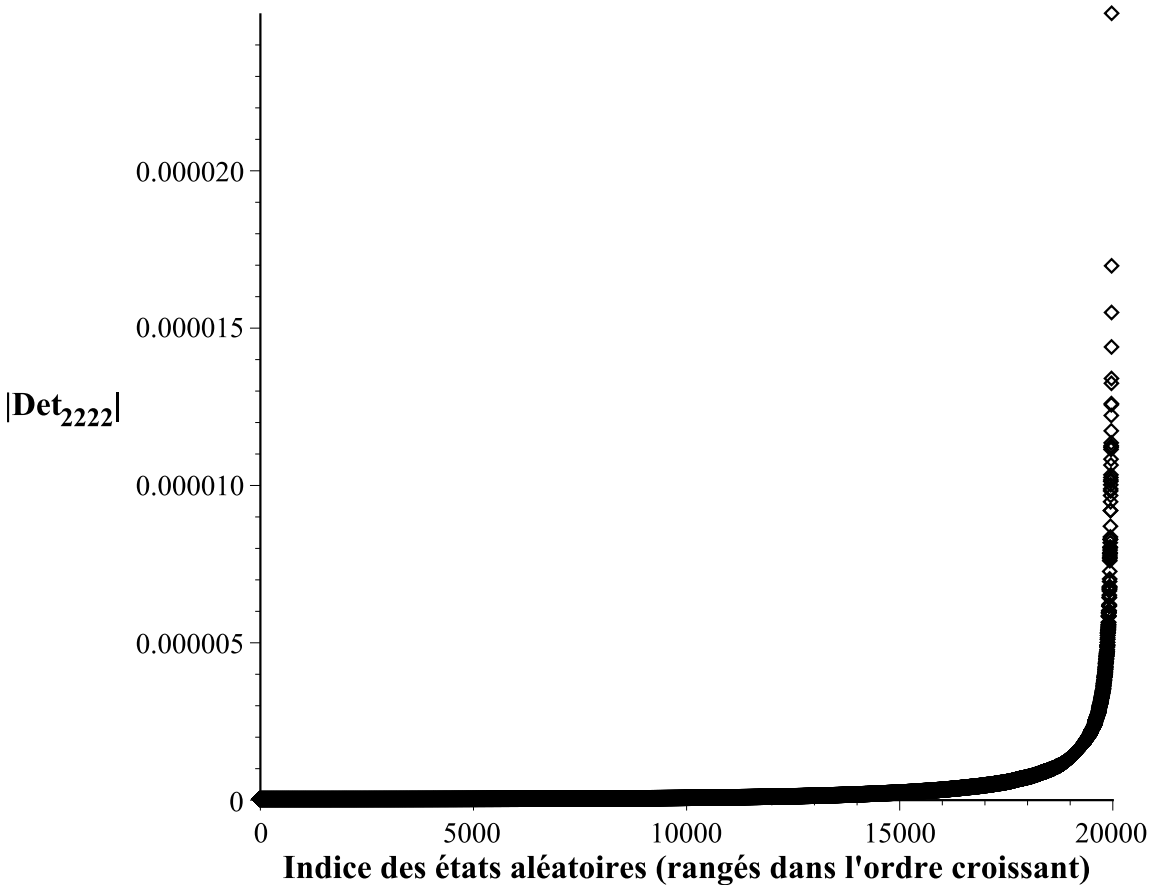


Figure 6.3 – Valeur de l'hyperdéterminant pour les 4-qubits, pour 20000 états aléatoires, rangés par ordre croissant.

6.4.2 Hyperdéterminant des 3-qutrits

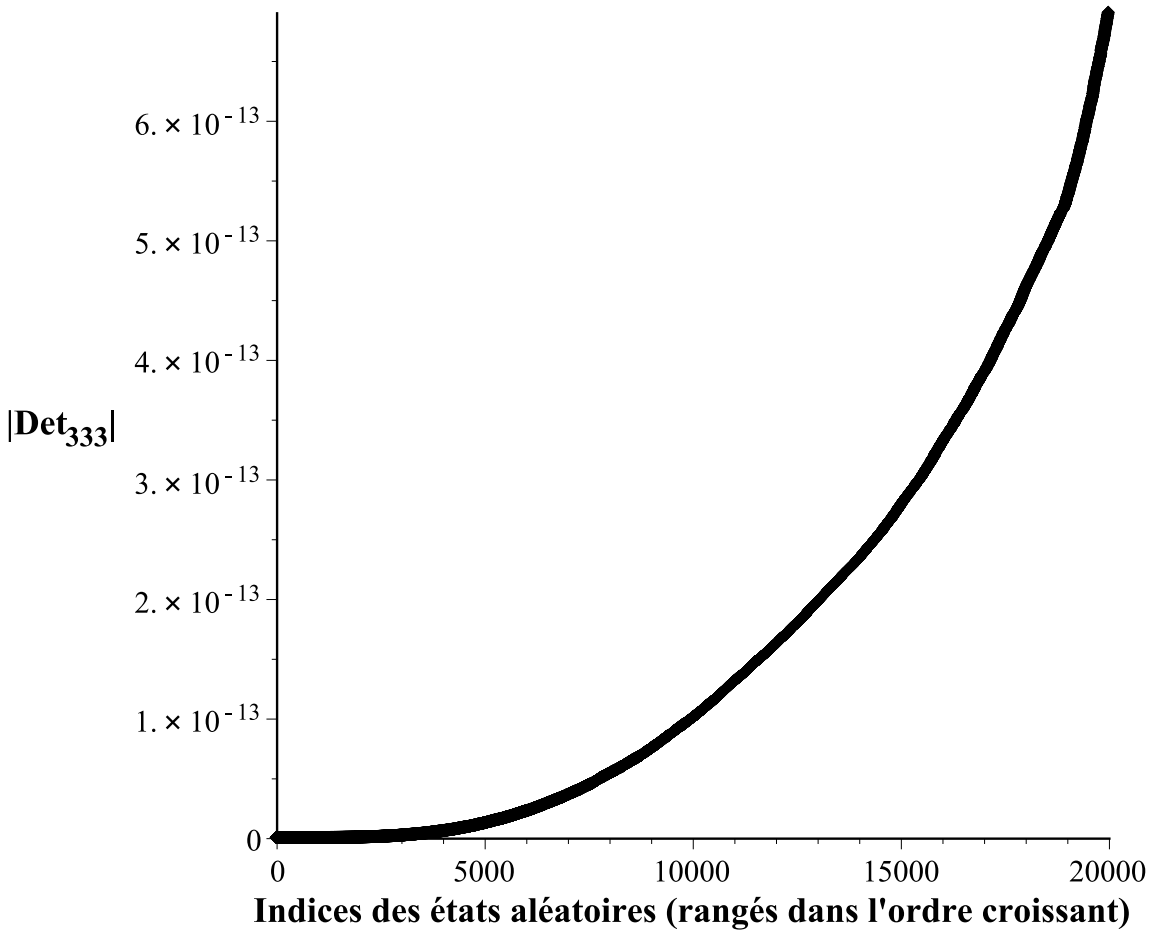


FIGURE 6.4 – Valeur de l'hyperdéterminant pour les 3-qutrits, pour 20000 états aléatoires, rangés par ordre croissant.

6.4.3 Discriminant des 6-qubits symétriques

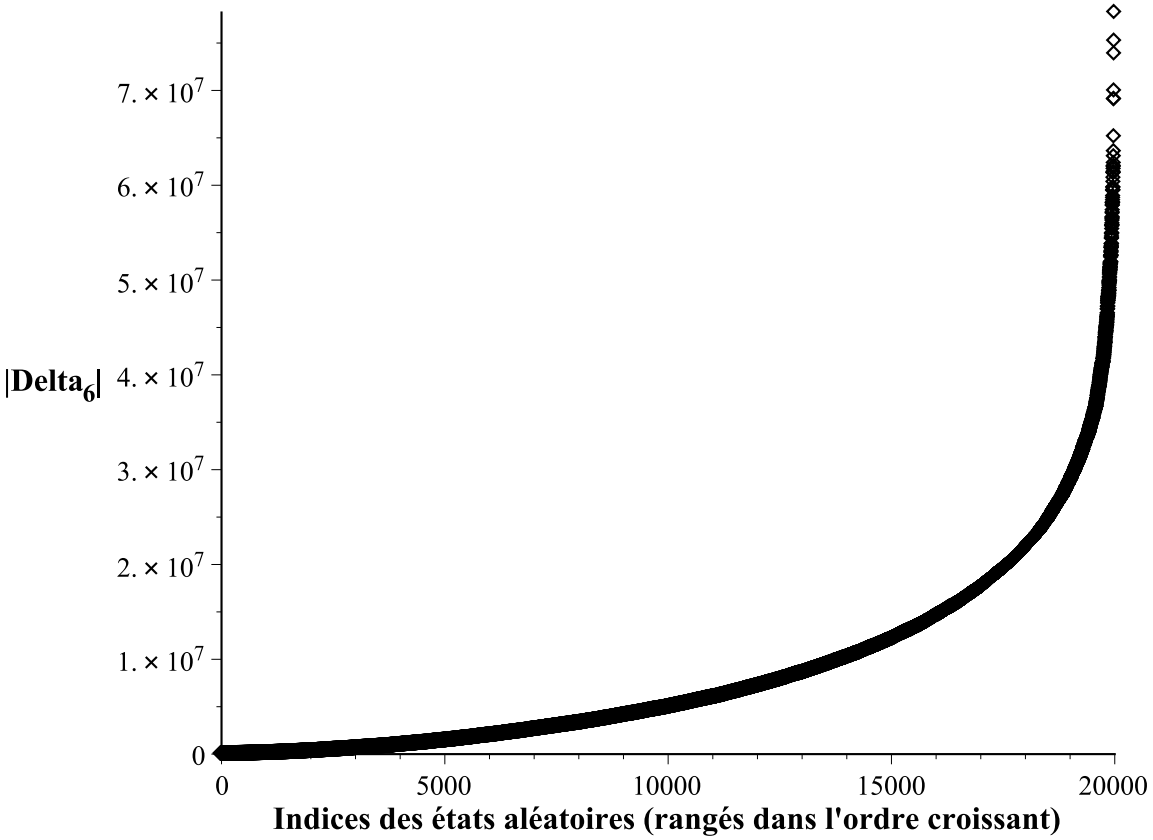


Figure 6.5 – Valeur du discriminant pour les 6-qubits symétriques, pour 20000 états aléatoires, rangés par ordre croissant.

6.4.4 Hyperpfaffien des états fermioniques (4,8)

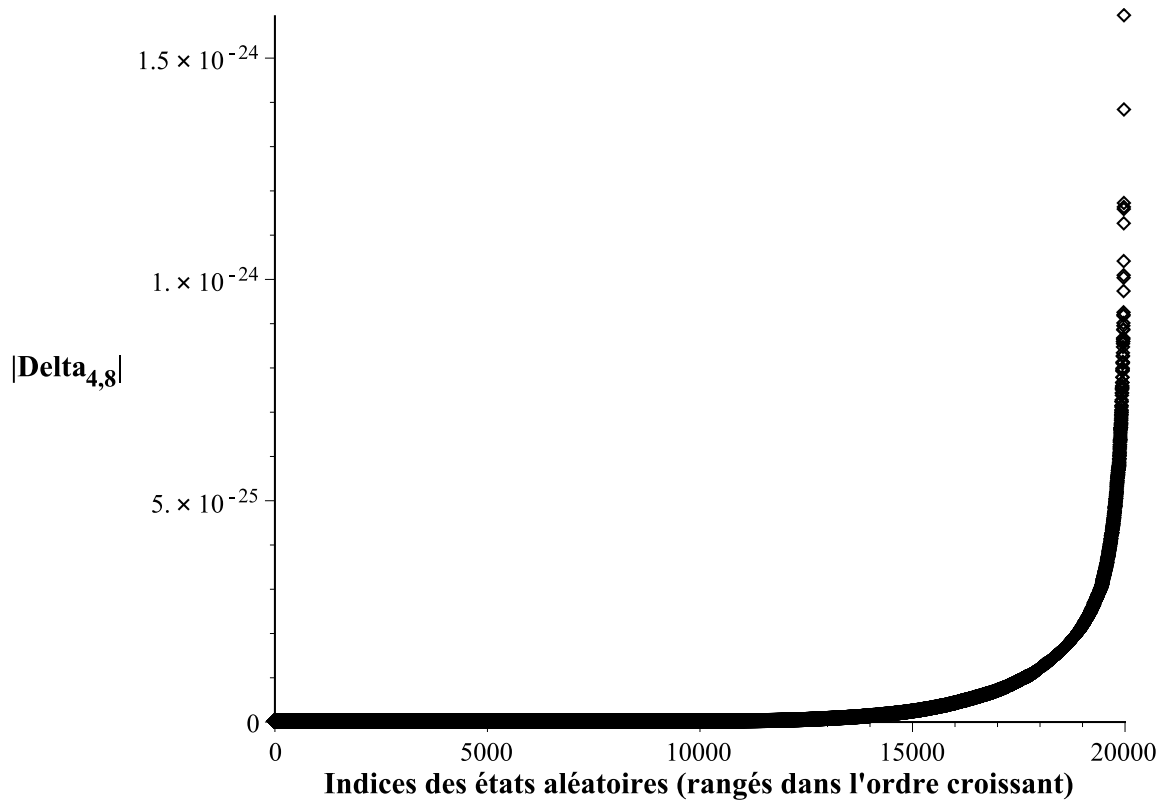


FIGURE 6.6 – Valeur de l'hyperpfaffien pour les états fermioniques $(k, n) = (4, 8)$, pour 20000 états aléatoires, rangés par ordre croissant.

6.5 Commentaires et remarques

6.5.1 États symétriques

Dans le cas où $n = 4, 6, 8, 12$ et 20, il a été remarqué dans [17] que les états symétriques possédant un solide platonicien comme représentation de Majorana sont liés à la recherche d'états absolument et maximalement intriqués. Au vu des résultats présentés, nous observons également une relation entre ces états et la maximisation ou annulation des invariants algébriques.

D'autre part, en cherchant à maximiser la valeur absolue de ces invariants, dans certains cas nous obtenons des états symétriques à la MGI supérieure aux autres états connus dans la littérature.

Dans d'autres cas, nous observons différents comportements et corrélations entre la valeur des invariants et la valeur de la MGI. Dans certains cas maximiser l'un revient à maximiser l'autre, mais dans d'autres cas c'est en maximisant un invariant et en minimisant un autre que l'on arrive à maximiser la valeur de la MGI. Ceci peut constituer une piste intéressante pour des études futures.

6.5.2 États aléatoires

Nous remarquons que globalement, la majorité des états générés aléatoirement présentent une valeur de l'hyperdéterminant assez faible. De plus, nous observons également que les états hautement intriqués sont assez rares (par exemple pour les 4-qubits). Aussi, les états connus comme étant maximalement intriqués ne sont parfois jamais atteint, ni approchés, lors de la génération des 20000 états.

Avoir une valeur de l'hyperdéterminant proche du maximum est un phénomène assez rare, ce qui peut expliquer la difficulté à déterminer une expression numérique ou exacte des états maximisant l'hyperdéterminant dans certains cas. De plus, on observe globalement la même allure de courbe, sauf dans certains cas (par exemple le cas des 3-qutrits).

6.6 Perspectives

Dans cette section nous proposons quelques idées et perspectives pour poursuivre le travail présenté dans ce chapitre.

Un premier travail possible serait de déterminer l'expression exacte des différents états maximisant les polynômes invariants et le discriminant pour les états symétriques, et d'observer pour ces états la répartition des points sur la sphère de Bloch à l'aide de la représentation de Majorana. Il serait également intéressant de pouvoir déterminer une expression exacte des états fermioniques maximisant l'hyperpfaffien et la mesure géométrique grassmannienne de l'intrication pour chaque cas étudié.

En second lieu, il pourrait être intéressant d'étudier plus en détail le lien entre la mesure géométrique de l'intrication (et la distance minimale aux états séparables) et le rang des tenseurs. Il pourrait être aussi intéressant de chercher à déterminer un majorant du rang en utilisant une approche analogue.

D'autre part, il est également possible d'approfondir le travail autour de la mesure géométrique grassmannienne de l'intrication, et de tenter d'établir des résultats généraux sur la forme des états séparables minimisant cette distance entre l'état fermionique considéré et la variété de Grassmann. Il serait également intéressant de poursuivre le travail de maximisation de la MGGI afin de confirmer ou non le caractère maximal de la valeur de la MGGI pour les états que nous avons proposé.

Aussi, un travail sur l'analyse plus précise de la distribution des états maximalement intriqués sur l'ensemble des états générés aléatoirement pourrait être mené. Les différentes courbes générées pourraient être étudiées plus en détail, et cette étude pourrait être étendue aux autres polynômes invariants et aux autres mesures de l'intrication (ou de non-localité).

Enfin, il m'apparaît intéressant d'étudier les corrélations possibles entre polynômes invariants, et entre les différentes mesures de l'intrication. Par exemple, dans le cas des 4-qubits, l'hyperdéterminant peut être défini à partir des deux invariants S et T [138],

et on pourrait étudier l'influence de la maximisation ou l'annulation de ces invariants sur la valeur de l'hyperdéterminant, dans le même esprit que ce qu'a initié Alsina [5]. Ceci peut également être fait pour les états symétriques, où la maximisation de certains invariants ou mesures géométriques de l'intrication semble liée.

Chapitre 7

Intrication et Réseaux de Neurones Artificiels

"A single neuron in the brain is an incredibly complex machine that even today we don't understand. A single neuron in a neural network is an incredibly simple mathematical function that captures a minuscule fraction of the complexity of a biological neuron", Andrew Ng.

Avec le développement récent des technologies d'Intelligence Artificielle (IA) et du *Machine Learning* (apprentissage machine), et avec l'abondance des données informatiques générées ou récoltées, de nombreux problèmes difficiles et intéressants pour la communauté scientifique ou les industriels ont pu être résolus, et ces technologies continuent de révolutionner le monde industriel ainsi que notre approche de la science.

Le Machine Learning est la discipline visant à enseigner aux machines une tâche spécifique, sans lui donner d'instructions explicites. L'apprentissage machine se divise en 3 branches principales : l'apprentissage supervisé, l'apprentissage non-supervisé et l'apprentissage par renforcement. La première vise à enseigner à travers la connaissance et l'abondance d'exemples, et implique de disposer de données pour lesquelles la réponse valide ou attendue est connue. La seconde repose sur les capacités de la machine à réorganiser par elle même les données, afin de produire une proposition de regroupement ou de représentation des données. La troisième approche vise à enseigner à la machine par un processus issu du *behaviorisme* : par une succession d'essais et d'échecs, la machine tente de maximiser un gain directement lié à l'accomplissement d'une tâche [150, 204].

Ces différentes approches permettent en effet d'étudier différents types de problèmes, en allant de la classification à la régression, en passant par la réduction de dimensions ou par le développement d'intelligences artificielles pour le jeu vidéo. Nous tentons alors de mettre à profit ces technologies émergentes afin d'étudier le problème de classification de l'intrication. Nous présentons dans ce chapitre un travail conjointement développé avec Dr. Luke Oeding, ayant mené à la production d'un article [149].

Dans ce chapitre, nous nous intéressons de ce fait à l'intrication quantique d'un point de vue qualitatif, en entraînant des réseaux de neurones artificiels, dans une approche purement supervisée, afin de classifier l'intrication quantique caractérisée par l'appartenance à certaines variétés algébriques. Nous proposons tout d'abord une présentation des travaux issus de la littérature liant des techniques de Machine Learning à l'intrication quantique. Nous introduisons ensuite le modèle des réseaux de neurones artificiels, et étudions par la suite comment concevoir l'architecture de ces derniers pour apprendre à reconnaître des variétés algébriques. Enfin, nous étudions un certain nombre de variétés algébriques liées à l'intrication, en entraînant les réseaux de neurones à reconnaître des points sur ces variétés, puis en utilisant ces réseaux entraînés pour effectuer des prédictions quant à la classe d'intrication d'états spécifiques en entrée.

7.1 Introduction

Les récents efforts déployés pour faire interagir les communautés le l'Information Quantique, du Calcul Quantique et du Machine Learning se sont principalement focalisés sur l'intégration d'algorithmes quantiques et d'informatique quantique dans les architectures d'apprentissage machine classiques [276, 174, 224, 236, 237, 277, 37, 241, 157, 286]. Une approche opposée peut aussi être adoptée, et c'est celle que nous nous proposons de présenter dans ce chapitre. En effet, nous exploitons des techniques de Machine Learning, plus précisément une approche d'apprentissage supervisée par réseaux de neurones artificiels, afin de développer des classifieurs permettant de distinguer plusieurs classes d'intrication quantique.

Les techniques de Machine Learning ont été utilisées pour étudier divers problèmes de physique ou d'information quantique, comme par exemple la tomographie d'états quantiques [220], la correction quantique de codes [197] et la reconstruction de fonctions d'ondes [25]. Dans notre cas, nous nous intéressons au phénomène d'intrication quantique. Tout en étant inspiré par l'approche liée à l'apprentissage de variétés algébriques développée par Breiding *et al.* [47], notre méthode diffère dans le sens où nous ne cherchons pas à trouver explicitement les équations intrinsèques définissant les modèles algébriques liés aux différents types d'intrication, mais plutôt de construire un classifieur nous permettant de directement déterminer la classe d'intrication.

Être en mesure de faire la différence entre différentes classes d'intrication trouve un intérêt particulier dans le cadre du problème de classification de l'intrication, notamment utile pour l'étude du calcul quantique et l'étude du rôle de l'intrication dans l'amélioration et l'efficacité des algorithmes quantiques (voir Partie II), des protocoles de communication quantiques, de protocoles de cryptographie quantique ou de jeux quantiques [148]. Notre méthode présentée dans ce chapitre pourrait se généraliser à l'étude des cas où toutes les classes d'intrication ne sont pas totalement connues, et à des cas où le nombre de classes n'est pas forcément fini (voir par exemple [165, Ch.10] ou [268]).

Ce n'est pas forcément le cas des approches adoptées jusqu'à présent dans la littérature. Nous proposons de présenter les principales études sur cette question dans ce qui suit.

7.1.1 État de l'art

L'apprentissage machine a été utilisé dans l'étude de la détection de l'intrication, la mesure de l'intrication ainsi que la classification de l'intrication. Une approche souvent abordée consiste à considérer le formalisme des matrices de densité, pour lequel décider de la séparabilité d'un état est un problème NP difficile.

Les réseaux de neurones ont pu être utilisés dans la littérature pour fournir une estimation de certaines mesures de l'intrication, notamment pour la mesure de négativité logarithmique, l'entropie de Rényi ou encore la concurrence pour les systèmes à 2-qubits (états purs et mixtes) ou pour les *many-body systems* [116, 34, 114]. Ces mêmes réseaux de neurones ont aussi servi à encoder des inégalités de type CHSH de manière simultanée dans un même réseau neuronal afin de pouvoir détecter des états intriqués [184]. Cet algorithme d'apprentissage supervisé a également été utilisé pour reconnaître les classes d'intrication pour les systèmes à 3-qubits [26], mais également à détecter certaines familles d'intrication dans le cas bipartite pour des qubits ou qutrits [283].

D'autre part, une approximation par enveloppe convexe combinée à l'algorithme d'arbres de décisions et l'approche *standard ensemble learning (bagging)* a été utilisée par Lu [176] afin de classifier les états séparables et intriqués. Dans un esprit similaire, l'algorithme de la forêt d'arbres décisionnels a été sollicité dans [269] pour détecter l'intrication d'états quantiques (allant jusqu'à 5-qubits), en comparant les résultats à une approche par tomographie. L'algorithme d'Analyse en Composantes Principales (ACP, ou PCA en anglais) a été exploité en 2018 pour déterminer la dimension et les équations intrinsèques de certaines variétés algébriques [47]. Enfin, dans le cas des systèmes à 2-qubits, les réseaux de neurones, les machines à vecteurs de support et les arbres de décisions ont été utilisés pour détecter des corrélations non-classiques comme l'intrication quantique, la non-localité ou le *quantum steering* [288].

De ce fait, les techniques issues du Machine Learning peuvent apparaître comme des outils prometteurs pour la détection de l'intrication, ou au moins l'être dans certains cas limités. Cependant, toutes les études précédentes se sont limitées pour la plupart au cas des 2-qubits ou au cas bipartite, principalement car il est possible de générer correctement (pour une approche supervisée) des états séparables, mixtes et intriqués, sous le formalisme des matrices de densité, en faisant appel au critère PPT ou à la décomposition de Schmidt. Il semble néanmoins difficile de généraliser ces approches supervisées à des dimensions plus grandes ou à des systèmes à un plus grand nombre de particules.

C'est pourquoi nous choisissons de nous intéresser au problème de détection et de classification de l'intrication à travers l'apprentissage de variétés algébriques caractérisant différentes classes d'intrication pour les états purs (voir Section 2.1). Nous espérons que notre approche pourra être généralisée à de plus hautes dimensions, fournissant un outils original pour distinguer des classes d'intrication non-équivalentes, pour des systèmes quantiques dont on ne connaît pas une classification complète ou pour lesquels nous ne connaissons pas d'algorithmes exacts (pour un exemple d'algorithme exact pour les 4-qubits, voir Annexe A.4) permettant de déterminer le type d'intrication.

Comme remarqué dans [47], il existe une multitude d'hypersurfaces de haut degré (comme celle des états dégénérés de $\mathcal{H}_n$) qu'il est simple d'échantillonner. En revanche, il y a peu d'espoir de pouvoir apprendre leurs équations à partir de ces échantillons, et c'est pourquoi les méthodes connues ne peuvent s'appliquer. Nous montrerons cependant qu'il est possible, dans certains cas, d'entraîner des réseaux de neurones artificiels afin de déterminer l'appartenance à ces hypersurfaces de haut degré (ce que les équations, inaccessibles, permettraient aussi de faire).

7.2 Réseaux de Neurones Artificiels et notions de base

Inspiré des réseaux de neurones biologiques, le modèle des Réseaux de Neurones Artificiels (RNA) est un modèle de calcul dont le but est de reproduire la structure et les fonctionnalités de base du cerveau humain [187]. Ils sont utilisés afin d'apprendre à réaliser des tâches spécifiques (comme la classification ou la régression), sans instructions ou règles explicitement formulées. Un réseau de neurones artificiel est composé d'un certain nombre de neurones artificiels, regroupés à travers une architecture spécifique, capable de réaliser des tâches précises à l'aide d'un algorithme d'apprentissage [125].

7.2.1 Le neurone artificiel

En 1943, McCulloch et Pitts proposèrent le premier modèle de neurone artificiel [187]. Un neurone artificiel (voir Figure 7.1) est défini par des entrées (provenant éventuellement d'autres neurones), de poids (poids synaptiques associés à chaque entrée), d'une somme pondérée (calculée à partir des deux éléments précédents), d'un seuil (aussi appelé biais), d'une fonction d'activation et d'une sortie [172, 21, 124, 125, 10].

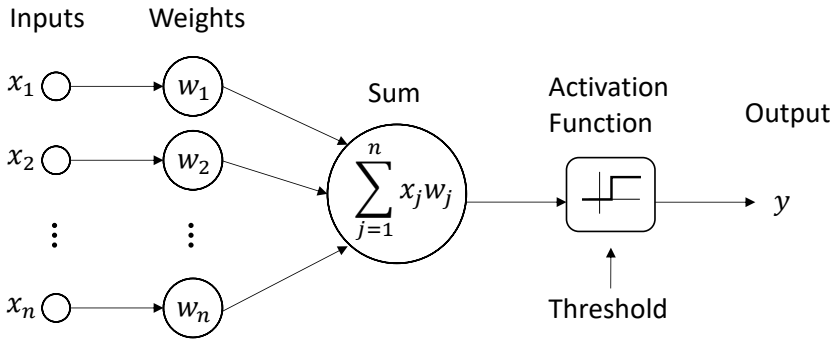


Figure 7.1 – Illustration d'un neurone artificiel.

La sortie d'un neurone est déterminée comme suit : si la *somme pondérée* des entrées est strictement supérieure au seuil, alors le neurone sera dit actif, et la sortie $y = g(\mathcal{U})$ du neurone artificiel sera alors égale à la fonction d'activation g appliquée à la *somme pondérée*, avec le seuil θ souvent ajouté à cette somme, et donc considéré comme un poids associée à une entrée égale à 1 [79]. En notant par $x_1, \ldots, x_n$ les entrées du neurone, et par w_i le poids associé à la i-ème entrée, alors la somme pondérée, souvent notée $\mathcal{U}$, est définit comme :

$$\mathcal{U} = w_1 x_1 + w_2 x_2 + \cdots + w_n x_n + \theta \ . \tag{7.1}$$

Pour cette définition, c'est lorsque cette quantité $\mathcal{U}$ est supérieure à 0 que le neurone sera actif. En ce qui concerne le choix de la fonction d'activation, il est généralement demandé qu'elle soit de nature *non-linéaires* afin de permettre aux réseaux de neurones de résoudre des problèmes non-triviaux en utilisant le moins de neurones possibles [79]. Il pourrait être possible de choisir des fonctions d'activation de type marche ou linéaire, mais cela amenerait certaines difficultés durant la phase d'apprentissage ou dans un problème de classification multi-classes. Il existe également d'autres propriétés préférées dans un contexte d'apprentissage pour ces fonctions d'activations, et nous pouvons citer parmi elles : *continue dérivable*, *monotone*, *lisse*, et *approximant l'identité proche de l'origine* [124, 125] (voir Figure 7.2 pour des exemples).

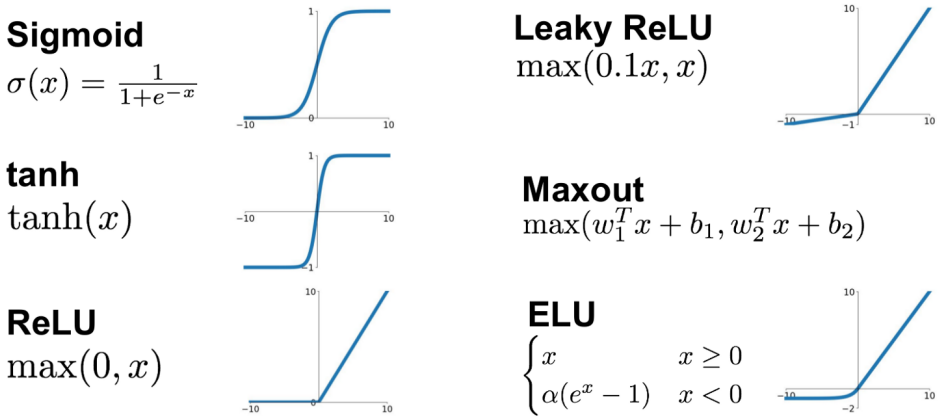


FIGURE 7.2 – Exemple de fonctions d'activation usuelles (Source).

Exemple 11 (Le `OU` logique)**.** Nous nous proposons d'étudier en guise de premier exemple le problème consistant à reproduire la fonction binaire de base qu'est le `OU` logique, à l'aide d'un neurone artificiel. Soient x_1 et x_2 les deux entrées du neurone, pouvant prendre des valeurs dans $\mathcal{B} = \{0, 1\}$. Pour rappel, la fonction `OU` renvoie 1 si une des entrées est à 1, et renvoie 0 sinon.

Pour ce faire, nous choisissons comme fonction d'activation g la fonction marche. On peut alors définir la somme pondérée et la sortie du neurone comme suit :

$$\mathcal{U} = w_1 x_1 + w_2 x_2 + \theta \ , \qquad g(\mathcal{U}) = \begin{cases} 1 & \text{if } \mathcal{U} > 0, \\ 0 & \text{sinon} \end{cases} \ .$$

Afin de pouvoir reproduire la fonction `OU` à l'aide d'un unique neurone, nous voulons que la sortie soit égale à 0 lorsque l'entrée est égale à $(x_1, x_2) = (0, 0)$, et 1 sinon. De ce fait, la sortie doit être égale à 0 si et seulement si la somme pondérée est inférieure ou égale à 0, et égale à 1 si et seulement la somme pondérée est strictement positive. Les conditions suivantes doivent alors être satisfaites :

$$\begin{array}{rcl@{\qquad}rcl} 0 \cdot w_1 + 0 \cdot w_2 + \theta & \leq & 0, & 0 \cdot w_1 + 1 \cdot w_2 + \theta & > & 0, \\ 1 \cdot w_1 + 0 \cdot w_2 + \theta & > & 0, & 1 \cdot w_1 + 1 \cdot w_2 + \theta & > & 0. \end{array}$$

Ceci revient à établir les inégalités suivantes :

$$\theta \leq 0,\ w_1 + \theta > 0,\ w_2 + \theta > 0\ .$$

En choisissant les paramètres définissant le neurone comme étant égaux à $\theta = -\frac{1}{2}$, $w_1 = 1$, $w_2 = 1$, alors le neurone reproduit la fonction booléenne voulue, pour toute entrée dans $\{0,1\}^2$. Une représentation de ce problème sous la forme d'un problème de classification binaire est fournie en Figure 7.3.

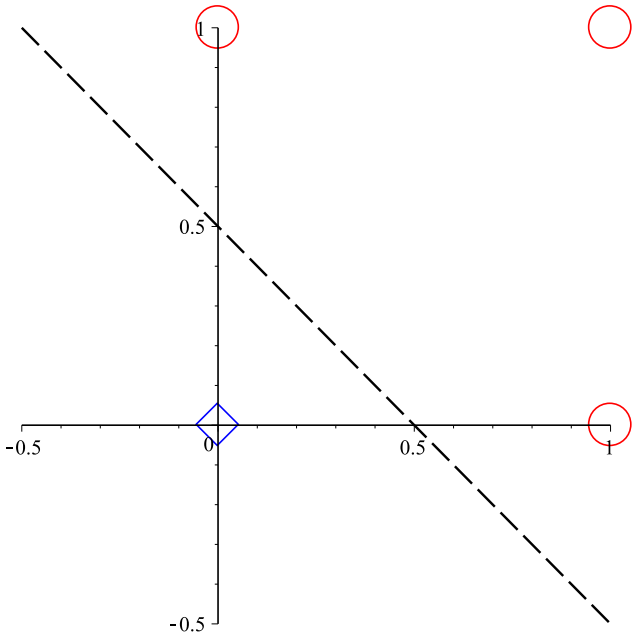


Figure 7.3 – Représentation du problème de classification associé à la fonction `OU`. Le losange bleu correspond à la première classe (fonction égale à 0), et les cercles rouges à la seconde classe. La ligne interrompue noire représente l'hyperplan, séparant les données d'entrées en deux classes, modélisée par le neurone artificiel défini par $\theta = -\frac{1}{2}$, $w_1 = 1$, $w_2 = 1$.

Géométriquement, si l'on peut trouver un hyperplan (de codimension 1) séparant les données en deux classes distinctes, alors le problème de classification binaire peut être résolu à l'aide d'un unique neurone artificiel [163, 270, 124, 73]. Ici, une équation d'hyperplan possible est donnée par $x_1 + x_2 - \frac{1}{2} = 0$, correspondant à l'équation $\mathcal{U} = 0$, définie par les précédentes valeurs choisies du seuil et des poids. ♢

En revanche, si on cherche à modéliser la fonction `XOR` (OU exclusif) à l'aide d'un seul neurone, on peut montrer que ceci est impossible, en suivant un raisonnement similaire à celui utilisé en Exemple 11 [40, 124, 41]. Il sera alors nécessaire de disposer de structures plus complexes, et de pouvoir associer différents neurones pour réaliser cette tâche. Ceci nous amène donc à considérer un modèle de réseau de neurones, que nous présentons en sous-section suivante.

7.2.2 *Multi-Layer Perceptron* et *Feed-Forward Networks*

Un des modèles de réseaux de neurones bien connu dans la littérature est celui de *Multi-Layer Perceptron* (MLP) [21, 125]. Comme son nom l'indique, il est composé de plusieurs couches, dont une d'entrée, une ou plusieurs couches cachées, et une couche de sortie. Chaque couche est composée d'un certain nombre de neurones, non connectés entre eux. Le concept de *Feed-Forward Network* impose une certaine architecture au réseau, et dans le cas d'une configuration dense, chaque neurone d'une couche donnée est connecté à chaque neurone de la couche précédente et de la couche suivante. Ainsi, le signal ne sera propagé que dans une seule direction : de la couche d'entrée vers la couche de sortie (par convention de gauche à droite) [172, 21, 158].

Apprentissage et erreur associée

Un réseau de neurones artificiel a la possibilité d'apprendre une tâche spécifique, ou une fonction spécifique, à partir d'exemple à travers un processus d'optimisation des poids du réseau. En effet, dans un contexte d'apprentissage supervisé, l'objectif du réseau de neurones sera d'apprendre comment déterminer la sortie correcte associée à un vecteur en entrée, à partir de plusieurs échantillons pour lesquels on connaît la valeur de sortie attendue.

Ces exemples forment les *données d'entraînement*, renfermant les paires d'entrées-sorties correctes, utilisées comme enseignement pour le réseau neuronal. La construction de tels neurones se fait à travers la phase d'entraînement, phase durant laquelle tous les poids et seuils seront optimisés afin de réduire au maximum l'erreur définie comme la distance entre la sortie donnée par le neurone et la sortie correcte fournie par les données d'entraînement. Dans un modèle feed-forward, l'algorithme de *back-propagation* de l'erreur est utilisé pour mettre à jour au cours de l'apprentissage les poids et seuils afin de réduire la fonction d'erreur, aussi connue comme fonction coût (ou *loss function* en anglais) [228, 168].

Après l'étape d'apprentissage, le réseau de neurone doit être capable de répondre correctement pour toutes les entrées provenant de l'ensemble d'apprentissage, mais doit également être capable de prédire correctement la sortie pour de nouvelles données en entrée. Afin de tester le réseau, on donne en entrée du réseau des *données de test* afin d'évaluer la capacité du réseau à généraliser l'apprentissage précédent afin d'effectuer des prédictions. De plus, il est possible de mettre en place des *données de validation* qui seront utilisées tout au long de la phase d'apprentissage, pour détecter ou éviter le sur-apprentissage. On peut alors évaluer un réseau de neurones en observant la proportion de réponses exactes pour les différents ensembles de données (entraînement, validation et test).

Fonctions d'activations

D'autre part, le choix de la fonction d'activation est primordial lors de la conception d'un réseau de neurone pour une tâche spécifique. De manière assez fréquente, les neurones présents dans une même couche auront la même fonction d'activation, alors que deux couches adjacentes peuvent avoir des fonctions d'activations différentes.

Pour la couche d'entrée, ainsi que les couches cachées, la fonction d'activation ReLU est communément utilisée. Les avantages de cette fonction ReLU est qu'elle est efficace en termes de calcul (convergence rapide du réseau), elle est non-linéaire, et admet une dérivée (et permet donc l'application de certains algorithmes nécessitant la dérivée pour la back-propagation). Cependant, lorsque les entrées approchent 0 ou deviennent négatives, le processus d'apprentissage devient plus difficile (connu sous le nom de *dying ReLU problem*). Pour remédier à cela, on pourra utiliser la fonction d'activation Leaky-ReLU, introduisant une légère pente dans la partie négative, facilitant la propagation arrière de l'erreur [124, 10].

La fonction d'activation pour les neurones de la couche de sortie dépendront du problème que l'on cherche à résoudre. Les fonctions d'activation Sigmoïde et SoftMax (voir Équation 7.2) sont les plus utilisées. En effet, si c'est un problème de classification binaire, alors la fonction Sigmoïde avec un seul neurone en couche de sortie sera plus efficace. Si on étudie un problème de classification multi-classes, alors il faudra considérer plusieurs neurones dans la couche de sortie (avec une représentation catégorique des données). Dès lors, si une entrée peut appartenir à plusieurs classes à la fois, alors il faudra utiliser des fonctions de type Sigmoïde. Dans le cas contraire, si chaque entrée ne peut appartenir qu'à une seule classe à la fois, alors une fonction d'activation de type SoftMax sera un bon choix.

$$\begin{aligned} \text{SoftMax}(\mathbf{z}) &= (\sigma(\mathbf{z})_1, \sigma(\mathbf{z})_2, \dots, \sigma(\mathbf{z})_K) \\ \text{avec } \mathbf{z} = (z_1, z_2, \dots, z_K) \text{ et } \sigma(\mathbf{z})_j &= \frac{\mathrm{e}^{z_j}}{\sum_{k=1}^{K} \mathrm{e}^{z_k}}, \forall j \in [\![1, K]\!] \ . \end{aligned} \tag{7.2}$$

Les fonctions d'erreur doivent également faire l'objet d'une étude et d'un choix dépendant du problème à résoudre. Les différents choix de fonctions d'activation pour la couche de sortie et de fonction coût sont regroupés en Table 7.1.

Problème	Type sortie	Fonction d'activation sortie	Fonction coût
Régression	Valeur numérique	Linéaire	Mean Squared Error
Classification	Nombre binaire	Sigmoïde	Binary Cross Entropy
Classification	Label unique Classes multiples	SoftMax	Categorical Cross Entropy
Classification	Labels multiples Classes multiples	Sigmoïde	Binary Cross Entropy

Table 7.1 – Résumé des fonctions d'activation et de coût pour la couche de sortie en fonction du problème considéré (Source).

Implémentation

Dans le cadre de notre travail, nous avons implémenté les réseaux de neurones en utilisant la bibliothèque Keras en langage Python [70]. Elle fournit une implémentation

flexible des réseaux de neurones dits *feed-forward* et permet le choix et la personnalisation des paramètres du réseau (architecture, fonctions d'activation, fonction d'erreur, solveur, etc.). Nous avons choisi d'implémenter le solveur *Nadam* fournit par Keras afin de minimiser la fonction coût durant la phase d'apprentissage. Pour une classification binaire, nous avons choisi le fonction de coût *binary cross-entropy*, tandis que la fonction *categorical cross-entropy* est retenue pour une classification multi-classes [253, 86]. Nous proposons une exemple d'implémentation en Annexe A.12.

Profondeur versus Largeur

Une fois que les fonctions d'activation et de coût sont fixées, les paramètres restants à choisir sont le nombre et la taille des couches. Le *Théorème d'Approximation Universel*, et les études associées [79, 140, 40, 124, 78, 177, 123], tendent à prouver que tout réseau de neurones artificiel peut approximer n'importe quelle fonction (sous certaines conditions). Un des énoncés connu du théorème est proposé par [78] : "un réseau de neurone de type feed-forward avec une couche d'entrée et une couche cachée munie d'un nombre fini de neurones peut approximer n'importe quelle fonction continue sur des ensembles compacts de $\mathbb{R}^n$". En 1989, le théorème à été prouvé en utilisant des fonctions d'activation de type Sigmoïde [79]. Kurt Hornik démontra quelques années plus tard que le théorème ne dépend pas de la fonction d'activation, mais plutôt de l'architecture multi-couche et feed-forward du réseau de neurones [140].

Ces résultats concernent le cas où la profondeur du réseau (nombre de couches) est limité. Dans un autre esprit, plusieurs travaux récents proposent un théorème analogue mais en limitant cette fois-ci la largeur des réseaux (nombre de neurones dans une couche), en utilisant des fonctions d'activation ReLU [177, 123]. Le problème consistant à fournir la meilleure architecture de réseau, en termes d'efficacité de calcul et de précision, pour un problème donné, est toujours ouvert et le choix de la profondeur et largeur du réseau est bien souvent réalisé à travers des essais pratiques. Concevoir un réseau de neurones amène souvent à devoir considérer un dilemme entre performance/fiabilité et coût de calcul. Certaines architectures, comme celle consistant à faire décroître le nombre de neurones à mesure que l'on avance en profondeur, semble présenter une certaine efficacité en pratique. Cependant, il n'y a pas de preuve théorique de la supériorité de ce type de réseau, et certains travaux tendent à montrer qu'un réseau avec le même nombre de neurones dans chaque couche pourrait présenter des prédictions tout aussi fiables.

Dans ce travail, nous avons voulu concevoir une architecture appropriée à notre problème, en choisissant de manière réfléchie la profondeur, la largeur et les fonctions d'activation du réseau. Dans la prochaine section, nous présentons un modèle de réseau de neurones artificiels pouvant être utilisé pour apprendre à reconnaître des variétés algébriques en lien direct avec le problème de classification de l'intrication.

Pour une introduction plus compète aux Réseaux de Neurones Artificiels ainsi qu'aux concepts et techniques d'apprentissage associés, le lecteur pourra s'orienter vers les références suivantes [172, 21, 158, 275, 261, 270, 124, 125, 10].

7.3 Apprentissage de variétés algébriques

Une variété algébrique est un objet géométrique défini comme le lieu des zéros d'un ensemble de polynômes (voir Section 2.1). Afin de pouvoir enseigner à une machine comment reconnaître des points appartenant à une variété algébrique, il est nécessaire d'encoder les équations polynomiales la définissant (ou une approximation de celle-ci) à l'intérieur du modèle. Nous voulons procéder à cet encodage de la manière la plus efficace possible (en utilisant le moins de paramètres possibles), afin d'éviter tout sur-apprentissage.

7.3.1 Espace linéaires

Exemple 12 (Apprendre des espaces linéaires affines)**.** Soit (L) une droite de $\mathbb{R}^2$, définie par l'équation $ax+by+c=0$, avec $a,b,c\in\mathbb{R}$. Supposons que nous voulons déterminer l'appartenance de poins à la droite (L). C'est un problème de classification binaire, pouvant être modélisé par un unique neurone artificiel, possédant trois entrées, dont x et y (et une entrée forcée à 1). Notons par w_1 (respectivement w_2) le poids associé à la première entrée x (respectivement y), et θ le seuil du neurone (qui est ici considéré comme un poids associé à l'entrée valant 1). L'expression de la somme pondérée $\mathcal{U}$ est alors :

$$\mathcal{U}=w_1x+w_2y+\theta\ .$$

Nous faisons remarquer ici que si on pose $w_1=a$, $w_2=b$ and $\theta=c$, nous retrouvons l'équation de la droite (L). Ceci implique que la somme pondérée du neurone sera égale à 0 si, et seulement si, les entrées (x,y) correspondent à un point sur la droite (L).

Cette observation peut se généraliser à n'importe quelle dimension supérieure. En effet, tout sous-espace linéaire de codimension 1 vivant dans un espace de dimension n, c'est-à-dire défini par une unique équation linéaire à n variables, peut être *modélisée* à l'aide d'un unique neurone artificiel avec n entrées correspondants aux n variables, comme cela a déjà été discuté dans [91, 172, 109, 158, 163, 40, 125, 10, 88, 41]. Par *modéliser* nous entendons le fait que la sortie du neurone est toujours égale à la même valeur (ici 0) lorsque les entrées représentent un point appartenant à ce sous-espace, et ceci en choisissant une fonction d'activation égale à l'identité. La proposition suivante vient donc naturellement :

Proposition 7.3.1. *Soit L un espace linéaire affine dans $\mathbb{R}^n$ défini par $a_1x_1+a_2x_2+\cdots+a_nx_n+a_{n+1}=0$, avec les variables réelles $(x_1,x_2,\ldots,x_n)$ et les coefficients réels $(a_1,a_2,\ldots,a_{n+1})$. Alors L peut être modélisé par un unique neurone artificiel, et ses poids devront satisfaire : $w_1=\lambda a_1, w_2=\lambda a_2,\ldots,w_n=\lambda a_n$ et $\theta=\lambda a_{n+1}$, avec $\lambda\in\mathbb{R}^*$, comme représenté en Figure 7.4.*

♢

Nous généralisons à présent le précédent exemple, en considérant un autre exemple en codimension supérieure.

Exemple 13. Soit (L_2) une droite dans $\mathbb{R}^3$. Une droite dans un espace à 3 dimensions est une variété algébrique de codimension 2, définie par un système à 2 équations linéaires. L'annulation de ces deux équations se définit comme l'intersection de deux

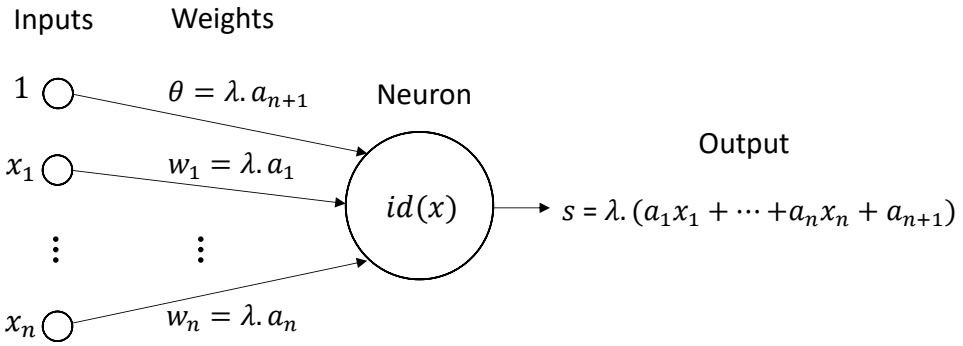


FIGURE 7.4 – Représentation d'un réseau modélisant un sous-espace linéaire de codimension 1 dans $\mathbb{R}^n$.

plans de $\mathbb{R}^3$, qui est en fait la droite (L_2). Nous pouvons alors combiner dans la même couche deux neurones artificiels modélisant les deux équations linéaires définissant la droite (voir Figure 7.5). La sortie du premier neurone doit alors être égale à 0 lorsque le point entrée du réseau appartient au premier plan, et de même pour le second neurone et le second plan.

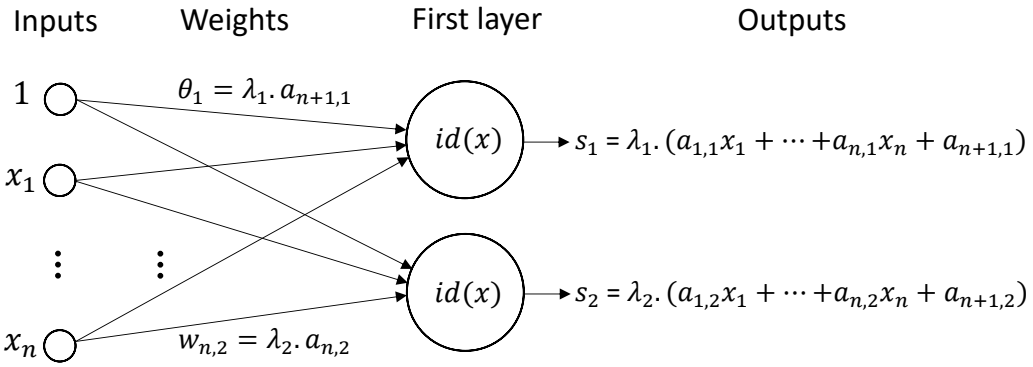


FIGURE 7.5 – Représentation d'un réseau modélisant un sous-espace linéaire de codimension 2 dans $\mathbb{R}^n$.

Si nous prenons la fonction identité comme fonction d'activation pour les 2 neurones, alors la sortie des deux neurones sera à $(0, 0)$ précisément lorsque le point en entrée est à la fois dans le premier et second plan, et de ce fait sur la droite (L_2). Ce résultat se généralise assez directement aux codimensions supérieures :

Proposition 7.3.2. *Soit (L_m) un sous-espace linéaire affine de codimension m, défini par m équations du type $a_{1,i}x_1+a_{2,i}x_2+\cdots+a_{n,i}x_n+a_{n+1,i} = 0$, avec des variables réelles $(x_1, x_2, \ldots, x_n)$ et des coefficients réels $(a_{1,i}, a_{2,i}, \ldots, a_{n+1,i})$, $\forall i \in [\![1, m]\!]$. Alors ce sous-espace peut être modélisé en combinant m neurones artificiels dans une couche, et les poids du i-ème neurone devront satisfaire : $w_{1,i} = \lambda_i a_{1,i}, w_{2,i} = \lambda_i a_{2,i}, \ldots, w_{n,i} = \lambda_i a_{n,i}$ et $\theta_i = \lambda_i a_{n+1,i}$, avec $\lambda_i \in \mathbb{R}^*, \forall i \in [\![1, m]\!]$.*

♢

7.3.2 Polynômes de degré 2

En pratique, le cas des sous-espaces linéaires est un cas très particulier de variété algébrique, et la majorité des variétés algébriques seront définies par des polynômes non nécessairement linéaires. Ceci nous amène donc à considérer des équations de plus haut degré, et nous nous proposons d'étudier le prochain exemple allant dans ce sens.

Exemple 14. [Courbes] Soit un cercle (C) de $\mathbb{R}^2$ défini par l'équation $x^2+y^2-r^2=0$, avec $r>0$ le rayon du cercle. En se restreignant uniquement à calculer la somme pondérée d'un neurone avec une fonction d'activation égale à l'identité, on ne pourra pas modéliser cette équation quadratique. L'idée ici est d'utiliser la fonction (carrée) $x \mapsto x^2$ comme fonction d'activation, afin d'introduire des termes de degré 2, dépendant des entrées, en sortie du neurone. Cette idée a déjà été utilisée dans [159] afin d'étudier la puissance des réseaux de neurones profonds (*deep neural networks*) munis de fonctions d'activation polynomiales. Les réseaux de neurones exploitant des équations polynomiales, dans la fonction d'activation ou le seuil, sont connus sous différentes formes dans la littérature [250, 144, 275, 163, 243, 244, 40, 124, 88]. Ces réseaux sont aussi connus sous le nom de *Polynomial Neural Networks* (PNN), et une architecture adaptative a été proposée en 2003 dans [203].

Pour tout neurone artificiel dont les poids w_1 et w_2 sont respectivement associés aux entrées x et y, avec θ le seuil et $g : x \mapsto x^2$ la fonction d'activation, alors la sortie s du neurone est égale à :

$$\begin{aligned} s &= g(\mathcal{U}) = (w_1 x + w_2 y + \theta)^2 \\ &= {w_1}^2 x^2 + {w_2}^2 y^2 + 2w_1 w_2 xy + 2w_1 \theta x + 2w_2 \theta y + \theta^2 \ . \end{aligned} \tag{7.3}$$

Si nous voulons modéliser l'équation d'un cercle, alors on montre qu'un seul neurone artificiel n'est pas suffisant. En revanche, ceci est possible en ajoutant un neurone dans la même couche, puis en combinant leur deux sorties dans un troisième neurone placé dans une autre couche (voir Figure 7.6). Ce résultat peut être généralisé comme suit :

Proposition 7.3.3. *Toute équation polynomiale de degré 2 à $n-1$ variables réelles x_i, c'est-à-dire de la forme $\mathcal{E}$: $\sum_{1\leq i<n} a_{i,i}x_i^2 + \sum_{1\leq i<j<n} 2a_{i,j}x_i x_j + \sum_{i=1}^{n-1} 2a_{i,n}x_i + a_{n,n}$, avec $a_{i,j} \in \mathbb{R}$, peut être modélisée à l'aide de n neurones artificiels : $n-1$ neurones avec une fonction d'activation $x \mapsto x^2$ dans une première couche, et un neurone avec une fonction d'activation identité dans une seconde couche.*

Démonstration. Soit $\mathcal{E}$ un polynôme de degré 2, comme défini dans la proposition, pouvant être représenté à l'aide de l'équation matricielle $\vec{x}^\top A \vec{x} = 0$, avec une matrice réelle symétrique $A = (a_{i,j})$, et $\vec{x} = (x_1, \cdots, x_{n-1}, 1)^\top$.

Soit $w_{i,j}$ le poids associé à la i-ème entrée et au j-ième neurone de la première couche. Soit b_k le poids associé à la sortie du k-ième neurone de la première couche et à l'unique neurone de la seconde couche. Soit $\theta_1, \ldots, \theta_{n-1}$ les seuils des $n-1$ neurones de la première couche, et θ_n le seuil du neurone de la seconde couche. Chaque neurone de la première couche a une fonction d'activation carrée, et le neurone de la seconde couche a une fonction d'activation identité. Si on note par $s_1, \ldots, s_{n-1}$ les sorties des neurones de la première couche, et par s_n la sortie du neurone de la seconde couche, alors :

$$s_n = \mathcal{U}_n = \sum_{i=1}^{n-1} b_i s_i + \theta_n \quad \text{avec} \quad s_i = \mathcal{U}_i{}^2 = \left(\sum_{j=1}^{n-1} w_{j,i} x_j + \theta_i \right)^2 . \tag{7.4}$$

Alors s_n est une combinaison non-homogène de formes linéaires affines élevées au carré. Ceci peut être représenté comme $\vec{v}^\top D \vec{v} = 0$ pour D une matrice diagonale réelle, et les entrées $v_1, \ldots, v_{n-1}$ de $\vec{v}$ sont les formes linéaires (avant l'élévation au carré) dans les expressions des sorties s_i, et $v_n = \sqrt{\theta}_n$.

Il en résulte alors que la proposition est équivalente à la diagonalisation de matrices symétriques réelles, et il est connu que cette diagonalisation est toujours possible via des matrices orthogonales. Les entrées des matrices orthogonales intervenant dans la diagonalisation donnent les poids du réseau de neurone. ♢

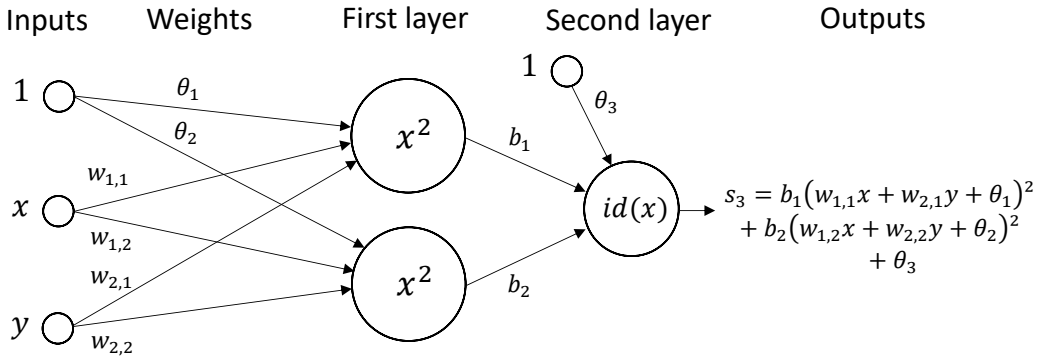


FIGURE 7.6 – Représentation d'un réseau modélisant une équation polynomiale de degré 2 à deux variables réelles et à coefficients réels.

♢

7.3.3 Polynômes homogènes de degré d

Il peut être intéressant de vouloir généraliser ce raisonnement à un degré quelconque. Afin de construire un réseau de neurones permettant de modéliser toute équation polynomiale de degré d en n variables, la détermination de la dimension peut donner une meilleure idée de l'architecture appropriée pour cette tâche. Le théorème d'Alexander-Hirschowitz (AH) (voir [43] pour une formulation plus récente) nous indique dans quels cas le calcul naïf de la dimension n'est pas correct. En effet, le théorème AH établit qu'un polynôme homogène général[1] p de degré d en n variables peut être exprimé somme la somme de $T = \lceil \frac{1}{n}\binom{d+n-1}{d} \rceil$ forme linéaires élevées au degré d (à l'exception des formes quadratiques (voir Proposition 7.3.3) et de quelques autres cas spéciaux). En d'autres termes, le théorème établit qu'on peut exprimer p comme étant égal à :

$$p(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{T} \left(\sum_{i=1}^{n} a_{ij} x_i \right)^d . \tag{7.5}$$

1. Par "général" nous entendons : ne faisant pas partie d'un ensemble de contre-exemples.

Ce résultat apporte en fait une solution au problème de Waring pour les polynômes, fournissant en fait le plus petit entier T tel que la variété des sécantes $\sigma_T(\nu_d(\mathbb{P}^{n-1}))$, associée à la variété de Veronese de degré d, remplit tout l'espace $\mathbb{P}(\mathrm{Sym}^d(\mathbb{P}^{n-1}))$ (voir Sections 2.1.4 et 2.1.6 pour plus d'informations).

En dé-homogénéisant le résultat du théorème de AH (en imposant la dernière variable à 1, par exemple), on obtient une borne pour les réseaux de neurones à 2 couches modélisant des hypersurfaces affines. En effet, nous pouvons implémenter $T = \lceil \frac{1}{n}\binom{d+n-1}{d} \rceil$ neurones dans la première couche possédant tous une fonction d'activation $g : x \mapsto x^d$. On combine ensuite linéairement leurs sorties en utilisant un neurone en seconde couche du neurone.

On suppose avoir n entrées correspondant aux n variables du polynôme homogène p. Si on note par $w_{i,j}$ le poids associé à la i-ème entrée x_i et au j-ième neurone de la première couche, et par θ_j le seuil du j-ième neurone, alors la sortie s_j du j-ième neurone de la première couche est :

$$s_j = g(\mathcal{U}_j) = \left(\sum_{i=1}^{n} w_{i,j} x_i + \theta_j \right)^d . \tag{7.6}$$

Le seuil θ_j introduit en effet une non-homogénéité, à laquelle on peut remédier en ajoutant une variable supplémentaire x_{n+1}, remplaçant alors θ_j par $\theta_j x_{n+1}$. Ensuite, en appliquant le théorème AH pour $n+1$ variables, et en imposant $x_{n+1} = 1$, nous obtenons la borne correspondante pour une forme non-homogène de la sorite. Cette idée apparaît aussi dans les travaux de Kileel *et al.* [159].

La dernière partie dans la conception du réseau est de résoudre effectivement le problème de classification, à savoir : est-ce que le point en entrée appartient (ou pas) à la variété algébrique définie par les équations modélisées par les deux premières couches du réseau ?

Nous rappelons qu'en sortie des deux premières couches, nous devons récupérer une valeur spécifique s (qui est ici 0), lorsque le point en entrée est sur la variété, et toute autre valeur différente de s lorsque le point en entrée ne l'est pas. De ce fait, la dernière étape est équivalente à reconnaître un nombre réel s dans un intervalle (donc la taille dépendra des données en entrée). Il n'est pas possible d'ajouter simplement un neurone avec une fonction Sigmoïde pour résoudre ce problème car un neurone unique ne peut résoudre que des inégalités et non des égalités [109, 163]. Nous avons donc besoin d'une autre couche avant la couche de sortie finale pour être en mesure de reconnaître une valeur spécifique s, et alors pouvoir résoudre le problème de classification binaire en sortie du réseau.

Après avoir testé plusieurs architectures différentes, la tâche de reconnaître un nombre réel dans un intervalle peut être réalisée à l'aide d'une seule couche à 4 neurones, chaque neurone disposant d'une fonction d'activation de type LeakyReLU. De ce fait, en ajoutant cette couche après les deux première couches (modélisant les équations de la variété), et en ajoutant une dernière couche pour la sortie (avec seulement un seul

neurone Sigmoïde), il est alors potentiellement possible d'apprendre à reconnaître toute variété définie par un exemple de polynômes homogènes (voir Figure 7.7).

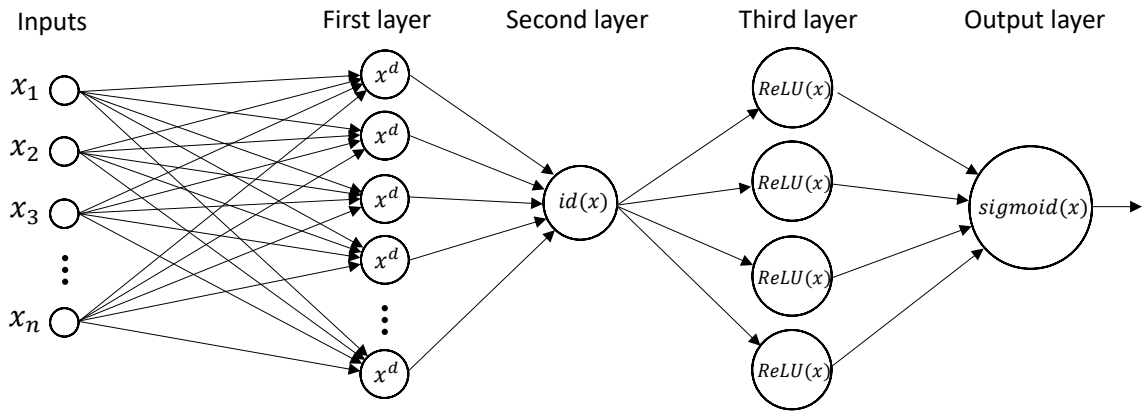


FIGURE 7.7 – Représentation du réseaux résolvant le problème de classification binaire lié à l'appartenance à une variété algébrique.

Néanmoins, la question de la capacité à entraîner un réseau de neurone, et la capacité pour l'optimiseur de trouver les bons poids et seuils est importante du point vue de l'implémentation informatique. Pour des équations polynomiales homogènes de degré bas avec peu de variables (comme le cas du cercle), le réseau est capable d'apprendre les bons poids, et on peut aussi retrouver l'équation du cercle à partir des poids et seuils du réseau entraîné.

En revanche, lorsque le degré devient élevé le nombre de variables conséquent, le nombre de neurones nécessaires dans la première couche augmente très rapidement, et il devient alors plus difficile de converger vers un ensemble de poids et seuils modélisant l'équation polynomiale désirée. Afin de pouvoir limiter cette difficulté, nous apportons quelques modifications à la structure du réseau afin de réduire le nombre de poids et de paramètres (voir Section 7.3.6).

7.3.4 Réseaux de neurones profonds et approximations

Pour des réseaux de neurones plus profonds, avec fonctions d'activation de degré d, nous pouvons appliquer le même principe de comptage de dimension (comme cela a été fait en exploitant le théorème AH), afin de déterminer la largeur maximale de chaque couche, afin d'éviter toute redondance ou sur-apprentissage dans le réseau. Pour des exemples concrets sur cette question, se référer à Kileel *et al.* [159, Sec. 3.2].

Considérons une construction récursive. Supposons pour la suite du raisonnement que nous travaillons avec les nombres complexes et que nous voulons approximer un polynôme homogène f de degré $d \times e$ comme une somme de puissances d'ordre d de p polynômes homogènes g_j de degré e en n variables, tel que

$$f \simeq \sum_{j=1}^{p} \lambda_j (g_j)^d \ . \tag{7.7}$$

Il n'est pas nécessaire dans ce cas de compter les paramètres λ_j, car nous pouvons remultiplier les g_j par une racine d-ième. De ce fait, nous avons besoin au plus de $\binom{n-1+de}{de}$ paramètres pour exprimer f, par application du théorème AH pour le polynôme f. En revanche, si on s'intéresse au membre de droite de l'équation ci-dessus, alors nous avons besoin de $p\binom{n-1+e}{e}$ paramètres.

On pourra alors procéder à une approximation de f seulement si $p\binom{n-1+e}{e} \geq \binom{n-1+de}{de}$, ce qui revient à imposer que

$$p \geq \left\lceil \frac{\binom{n-1+de}{de}}{\binom{n-1+e}{e}} \right\rceil . \tag{7.8}$$

Cette borne nous donne donc une idée du nombre minimal de neurones nécessaire à une telle approximation. D'autre part, dans le cas général où f est de degré d et que les fonctions g_j sont issues d'un espace nécessitant M paramètres, alors en répétant le même argument, tant que nous avons p neurones avec

$$p\binom{M-1+e}{e} \geq \binom{n-1+de}{de} , \tag{7.9}$$

alors il peut être possible d'approximer f. Pour un nombre plus important de couches, on itère la construction récursive en Équation 7.9. Par exemple, dans le cas d'un réseau à 3 couches, avec p_j neurones dans la couche d'indice j utilisant une fonction d'activation de degré d_j, si nous avons

$$p_1\binom{p_2\binom{p_3\binom{n-1+d_3}{d_3}-1+d_2}{d_2} - 1 + d_1}{d_1} \geq \binom{n-1+d_1d_2d_3}{d_1d_2d_3} , \tag{7.10}$$

alors on peut être en mesure de modéliser une fonction f de degré $d_1 \times d_2 \times d_3$. On pourrait imaginer qu'un résultat de classification similaire au critère élaboré à partir du théorème AH est toujours valable, mais relativement peu d'informations sont connues à ce sujet. On pourra regarder [159, Thm. 10] pour une autre proposition de borne.

7.3.5 Réseaux de neurones et interpolation polynomiale

La capacité des réseaux de neurones d'approximer toute fonction, au sens du théorème universel d'approximation, peut nous amener à nous questionner dans quelle mesure ceci diffère de l'interpolation polynomiale. Dans [67], un argument analytique supporte que les réseaux de neurones sont en fait essentiellement des modèles de régression polynomiale, avec le degré effectif du polynôme augmentant à chaque couche cachée du réseau. Selon les auteurs, si la fonction d'activation est polynomiale alors le réseau de neurone réalise exactement une régression polynomiale. Dans le même esprit, les architectures de réseau de neurones proposés dans [170] montrent une correspondance entre la valeur des fonctions à interpoler, les fonctions de base et les points de base, d'une part, et entre les poids, les fonctions d'activations et les seuils (biais), d'autre part.

Néanmoins, en ce qui concerne les applications pratiques, les données sont souvent incomplètes et bruitées, et l'interpolation polynomiale est généralement sujette au sur-apprentissage [284], alors que les réseaux de neurones sont capables d'être performants en présence de données bruitées et incomplètes, et sont capables de généraliser à partir de ces données d'entraînement [206].

Ce dilemme, entre avoir une bonne précision pour les données d'entraînement et être en mesure de généraliser les modèles à des données non rencontrées, est connu sous le nom de *bias-variance trade-off*, et est discuté dans [27]. Raturi explique dans [222] que résoudre le même problème que celui de l'interpolation polynomiale requiert bien moins de ressources et de temps de calcul en utilisant les réseaux de neurones. Dans le même article, il démontre que les réseaux de neurones fournissent de meilleures approximations pour deux fonctions spécifiques, comparé à l'interpolation de Lagrange.

Enfin, il a été démontré dans [173] que les réseaux de neurones peuvent interpoler et modéliser une fonction à l'aide de fonction Sigmoïdes afin d'approximer n échantillons de toute dimensions, avec une précision arbitraire et sans entraînement.

7.3.6 Réseaux de neurones hybrides

Dans cette sous-section nous introduisons une architecture de réseau plus simple pour classifier l'appartenance à une variété algébrique. Nous avons observé que durant la phase d'apprentissage, qui est équivalente à un processus d'optimisation, l'algorithme n'est pas toujours capable d'atteindre un ensemble de poids minimisant la fonction d'erreur. Ceci est notamment dû à la présence de minima locaux dans la fonction coût, observation liée à l'utilisation de fonction d'activation non-convexes $x \mapsto x^d$.

Dans la version du réseau de neurones présentée précédemment (voir Figure 7.7), la seconde couche ne contient qu'un unique neurone (avec une fonction d'activation identité), introduite afin de permettre le calcul de la combinaison linéaire de puissances d de sommes pondérées des variables d'entrée. L'idée ici est de retirer cette couche, et de directement relier la première couche avec la troisième couche (contenant uniquement des neurones avec une fonction d'activation de type LeakyReLU). Nous les appelerons *réseaux de neurones hybrides*, car combinant à la fois des couches avec des fonctions d'activation $x \mapsto x^d$ et LeakyReLU.

De plus, l'interprétation géométrique du réseau de neurone est à présent différente car chaque neurone de la nouvelle seconde couche (celle associée à la fonction Leaky-ReLU) prend en entrée un combinaison différente de formes linéaires à la puissance d. La seconde couche combine alors différents polynômes homogènes, qui ne sont pas nécessairement égaux au polynôme définissant la variété algébrique, mais peuvent être utilisés pour approximer ce dernier comme un ensemble d'inégalités. La troisième et dernière couche du réseau de neurones est la couche de sortie, qui dépendera du problème de classification que l'on désire résoudre (classification binaire, multi-classe, etc.). L'architecture de réseau de neurones est représentée en Figure 7.8.

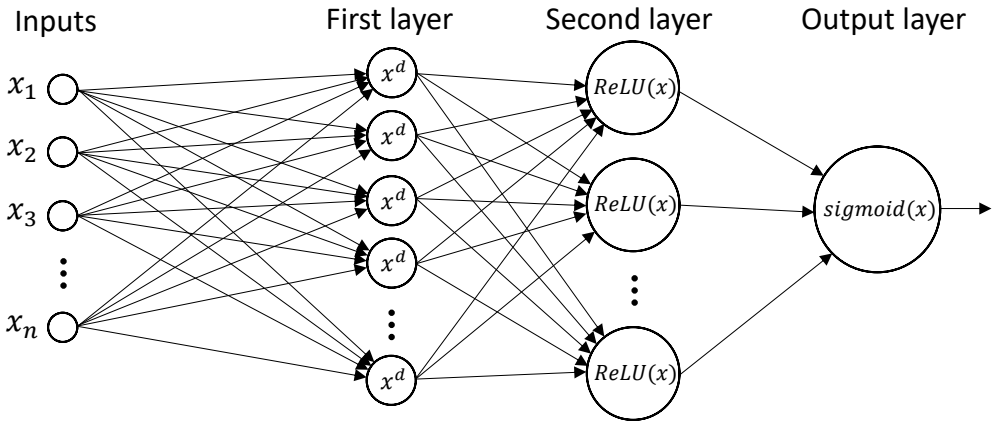


Figure 7.8 – Représentation d'un réseau de neurones hybride pour l'apprentissage d'équations polynomiales homogènes de degré d à n variables et à coefficients dans $\mathbb{R}$.

Ce type de réseau montre de meilleurs résultats et un apprentissage plus rapide que la précédente version du réseau. Le théorème AH peut toujours être utilisé pour donner un ordre d'idée du nombre de neurones dans la première couche, et parfois certains neurones peuvent être ajoutés ou retirés pour améliorer la performance du réseau durant la phase d'apprentissage. Après plusieurs essais, le nombre de neurones dans la deuxième couche peut être choisi assez petit (entre 4 et 12) pour une équation polynomiale à modéliser (un problème de classification binaire), et on adaptera aussi ce nombre en fonction du nombre de classes et donc du nombre de neurones dans la couche de sortie.

Par exemple, si 3 équations polynomiales définissent une variété, alors on additionnera, pour chaque couche, le nombre de neurones nécessaires à la modélisation de chaque équation séparément. En procédant ainsi, on s'assure de ne pas sous dimensionner le réseau pour pouvoir classifier correctement les points en entrée du réseau.

Nous utilisons ces réseaux de neurones hybrides afin de résoudre les différents problèmes de classification présentés dans la section suivante. Nous utilisons également des réseaux totalement composés de neurones LeakyReLU (ces réseaux étant assez répandus dans la littérature, comme premier test) afin de comparer les différentes performances et le nombre de paramètres de chaque architecture.

7.4 Étude de cas – Entraînement des réseaux de neurones

Dans cette section, nous étudions un certain nombre de problèmes de classification concrets, servants de preuve-de-concept pour appuyer le fait que les réseaux de neurones artificiels peuvent être entraînés pour construire des classifieurs efficaces et pratiques pour l'intrication quantique.

Nous commençons par présenter le principe global d'implémentation des réseaux de neurones pour le problème de classification. Nous abordons ensuite chacun des trois

problèmes de classification séparément, en présentant la manière dont les données d'entraînement sont générées, les architectures de réseaux utilisées, et les résultats après la phase d'entraînement. L'utilisation de ces réseaux de neurones pour des applications sera présentée en Section 7.5 suivante.

7.4.1 Modélisation des états quantiques

Dans nos expérimentations, nous nous sommes intéressés uniquement au cas d'états réels, c'est-à-dire à des états quantiques à n-qudits représentés comme des tenseurs dans $(\mathbb{R}^d)^{\otimes n}$. Ces états peuvent être représentés comme un vecteur à d^n entrées dans $\mathbb{R}$, et ce vecteur sera utilisé comme vecteur d'entrée pour le réseau de neurones.

Nous nous sommes limités ici à l'étude des tenseurs réels principalement pour des limitations liées à l'implémentation des réseaux de neurones. Nous voulions que ce travail serve de premier exemple de classification de variétés algébriques par des réseaux de neurones, et par conséquent nous nous sommes limités à une configuration simple pour une implémentation plus directe sous Keras en Python. Le travail avec des tenseurs réels introduit quelques différences dans l'étude des variétés algébriques, notamment pour la question du rang, comme cela est discuté en Section 7.4.4. Le passage au corps des complexes constitue une des pistes d'amélioration évoquées en Section 7.6.

Note sur l'échantillonnage uniforme

Pour ce qui concerne la construction des données d'apprentissage, nous avons la possibilité de générer nous même ces données, et c'est aussi la motivation principale pour adopter une démarche supervisée. De manière générale, nous construisons des points sur les variétés algébriques en passant par des fonctions de paramétrisation de la forme $\varphi\colon U \to V$, avec φ une fonction rationnelle, et U, V des sous-ensembles d'un espace linéaire normé. Si on échantillonne de manière uniforme la source U, alors de manière générale $\varphi(U)$ ne suivra pas une distribution uniforme de l'image.

À défaut de tenter d'échantillonner uniformément l'image de ces variétés, comme cela peut être fait dans la littérature [127, 209, 92], nous tentons de proposer des données construites d'une manière très proche de celle utilisée pour générer (informatiquement ou expérimentalement) les états sur lesquels on voudrait une prédiction du classifieur. Le caractère raisonnable ou non de cette supposition est bien entendu ouvert à toute discussion.

D'une part, il sera toujours possible pour une entité hostile de construire un jeu de données appartenant à la même variété algébrique, mais pour lequel notre classifieur donnera une réponse inexacte. D'autre part, si on dit que les données pour entraîner le réseau sont générées selon une certaine procédure, alors nous pouvons être assez confiants quant à la fiabilité de notre réseau pour prédire des résultats liés à des données à tester générées selon la même procédure.

Pour chacun des classifieurs considérés dans les sections suivantes, nous choisissons principalement d'échantillonner uniformément des opérateurs du groupe SLOCC, afin de générer des états aléatoirement équivalents à des états construits selon une certaine

procédure déterministe ou aléatoire, afin de favoriser une distribution plus uniforme. En fonction de la dimension des systèmes quantiques, les opérateurs SLOCC peuvent être modélisés comme un produit tensoriel de matrices carrées (représentant une action locale), de taille variable selon le nombre d'états de base d'une particule, et de déterminant égal à 1. Nous générons les matrices locales SL_n en générant les coefficients de la matrice selon une loi uniforme (tant que le déterminant de la matrice est négatif), puis nous divisons toute la matrice par la racine n-ième du déterminant, afin d'assurer une valeur de ce dernier égale à 1. Nous réalisons ensuite le produit tensoriel des matrices locales pour générer un opérateur SLOCC qui agira sur le système dans sa globalité.

7.4.2 Détecter des états séparables

Supposons que $\mathcal{H} = \mathbb{R}^d$. On rappelle qu'un état $|\varphi\rangle \in \mathcal{H}^{\otimes n}$ est dit séparable, factorisé ou non-intriqué, s'il peut être exprimé comme le produit tensoriel d'états purs comme suit

$$|\varphi\rangle = |\varphi_1\rangle \otimes \cdots \otimes |\varphi_n\rangle \ , \tag{7.11}$$

avec pour tout i, $|\varphi_i\rangle \in \mathcal{H}$. Comme cela a été introduit au Chapitre 2, la variété projective des états séparables est la variété de Segre. Nous rappelons en Proposition 7.4.1 une équivalence établie par Segre dans les années 1900, et qui sera exploitée pour générer des états séparables.

Proposition 7.4.1. *Un état $|\varphi\rangle \in \mathcal{H}^{\otimes n}$ est séparable si et seulement si une des conditions équivalentes suivantes est vérifiée :*

1. *$|\varphi\rangle$ est dans l'orbite SLOCC de $|00\cdots0\rangle$,*
2. *Tous les n possibles 1-flattenings $F_i(|\varphi\rangle)\colon \mathcal{H}^{\otimes(n-1)} \to \mathcal{H}$ sont de rang 1.*

Les *1-flattenings* sont une ré-écriture des tenseurs (pouvant être représentés par des matrices multidimensionnelles) sous la forme de matrices, pouvant s'assimiler à une sorte d'aplatissement des tenseurs. Par exemple, dans le cas des 3-qubits, si on définit $|\varphi\rangle \in \mathcal{H}^{\otimes 3} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ ayant les coordonnées

$$\varphi_{ijk} = \langle ijk|\varphi\rangle \ , \tag{7.12}$$

alors les 3 possibles *1-flattenings* s'expriment comme suit :

$$F_1(|\varphi\rangle) = (\varphi_{ijk})_{i,jk}, \quad F_2(|\varphi\rangle) = (\varphi_{ijk})_{j,ik}, \quad F_3(|\varphi\rangle) = (\varphi_{ijk})_{k,ij} \ . \tag{7.13}$$

Les rangs de ces *flattenings* forment un vecteur appelé le *rang multilinéaire*. Aucun *flattening* ne peut avoir de rang égal à 0, compte tenu du fait que cela n'arrive que si $|\varphi\rangle = 0$ et que $|\varphi\rangle$ est un vecteur de norme 1. Si le rang multilinéaire est égal à $(1,1,1)$, alors $|\varphi\rangle$ est séparable (Proposition 7.4.1). De même, un état de classe biséparable (A-BC) aura un rang multilinéaire de (1,2,2) (à une permutation des qubits près). Enfin, si le rang multilinéaire est $(2,2,2)$, alors l'état est SLOCC équivalent soit à l'état $|GHZ\rangle$, soit à l'état $|W\rangle$ [191, 135].

De ce fait, une manière de déterminer si un état est séparable est de calculer la forme compacte de la SVD (*singular value decomposition*) de chaque *1-flattenings*. Il existe alors déjà des méthodes pour déterminer si un état est séparable ou non. Nous désirons mettre en évidence que les réseaux de neurones artificiels constituent également un outil pour détecter la séparabilité, et donc l'intrication d'un état ou d'un tenseur en entrée.

Génération des états séparables

On génère de manière uniforme des échantillons de l'ensemble des états séparables en générant uniformément des points sur un produit de sphères via l'application de Segre

$$\mathcal{SH} \times \cdots \times \mathcal{SH} \to \mathcal{SH}^{\otimes n} \ , \tag{7.14}$$

où $\mathcal{SH}$ désigne les états de normalisés de $\mathcal{H}$, et de même pour $\mathcal{SH}^{\otimes n}$. La notation adoptée en Équation 7.14 diffère de celle introduite en Équation 2.7 pour insister sur la condition de normalisation imposée sur chaque qubit. On génère alors uniformément n points sur la sphère, et réalise le produit tensoriel de ces états pour former un état séparable. La classe correspondant aux états séparables est labellisée '0', et représente 50% des données d'entraînement. L'autre moitié de ces données correspond à la classe des états intriqués, labellisée '1', et est construire en générant aléatoirement des tenseurs de rang supérieur ou égal à 1, en sommant des états séparables aléatoires (et donc de rang 1). En se basant sur la Proposition 7.4.1, il est possible de s'aider du rang multilinéaire afin de certifier la validité des données d'entraînement générées, et de supprimer un éventuel bruit dans ces données. Afin d'illustrer notre méthode, nous présentons à présent comment nous entraînons les réseaux de neurones pour réaliser cette tâche.

Architecture pour les états séparables

On rappelle que l'ensemble des états séparables se définit comme le lieu des zéros des 2 par 2 mineurs des *1-flattenings*, et est donc défini par un ensemble de polynômes homogènes de degré 2. Dans le cas 2×2, il n'y a qu'une seule équation définissant les états séparables, qui est le déterminant 2×2. Pour des dimensions supérieures, un certain nombre d'équations de degré 2 définissent la variété de Segre. Pour choisir le nombre d'équations, nous prenons (au minimum) la codimension de la variété de Segre dans l'espace projectif.

Pour chaque équation quadratique, nous utilisons notre critère (voir Proposition 7.3.3) afin de déterminer le nombre de neurones nécessaire et ainsi dimensionner les réseaux hybrides. Dans certains cas, nous choisissons d'ajouter des neurones supplémentaires dans la première couche (avec une fonction d'activation quadratique) pour faciliter le processus d'apprentissage. Comme expliqué précédemment, la seconde couche contient uniquement des neurones avec fonction d'activation LeakyReLU. La dernière couche contiendra uniquement un seul neurone, avec une fonction d'activation Sigmoïde dans ce cas, du fait de la nature binaire du problème de classification.

Nos avons également implémenté des réseaux de neurones ne faisant apparaître que des fonctions d'activation LeakyReLU (sauf pour la couche de sortie). Pour tous

les cas considérés, nous avons utilisé la même architecture de réseau, composée de 4 premières couches et une couche de sortie. Nous avons choisi d'implémenter une structure décroissante pour le réseau, avec 100 neurones pour la première couche, 50 pour la seconde, 25 pour la troisième et 16 pour la dernière. La couche de sortie est la même que celle des réseaux hybrides.

Nous nous proposons à présent de présenter les résultats et performances d'apprentissage.

Résultats

Dans la Table 7.2 nous présentons les résultats pour les cas 2×2, $2 \times 2 \times 2$, $2^{\times 4}$ et $3 \times 3 \times 3$ en utilisant les réseaux hybrides. Dans les cas 2×2, $2 \times 2 \times 2$ et $3 \times 3 \times 3$, nous avons utilisé un ensemble de données d'entraînement de taille 56200, un ensemble de validation de taille 12800 et un ensemble de test de taille 32000. Dans le cas $2^{\times 4}$, nous avons uniquement doublé la taille de l'ensemble d'entraînement (même taille pour l'ensemble de test). Nous atteignons une précision moyenne de 93% pour les ensembles de test pour le problème de classification des états séparables et intriqués.

Système	Architecture	Entraînement	Validation	Test	Erreur
2×2	(4,4,1)	96.65%	96.60%	96.63%	0.092
$2 \times 2 \times 2$	(21,8,1)	94.57%	94.06%	94.44%	0.15
$2^{\times 4}$	(1188,8,1)	91.72%	91.60%	91.33%	0.26
$3 \times 3 \times 3$	(332,12,1)	94.68%	92.89%	92.94%	0.15

Table 7.2 – Architectures des réseaux hybrides et pourcentages de précision pour chaque taille de système quantique, pour le problème de séparabilité.

Nous avons également utilisé les réseaux de type LeakyReLU afin d'étudier les mêmes cas que pour les réseaux hybrides, en ajoutant le cas $2^{\times 5}$. Les résultats sont regroupés en Table 7.3. Dans les cas 2×2 et $2 \times 2 \times 2$, nous avons utilisé un ensemble d'entrainement de taille 102400, un ensemble de validation de taille 25600 et un ensemble de test de 32000. Dans les cas $2^{\times 4}$, $2^{\times 5}$ et $3 \times 3 \times 3$, nous avons utilisé un ensemble d'entraînement de taille 502600, un ensemble de validation de taille 55600 et un ensemble de test de 32000. Nous atteignons une précision moyenne de 98% pour les ensembles de test pour le problème de classification des états séparables et intriqués.

Complexité et efficacité

Ces résultats montrent qu'un réseau de neurone artificiel peut être entraîné afin de distinguer les états séparables des états intriqués pour les états purs. Du point de vue de la géométrie algébrique, déterminer si un tenseur appartient à la variété de Segre c'est déterminer s'il est de rang 1, et cette tâche peut être réalisée à l'aide d'une forme tronquée de la SVD sur chaque *flattening*. La complexité associée au calcul de la valeur singulière d'une matrice $m \times n$ est en $\mathcal{O}(mn \min\{m, n\})$. Ceci est à peu près $\min\{m, n\}$ fois la complexité associée à la lecture de la matrice. Calculer les valeurs singulières du *i-flattening* d'un tenseur de taille $n_1 \times \cdots \times n_t$ a une complexité en

Système	Architecture	Entraînement	Validation	Test	Erreur
2×2	(100,50,25,16,1)	98.92%	98.78%	98.83%	0.043
$2 \times 2 \times 2$	(100,50,25,16,1)	97.80%	97.42%	97.55%	0.074
$2^{\times 4}$	(100,50,25,16,1)	99.62%	99.50%	99.53%	0.016
$2^{\times 5}$	(100,50,25,16,1)	98.83%	98.55%	98.55%	0.037
$3 \times 3 \times 3$	(100,50,25,16,1)	98.55%	98.01%	97.92%	0.051

TABLE 7.3 – Architectures des réseaux LeakyReLU et pourcentages de précision pour chaque taille de système quantique, pour le problème de séparabilité.

$$\mathcal{O}\left(n_i(\frac{n_1 \cdots n_t}{n_i}) \min\{n_i, (\frac{n_1 \cdots n_t}{n_i})\}\right) = \mathcal{O}\left((n_1 \cdots n_t) \min\{n_i, (\frac{n_1 \cdots n_t}{n_i})\right) \ . \quad (7.15)$$

Pour les cas "équilibrés" où $2n_i \leq \sum_i n_i$, cette complexité est au plus

$$\mathcal{O}\left((n_1 \cdots n_t)n_i\right) \ , \quad (7.16)$$

ce qui est environ n_i fois la complexité de lire le tenseur. Calculer toutes les valeurs singulières d'un tenseur (de manière naïve, sans lier les résultats d'un calcul avec un autre), implique une complexité de l'ordre de $\mathcal{O}\left((n_1 \cdots n_t)(\sum_i n_i)\right)$.

D'autre part, le coût d'évaluation d'un réseau de neurones entraîné est égal au coût de la propagation du signal de l'entrée à la sortie du réseau, ce qui requiert le calcul de toutes les sommes pondérées (ce qui est équivalent à calculer des produits matriciels) et l'évaluation des fonctions d'activation, et ce pour chaque neurone. La complexité de ce calcul dépendra en effet de l'architecture du réseau de neurones. Si on pose l le nombre de couches (sans compter la couche d'entrée), et par $m_1, m_2, \ldots, m_l$ le nombre de neurones pour chaque couche, alors on a une complexité environ de l'ordre de $\mathcal{O}((n_1 \cdots n_t)m_1 + m_1m_2 + \cdots + m_{l-1}m_l)$.

Ceci indique que plus la dimension de l'espace augmente, plus de le coût d'évaluation d'un réseau de neurone déjà entraîné devrait être inférieur au coût du calcul de SVD de *flattenings*. Même si le coût lié à l'entraînement du réseau de neurone ne peut être négligé, cette étape ne sera réalisée qu'une seule fois, et le réseau issu de l'entraînement peut être utilisé pour être évalué sur un jeu de tests conséquent. De plus, lorsque le rang devient supérieur à la dimension de chacun des facteurs, il existe très peu de méthodes pratiques pour déterminer le rang, et des réseaux de neurones artificiels vu comme des classifieurs pourraient apporter une aide intéressante.

7.4.3 Détecter des états dégénérés

Nous rappelons tout d'abord (un résultat d'algébre linéaire) qu'une matrice $A \in \mathbb{R}^{m \times n}$ est dite *dégénérée* si et seulement une des conditions équivalentes suivantes est vérifiée :

1. Il existe deux vecteurs non-nuls $u \in \mathbb{R}^m$ et $v \in \mathbb{R}^n$ tels que $u^\top Ax = 0$ pour tout $x \in \mathbb{R}^n$, et $y^\top Av = 0$ pour tout $y \in \mathbb{R}^m$,
2. Dans le cas où $m = n$, le déterminant s'annule : $\det(A) = 0$,

3. À une élimination de Gauss près, A a une colonne nulle et une ligne nulle.

Ces conditions se généralisent aussi pour les tenseurs, on peut se référer à [106]. Un état $|\varphi\rangle \in \mathcal{H}^{\otimes n}$ sera dit *dégénéré* si et seulement une des conditions équivalentes suivantes est vérifiée :

1. Il existe un état pur $x = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \in \mathcal{H}^{\otimes n}$ telle que la contraction suivante vérifie
$$(\langle x_1| \otimes \cdots \otimes \langle x_{i-1}| \otimes \langle h_i| \otimes \langle x_{i+1}| \otimes \cdots \otimes \langle x_n|)\,|\varphi\rangle = 0\ ,$$
pour tout i et pour tout $|h_i\rangle \in \mathcal{H}$,
2. L'hyperdéterminant s'annule : $\mathrm{Det}(A) = 0$, où A où A est l'hypermatrice satisfaisant $A_I = \langle I|\varphi\rangle$,
3. À une action SLOCC près, les coordonnées $\varphi_I = 0$ pour tout I de distance de Hamming ≤ 1 par rapport à $(00\cdots0)$ (voir Figure 7.9).

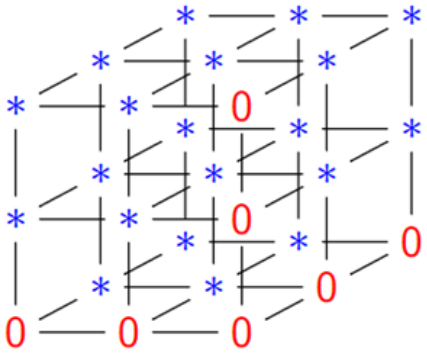


Figure 7.9 – Représentation d'un exemple de base, pour la troisième condition, pour un état dégénéré à 3-qutrits. Les étoiles bleues peuvent prendre n'importe quelle valeur.

Comme évoqué tout au long de cette thèse, l'hyperdéterminant est un polynôme permettant de caractériser l'intrication, et peut aussi la quantifier d'une certaine manière. Alors que c'est aussi un polynôme permettant de tester la dégénérescence des tenseurs, il est de très haut degré et il est rarement possible de le calculer explicitement, à part pour les cas les plus simples. Ceci est notamment le cas des 3-qubits et 4-qubits, et récemment, et pour les hyperdéterminants issus de E_8 [139] (voir Section 6.3).

Nous voulons démontrer qu'il est toujours possible d'apprendre à reconnaître les états dégénérés même dans les cas où une expression ou une méthode d'évaluation de l'hyperdéterminant n'est pas explicitement connue.

Génération des états dégénérés

La description des états dégénérés sous l'équivalence SLOCC fournit une manière d'échantilloner l'ensemble des états dégénérés. Nous prenons un état aléatoire $|\varphi\rangle$ dont les coordonnées $\varphi_I = 0$ pour tout I de distance de Hamming ≤ 1 par rapport à $(00\cdots0)$, et nous re-normalisons l'état, puis lui appliquons un élément aléatoire du groupe SLOCC. Les états dégénérés forment la moitié de l'ensemble des données d'entraînement, et sont labellisés comme étant la classe '0'.

D'autre part, nous générons des états aléatoires de $\mathcal{H}^{\otimes n}$ pour construire la seconde partie de l'ensemble d'entraînement, correspondant, avec une haute probabilité, aux états non-dégénérés, et sont labellisés comme étant la classe '1'. En effet, par "haute probabilité" nous entendons le fait que, pour les nombres réels, l'ensemble des états dégénérés a une codimension au moins égale à 1 dans l'espace ambiant $\mathbb{R}^{d^n}$. De ce fait, la probabilité qu'un tenseur choisit aléatoirement dans $\mathbb{R}^{d^n}$ appartienne aux états dégénérés est (quasi) nulle. Même si nous utilisons une précision décimale de l'ordre du *float*, on peut fortement espérer que cette probabilité reste quasi-nulle dans le cas discret.

Néanmoins, lorsqu'une méthode analytique pour l'évaluation de l'hyperdéterminant existe, nous l'utilisons pour retirer tout le bruit possible dans l'ensemble d'entraînement (notamment retirer tous les états aléatoires n'étant pas des états non-dégénérés pour la classe '1').

Architecture pour les états dégénérés

L'hyperdéterminant $2^{\times n}$ est un polynôme homogène, dont le degré est égal à $4, 24, 128$ respectivement pour $n = 3, 4, 5$ et son degré est de 36 pour le cas $3 \times 3 \times 3$ (voir [106] pour des expressions concrètes).

Dans le cas $2 \times 2 \times 2$, la première couche du réseau hybride devra contenir au moins $\lceil \frac{1}{8}\binom{4+8-1}{4} \rceil = 42$ neurones avec une fonction d'activation $x \mapsto x^4$. Nous choisissons d'implémenter 60 neurones pour la première couche pour le cas des 3-qubits. Dans les deux autres cas, le nombre de neurones nécessaires est trop élevé pour espérer une implémentation efficace via Keras. Il pourrait tout de même être possible d'utiliser moins de neurones pour approximer l'hyperdéterminant en utilisant les réseaux hybrides, et même si la précision ne serait pas parfaite est qu'elle atteint par exemple 60% à l'apprentissage, il serait possible d'utiliser l'idée développée en Section 7.5 pour avoir une meilleure précision globale lors de la prédiction. Une autre possibilité serait d'utiliser le *Standard Ensemble Learning* (aussi connu sous le nom de *bagging*), et entraîner différents neurones afin de construire un comité qui pourra répondre avec une meilleure précision pour la détection d'état dégénérés. Une des limitations de notre approche par réseaux hybrides et le Théorème de AH réside donc dans l'impossibilité de construire en pratique le réseau lorsque le nombre de neurones de la première couche est élevé (ce qui implique un haut degré et/ou un grand nombre de variables d'entrées).

La seconde possibilité est d'utiliser des réseaux LeakyReLU, comme cela a été fait pour la classification des états séparables et intriqués (voir Section 7.4.2). Nous utilisons aussi la même structure décroissante avec quatre couches, sauf dans le cas des 4-qubits, où nous doublons le nombre de neurones dans les trois premières couches.

Dans le cas 2×2, les états non-dégénérés sont en fait les états non-séparables. Ce cas est donc déjà résolu par le classifieur de séparabilité pour le cas 2×2 présenté en Section 7.4.2.

Résultats et discussions

Dans la Table 7.4 nous présentons les résultats pour le cas $2 \times 2 \times 2$ pour le réseau hybride. Nous avons utilisé un ensemble d'entraînement de taille 202600, un ensemble de validation de taille 25600 et un ensemble de test de 32000. Nous avons atteint un pourcentage de 92% de bonne classification pour l'ensemble de test.

Système	Architecture	Entraînement	Validation	Test	Erreur
$2 \times 2 \times 2$	(60,10,1)	92.49%	92.18%	92.09%	0.1837

Table 7.4 – Architectures des réseaux hybrides et pourcentages de précision pour chaque taille de système quantiques, pour le problème de classification des états dégénérés et non-dégénérés.

En Table 7.5 nous présentons les résultats pour les $2 \times 2 \times 2$, $2^{\times 4}$, $2^{\times 5}$, et $3 \times 3 \times 3$ avec des réseaux LeakyReLU. Dans le cas $2 \times 2 \times 2$, nous avons utilisé un ensemble d'entraînement de taille 502600, un ensemble de validation de taille 55600 et un ensemble de test de 32000. Dans les cas $2^{\times 4}$ et $2^{\times 5}$, nous avons utilisé un ensemble d'entraînement de taille 252400, un ensemble de validation de taille 55600 et un ensemble de test de 52000. Dans le cas $3 \times 3 \times 3$, nous avons utilisé un ensemble d'entraînement de taille 352400, un ensemble de validation de taille 55600 et un ensemble de test de 52000. Nous atteignons une précision moyenne de 96% pour les ensembles de test pour le problème de classification des états dégénérés.

Système	Architecture	Entraînement	Validation	Test	Erreur
$2 \times 2 \times 2$	(100,50,25,16,1)	93.44%	92.53%	92.74%	0.1629
$2^{\times 4}$	(200,100,50,16,1)	99.50%	95.95%	95.94%	0.01791
$2^{\times 5}$	(100,50,25,16,1)	99.95%	98.74%	98.83%	0.001533
$3 \times 3 \times 3$	(100,50,25,16,1)	98.18%	96.78%	96.83%	0.04770

Table 7.5 – Architectures des réseaux LeakyReLU et pourcentages de précision pour chaque taille de système quantiques, pour le problème de classification des états dégénérés et non-dégénérés.

Les résultats obtenus sont assez intéressants, notamment dans le cas des 5-qubits. En effet, comme mentionné précédemment, il n'existe pas d'expression explicite de l'hyperdéterminant de taille $2^{\times 5}$, principalement à cause des complications en termes de calcul. Le réseau de neurone montre des pourcentages de précision intéressants lorsqu'ils sont évalués sur les ensembles de tests. Ceci implique que nous pouvons déterminer avec une assurance assez forte si un tenseur généré de la même manière que nos ensembles de données est dégénéré ou non, ce qui est équivalent à déterminer si l'hyperdéterminant s'annule ou non.

Dans le contexte d'une caractérisation qualitative de l'intrication, il est suffisant de savoir si l'hyperdéterminant s'annule ou non, la valeur en elle même n'est pas utile. De ce fait, nous proposons alors une méthode originale pour l'évaluation de la nullité de

l'hyperdéterminant pour des tenseurs réels de taille $2^{\times 5}$. Nous utilisons cette méthode pour étudier l'intrication de certains états à 5-qubits générés de manière différente en Section 7.5.3.

7.4.4 Classification du rang et rang de bord

Nous rappelons qu'un état $|\varphi\rangle \in \mathcal{H}^{\otimes n}$ est dit de rang $\leq R$ s'il existe une expression de cet état telle que $|\varphi\rangle = \sum_{r=1}^{R} \lambda_i |\varphi_i\rangle$ avec $\lambda_i \in \mathcal{H}$ et $|\varphi_i\rangle \in \mathcal{H}^{\otimes n}$ [57]. Il est connu que lorsque $n > 2$ le rang n'est pas une condition fermée, et n'est pas semi-continu. Le premier exemple est celui des 3-qubits, où l'état $|W\rangle$ est de rang, et appartient à la fermeture de l'orbite générique de $|GHZ\rangle$, qui lui est de rang 2 [135] (voir Section 2.1.6).

Dans un autre contexte, Bini définit la notion de rang de bord (voir Section 2.1.6) pour retrouver la prioriété de semi-continuité. On rappelle qu'un état $|\varphi\rangle \in \mathcal{H}^{\otimes n}$ est de rang de bord $\leq R$ s'il existe une famille d'états de rang R $\{|\varphi^\epsilon\rangle \mid \epsilon > 0\}$ et $\lim_{\epsilon \to 0} |\varphi^\epsilon\rangle = |\varphi\rangle$. De manière équivalente, l'ensemble des états de rang de bord $\leq R$, noté σ_R (pour la variété des sécantes d'ordre R) est la fermeture de Zariski des états de rang $\leq R$.

Par construction, lorsque $\mathcal{H} = \mathbb{C}^d$, nous avons la chaîne

$$\sigma_1 \subsetneq \sigma_2 \subsetneq \cdots \subsetneq \sigma_g = \mathcal{H}^{\otimes n} \ , \tag{7.17}$$

qui se termine à $\mathcal{H}^{\otimes n}$, car l'ensemble des états séparable est linéairement non-dégénéré dans $\mathcal{H}^{\otimes n}$. Le plus petit entier g pour lequel la variété des sécantes $\sigma_g = \mathcal{H}^{\otimes n}$ remplit l'espace est appelé le *rang générique*. Par un calcul de dimensions on obtient la valeur attendue du rang générique, notée e, qui est :

$$e = \left\lceil \frac{d^n}{n(d-1)+1} \right\rceil \ . \tag{7.18}$$

Le seul cas connu pour lequel des tenseurs de taille $d^{\times n}$ ont un rang générique qui diffère du rang générique attendu est le cas $d = 3, n = 3$, ce qui correspond aux états à 3-qutrits, pour lesquels le rang générique est 5 au lieu de 4. Dans le cas $d = 2, n = 4$ qui correspond aux 4-qubits, le rang générique est bien celui attendu, qui est de 4, même s'il est connu que l'ensemble des tenseurs de rang 3 est défectif (la dimension n'est pas celle attendue). Il est conjecturé que ces deux cas sont les seuls [24, 2, 69].

Soit σ_s° la variété des états de rang égal exactement à s. Lorsque $\mathcal{H} = \mathbb{R}^d$, il peut exister plus d'un ensemble semi-algébrique σ_s° qui est de dimension maximale. On utilise alors l'appellation de *typical ranks*, ou rang typiques. En posant μ une probabilité de mesure sur $\mathcal{H}^{\otimes n}$, alors la mesure de σ_s° représente la probabilité qu'un état aléatoire ait un rang égal à s.

Nous nous proposons d'illustrer la situation des rangs typiques pour les tenseurs réels à travers un exemple tiré de [82].

Exemple 15. Nous nous plaçons dans le cas $n = 3$, $d = 2$ des 3-qubits réels, pour lequel les rangs 2 et 3 sont tout deux des rangs typiques. L'hyperdéterminant $2 \times 2 \times 2$ de Cayley Det_{222} sépare $\mathbb{R}^{2\times 2\times 2}$ en plusieurs régions de rang typique constant.

Nous construisons un ensemble d'échantillons de tenseurs réels de rang au plus égal à 3 comme suit. Nous construisons des états de rang 1 par produit tensoriel de trois vecteurs dont les entrées sont uniformément distribuées $[-.5, .5]$, puis nous renormalisons. Nous prenons ensuite la somme de 3 de ces vecteurs de rang 1 et nous renormalisons à nouveau. Pour une telle distribution de tenseurs, nous obtenons les fréquences suivantes :

1. avec une fréquence approximative de 86.6% $Det_{222}(\varphi) > 0$, qui dans ce cas correspond à un $\mathbb{R}$-rang de 2,
2. avec une fréquence approximative de 13.4% $Det_{222}(\varphi) < 0$, qui dans ce cas correspond à un $\mathbb{R}$-rang de 3,
3. avec une fréquence de 0% $Det_{222}(\varphi) = 0$, où dans ce cas le $\mathbb{R}$-rang peut être de 0, 1, 2 ou 3. ♢

Construction des réseaux et des tenseurs

Dans la construction des classifieurs pour le problème du rang, nous distinguons deux problèmes de classification : pour le cas des 3-qubits, nous nous intéressons uniquement à la classification du rang exact ; pour les autres cas, nous cherchons à classifier le rang de bord des états en entrée.

Ces problèmes de classification sont des problèmes multi-classes, contrairement aux deux problèmes de classification binaires présentés précédemment. Le nombre de classes correspond au nombre de rangs possibles, et la couche de sortie possédera alors le nombre de neurones correspondant au nombre de classes. Comme un tenseur n'a qu'une valeur unique de rang, alors chaque état en entrée n'appartiendra qu'à une unique classe (représentant une valeur de rang ou de rang de bord précise), et donc on ne pourra cumuler l'appartenance à plusieurs classes, et ceci déterminera aussi la fonction d'activation à choisir pour la couche de sortie (fonction d'activation SoftMax ici).

Dans le cas $2 \times 2 \times 2$, nous entraînons les réseaux de neurones pour reconnaître le rang exact des tenseurs. En effet, pour construire la base de données d'entraînement, nous générons alors des tenseurs de rang 1 comme cela a été fait pour la variété de Segre. Nous générons des tenseurs SLOCC équivalents aux états biséparable et $|GHZ\rangle$ pour constituer les états de rang 2. Nous générons des tenseurs SLOCC équivalents à l'état $|W\rangle$ pour les tenseurs de rang 3, conformément à la classification des 3-qubits. Nous avons également pris en compte les spécificités liées au cas des tenseurs réels, plus précisément le rang typique (voir Exemple 15) et nous avons utilisé le signe de l'hyperdéterminant Det_{222} afin de générer des tenseurs de rang 2 et 3, à partir de la somme de 3 tenseurs aléatoires de rang 1.

Dans les cas $2^{\times 4}$ et $2^{\times 5}$, nous générons les tenseurs de chaque classe 'k' en prenant la somme de $k+1$ tenseurs de rang 1 (puis en renormalisant). La classe '0' correspond aux tenseurs de rang 1, alors que la classe 'r' correspond aux tenseurs avec un rang de bord $r+1$. L'ensemble des données d'entraînement est subdivisé de manière équilibrée, de telle sorte que nous avons le même nombre d'échantillons pour chaque classe. Dans le cas $2^{\times 4}$, nous générons des tenseurs jusqu'à un rang de bord de 4, et pour le cas $2^{\times 5}$ jusqu'à un rang de bord de 5. En utilisant cette manière de générer les états de chaque

classe, nous introduisons du bruit dans les données, et plus particulièrement dans le cas réel (comparé au cas complexe), comme suggéré dans l'Exemple 15, où la somme de 3 tenseurs aléatoires de rang 1 donne le plus souvent un tenseur de rang 2 (et donc de rang de bord 2).

Résultats et génération des tenseurs

Dans la Table 7.6 nous présentons les résultats pour le problème de classification du rang pour les états à 3-qubits avec les réseaux de neurones hybrides. Nous utilisons une base de données d'entraînement de taille 102400, une base de validation de taille 102400 et une base de test de taille 32000. Nous atteignons une fiabilité de 87% pour l'ensemble des données de test.

Système	Architecture	Entraînement	Validation	Test	Erreur
$2 \times 2 \times 2$	(169,25,3)	88.19%	88.03%	87.95%	0.3028

TABLE 7.6 – Architectures des réseaux hybrides et pourcentage de fiabilité pour les systèmes à 3-qubits, pour le problème de classification du rang.

Dans la Table 7.7 nous présentons les résultats pour classification du rang pour le cas $2 \times 2 \times 2$, et pour la classification du rang de bord pour les cas $2^{\times 4}$ et $2^{\times 5}$, à l'aide de réseaux de neurones LeakyReLU. Pour le cas $2 \times 2 \times 2$, nous utilisons une base de données d'entraînement de taille 502500, une base de validation de taille 55600 et une base de test de taille 52000. Pour les cas $2^{\times 4}$ et $2^{\times 5}$, nous utilisons respectivement une base de données d'entraînement de taille 502400 et 802400, une base de validation de taille 55600 et une base de test de taille 52000.

Système	Architecture	Entraînement	Validation	Test	Erreur
$2 \times 2 \times 2$	(200,100,50,25,3)	94.19%	94.07%	93.79%	0.1674
$2^{\times 4}$	(200,100,50,25,3)	85.49%	84.45%	84.47%	0.3144
$2^{\times 5}$	(200,100,50,25,3)	81.39%	79.88%	79.77%	0.4230

TABLE 7.7 – Architectures des réseaux LeakyReLU et pourcentage de fiabilité pour chaque taille de système, pour le problème de classification du rang et du rang de bord.

Nous observons que, même en présence de bruit dans les données, le réseau de neurones est tout de même capable d'apprendre et de prédire le rang de bord des états avec une fiabilité plus ou moins intéressant (84% pour les 4-qubits, 80% pour les 5-qubits) pour les données de test générées selon le même processus. Les résultats peuvent ne pas être aussi élevés pour des états extérieurs non générés selon le même processus. Néanmoins, les réseaux peuvent tout de même produire des résultats intéressants pour certains états quantiques (voir Section 7.5.3 pour un exemple avec l'état $|W\rangle$). Cette manière de générer les tenseurs réels d'un certain rang de bord constitue une des pistes d'amélioration de notre travail proposée en Section 7.6.

7.5 Étude de cas – Prédictions et classification

7.5.1 Prédictions pour un état quantique

Tout au long de ce chapitre, nous nous sommes intéressés à l'intrication du point de vue qualitatif. Les propriétés de séparabilité, dégénérescence et la notion de rang sont invariants par action du groupe SLOCC [135]. Par conséquent, nos classifieurs doivent théoriquement répondre la même chose pour des états SLOCC équivalents.

Cependant, la fiabilité de nos classifieurs, issus d'un entraînement de réseau de neurones, n'est jamais de 100%, et de ce fait, la probabilité de ne pas classifier correctement un état en entrée est non nulle, ce qui donne peu de poids à une unique évaluation du réseau pour déterminer la classe. Afin de significativement réduire la proportion d'erreur dans la classification d'un état donné, nous proposons de générer un ensemble d'états SLOCC équivalents à notre état donné, et d'observer la réponse la plus fréquente donnée par le réseau de neurone. Toutes les réponses peuvent être regroupées sur la forme d'un histogramme, afin de fournir une représentation graphique de la distribution des sorties du réseau de neurones.

7.5.2 Classification des 3-qubits

Le cas des 3-qubits est le premier cas historiquement à illustrer l'existence d'états intriqués non-équivalents, à savoir les états $|GHZ\rangle$ et $|W\rangle$ [87]. La classification des 3-qubits est rappelée en Section 2.2.2, et nous présentons en Table 2.1 les représentants de chaque orbite. La connaissance du rang et de la nullité de l'hyperdéterminant permet de distinguer les différentes classes d'intrication des systèmes purs à 3-qubits.

De ce fait, nos classifieurs développés en Section 7.4 peuvent être utilisés afin de déterminer l'appartenance d'un état donné à une classe d'intrication pour les 3-qubits. En effet, les états séparables peuvent être détectés à l'aide du classifieur binaire reconnaissant les tenseurs de la variété de Segre, présenté en Section 7.4.2. Tous les états SLOCC équivalents à l'état $|GHZ\rangle$ correspondent aux états non-dégénérés, et peuvent alors être reconnus en utilisant le classifieur binaire pour les tenseurs de la variété duale de la variété de Segre, présenté en Section 7.4.3. Enfin, pour distinguer les états biséparables des états équivalents à $|W\rangle$, nous exploitons l'information du rang des tenseurs, en utilisant le classifieur de rang, présenté en Section 7.4.4, afin de distinguer les tenseurs de rang 2 et de rang 3. Tous les résultats sont regroupés dans les Figures 7.10, 7.11, 7.12, 7.13.

7.5.3 Intrication de systèmes à 5-qubits

Dans le cas des 5-qubits, comme aucune classification complète ou dépendant de paramètres n'est connue, différencier et distinguer différentes classes d'intrication est une tâche très difficile. Quelques travaux présents dans la littérature ont cherché comment caractériser l'intrication, en utilisant des filtres [208] ou des polynômes invariants [181]. Dans ces travaux, quatre états à 5-qubits sont étudiés, et nous les noterons $|\Phi_1\rangle$, $|\Phi_2\rangle$, $|\Phi_3\rangle$, et $|\Phi_4\rangle$ (voir Équations 7.19, 7.20, 7.21, 7.22).

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}\left(|00000\rangle + |11111\rangle\right) \ , \tag{7.19}$$

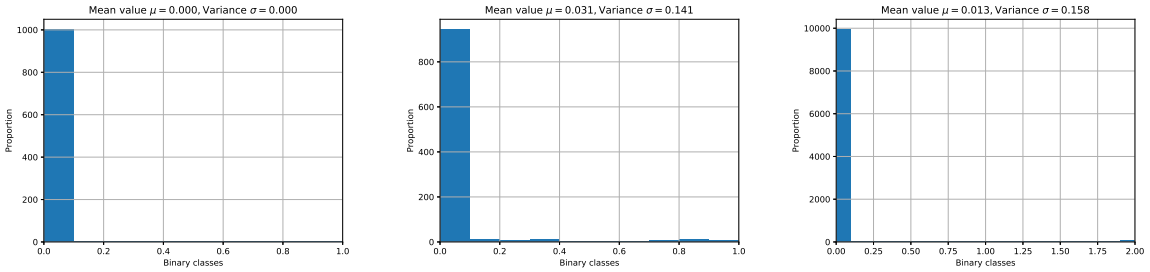


FIGURE 7.10 – Représentation sous forme d'histogramme des résultats de prédiction, pour l'état séparable $|000\rangle$ en entrée, pour les 3 classifieurs suivants (dans l'ordre, de gauche à droite) : séparabilité, dégénérescence et rang. Le graphique de gauche montre que l'état est bien séparble (classe '0'), en générant 1000 états SLOCC équivalents. Le graphique du milieu montre que l'état est dégénéré (classe '0'), en générant 1000 états équivalents. Le graphique de droite montre que l'état est de rang 1 (classe '0'), en générant 10000 états équivalents.

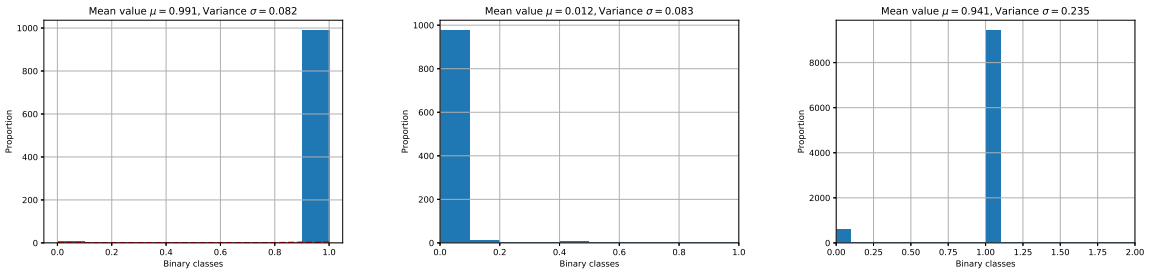


FIGURE 7.11 – Représentation sous forme d'histogramme des résultats de prédiction, pour l'état biséparable $\frac{1}{\sqrt{2}}(|000\rangle + |011\rangle)$ en entrée, pour les 3 classifieurs suivants (dans l'ordre, de gauche à droite) : séparabilité, dégénérescence et rang. Le graphique de gauche montre que l'état est intriqué (classe '1'), en générant 1000 états SLOCC équivalents. Le graphique du milieu montre que l'état est dégénéré (classe '0'), en générant 1000 états équivalents. Le graphique de droite montre que l'état est de rang 2 (classe '1'), en générant 10000 états équivalents.

$$|\Phi_2\rangle = \frac{1}{2}\left(|11111\rangle + |11100\rangle + |00010\rangle + |00001\rangle\right) \ , \tag{7.20}$$

$$|\Phi_3\rangle = \frac{1}{\sqrt{6}}\left(\sqrt{2}|11111\rangle + |11000\rangle + |00100\rangle + |00010\rangle + |00001\rangle\right) \ , \tag{7.21}$$

$$|\Phi_4\rangle = \frac{1}{2\sqrt{2}}\left(\sqrt{3}|11111\rangle + |10000\rangle + |01000\rangle + |00100\rangle + |00010\rangle + |00001\rangle\right) \ . \tag{7.22}$$

Ces états n'appartiennent pas à la même classe d'intrication, comme cela a été montré dans [208, 181]. Cependant, nous pouvons toujours nous demander si ces états sont dégénérés ou non, par exemple. Nous avons utilisé notre classifieur d'états dégénérés pour les 5-qubits afin d'étudier cette question. Il en ressort que pour tous ces états, le réseau de neurones répond la classe '0', ce qui implique que ces états sont dégénérés, et donc que l'hyperdéterminant s'annule. Les évaluations du réseaux de neurones sont représentées en Figure 7.14.

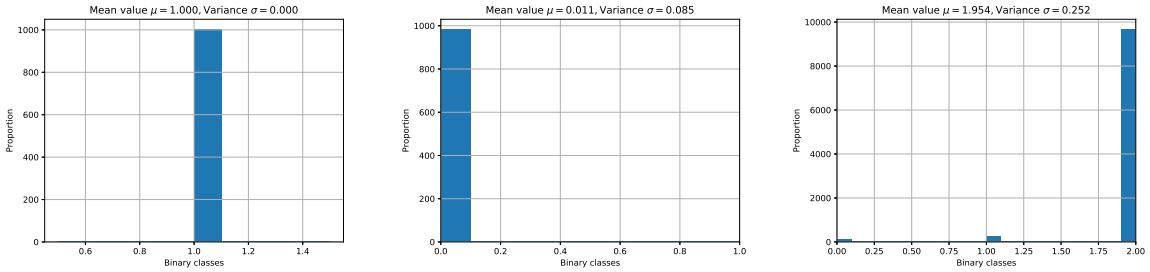


Figure 7.12 – Représentation sous forme d'histogramme des résultats de prédiction, pour l'état $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ en entrée, pour les 3 classifieurs suivants (dans l'ordre, de gauche à droite) : séparabilité, dégénérescence et rang. Le graphique de gauche montre que l'état est intriqué (classe '1'), en générant 1000 états SLOCC équivalents. Le graphique du milieu montre que l'état est dégénéré (classe '0'), en générant 1000 états équivalents. Le graphique de droite montre que l'état est de rang 3 (classe '2'), en générant 10000 états équivalents.

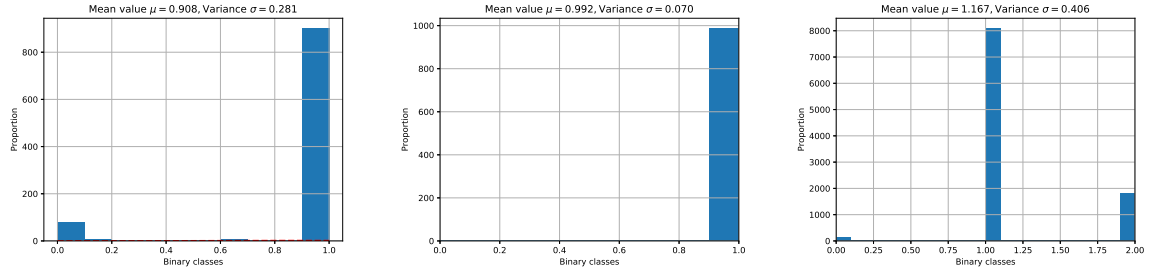


Figure 7.13 – Représentation sous forme d'histogramme des résultats de prédiction, pour l'état $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ en entrée, pour les 3 classifieurs suivants (dans l'ordre, de gauche à droite) : séparabilité, dégénérescence et rang. Le graphique de gauche montre que l'état est intriqué (classe '1'), en générant 1000 états SLOCC équivalents. Le graphique du milieu montre que l'état est non-dégénéré (classe '0'), en générant 1000 états équivalents. Le graphique de droite montre que l'état est de rang 2 (classe '1'), en générant 10000 états équivalents.

D'autre part, nous pouvons aussi proposer des états à 5-qubits non-dégénérés à l'aide de notre classifieur. Par exemple, les états $|\delta_1\rangle$ et $|\delta_2\rangle$ (voir Équations 7.23 et 7.24) sont non-dégénérés, et ceci est confirmé par les résultats des prédictions du classifieur. Ces résultats sont présentés en Figure 7.15. La propriété de non-dégénérescence de ces états peut aussi être confirmée à l'aide de l'étude des singularités des hypersurfaces associées à ces deux états, comme cela est développé en Chapitre 5, et nous l'utilisons afin de valider cet exemple.

$$|\delta_1\rangle = \frac{1}{\sqrt{14}}\big(|00000\rangle + \sqrt{3}|00011\rangle + |00100\rangle + |01000\rangle + |01001\rangle + \sqrt{2}|01111\rangle + |10001\rangle + |10110\rangle + |11000\rangle + |11011\rangle + |11101\rangle\big)\ , \tag{7.23}$$

$$|\delta_2\rangle = \frac{1}{\sqrt{11}}\big(|00000\rangle + |00100\rangle + |00111\rangle + |01010\rangle - |01101\rangle + |10001\rangle + |10011\rangle + |10111\rangle - |11000\rangle + |11110\rangle\big)\ . \tag{7.24}$$

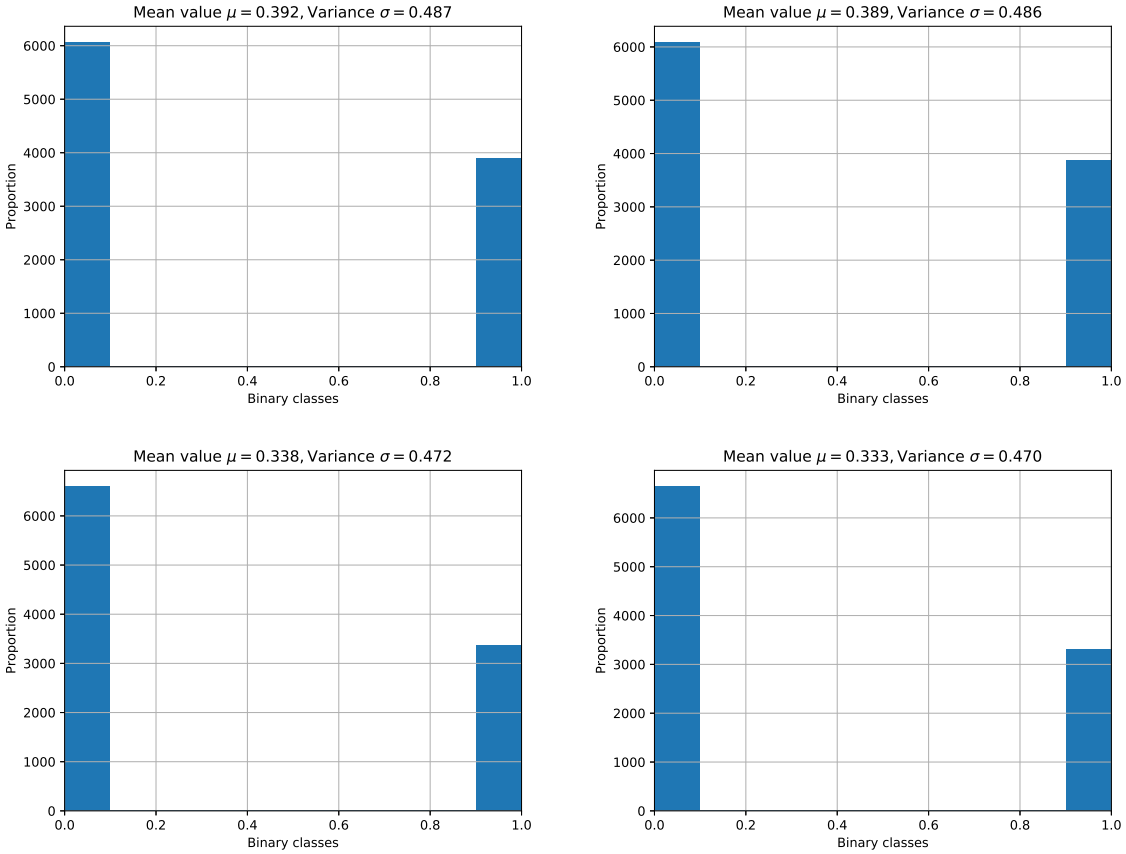


FIGURE 7.14 – Représentation sous forme d'histogramme des résultats de prédiction du classifieur d'états dégénérés pour les quatre états $|\Phi_1\rangle$, $|\Phi_2\rangle$, $|\Phi_3\rangle$ et $|\Phi_4\rangle$. Le graphique en haut à gauche correspond à l'état $|\Phi_1\rangle$, celui en haut à droite à l'état $|\Phi_2\rangle$, et celui en bas droite à l'état $|\Phi_4\rangle$. Sur les axes horizontaux, la classe '0' représente les états dégénérés, alors que la classe '1' réfère aux états non-dégénérés. Dans ce cas, tous les états sont dégénérés, et 10000 points SLOCC équivalents ont été générés pour chacun des états $|\Phi_i\rangle$.

Enfin, le classifieur du rang de bord développé pour les états à 5-qubits pourrait également servir à différencier certains états du point de vue de l'intrication. À titre d'exemple, si on évalue le réseau de neurones avec en entrée l'état $|W_5\rangle = \frac{1}{\sqrt{5}}(|00001\rangle + |00010\rangle + |00100\rangle + |01000\rangle + |10000\rangle)$ nous obtenons comme réponse la plus fréquence la classe '1' (voir Figure 7.16), ce qui correspond à la classe des tenseurs de rang de bord 2, comme attendu.

Ces outils peuvent s'avérer utile en l'absence de l'expression exacte des polynômes définissant les variétés, ou en absence d'outils pour la détermination du rang. Typiquement, dans le cas des 5 qubits, il n'est pas connu d'expression pour l'hyperdéterminant mais nous pouvons néanmoins proposer une réponse (plus ou moins précise) de l'annulation ou non de l'hyperdéterminant pour certains tenseurs. De même, comme observé pour l'état $|W_5\rangle$, nos outils peuvent aider à estimer le rang de bord de certains

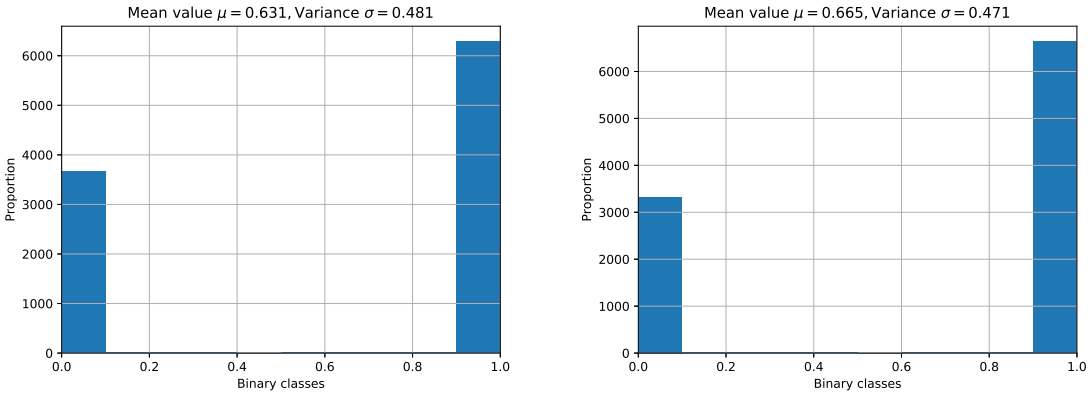


Figure 7.15 – Représentation sous forme d'histogramme des résultats de prédiction du classifieur d'état dégénérés pour les états $|\delta_1\rangle$ et $|\delta_2\rangle$. Le graphique de gauche concerne à l'état $|\delta_1\rangle$, et celui de droite à l'état $|\delta_2\rangle$. Sur les axes horizontaux, la classe '0' représente les états dégénérés, alors que la classe '1' réfère aux états non-dégénérés. Dans ce cas, les états sont non-dégénérés, et 10000 points SLOCC équivalents ont été générés pour chacun des états.

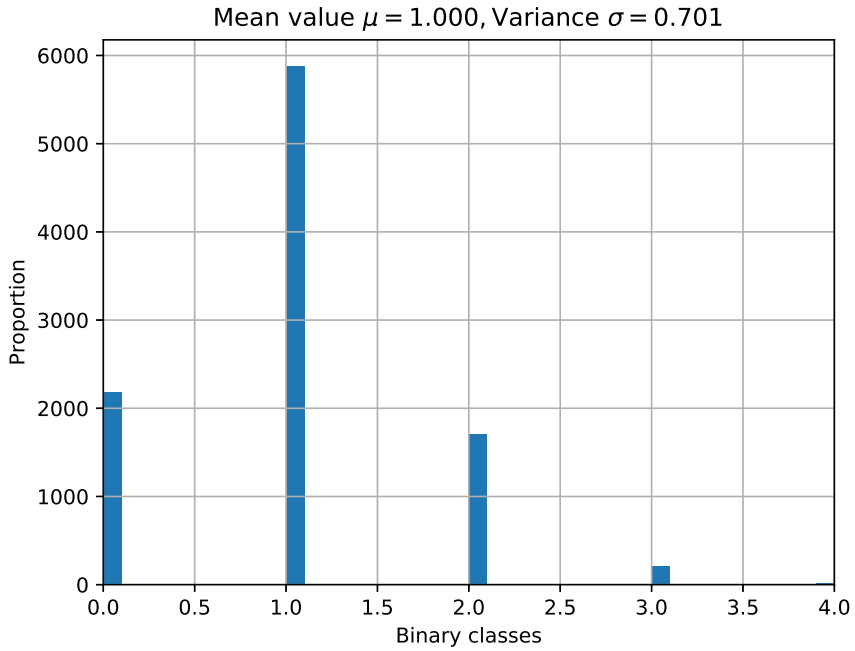


Figure 7.16 – Représentation sous forme d'histogramme des résultats de prédiction du classifieur de rang de bord pour l'état $|W_5\rangle$. L'histogramme montre que la réponse la plus obtenue est un rang de bord égal à 2 (classe '1'), avec 10000 points SLOCC équivalents générés.

tenseurs. Nous espérons, en les construisant selon la même approche, que ces outils puissent également être utiles en dimensions supérieures, là où les problèmes considérés sont d'autant plus difficiles à résoudre.

7.6 Perspectives

Dans cette section nous proposons un certain nombre de pistes d'amélioration et de perspectives pour le travail présenté dans ce chapitre.

7.6.1 Architecture hybride

Il pourrait être possible de pousser plus loin l'idée d'exploiter les PNN (polynomial neural networks) pour modéliser des équations polynomiales et des variétés algébriques, afin d'améliorer la structure actuelle des réseaux hybrides proposés en Section 7.3.6. En effet, l'architecture actuelle est limitée par le fait que le nombre de neurones nécessaire en première couche augmente très rapidement avec le degré et le nombre de variables. Comme le nombre de variables en entrée varie exponentiellement quand le nombre de qubits augmente, la limite peut vite être atteinte.

Une idée serait de choisir des fonctions d'activation utilisant des polynômes plus complexes que de seulement élever à la puissance d la somme pondérée en entrée. Cela pourrait éventuellement permettre d'ajouter un certain nombre de monômes en sortie, sans pour autant augmenter le nombre de neurones. On cherchera alors aussi à établir un résultat permettant de déterminer le nombre de neurones nécessaires dans la première couche.

Il est aussi possible d'ajouter plusieurs couches de neurones à la fonction d'activation d'élévation à un certain degré ou un polynôme plus complexe, comme discuté en Section 7.3.4, dans le cas où le degré du polynôme à modéliser se décompose en produit de plusieurs entiers. Comme la limitation actuelle concerne la largeur du réseau, il peut être judicieux d'envisager une déclinaison en profondeur de l'approche actuelle.

7.6.2 Génération des données

La qualité des données utilisées pour entraîner un réseau de neurone est un critère important dans la réussite du processus d'apprentissage. Nous pouvons encore améliorer la manière dont on génère les états de certaines classes, et tenter d'uniformiser d'avantage l'échantillonnage des tenseurs.

Dans le cas des tenseurs dégénérés, nous utilisons un tenseur vérifiant les conditions $\varphi_I = 0$ comme expliqué en Section 7.4.3 puis appliquons des changements de base locaux pour générer des états SLOCC équivalents et donc dégénérés également. Ceci ne prend pas en compte toute la variété possible des états dégénérés, notamment car il est possible d'avoir des zéros présents à d'autres endroits de l'hypermatrice représentant le tenseur, et c'est un aspect que nous n'avions pas pris en compte lors de la génération des états dégénérés. Ceci permettrait notamment d'améliorer les résultats des classifieurs pour la variété duale, et de produire une réponse encore plus confirmée de la classe en sortie du réseau.

Dans la question de génération de tenseurs d'un certain rang, ou rang de bord, la sommation de tenseurs de rang aléatoires de rang 1 est une manière assez intuitive de procéder, mais introduit un bruit non négligeable dans le cas réel notamment, comme

discuté pour le cas des 3-qubits. Il faudra alors étudier différentes solutions pour avoir un meilleur contrôle sur le rang ou le rang de bord effectif des états générés. Une solution possible est de partir d'un ensemble d'états pour lesquels on connaît le rang ou le rang de bord, de par des travaux précédents par exemple, puis de générer des états équivalents par opérateur SLOCC aléatoire. Cette méthode n'assurera pas une uniformisation des échantillons pour un rang ou rang de bord donné, mais permettrait une réduction considérable du bruit dans les données. Une solution envisageable est de passer au cas complexe, afin de réduire ce phénomène lié au rang typique, et constitue notamment la prochaine perspective présentée.

7.6.3 Tenseurs complexes

Nous avons utilisé dans ce travail uniquement des tenseurs aux coefficients réels pour une première approche et une implémentation plus aisée. Une manière de poursuivre ce travail serait de se déplacer vers le cas des complexes, plus proche du contexte d'étude en théorie de l'information quantique. Cela permettrait également d'utiliser d'autres résultats de géométrie algébrique concernant le rang des tenseurs complexes, comme suggéré en sous-section précédente.

Il n'est pas évident que l'outil Keras puisse travailler directement avec des entrées et poids complexes, et cela pourrait notamment poser problème durant la phase d'apprentissage où les algorithmes d'optimisation et les méthodes de différentiation ne sont peut être pas adaptés.

7.6.4 Dimensions plus élevées

Il pourrait être intéressant d'étudier dans quelle mesure notre approche actuelle peut se généraliser aux dimensions supérieures, et quelles peuvent être les performances pour les différents problèmes de classification.

Pouvoir décider rapidement de la séparabilité d'états purs à 20-qubits par exemple, pourrait éventuellement s'avérer utile, et pourrait être comparé à la performance des techniques actuelles de détection des tenseurs de rang 1. Aussi, la question d'évaluation de la nullité de l'hyperdéterminant pour des tenseurs de taille importante pourrait intéresser la communauté de la géométrie algébrique, compte tenu de la difficulté d'établir une méthode d'évaluation ou d'expression de ce polynôme pour des dimensions et degrés élevés. Enfin, dans l'éventualité où l'approche utilisée pour classifier le rang est améliorée et contrôlée pour toute dimension, cela pourrait également permettre une grande avancée sur la question, permettant éventuellement de déterminer le rang de tenseurs liés au produit matriciel, ou de vérifier des conjectures sur le rang supposé de certains tenseurs.

7.6.5 Réseaux de neurones convolutifs

Une évolution possible de ce travail est de considérer d'autres modèles de réseaux de neurones pour résoudre les différents problèmes de classification considérés.

Une solution possible est donnée par les réseaux de neurones convolutifs, majoritairement utilisés dans la littérature pour l'analyse d'images et la reconnaissance de formes, car permettant de capturer des propriétés locales et de les combiner. Cela permettrait notamment de pouvoir étudier localement un état, tout en tentant de garder une information sur son aspect global de l'état, ce qui pourrait mieux mettre en évidence l'intrication dans ces états.

7.6.6 Autres algorithmes de Machine Learning

D'autre part, il est possible d'envisager d'autres algorithmes supervisés pour exploiter notre possibilité de générer des tenseurs de certaines variétés algébriques liées à la notion d'intrication. Des algorithmes tels que les *Support Vector Machine* ou les *Decision Trees* peuvent être exploités avant de classifier et de séparer l'espace des tenseurs en différentes classes à partir des données d'apprentissage. Une interprétation du problème d'apprentissage des variétés algébriques comme un problème de régression, au lieu d'un problème de classification, pourrait également nous permettre de nous diriger vers une autre direction à l'aide d'autres outils d'apprentissage supervisé.

Aussi, il est possible d'utiliser une approche non-supervisée afin de regrouper les différents tenseurs par groupe. Il serait intéressant si les algorithmes de type *K plus proches voisins* ou *Analyse en Composantes Principales* permettraient de faire émerger naturellement des clusters ou groupes de tenseurs correspondant justement aux différentes classes d'intrication, ou valeur de rang par exemple, puis de comparer et d'évaluer ce regroupement à partir des données pour lesquelles nous avons une classification correcte ou connue.

Enfin, l'approche d'apprentissage par renforcement ne semble peut être pas la plus adaptée à notre problème de classification, mais on pourrait tout de même imaginer un processus de classification par *trial/errors*, auquel on associerait une fonction récompense permettant de guider la machine vers une classification correcte. Aussi, cette approche peut être utilisée afin de construire des états maximalement intriqués, en définissant la fonction gain comme une mesure de l'intrication ou de la non-localité (entropie, polyômes de Mermin, hyperdéterminant ou invariants, mesure géométrique de l'intrication, ...) et en permettant à la machine de réaliser diverses actions locales et globales (portes à contrôles par exemple, Transformée de Fourier Quantque, etc.) sur les états quantiques jusqu'à arriver à un potentiel état maximalement intriqué.

Annexe A

Implémentations informatiques

Dans ce chapitre d'annexes, nous renseignons les différents algorithmes et codes utilisés pour mener à bien les calculs nécessaires à l'établissement des résultats présentés durant cette thèse. Ceci afin de permettre notamment la reproduction et la poursuite de nos travaux. Nous présentons alors, lorsque cela est pertinent, les algorithmes utilisés et nous renvoyons dans d'autres cas vers un répertoire en ligne (Github) permettant d'avoir directement accès au code Java, Maple ou Python.

A.1 Classification des 3-qubits

Nous renvoyons le lecteur à la Section 2.2.2 pour un rappel de la classification des 3-qubits. Nous présentons ci-dessous l'ensemble des polynômes covariants et invariants, ainsi que l'algorithme, utilisé pour la classification des 3-qubits. Le lecteur pourra retrouver un exemple d'implémentation en langage Maple au lien suivant : `https://github.com/hjaffali/annexes-these/tree/master/classification%20de%20l'intrication/2x2x2`.

Tout système à 3-qubits $|\psi\rangle \in \mathcal{H}_3 = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ peut s'écrire dans la base canonique sous la forme :

$$|\Psi\rangle = \sum_{i,j,k \in [\![0,1]\!]} a_{ijk} \, |ijk\rangle, \tag{A.1}$$

On rappelle qu'à chaque état à 3-qubits on peut associer une forme tri-linéaire que l'on notera A :

$$A = \sum_{i,j,k \in [\![0,1]\!]} a_{ijk} \cdot x_i y_j z_k \ . \tag{A.2}$$

On définit trois polynômes covariants $B_x(x)$, $B_y(y)$ et $B_z(z)$, formes quadratiques, comme suit :

$$B_x(x) = \det \left(\frac{\partial^2 A}{\partial y_j \partial z_k} \right)_{0 \leq j,k \leq 1} , \tag{A.3}$$

$$B_y(y) = \det \left(\frac{\partial^2 A}{\partial x_i \partial z_k} \right)_{0 \leq i,k \leq 1} , \tag{A.4}$$

$$B_z(z) = \det\left(\frac{\partial^2 A}{\partial x_i \partial y_j}\right)_{0\leq i,j\leq 1} . \tag{A.5}$$

On définit également le covariant $C(x, y, z)$ par :

$$C(x, y, z) = \begin{vmatrix} \frac{\partial A}{\partial x_0} & \frac{\partial A}{\partial x_1} \\ \frac{\partial B_x}{\partial x_0} & \frac{\partial B_x}{\partial x_1} \end{vmatrix} . \tag{A.6}$$

Enfin, nous rappelons l'expression de l'hyperdéterminant de Cayley Δ_{222} :

$$\begin{aligned} \Delta_{222}(|\Psi\rangle) = a_{000}^2 a_{111}^2 + a_{001}^2 a_{110}^2 + a_{010}^2 a_{101}^2 + a_{100}^2 a_{011}^2 \\ -2a_{000}a_{001}a_{110}a_{111} - 2a_{000}a_{010}a_{101}a_{111} - 2a_{000}a_{011}a_{100}a_{111} \\ -2a_{001}a_{010}a_{101}a_{110} - 2a_{001}a_{011}a_{110}a_{100} - 2a_{010}a_{011}a_{101}a_{100} \\ +4a_{000}a_{011}a_{101}a_{110} + 4a_{001}a_{010}a_{100}a_{111} . \end{aligned} \tag{A.7}$$

À l'aide de ces covariants et invariants, nous pouvons construire un vecteur V défini dans l'Équation A.8. Lorsque la valeur du polynôme est non nulle, on la remplace par la valeur 1 dans le vecteur d'évaluation. Ainsi, les éléments du vecteur V ne prendront que des valeurs binaires.

$$V = [B_x, B_y, B_z, C, \Delta_{222}] . \tag{A.8}$$

Nous présentons à présent l'Algorithme 3 de classification des états à 3-qubits :

Algorithme 3 Classification3qubits [135]

Require: Y un vecteur de taille 8, représentant l'état à 3-qubit
Ensure: Classe d'intrication associée à Y

vectCov $\leftarrow [B_x, B_y, B_z, C, \Delta_{222}]$
eval $\leftarrow$ evaluer(vectCov,Y)
if eval $= [0, 0, 0, 0, 0]$ **then**
  retourner $\mathcal{O}_1$
else if eval $= [0, 1, 0, 0, 0]$ **then**
  retourner $\mathcal{O}_2$
else if eval $= [1, 0, 0, 0, 0]$ **then**
  retourner $\mathcal{O}_3$
else if eval $= [0, 0, 1, 0, 0]$ **then**
  retourner $\mathcal{O}_4$
else if eval $= [1, 1, 1, 1, 0]$ **then**
  retourner $\mathcal{O}_5$
else if eval $= [1, 1, 1, 1, 1]$ **then**
  retourner $\mathcal{O}_6$
end if

A.2 Classification des systèmes à $2 \times 2 \times 3$

Nous renvoyons le lecteur à la Section 3.3.2 pour un rappel de la classification des systèmes quantiques de taille $2 \times 2 \times 3$, ainsi que vers [135] pour une définition

des invariants et covariants. Le lecteur pourra retrouver un exemple d'implémentation en langage Maple au lien suivant : https://github.com/hjaffali/annexes-these/tree/master/classification%20de%20l'intrication/3x2x2.

A.3 Classification des systèmes à $2 \times 3 \times 3$

Nous renvoyons le lecteur à la Section 3.3.3 pour un rappel de la classification des systèmes quantiques de taille $2 \times 2 \times 3$, ainsi que vers [135] pour une définition des invariants et covariants. Le lecteur pourra retrouver un exemple d'implémentation en langage Maple au lien suivant : https://github.com/hjaffali/annexes-these/tree/master/classification%20de%20l'intrication/2x3x3

A.4 Classification des 4-qubits

Nous renvoyons le lecteur à la Section 2.2.2 pour un rappel de la classification des 4-qubits. Nous présentons ci-dessous les principaux polynômes invariants, ainsi que les algorithmes, utilisés pour la classification des 4-qubits. Le lecteur pourra retrouver un exemple d'implémentation ainsi que les fichiers contenant les covariants en langage Maple au lien suivant : https://github.com/hjaffali/annexes-these/tree/master/classification%20de%20l'intrication/2x2x2x2

A.4.1 Invariants et covariants des 4-qubits

Dans cette sous-section, nous définissons les polynômes invariants et covariants utilisés pour implémenter les algorithmes de classification concernant les strates du cône nilpotent et les familles des 4-qubits.

Tout d'abord, on rappelle que tout système à 4-qubits $|\psi\rangle \in \mathcal{H}_4 = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ peut s'écrire dans la base canonique sous la forme :

$$|\Psi\rangle = \sum_{i,j,k,l \in [\![0,1]\!]} a_{ijkl} \, |ijkl\rangle, \tag{A.9}$$

On rappelle qu'à chaque état à 4-qubits on peut associer une forme quadri-linéaire que l'on notera A :

$$A = \sum_{i,j,k,l \in [\![0,1]\!]} a_{ijkl} \cdot x_i y_j z_k t_l \ . \tag{A.10}$$

On peut également définir des polynômes invariants, sous l'action du groupe SLOCC, permettant de différencier différentes classes d'équivalences. Il a été démontré que l'anneau des polynômes invariants pour les 4-qubits est généré à l'aide de quatre polynômes invariants H, L, M, et D_{xy} [180], définis comme suit :

$$\begin{aligned} H = {} & a_{0000}a_{1111} - a_{1110}a_{0001} - a_{0010}a_{1101} + a_{1100}a_{0011} \\ & - a_{0100}a_{1011} + a_{1010}a_{0101} + a_{0110}a_{1001} - a_{1000}a_{0111} \ , \end{aligned} \tag{A.11}$$

$$L = \begin{vmatrix} a_{0000} & a_{0010} & a_{0001} & a_{0011} \\ a_{1000} & a_{1010} & a_{1001} & a_{1011} \\ a_{0100} & a_{0110} & a_{0101} & a_{0111} \\ a_{1100} & a_{1110} & a_{1101} & a_{1111} \end{vmatrix}, \tag{A.12}$$

$$M = \begin{vmatrix} a_{0000} & a_{0001} & a_{0100} & a_{0101} \\ a_{1000} & a_{1001} & a_{1100} & a_{1101} \\ a_{0010} & a_{0011} & a_{0110} & a_{0111} \\ a_{1010} & a_{1011} & a_{1110} & a_{1111} \end{vmatrix}, \tag{A.13}$$

$$N = -L - M, \tag{A.14}$$

$$b_{xy} = \det\left(\frac{\partial^2 A}{\partial z_i \partial t_j}\right)_{i,j\in[\![0,1]\!]} = [x_0^2, x_0x_1, x_1^2]\ B_{xy} \begin{bmatrix} y_0^2 \\ y_0y_1 \\ y_1^2 \end{bmatrix}. \tag{A.15}$$

La matrice B_{xy} de taille 3×3 est construite en identifiant les coefficients devant les termes $x_ix_jy_ky_l$ avec $i, j, k, l \in [\![0, 1]\!]$ dans la forme quadrique $b_{x,y}$.

$$D_{xy} = -\det(B_{xy})\ . \tag{A.16}$$

Il est également nécessaire d'introduire trois quartiques, dont les coefficients sont définis à l'aide des invariants fondamentaux pour les 4-qubits,

$$\mathcal{Q}_1(|\Psi\rangle) = x^4 - 2H\cdot x^3y + (H^2 + 2L + 4M)\cdot x^2y^2 + (4D_{xy} - 4H(M + \frac{1}{2}L))\cdot xy^3 + L^2\cdot y^4, \tag{A.17}$$

$$\mathcal{Q}_2(|\Psi\rangle) = x^4 - 2H\cdot x^3y + (H^2 - 4L - 2M)\cdot x^2y^2 + (-2MH + 4D_{xy})\cdot xy^3 + M^2\cdot y^4, \tag{A.18}$$

$$\mathcal{Q}_3(|\Psi\rangle) = x^4 - 2H\cdot x^3y + (H^2 + 2L - 2M)\cdot x^2y^2 - (2LH + 2MH - 4D_{xy})\cdot xy^3 + N^2\cdot y^4\ . \tag{A.19}$$

Nous définissons également deux polynômes invariants des quartiques, I_2 et I_3 définis comme suit :

$$I_2(\mathcal{Q}_1) = I_2(\mathcal{Q}_2) = I_2(\mathcal{Q}_3) = \frac{4}{3}L^2 - \frac{4}{3}H^2M + \frac{4}{3}LM + \frac{4}{3}M^2 + 2HD_{xy} + \frac{1}{12}H^4 - \frac{2}{3}H^2L, \tag{A.20}$$

$$\begin{aligned} I_3(\mathcal{Q}_1) = I_3(\mathcal{Q}_2) = I_3(\mathcal{Q}_3) = {} & \frac{8}{27}L^3 - \frac{1}{216}H^6 - \frac{8}{27}M^3 - \frac{1}{6}DxyH^3 + \frac{4}{3}HMDxy \\ & - \frac{5}{9}H^2ML + \frac{2}{3}HLDxy - \frac{2}{9}H^2L^2 - \frac{5}{9}H^2M^2 - {D_{xy}}^2 \\ & + \frac{4}{9}L^2M + \frac{1}{18}H^4L + \frac{1}{9}H^4M - \frac{4}{9}LM^2\ . \end{aligned} \tag{A.21}$$

Les trois quartiques $\mathcal{Q}_1$, $\mathcal{Q}_2$ et $\mathcal{Q}_3$ définies précédemment ainsi que les deux polynômes invariants I_2 et I_3 associés sont étroitement liés à l'hyperdéterminant des 4-qubits. En effet, l'hyperdéterminant Det_{2222} de taille $2\times2\times2\times2$ peut être vu comme le

discriminant d'une des quartiques $Det_{2222} = \Delta(\mathcal{Q}_i)$. D'autre part, l'hyperdéterminant s'exprime aussi uniquement à partir des invariants, tel que $Det_{2222} = {I_2}^3 - 27{I_3}^2$ [180, 179].

Dans l'Algorithme 5 présenté en sous-section suivante, il est nécessaire de pouvoir étudier la nature et la multiplicité des racines des quartiques pour différencier les différentes familles de Verstraete *et al.*. On utilise alors deux polynômes covariants supplémentaires, plus précisément la Hessienne et le Jacobien de la Hessienne pour une quartique, définis comme suit :

$$Hess(Q) = \begin{vmatrix} \frac{\partial^2 Q}{\partial x^2} & \frac{\partial^2 Q}{\partial x \partial y} \\ \frac{\partial^2 Q}{\partial y \partial x} & \frac{\partial^2 Q}{\partial y^2} \end{vmatrix}, \tag{A.22}$$

$$T(Q) = \begin{vmatrix} \frac{\partial Q}{\partial x} & \frac{\partial Q}{\partial y} \\ \frac{\partial Hess(Q)}{\partial x} & \frac{\partial Hess(Q)}{\partial y} \end{vmatrix}. \tag{A.23}$$

A.4.2 Algorithmes de classification

Les polynômes invariants et covariants liés aux états à 4-qubits, introduits à la sous-section précédente, permettent de déterminer la classe d'intrication, ou la famille d'orbites (la strate), correspondant à un registre quantique donné à 4-qubits. Dans cette sous-section, nous présentons deux algorithmes proposés par Holweck *et al.* exploitant ces polynômes afin de déterminer l'orbite sous SLOCC correspondant à un vecteur en entrée.

Cône nilpotent

Nous renvoyons le lecteur à la Section 2.2.2 pour la définition du cône nilpotent, et des covariants et vecteur d'évaluation utilisés dans l'algorithme. Dans l'Algorithme 4, on reproduit [136] la procédure prenant en entrée un état à 4-qubit et retournant la strate correspondante dans le cône nilpotent, ou une erreur si l'état n'est pas nilpotent. On suppose fournie la fonction **isInNullcone(Y)** permettant de savoir si l'état Y est nilpotent ou pas (en vérifiant s'il annule tous les invariants, et pour cela il suffit de vérifier qu'il annule les 4 invariants fondamentaux).

Algorithme 4 NilpotentType [136]

Require: Y un vecteur de taille 16, représentant l'état à 4-qubit
Ensure: La strate du cône nilpotent $\mathcal{N}$ associée à Y

if isInNullcone(Y) **then**
  vectCov $\leftarrow [A, P_B, P_C^1, P_C^2, P_D^1, P_D^2, P_F, P_L]$
  eval $\leftarrow$ evaluer(vectCov,Y)
  if eval $= [0,0,0,0,0,0,0,0]$ **then**
    retourner Gr_0
  else if eval $= [1,0,0,0,0,0,0,0]$ **then**
    retourner Gr_1
  else if eval $= [1,1,0,0,0,0,0,0]$ **then**
    retourner Gr_2
  else if eval $= [1,1,1,0,0,0,0,0]$ **then**
    retourner Gr_3
  else if eval $= [1,1,1,0,1,0,0,0]$ **then**
    retourner Gr_4
  else if eval $= [1,1,1,1,0,0,0,0]$ **then**
    retourner Gr_5
  else if eval $= [1,1,1,1,1,1,0,0]$ **then**
    retourner Gr_6
  else if eval $= [1,1,1,1,1,1,1,0]$ **then**
    retourner Gr_7
  else if eval $= [1,1,1,1,1,1,1,1]$ **then**
    retourner Gr_8
  end if
else
  retourner "Y n'appartient pas au cône nilpotent"
end if

Familles de Verstraete

Dans l'Algorithme 5, nous reproduisons [138] la procédure prenant en entrée un état à 4-qubit et retournant la famille ou sous-famille de Verstraete *et al.*. L'algorithme raisonne sur le nombre et la multiplicité des racines nulles et non-nulles des polynômes quartiques afin de distinguer les différents cas, faisant appel aux invariants fondamentaux et à la matrice Hessienne et son jacobien notamment pour distinguer les configurations de racines, évaluant ensuite différents vecteurs de covariants pour différencier entre les différentes sous-familles.

Algorithme 5 VerstraeteType [138]

Require: Y un vecteur de taille 16, représentant l'état à 4-qubit
Ensure: La famille de Verstraete *et al.* correspondante à Y

Hess1 $\leftarrow Hess(\mathcal{Q}_1)$
Hess2 $\leftarrow Hess(\mathcal{Q}_2)$
Hess3 $\leftarrow Hess(\mathcal{Q}_3)$
T1 $\leftarrow T(\mathcal{Q}_1)$
T2 $\leftarrow T(\mathcal{Q}_2)$
T3 $\leftarrow T(\mathcal{Q}_3)$

▷ Si l'état en entrée appartient au cône nilpotent
if isInNullcone(Y) **then**
  retourner NilpotentType(Y)
end if

▷ Les trois quartiques ont au moins une racine nulle
if $L = 0$ et $M = 0$ **then**
  ▷ Toutes les racines sont simples
  if $D_{xy} \neq 0$ et $Hyper \neq 0$ **then**
    retourner G_{abc0}

  ▷ Toutes les racines nulles sont simples, et il y a une racine double non-nulle
  else if $D_{xy} \neq 0$ et $Hyper = 0$ **then**
    vectCov $\leftarrow [\mathcal{L}]$
    eval $\leftarrow$ evaluer(vectCov,Y)
    if eval $= [0]$ **then**
      retourner $G_{aa(-2a)0}$
    else
      retourner $L_{0b(\frac{b}{2})_2}$
    end if

  ▷ Toutes les racines nulles sont doubles
  else if $D_{xy} = 0$ et $H \neq 0$ **then**
    vectCov $\leftarrow [\overline{\mathcal{G}}, \mathcal{G}, \mathcal{H}, \mathcal{L}]$
    eval $\leftarrow$ evaluer(vectCov,Y)
    if eval $= [0,0,0,0]$ **then**
      retourner G_{00cc}
    else if eval $= [0,1,1,0]$ **then**
      retourner L_{aa0_2}
    else if eval $= [0,0,1,0]$ **then**
      retourner L_{00c_2}
    else if eval $= [1,1,1,0]$ **then**
      retourner $L_{0_2b_2}$
    else if eval $= [1,1,1,1]$ **then**
      retourner $L_{a_20_{3\oplus\overline{1}}}$
    end if
  end if

▷ Seulement une des quartiques $\mathcal{Q}_i$ a une racine nulle
▷ La quartique $\mathcal{Q}_1$ a une racine nulle

else if $L = 0$ and $M \neq 0$ **then**

▷ $\mathcal{Q}_1$ n'a que des racines simples

if $Hyper \neq 0$ **then**
retourner G_{abc0}

▷ $\mathcal{Q}_1$ a une racine nulle double et deux racines simples

else if $D_{xy} = H \cdot M$ et $H^2 + 4M \neq 0$ **then**
vectCov $\leftarrow [\mathcal{K}_3, \mathcal{L}]$
eval $\leftarrow$ evaluer(vectCov,Y)
if eval $= [0, 0]$ **then**
retourner G_{ab00}
else if eval $= [1, 0]$ **then**
retourner L_{ab0_2}
else if eval $= [1, 1]$ **then**
retourner $L_{a_2b_2}$
end if

▷ $\mathcal{Q}_1$a une racine double non-nulle et deux racines simples

else if $D_{xy} \neq H \cdot M$ et T1$\neq 0$ ets T2$\neq 0$ **then**
vectCov $\leftarrow [\mathcal{L}]$
eval $\leftarrow$ evaluer(vectCov,Y)
if eval $= [0]$ **then**
retourner G_{abb0}
else if eval $= [1]$ **then**
retourner L_{a0c_2}
end if

▷ $\mathcal{Q}_1$ a une racine triple nulle et une racine simple

else if $D_{xy} = H \cdot M$ et $H^2 + 4M = 0$ et Hess2$= 0$ **then**
vectCov $\leftarrow [\mathcal{C}, \mathcal{D}, \mathcal{K}_5, \mathcal{L}]$
eval $\leftarrow$ evaluer(vectCov,Y)
if eval $= [0, 0, 0, 0]$ **then**
retourner G_{a000}
else if eval $= [1, 0, 0, 0]$ **then**
retourner L_{a00_2}
else if eval $= [1, 1, 1, 0]$ **then**
retourner L_{0b_3}
else if eval $= [1, 1, 0, 0]$ **then**
retourner $L_{a_2a_2}$
else if eval $= [1, 1, 1, 1]$ **then**
retourner L_{a_4}
end if

▷ $\mathcal{Q}_1$ a une racine triple non-nulle

else if $D_{xy} \neq H \cdot M$ et $I_2 = 0$ et $Hyper = 0$ **then**
  vectCov $\leftarrow [\mathcal{D}, \mathcal{L}]$
  eval $\leftarrow$ evaluer(vectCov,Y)
  if eval $= [0,0]$ **then**
    retourner G_{aaa0}
  else if eval $= [1,0]$ **then**
    retourner L_{0bb_2}
  else if eval $= [1,1]$ **then**
    retourner L_{a0_3}
  end if
end if

▷ La quartique $\mathcal{Q}_2$ a une racine nulle

else if $M = 0$ and $L \neq 0$ **then**

▷ $\mathcal{Q}_2$ n'a que des racines simples

  if $Hyper \neq 0$ **then**
    return G_{abc0}

▷ $\mathcal{Q}_2$ a une racine double nulle et deux racines simples

  else if $D_{xy} = 0$ et $H^2 \neq 4L$ **then**
    vectCov $\leftarrow [\mathcal{K}_3, \mathcal{L}]$
    eval $\leftarrow$ evaluer(vectCov,Y)
    if eval $= [0,0]$ **then**
      retourner G_{ab00}
    else if eval $= [1,0]$ **then**
      retourner L_{ab0_2}
    else if eval $= [1,1]$ **then**
      retourner $L_{a_2b_2}$
    end if

▷ $\mathcal{Q}_2$ a une racine double non-nulle et deux racines simples

  else if $D_{xy} \neq 0$ et T1$\neq 0$ et T2$\neq 0$ **then**
    vectCov $\leftarrow [\mathcal{L}]$
    eval $\leftarrow$ evaluer(vectCov,Y)
    if eval $= [0]$ **then**
      retourner G_{abb0}
    else if eval $= [1]$ **then**
      retourner L_{a0c_2}
    end if

▷ $\mathcal{Q}_2$ a une racine triple nulle et une racine simple

else if $D_{xy} = 0$ et $H^2 = 4L$ **then**
  vectCov $\leftarrow [\mathcal{C}, \mathcal{D}, \mathcal{K}_5, \mathcal{L}]$
  eval $\leftarrow$ evaluer(vectCov,Y)
  if eval $= [0,0,0,0]$ **then**
    retourner G_{a000}
  else if eval $= [1,0,0,0]$ **then**
    retourner L_{a00_2}
  else if eval $= [1,1,1,0]$ **then**
    retourner L_{0b_3}
  else if eval $= [1,1,0,0]$ **then**
    retourner $L_{a_2a_2}$
  else if eval $= [1,1,1,1]$ **then**
    retourner L_{a_4}
  end if

▷ $\mathcal{Q}_2$ a une racine triple non-nulle

else if $D_{xy} \neq 0$ et $I_2 = 0$ et $Hyper = 0$ **then**
  vectCov $\leftarrow [\mathcal{D}, \mathcal{L}]$
  eval $\leftarrow$ evaluer(vectCov,Y)
  if eval $= [0,0]$ **then**
    retourner G_{aaa0}
  else if eval $= [1,0]$ **then**
    retourner L_{0bb_2}
  else if eval $= [1,1]$ **then**
    retourner L_{a0_3}
  end if
end if

▷ La quartique $\mathcal{Q}_3$ a une racine nulle

else if $N = 0$ et $L \neq 0$ et $M \neq 0$ **then**

▷ $\mathcal{Q}_3$ n'a que des racines simples

  if $Hyper \neq 0$ **then**
    retourner G_{abc0}

▷ $\mathcal{Q}_3$ a une racine double nulle et deux racines simples

  else if $D_{xy} = 0$ et $H^2 \neq 4M$ **then**
    vectCov $\leftarrow [\mathcal{K}_3, \mathcal{L}]$
    eval $\leftarrow$ evaluer(vectCov,Y)
    if eval $= [0,0]$ **then**
      retourner G_{ab00}
    else if eval $= [1,0]$ **then**
      retourner L_{ab0_2}
    else if eval $= [1,1]$ **then**
      retourner $L_{a_2b_2}$
    end if

▷ $\mathcal{Q}_3$ a une racine double non-nulle et deux racines simples
else if $D_{xy} \neq 0$ et T1$\neq 0$ et T2$\neq 0$ **then**
  vectCov $\leftarrow [\mathcal{L}]$
  eval $\leftarrow$ evaluer(vectCov,Y)
  if eval $= [0]$ **then**
    retourner G_{abb0}
  else if eval $= [1]$ **then**
    retourner L_{a0c_2}
  end if

▷ $\mathcal{Q}_3$ a une racine triple nulle et une racine simple
else if $D_{xy} = 0$ et $H^2 = 4M$ **then**
  vectCov $\leftarrow [\mathcal{C}, \mathcal{D}, \mathcal{K}_5, \mathcal{L}]$
  eval $\leftarrow$ evaluer(vectCov,Y)
  if eval $= [0,0,0,0]$ **then**
    retourner G_{a000}
  else if eval $= [1,0,0,0]$ **then**
    retourner L_{a00_2}
  else if eval $= [1,1,1,0]$ **then**
    retourner L_{0b_3}
  else if eval $= [1,1,0,0]$ **then**
    retourner $L_{a_2a_2}$
  else if eval $= [1,1,1,1]$ **then**
    retourner L_{a_4}
  end if

▷ $\mathcal{Q}_3$ a une racine triple non-nulle
else if $D_{xy} \neq 0$ et $I_2 = 0$ et $Hyper = 0$ **then**
  vectCov $\leftarrow [\mathcal{D}, \mathcal{L}]$
  eval $\leftarrow$ evaluer(vectCov,Y)
  if eval $= [0,0]$ **then**
    retourner G_{aaa0}
  else if eval $= [1,0]$ **then**
    retourner L_{0bb_2}
  else if eval $= [1,1]$ **then**
    retourner L_{a0_3}
  end if
end if

▷ Toutes les quartiques ont uniquement des racines non-nulles

else

▷ Toutes les racines sont simples

if $Hyper \neq 0$ **then**
retourner G_{abcd}

▷ Chaque quartique a une racine double et deux racines simples

else if T1 $\neq 0$ et T2 $\neq 0$ et T3 $\neq 0$ et $I_2 \neq 0$ et $I_3 \neq 0$ **then**
vectCov $\leftarrow [\mathcal{L}]$
eval $\leftarrow$ evaluer(vectCov,Y)
if eval $= [0]$ **then**
retourner G_{abcc}
else if eval $= [1]$ **then**
retourner L_{abc_2}
end if

▷ Chaque quartique a une unique racine simple et une racine triple

else if $I_2 \neq 0$ et $I_3 \neq 0$ et Hess1 $\neq 0$ **then**
vectCov $\leftarrow [\mathcal{K}_5, \mathcal{L}]$
eval $\leftarrow$ evaluer(vectCov,Y)
if eval $= [0, 0]$ **then**
retourner G_{abbb}
else if eval $= [1, 0]$ **then**
retourner L_{abb_2}
else if eval $= [1, 1]$ **then**
retourner L_{ab_3}
end if

end if

end if

A.5 Invariants des état symétriques

Nous renvoyons le lecteur vers la Section 6.2 pour la définition des invariants associés aux état symétriques. Le lecteur pourra retrouver un exemple d'implémentation de ces invariants en langage Maple au lien suivant : `https://github.com/hjaffali/annexes-these/tree/master/invariants%20%C3%A9tats%20sym%C3%A9triques`

A.6 Algorithme de Grover

Nous présentons ici l'algorithme de Grover utilisé pour étudier l'intrication. Nous implémentons l'opérateur de diffusion en réalisant une symétrie des amplitudes par rapport à la moyenne, plutôt que d'utiliser la version matricielle, pour économiser des ressources de calcul.

Algorithme 6 GroverAlgorithm

Require: liste : liste des indices des éléments recherchés
Require: n : nombre de qubits
Require: m : nombre d'itérations de l'algorithme
Ensure: Y un vecteur de taille 2^n représentant l'état à n-qubits, résultat de m itérations de l'algorithme de Grover

$Y \leftarrow Vector(2^n, |+\rangle^{\otimes n})$ ▷ Initialisation du registre à l'état superposé
s ← size(liste) ▷ Nombre d'éléments recherchés
for i **from** 1 **to** m **do** ▷ Pour chaque itération de l'algorithme
  for j **from** 1 **to** s **do** ▷ Application de l'Oracle
    $Y[\text{liste}(j)] \leftarrow -Y[\text{liste}(j)]$
  end for
  moyenne ← $mean(Y)$ ▷ Calcul de la valeur moyenne
  for j **from** 1 **to** 2^n **do** ▷ Application de la Diffusion
    $Y[j] \leftarrow 2 \cdot \text{moyenne} - Y[j]$
  end for
end for
retourner Y

A.7 Transformée de Fourier Quantique et États périodiques

A.7.1 États périodiques

Nous présentons dans cette sous-section l'algorithme permettant de générer les états périodiques comme définis en Equation 1.54.

Algorithme 7 GeneratePeriodicStates

Require: l : le shift de l'état périodique
Require: r : la période de l'état périodique
Require: n : nombre de qubits
Ensure: Y un vecteur de taille 2^n représentant l'état périodique $\left|\Psi^n_{l,r}\right\rangle$ à n-qubits

$Q \leftarrow 2^n$
A ← $\lceil \frac{Q-l}{r} \rceil$ ▷ Nombre d'états de base dans l'écriture
$Y \leftarrow Vector(2^n, 0)$ ▷ Initialisation du registre à l'état nul
for i **from** 0 **to** $A - 1$ **do** ▷ Pour chaque état figurant dans l'écriture
  $Y[l + i \cdot r + 1] \leftarrow 1$
end for
$Y \leftarrow Normalize(Y, EuclideanNorm)$ ▷ Renormalisation
retourner Y

A.7.2 Transformée de Fourier Quantique

Nous présentons dans cette sous-section un algorithme afin d'appliquer la Transformée de Fourier Quantique à un état en entrée.

Algorithme 8 QuantumFourierTransform

Require: Y un vecteur de taille 2^n représentant l'état à n-qubits
Require: n : nombre de qubits
Ensure: Y_{TFQ} un vecteur de taille 2^n représentant l'état Y après application de la TFQ

$N \leftarrow 2^n$
$\omega \leftarrow e^{\frac{2i\pi}{N}}$ ▷ Racine n-ième de l'unité
$TFQ \leftarrow Matrix([N, N], 0)$ ▷ Initialisation de la matrice
for i **from** 1 **to** N **do** ▷ Pour chaque état figurant dans l'écriture
  for j **from** 1 **to** N **do**
    $TFQ[i, j] \leftarrow \frac{1}{\sqrt{N}} \cdot \omega^{(i-1)(j-1)}$
  end for
end for
$Y_{TFQ} \leftarrow TFQ \cdot Y$
retourner Y_{TFQ}

A.8 Algorithmes d'optimisation

Nous avons utilisé tout au long de la thèse des algorithmes d'optimisation (basés gradient, ou des méta-heuristiques) afin de maximiser ou minimiser certaines quantités (mesures ou polynômes) : l'algorithme de promenade aléatoire, la méthode du gradient, et l'algorithme d'optimisation par essaim particulaire. Ces optimisations sont parfois contraintes par la relation de normalisation, et nous intégrons parfois directement cette contrainte dans l'algorithme d'optimisation. Le lecteur pourra trouver une implémentation de ces algorithmes en Maple ou Java au lien suivant : `https://github.com/hjaffali/annexes-these/tree/master/optimisation%20num%C3%A9rique`.

A.9 Polynômes de Mermin

Nous présentons les polynômes de Mermin, et la mesure associée de la non-localité en Section 2.2.3. L'implémentation des polynômes de Mermin en Maple est accessible via ce lien : `https://github.com/hjaffali/annexes-these/tree/master/polyn%C3%B4mes%20de%20Mermin`. Nous utilisons les algorithmes d'optimisation présentés en section précédente pour optimiser les observables afin de maximiser la valeur des polynômes. Nous séparons l'utilisation des polynômes du Mermin dans le cas de l'algorithme de Grover (où le nombre de paramètres est réduit à 6) de celle dans le cas général, cas où nous avons notamment cherché à évaluer ces polynômes pour les états issus de la TFQ (où le nombre de paramètres est de $6n$, avec n le nombre de qubits).

A.10 Calcul des singularités des hypersurfaces

Nous rappelons qu'une méthode de détermination de la singularité simple d'un hypersurface à partir de classification d'Arnold est présentée en Section 5.2. Un exemple d'implémentation en Maple pour les 5-qubits est disponible au lien suivant : https://github.com/hjaffali/annexes-these/tree/master/singularit%C3%A9s%20des%20hypersurfaces.

A.11 Mesure géométrique de l'intrication

Nous définissons la mesure géométrique de l'intrication pour les systèmes à n-qubits (et les états symétriques) en Section 2.2.3, et en Section 6.3.2 pour les états fermioniques. Nous proposons une implémentation en Maple de ces mesures dans le lien suivant : https://github.com/hjaffali/annexes-these/tree/master/mesure%20g%C3%A9om%C3%A9trique%20de%20l'intrication. Les optimisations sont menées à l'aide des algorithmes précédemment présentés.

A.12 Réseaux de neurones avec Keras

Nous présentons ci-dessous un exemple de code Python, utilisant la bibliothèque Keras, pour entrainer et évaluer un réseau de neurone pour le problème de classification des points sur/à l'extérieur de la variété de Segre pour les états à 5-qubits. Cet exemple est également accessible à travers le lien suivant : https://github.com/hjaffali/annexes-these/tree/master/r%C3%A9seaux%20de%20neurones%20artificiels.

```
from keras.models import Sequential
from keras.layers import Dense, Dropout, Activation
from keras.optimizers import SGD
from keras import utils
from keras import layers
from keras.callbacks import EarlyStopping, ModelCheckpoint
from random import randint
from scipy.stats import norm
from scipy.stats import ortho_group

import numpy as np
import sys
import matplotlib.mlab as mlab
import matplotlib.pyplot as plt


#size of the training dataset
training_size = 502600
#size of the validation dataset
validation_size = 55600
#size of the testing dataset
testing_size = 32000
#number of epochs
nbEpochs = 100
```

```
#size of a single input vector
input_data_size = 2*2*2*2*2
#size of the output
output_data_size = 1
#number of classes in the classification problem
nb_of_classes = 2


def power_2_activation(x):
  """
    Square activation function : x -> x^2
    Parameters :
    - x: input number (weighted sum in the context of activation
   function)
    Return : x^2, the input number squared
    """
  return (x**2)



def generate_data(size,input_data_size,nb_of_classes):
  """
    Function used to generate datasets (training, validation and
   testing)
    Parameters :
    - size : size of the datasets, number of vectors
    - input_data_size : size of each vector (number of entries) of the
    dataset
    - nb_of_classes : number of classes in the classification problem
   (used to divide equally the dataset)
    Return :
    - inputs : multidimentional array regrouping all input vectors.
   The array is of size : size*input_data_size
    - outputs : array regrouping all outputs associated to each input
   vector. The array is of size : size
  """

  # initializing inputs and outputs arrays
  inputs = np.empty([size, input_data_size])
  outputs = np.empty([size, 1])

  # subdividing the dataset depending on the number of classes
  temp = int(size/nb_of_classes)
  for i in range(0,temp):
    #rank 1 tensors, separable states
    state = generate_point_on_segre_variety()
    inputs[i] = state.copy()
    outputs[i]= [0]

  for i in range(temp,temp+int((size-temp)/5)):
    #rank 2 tensors
    state = normalize(random_rank_one(5)+random_rank_one(5))
    inputs[i] = state.copy()
    outputs[i]= [1]

  for i in range(temp+int((size-temp)/5),temp+2*int((size-temp)/5)):
    #border rank 3 tensors
```

```
    state = normalize(random_rank_one(5)+random_rank_one(5)+
   random_rank_one(5))
    inputs[i] = state.copy()
    outputs[i]= [1]

  for i in range(temp+2*int((size-temp)/5),temp+3*int((size-temp)/5)):
    #border rank 4 tensors
    state = normalize(random_rank_one(5)+random_rank_one(5)+
   random_rank_one(5)+random_rank_one(5))
    inputs[i] = state.copy()
    outputs[i]= [1]

  for i in range(temp+3*int((size-temp)/5),temp+4*int((size-temp)/5)):
    #border rank 5 tensors
    state = normalize(random_rank_one(5)+random_rank_one(5)+
   random_rank_one(5)+random_rank_one(5)+random_rank_one(5))
    inputs[i] = state.copy()
    outputs[i]= [1]

  for i in range(temp+4*int((size-temp)/5),size):
    #random tensors
    state = random_tensor(5)
    inputs[i] = state.copy()
    outputs[i]= [1]

  return inputs, outputs

def random_rank_one(dimension):
  """
    Generate a rank one tensor
    Parameters :
    - dimension : number of qubits
    Return :
    - vector : normalized rank one tensor of size 2^dimension
  """
  vector = np.random.random(2)*2-1
  for i in range(0,dimension-1):
    # Kronecker product
    vector = np.kron(vector,np.random.random(2)*2-1)
  vector = normalize(vector)
  return vector

def random_tensor(dimension):
  """
    Generate a random tensor
    Parameters :
    - dimension : number of qubits
    Return :
    - vector : normalized random tensor of size 2^dimension
  """
  vector = np.random.random(2**dimension)*2-1
  vector = normalize(vector)
  return vector

def generate_point_on_segre_variety():
  """
    Generate a 5-qubit separable state
```

```
    Return :
    - vector : 5-qubit normalized separable state
  """
  vector = random_rank_one(5)
  return vector

def generate_SLOCC_2x2():
  """
    Generate a random 2x2 SLOCC operator
    Return :
    - vec : XXXXXXXX
  """
  vec = np.random.random((2,2))*2 -1
  det = np.linalg.det(vec)
  while (det<0):
    vec = np.random.random((2,2))*2 -1
    det = np.linalg.det(vec)
  vec = vec/np.sqrt(det)
  return vec

def apply_SLOCC(vector):
  """
    Act on the vector in parameter with a random element of the SLOCC
   group
  """
  slocc1 = generate_SLOCC_2x2()
  slocc2 = generate_SLOCC_2x2()
  slocc3 = generate_SLOCC_2x2()
  slocc4 = generate_SLOCC_2x2()
  slocc5 = generate_SLOCC_2x2()
  matrix = np.kron(np.kron(np.kron(np.kron(slocc1,slocc2),slocc3),
   slocc4),slocc5)
  return matrix.dot(vector)

def normalize(v):
  """
    Normalize the vector in parameter
    Parameters :
    - v : the vector to be normalized
    Return :
  """
  norm=np.linalg.norm(v, ord=1)
  if norm==0:
    return v
  else :
    return v / norm



# define the LeakyReLU activation fuction
leakyRELU = layers.LeakyReLU(alpha=0.4)

# define the neural network model
model = Sequential()

## Input Layer
# Dense(100) is a fully-connected layer with 100 hidden units.
```

```
# in the first layer, you must specify the expected input data shape
model.add(Dense(100, input_dim=input_data_size, init='uniform'))
model.add(leakyRELU)

## Hidden Layer
model.add(Dense(50, init='uniform'))
model.add(leakyRELU)

## Hidden Layer
model.add(Dense(25, init='uniform'))
model.add(leakyRELU)

## Hidden Layer
model.add(Dense(16, init='uniform'))
model.add(leakyRELU)

## Output Layer
model.add(Dense(output_data_size, init='uniform'))
model.add(Activation('sigmoid'))


# compiling the model
model.compile(loss='binary_crossentropy',
      optimizer='nadam',
      metrics=['binary_accuracy'])


# generate dummy training data
x_train, y_train = generate_data(training_size,input_data_size,
   nb_of_classes)
print(x_train,y_train)

# generate dummy validation data
x_validation, y_validation = generate_data(validation_size,
   input_data_size,nb_of_classes)
print(x_validation,y_validation)

# generate dummy test data
x_test, y_test = generate_data(testing_size,input_data_size,
   nb_of_classes)
print(x_test,y_test)

# train the neural network model
model.fit(x_train, y_train,
      nb_epoch=nbEpochs,
      batch_size=128,
      verbose=1,
      shuffle=True,
      validation_data=(x_validation, y_validation))

# evaluate the trained model on the training , validation and testing
   models
loss_train, acc_train = model.evaluate(x_train, y_train, batch_size
   =128)
loss_validation, acc_validation = model.evaluate(x_validation,
   y_validation, batch_size=128)
loss_test, acc_test = model.evaluate(x_test, y_test, batch_size=128)
```

```
# printing all the losses, accuracies, and the neural network weights
print(loss_train, acc_train)
print(loss_validation, acc_validation)
print(loss_test, acc_test)
print(model.metrics_names)
print(model.get_weights())


# saving the model in a .h5 file
model.save('model_ReLu_point_in_segre_2x2x2x2x2_database_'+str(
    training_size)+'_validation_'+str(validation_size)+'_test_'+str(
    testing_size)+'_epoch_'+str(nbEpochs)+'.h5')


######### USING THE MODEL FOR PREDICTIONS #############
#suppose we want to make predictions for the state Phi 5
def generate_state_phi_5():
  vector = np.zeros(2*2*2*2*2)
  vector[0] = 1
  vector[7] = 1
  vector[11] = 1
  vector[13] = 1
  vector[14] = 1
  vector[19] = 1
  vector[21] = 1
  vector[22] = 1
  vector[25] = 1
  vector[26] = 1
  vector[28] = 1
  vector[31] = 1
  vector = normalize(apply_SLOCC(vector))
  return vector

def generate_data_phi_5(size,input_data_size):
  inputs = np.empty([size, input_data_size])
  for i in range(0,size):
    state = generate_state_phi_5()
    inputs[i] = state.copy()
  return inputs

# size of the predicition dataset, which is the number of SLOCC
    equivalent states used to make the prediction
data_size = 10000

# generate the prediction dataset
prediction_X = generate_data_phi_5(data_size,input_data_size)

# making prediction with the trained network
prediction = model.predict(prediction_X,verbose=1)

print(prediction)

# best fit of data, determining mean and variance
(mu, sigma) = norm.fit(prediction)

# constructing the histogram of the data
n, bins, patches = plt.hist(prediction,bins
```

```
    =[0.0,0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1.0],align='mid')
print(n,bins,patches)

#plotting the histogram
plt.xlabel('Binary classes')
plt.ylabel('Proportion')
plt.xlim(0, 1)
plt.title(r'$\mathrm{Mean\ value}\  \mu=%.3f,\mathrm{Variance}\ \sigma
    =%.3f$' %(mu, sigma))
plt.grid(True)
plt.show()
```

Listing A.1 – Exemple d'entraînement et de prédiction, pour le problème de classification des états séparables à 5-qubits.

Bibliographie

[1] Maplesoft a division of Waterloo Maple Inc. Waterloo Ontario., *Maple 17*, 2017.

[2] H. Abo, G. Ottaviani, and C. Peterson, *Induction for secant varieties of Segre varieties*, Trans. Amer. Math. Soc. **361** (2009), no. 2, 767–792.

[3] Satyabrata Adhikari and A. S. Majumdar, *An analytical condition for the violation of mermin's inequality by any three qubit state*, arXiv preprint arXiv :1602.02619 (2016).

[4] Seiki Akama, *Elements of quantum computing : History, theories and engineering applications*, Springer International Publishing Switzerland, 2015.

[5] Daniel Alsina, *Phd thesis : Multipartite entanglement and quantum algorithms*, arXiv preprint arXiv :1706.08318 (2017).

[6] Daniel Alsina, Alba Cervera, Dardo Goyeneche, José I. Latorre, and Karol Życzkowski, *Operational approach to bell inequalities : Application to qutrits*, Physical Review A **94** (2016), no. 3, 32102.

[7] Daniel Alsina and José Ignacio Latorre, *Experimental test of mermin inequalities on a five-qubit quantum computer*, Physical Review A **94** (2016), no. 1, 12314.

[8] Grâce Amouzou, Jeoffrey Boffelli, Hamza Jaffali, Kossi Atchonouglo, and Frédéric Holweck, *Entanglement and non-locality of four-qubit connected hypergraph states*, 2020.

[9] Namit Anand and Arun Kumar Pati, *Coherence and entanglement monogamy in the discrete analogue of analog grover search*, arXiv preprint arXiv :1611.04542 (2016).

[10] Martin Anthony and Peter L Bartlett, *Neural network learning : Theoretical foundations*, Cambridge University Press, 2009.

[11] V. I. Arnold, V. V. Goryunov, O. V. Lyashko, and V. A. Vasil'ev, *Singularity theory i*, 0938-0396, Springer, Berlin, Heidelberg, 1998.

[12] Vladimir Igorevich Arnol'd, *Normal forms for functions near degenerate critical points, the weyl groups of a_k, d_k, e_k and lagrangian singularities*, Funktsional'nyi Analiz i ego Prilozheniya **6** (1972), no. 4, 3–25.

[13] Enrique Arrondo, Alessandra Bernardi, Pedro Macias Marques, and Bernard Mourrain, *Skew-symmetric tensor decomposition*, arXiv preprint arXiv :1811.12725 (2018).

[14] Alain Aspect, *Proposed experiment to test the nonseparability of quantum mechanics*, Phys. Rev. D **14** (1976), 1944–1951.

[15] H. Atmanspacher and T. Filk, *Discrimination and sequentialization of events in perception*, The Nature of Time : Geometry, Physics and Perception (2003), 67–75.

[16] Martin Aulbach, *Classification of entanglement in symmetric states*, International Journal of Quantum Information **10** (2012), no. 7, 1230004.

[17] Martin Aulbach, Damian Markham, and Mio Murao, *The maximally entangled symmetric state in terms of the geometric measure*, New Journal of Physics **12** (2010), no. 7, 73025.

[18] ———, *Geometric entanglement of symmetric states and the majorana representation*, Lecture Notes in Computer Science **6519** (2011), 141.

[19] Kraus B, *Local unitary equivalence of multipartite pure states.*, Physical Review Letters **104** (2010), no. 2, 20504.

[20] Paul Baird, *Géométrie algébrique – les variétés projectives*, Université de Brest, 1999.

[21] Andrew Barron and Roger Barron, *Statistical learning networks : A unifying view*, Proceedings of the 20th Symposium Computer Science and Statistics (1988).

[22] Marc Bataille and Jean-Gabriel Luque, *Quantum circuits of $c-z$ and swap gates : optimization and entanglement*, Journal of Physics A **52** (2019), no. 32, 325302.

[23] J. Batle, C. H. Ooi, Ahmed Farouk, M. S. Alkhambashi, and S. Abdalla, *Global versus local quantum correlations in the grover search algorithm*, Quantum Information Processing **15** (2016), no. 2, 833–849.

[24] K. Baur, J. Draisma, and W. A. de Graaf, *Secant dimensions of minimal orbits : computations and conjectures*, Experiment. Math. **16** (2007), no. 2, 239–250.

[25] Matthew J. S. Beach, Isaac De Vlugt, Anna Golubeva, Patrick Huembeli, Bohdan Kulchytskyy, Xiuzhe Luo, Roger G. Melko, Ejaaz Merali, and Giacomo Torlai, *QuCumber : wavefunction reconstruction with neural networks*, SciPost Phys. **7** (2019), 9.

[26] Elizabeth C. Behrman and James Edward Steck, *Dynamic learning of pairwise and three-way entanglement*, 2011 Third World Congress on Nature and Biologically Inspired Computing, 2011, pp. 99–104.

[27] Mikhail Belkin, Daniel Hsu, Siyuan Ma, and Soumik Mandal, *Reconciling modern machine-learning practice and the classical bias–variance trade-off*, Proceedings of the National Academy of Sciences **116** (2019), no. 32, 15849–15854.

[28] John Stewart Bell, *On the einstein podolsky rosen paradox*, Physics **1** (1964), no. 3, 195–200.

[29] Yacob Ben-Aryeh, *Quantum and classical correlations in bell three and four qubits, related to hilbert-schmidt decomposition.*, arXiv preprint arXiv :1411.2720 (2014).

[30] I. Bengtsson and K. Życzkowski, *Geometry of quantum states : An introduction to quantum entanglement*, Cambridge University Press, 2017.

[31] Ingemar Bengtsson and Karol Zyczkowski, *Geometry of quantum states : An introduction to quantum entanglement*, 2006.

[32] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters, *Quantum nonlocality without entanglement*, Physical Review A **59** (1999), no. 2, 1070–1091.

[33] Charles H. Bennett, Sandu Popescu, Daniel Rohrlich, John A. Smolin, and Ashish V. Thapliyal, *Exact and asymptotic measures of multipartite pure-state entanglement*, Phys. Rev. A **63** (2000), 012307.

[34] Richard Berkovits, *Extracting many-particle entanglement entropy from observables using supervised machine learning*, Phys. Rev. B **98** (2018), no. 24.

[35] Daniel J. Bernstein, *Grover vs. mceliece*, PQCrypto'10 Proceedings of the Third international conference on Post-Quantum Cryptography (2010), 73–80.

[36] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn, *Sphincs : practical stateless hash-based signatures*, theory and application of cryptographic techniques **9056** (2015), 368–397.

[37] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd, *Quantum machine learning*, Nature **549** (2017), no. 7671, 195–202 (English (US)).

[38] Ofer Biham, Michael A. Nielsen, and Tobias J. Osborne, *Entanglement monotone derived from grover's algorithm*, Physical Review A **65** (2002), no. 6.

[39] Ofer Biham, Daniel Shapira, and Yishai Shimoni, *Analysis of grover's quantum search algorithm as a dynamical system*, Physical Review A **68** (2003), no. 2.

[40] Christopher M. Bishop, *Neural networks for pattern recognition*, Oxford University Press, Inc., USA, 1995.

[41] Pierre Borne, Mohamed Benrejeb, and Joseph Haggege, *Les réseaux de neurones. présentation et applications*, 01 2007.

[42] A Borras, A R Plastino, J Batle, C Zander, M Casas, and A Plastino, *Multiqubit systems : highly entangled states and entanglement distribution*, Journal of Physics A : Mathematical and Theoretical **40** (2007), no. 44, 13407–13421.

[43] Maria Chiara Brambilla and Giorgio Ottaviani, *On the alexander–hirschowitz theorem*, Journal of Pure and Applied Algebra **212** (2008), no. 5, 1229–1251.

[44] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp, *Quantum amplitude amplification and estimation*, arXiv preprint arXiv :quant-ph/0005055 (2000).

[45] Samuel L. Braunstein and Arun K. Pati, *Speed-up and entanglement in quantum searching*, Quantum Information & Computation **2** (2002), no. 5, 399–409.

[46] Sergei Bravyi, *Entanglement entropy of multipartite pure states*, Phys. Rev. A **67** (2003), 012313.

[47] Paul Breiding, Sara Kališnik, Bernd Sturmfels, and Madeleine Weinstein, *Learning algebraic varieties from samples*, Revista Matemática Complutense **31** (2018), no. 3, 545–593.

[48] Murray R. Bremner, *On the hyperdeterminant for 2×2×3 arrays*, Linear & Multilinear Algebra **60** (2012), no. 8, 921–932.

[49] Murray R. Bremner and Jiaxiong Hu, *Fundamental invariants for the action of* $\mathrm{SL}_3(\mathbb{C}) \times \mathrm{SL}_3(\mathbb{C}) \times \mathrm{SL}_3(\mathbb{C})$ *on* $3 \times 3 \times 3$ *arrays*, Mathematics of Computation **82** (2013), no. 284, 2421–2438.

[50] Murray R. Bremner, Jiaxiong Hu, and Luke Oeding, *The 3 × 3 × 3 hyperdeterminant as a polynomial in the fundamental invariants for sl 3 (c) × sl 3 (c) × sl 3 (c).*, Mathematics in Computer Science **8** (2014), 147–156.

[51] Emmanuel Briand, Jean-Gabriel Luque, Jean-Yves Thibon, and Frank Verstraete, *The moduli space of three-qutrit states*, Journal of Mathematical Physics **45** (2004), no. 12, 4855–4867.

[52] Hans J. Briegel and Robert Raussendorf, *Persistent entanglement in arrays of interacting particles*, Physical Review Letters **86** (2001), no. 5, 910–913.

[53] Dorje C. Brody and Lane P. Hughston, *Geometric quantum mechanics*, Journal of Geometry and Physics **38** (2001), no. 1, 19–53.

[54] Iain D K Brown, Susan Stepney, Anthony Sudbery, and Samuel L Braunstein, *Searching for highly entangled multi-qubit states*, Journal of Physics A **38** (2005), no. 5, 1119–1131.

[55] Jean-Luc Brylinski, *Algebraic measures of entanglement*, arXiv preprint arXiv :quant-ph/0008031 (2000).

[56] Lucas Budai, Hamza Jaffali, and Ismaël Nounouh, *Principes fondamentaux de l'information quantique*, June 2014.

[57] Enrico Carlini, Nathan Grieve, and Luke Oeding, *Four lectures on secant varieties*, Connections Between Algebra, Combinatorics, and Geometry (New York, NY) (Susan M. Cooper and Sean Sather-Wagstaff, eds.), Springer New York, 2014, pp. 101–146.

[58] Arthur Cayley, *The collected mathematical papers : On the theory of determinants*, (2009).

[59] ———, *The collected mathematical papers : On the theory of linear transformations*, (2009).

[60] Alba Cervera-Lierta, *Maximal entanglement in quantum computation*, Book of abstracts (2019), 36–37.

[61] Shantanav Chakraborty, Subhashish Banerjee, Satyabrata Adhikari, and Atul Kumar, *Entanglement in the grover's search algorithm*, arXiv preprint arXiv :1305.4454 (2013).

[62] Daniel Chan, *Adventures in pure mathematics – projective varieties*, May 2017.

[63] ———, *Adventures in pure mathematics – quadric surface*, August 2017.

[64] Kai Chen and Ling-An Wu, *The generalized partial transposition criterion for separability of multipartite quantum states*, Physics Letters A **306** (2002), no. 1, 14–20.

[65] Lin Chen and Dragomir Ž. Đoković, *Proof of the gour-wallach conjecture*, Physical Review A **88** (2013), no. 4.

[66] Zeqian Chen, *Maximal violation of mermin's inequalities*, arXiv preprint arXiv :quant-ph/0407029 (2004).

[67] Xi Cheng, Bohdan Khomtchouk, Norman Matloff, and Pete Mohanty, *Polynomial regression as an alternative to neural nets*, (2018), Preprint .

[68] A Yu Chernyavskiy, *Entanglement measure for multipartite pure states and its numerical calculation*, arXiv preprint (2009).

[69] L. Chiantini, G. Ottaviani, and N. Vannieuwenhoven, *An algorithm for generic and low-rank specific identifiability of complex tensors*, SIAM J. Math. Anal. **35** (2014), no. 4, 1265–1287.

[70] François Chollet et al., *Keras*, 2015, `https://keras.io`.

[71] Matthias Christandl and Andreas Winter, *"squashed entanglement" : An additive entanglement measure*, Journal of Mathematical Physics **45** (2004), no. 3, 829–840.

[72] Oleg Chterental and Dragomir Z. Djokovic, *Normal forms and tensor ranks of pure states of four qubits*, arXiv preprint arXiv :quant-ph/0612184 (2006).

[73] Giansalvo Cirrincione and Maurizio Cirrincione, *Neural-based orthogonal data fitting : The exin neural networks*, 2010.

[74] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt, *Proposed experiment to test local hidden variable theories*, Physical Review Letters **23** (1969), no. 15, 880–884.

[75] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo, *How to share a quantum secret*, Phys. Rev. Lett. **83** (1999), 648–651.

[76] Daniel Geoffrey Collins, Nicolas Gisin, Sandu Popescu, David Anthony Roberts, and Valerio Scarani, *Bell-type inequalities to detect true n-body nonseparability*, Physical Review Letters **88** (2002), no. 17, 170405.

[77] D.A. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, Graduate Texts in Mathematics, Springer New York, 2005.

[78] Balázs Csanád Csáji et al., *Approximation with artificial neural networks*, Faculty of Sciences, Etvs Lornd University, Hungary **24** (2001), no. 48, 7.

[79] George Cybenko, *Approximation by superpositions of a sigmoidal function*, Mathematics of Control, Signals, and Systems **5** (1989), no. 4, 455–455.

[80] Aidan Dang, Charles D. Hill, and Lloyd C. L. Hollenberg, *Optimising matrix product state simulations of shor's algorithm*, arXiv preprint arXiv :1712.07311 **3** (2019), 116.

[81] Henri de Boutray, Hamza Jaffali, Frédéric Holweck, Alain Giorgetti, and Pierre-Alain Masson, *Mermin polynomials for entanglement evaluation in grover's algorithm and quantum fourier transform*, 2020.

[82] V. de Silva and L.-H. Lim, *Tensor rank and the ill-posedness of the best low-rank approximation problem*, SIAM J. Matrix Anal. Appl. **30** (2008), 1084–1127.

[83] Olivier Debarre, *Introduction à la géométrie algébrique*, Université Louis Pasteur, 1999.

[84] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, *Singular 3-1-6 – A computer algebra system for polynomial computations*, `http://www.singular.uni-kl.de`, 2013.

[85] Alexandru Dimca, *Milnor numbers and multiplicities of dual varieties*, Revue Roumaine de Mathématiques Pures et Appliquées **31** (1986), no. 6, 535–538.

[86] Timothy Dozat, *Incorporating Nesterov momentum into Adam*, 2016, Available at `http://cs229.stanford.edu/proj2015/054_report.pdf`.

[87] W. Dür, G. Vidal, and J. I. Cirac, *Three qubits can be entangled in two inequivalent ways*, Physical Review A **62** (2000), no. 6, 62314.

[88] G Dreyfus, Martinez J.-M., M Samuelides, M B Gordon, F Badran, S Thiria, and L Hérault, *Réseaux de neurones - méthodologie et applications*, (2002).

[89] Christoph Dürr, Mark Heiligman, Peter HOyer, and Mehdi Mhalla, *Quantum query complexity of some graph problems*, SIAM Journal on Computing **35** (2006), no. 6, 1310–1328.

[90] Christoph Dürr and Peter Høyer, *A quantum algorithm for finding the minimum*, arXiv preprint arXiv :quant-ph/9607014 (1996).

[91] Richard O. Duda and Peter E. Hart, *Pattern classification and scene analysis*, A Wiley-Interscience Publication (1973).

[92] Emilie Dufresne, Parker Edwards, Heather Harrington, and Jonathan Hauenstein, *Sampling real algebraic varieties for topological data analysis*, 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), IEEE, 2019, pp. 1531–1536.

[93] Eugene Dumitrescu, *Tree tensor network approach to simulating shor's algorithm*, Physical Review A **96** (2017), no. 6.

[94] Albert Einstein, Boris Podolsky, and Nathan Rosen, *Can quantum mechanical description of physical reality be considered complete*, Physical Review **47** (1935), no. 10, 777–780.

[95] Jens Eisert and Hans J. Briegel, *Schmidt measure as a tool for quantifying multiparticle entanglement*, Physical Review A **64** (2001), no. 2.

[96] Artur K. Ekert and R. Jozsa, *Quantum algorithms : entanglement-enhanced information processing*, Philosophical Transactions of the Royal Society B (1998).

[97] M Enríquez, I Wintrowicz, and K Życzkowski, *Maximally entangled multipartite states : A brief survey*, Journal of Physics : Conference Series **698** (2016), 012003.

[98] Yiyuan Fang, Dagomir Kaszlikowski, Chunming Chin, Ken Tay, L.C. Kwek, and C.H. Oh, *Entanglement in the grover search algorithm*, Physics Letters A **345** (2005), no. 4, 265–272.

[99] Richard P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics **21** (1982), no. 6, 467–488.

[100] Richard P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics **21** (1999), 133–153.

[101] Gerd Fischer and Jens Piontkowski, *Ruled varieties : An introduction to algebraic differential geometry*, 2001.

[102] T. M. Forcer, A. J. G. Hey, D. A. Ross, and P. G. R. Smith, *Superposition, entanglement and quantum computation*, Quantum Information & Computation **2** (2002), no. 2, 97–116.

[103] Kazuo Fujikawa, C. H. Oh, and Koichiro Umetsu, *A classical limit of grover's algorithm induced by dephasing : Coherence versus entanglement*, Modern Physics Letters A **34** (2019), 1950146.

[104] Wojciech Ganczarek, Marek Kuś, and Karol Życzkowski, *Barycentric measure of quantum entanglement*, Physical Review A **85** (2012), no. 3, 32314.

[105] Remi Geiger and Michael Trupke, *Proposal for a quantum test of the weak equivalence principle with entangled atomic species*, Phys. Rev. Lett. **120** (2018), 043602.

[106] Izrail Moiseevich Gelfand, M. M. Kapranov, and Andrey V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, 1994.

[107] V. Di Gesù and G.M. Palma, *Quantum computing : A way to break complexity ?*, The Nature of Time : Geometry, Physics and Perception (2003), 209–220.

[108] Sibasish Ghosh, Guruprasad Kar, Anirban Roy, Aditi Sen, and Ujjwal Sen, *Distinguishability of bell states.*, Physical Review Letters **87** (2001), no. 27, 277902.

[109] G.J. Gibson and C.F.N. Cowan, *On the decision regions of multilayer perceptrons*, Proceedings of the IEEE **78** (1990), no. 10, 1590–1594.

[110] N. Gisin, *Bell's inequality holds for all non-product states*, Physics Letters A **154** (1991), 201–202.

[111] Tim Güneysu, Vadim Lyubashevsky, and Thomas Pöppelmann, *Practical lattice-based cryptography : a signature scheme for embedded systems*, CHES'12 Proceedings of the 14th international conference on Cryptographic Hardware and Embedded Systems, 2012, pp. 530–547.

[112] Gilad Gour and Nolan R. Wallach, *Entanglement of subspaces and error-correcting codes*, Phys. Rev. A **76** (2007), 042309.

[113] Gilad Gour and Nolan R. Wallach, *All maximally entangled four-qubit states*, Journal of Mathematical Physics **51** (2010), no. 11, 112201–112201.

[114] Lishen. Govender, *Determination of quantum entanglement concurrence using multilayer perceptron neural networks.*, Ph.D. thesis, 2017.

[115] Markus Grassl, Martin Rotteler, and Thomas Beth, *Computing local invariants of qubit systems*, Physical Review A **58** (1998), no. 3, 1833–1839.

[116] Johnnie Gray, Leonardo Banchi, Abolfazl Bayat, and Sougato Bose, *Machine-learning-assisted many-body entanglement measurement*, Phys. Rev. Lett. **121** (2018), no. 15.

[117] Lov K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, 1996, pp. 212–219.

[118] B. Gurevich, G. B., J. R. M. Radok, and A. J. M. Spencer, *Foundations of the theory of algebraic invariants*, American Mathematical Monthly **73** (1966), no. 4, 434.

[119] Saeed Haddadi and Mohammad Bohloul, *A brief overview of bipartite and multipartite entanglement measures*, International Journal of Theoretical Physics **57** (2018), no. 12, 3912–3916.

[120] S. Hameroff, *Time, consciousness and quantum events in fundamental spacetime geometry*, The Nature of Time : Geometry, Physics and Perception (2003), 77–89.

[121] Muhammad Hamidullah, *Le noble coran et la traduction en langue française de ses sens*, Sana, 2004, S36 - V40.

[122] Yassine Hamoudi and Frédéric Magniez, *Quantum chebyshev's inequality and applications*, arXiv preprint arXiv :1807.06456 (2018).

[123] Boris Hanin, *Universal function approximation by deep neural nets with bounded width and ReLU activations*, Mathematics **7** (2019), no. 10, 992.

[124] M.H. Hassoun, *Fundamentals of artificial neural networks*, 1995.

[125] Simon Haykin, *Neural networks : A comprehensive foundation*, 1998.

[126] M. Hebenstreit, C. Spee, and B. Kraus, *Maximally entangled set of tripartite qutrit states and pure state separable transformations which are not possible via local operations and classical communication*, Physical Review A **93** (2016), no. 1.

[127] Victoria Hernández-Mederos and Jorge Estrada-Sarlabous, *Sampling points on regular parametric curves with control of their distribution*, Computer Aided Geometric Design **20** (2003), no. 6, 363–382.

[128] Hoshang Heydari, *Geometrical structure of entangled states and the secant variety*, Quantum Information Processing **7** (2008), no. 1, 43–50.

[129] A. Higuchi and A. Sudbery, *How entangled can two couples get*, Physics Letters A **273** (2000), no. 4, 213–217.

[130] Frank L Hitchcock, *Multiple invariants and generalized rank of a p-way matrix or tensor*, Journal of Mathematics and Physics **7** (1928), 39–79.

[131] Frédéric Holweck and Hamza Jaffali, *Three-qutrit entanglement and simple singularities*, Journal of Physics A **49** (2016), no. 46, 465301.

[132] Frédéric Holweck, Hamza Jaffali, and Jean-Gabriel Luque, *Maximally entangled symmetric states from invariants of binary forms*, 2021.

[133] Frédéric Holweck, Hamza Jaffali, and Ismaël Nounouh, *Grover's algorithm and the secant varieties*, Quantum Information Processing **15** (2016), no. 11, 4391–4413.

[134] Frédéric Holweck, Hamza Jaffali, and Luke Oeding, *Entanglement of fermionic systems from hyperpfaffians*, 2021.

[135] Frédéric Holweck, Jean-Gabriel Luque, and Jean-Yves Thibon, *Geometric descriptions of entangled states by auxiliary varieties*, Journal of Mathematical Physics **53** (2012), no. 10, 102203.

[136] ———, *Entanglement of four qubit systems : A geometric atlas with polynomial compass i (the finite world)*, Journal of Mathematical Physics **55** (2014), no. 1, 12202.

[137] Frédéric Holweck, Jean-Gabriel Luque, and Michel Planat, *Singularity of type d4 arising from four-qubit systems*, Journal of Physics A : Mathematical and Theoretical **47** (2014), no. 13, 135301.

[138] Frédéric Holweck, Jean-Gabriel Luque, and Jean-Yves Thibon, *Entanglement of four-qubit systems : A geometric atlas with polynomial compass ii (the tame world)*, Journal of Mathematical Physics **58** (2017), no. 2, 022201.

[139] Frédéric Holweck and Luke Oeding, *Hyperdeterminants from the E_8 Discriminant*, arxiv e-prints (2018), arxiv :1810.05857.

[140] Kurt Hornik, *Approximation capabilities of multilayer feedforward networks*, Neural Networks **4** (1991), no. 2, 251–257.

[141] Y. Huang, *Entanglement detection : Complexity and shannon entropic criteria*, IEEE Transactions on Information Theory **59** (2013), no. 10, 6774–6778.

[142] Robert Hübener, Matthias Kleinmann, Tzu-Chieh Wei, Carlos González-Guillén, and Otfried Gühne, *Geometric measure of entanglement for symmetric states*, Physical Review A **80** (2009), no. 3, 032324.

[143] Peter Huggins, Bernd Sturmfels, Josephine Yu, and Debbie S. Yuster, *The hyperdeterminant and triangulations of the 4-cube*, Mathematics of Computation **77** (2008), no. 263, 1653–1679.

[144] A. G. Ivakhnenko, *Polynomial theory of complex systems*, systems man and cybernetics **1** (1971), no. 4, 364–378.

[145] Toshihiro Iwai, *The geometry of multi-qubit entanglement*, Journal of Physics A **40** (2007), no. 40, 12161–12184.

[146] Toshihiro Iwai, Naoki Hayashi, and Kimitake Mizobe, *The geometry of entanglement and grover's algorithm*, Journal of Physics A **41** (2008), no. 10, 105202.

[147] Hamza Jaffali and Frédéric Holweck, *Quantum entanglement involved in grover's and shor's algorithms : the four-qubit case*, Quantum Information Processing **18** (2019), no. 5, 133.

[148] Hamza Jaffali and Ismaël Nounouh, *Théorie de l'information quantique : Applications à l'energie*, January 2017.

[149] Hamza Jaffali and Luke Oeding, *Learning algebraic models of quantum entanglement*, Quantum Information Processing **19** (2020), no. 9, 279.

[150] Gareth James, Daniela Witten, Trevor Hastie, and Robert Tibshirani, *An introduction to statistical learning : with applications in r*, Springer-Verlag New York, 2013.

[151] Kristan Jensen and Andreas Karch, *Holographic dual of an einstein-podolsky-rosen pair has a wormhole.*, Physical Review Letters **111** (2013), no. 21, 211602.

[152] Camille Jordan, *Réduction d'un réseau de formes quadratiques oubilinéaires (deuxième partie)*, Journal de mathématiques pures et appliquées 6ème série **Tome 3** (1907), 5–51.

[153] Antoine Joux, *A one round protocol for tripartite diffie–hellman*, Journal of Cryptology **17** (2004), no. 4, 263–276.

[154] Richard Jozsa and Noah Linden, *On the role of entanglement in quantum-computational speed-up*, arXiv preprint arXiv :quant-ph/0201143 **459** (2003), no. 2036, 2011–2032.

[155] V.G. Kac, *Some remarks on nilpotent orbits*, Journal of Algebra **64** (1980), no. 1, 190–213.

[156] Vivien M. Kendon and William J. Munro, *Entanglement and its role in shor's algorithm*, Quantum Information & Computation **6** (2006), no. 7, 630–640.

[157] Iordanis Kerenidis, Jonas Landman, Alessandro Luongo, and Anupam Prakash, *q-means : A quantum algorithm for unsupervised machine learning*, Advances in Neural Information Processing Systems, 2019, pp. 4136–4146.

[158] Tarun Khanna, *Foundations of neural networks*, 1990.

[159] Joe Kileel, Matthew Trager, and Joan Bruna, *On the expressive power of deep polynomial neural networks*, Advances in Neural Information Processing Systems, 2019, pp. 10310–10319.

[160] Benoit Kloeckner, *Un bref aperçu de la géométrie projective*, 2012.

[161] Friedrich Knop, *Ein neuer zusammenhang zwischen einfachen gruppen und einfachen singularitäten*, Inventiones Mathematicae **90** (1987), no. 3, 579–604.

[162] Joseph P. S. Kung and Gian-Carlo Rota, *The invariant theory of binary forms*, Bulletin of the American Mathematical Society **10** (1984), no. 1, 27–85.

[163] S. Y. Kung, K. Diamantaras, W. D. Mao, and J. S. Taur, *Generalized perceptron networks with nonlinear discriminant functions*, Neural Networks (1992), 245–279.

[164] J. M. Landsberg, *The border rank of the multiplication of 2×2 matrices is seven*, Journal of the American Mathematical Society **19** (2006), no. 2, 447–459.

[165] ———, *Tensors : Geometry and applications*, 2011.

[166] B P Lanyon, T J Weinhold, Nathan K Langford, M Barbieri, Df James, Alexei Gilchrist, and A G White, *Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement*, Physical Review Letters **99** (2007), no. 25.

[167] Constantin Le Paige, *Sur la théorie des formes binaires à plusieurs séries de variables*, Bull. Acad. Roy. Sci.Belgique **3** (1881), no. bf 2, 40–53.

[168] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, *Deep learning*, Nature **521** (2015), no. 7553, 436–444.

[169] Matthew S. Leifer, N. Linden, and A. Winter, *Measuring polynomial invariants of multiparty quantum states*, Physical Review A **69** (2004), no. 5, 52304.

[170] Hong-Xing Li and E.S. Lee, *Interpolation functions of feedforward neural networks*, Computers & Mathematics With Applications **46** (2003), no. 12, 1861–1874.

[171] N. Linden and S. Popescu, *On multi-particle entanglement*, Protein Science **46** (1998), 567–578.

[172] Richard P. Lippmann, *An introduction to computing with neural nets*, ACM Sigarch Computer Architecture News **16** (1988), no. 1, 7–25.

[173] B. Llanas and F. J. Sainz, *Constructive approximate interpolation by neural networks*, Journal of Computational and Applied Mathematics **188** (2006), no. 2, 283–308.

[174] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost, *Quantum principal component analysis*, Nature Physics **10** (2014), no. 9, 631–633.

[175] Chao-Yang Lu, Daniel E. Browne, Tao Yang, and Jian-Wei Pan, *Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits.*, Physical Review Letters **99** (2007), no. 25, 250504.

[176] Sirui Lu, Shilin Huang, Keren Li, Jun Li, Jianxin Chen, Dawei Lu, Zhengfeng Ji, Yi Shen, Duanlu Zhou, and Bei Zeng, *Separability-entanglement classifier via machine learning*, Phys. Rev. A **98** (2018), no. 1.

[177] Zhou Lu, Hongming Pu, Feicheng Wang, Zhiqiang Hu, and Liwei Wang, *The expressive power of neural networks : A view from the width*, neural information processing systems (2017), 6231–6239.

[178] Yu Luo and Yongming Li, *Monogamy of αth power entanglement measurement in qubit systems*, Annals of Physics **362** (2015), no. Supplement C, 511 – 520.

[179] Jean-Gabriel Luque, *Invariants of hypermatrices*, Habilitation à diriger des recherches, Université de Marne la Vallée, December 2008.

[180] Jean-Gabriel Luque and Jean-Yves Thibon, *Polynomial invariants of four qubits*, Physical Review A **67** (2003), no. 4, 42303.

[181] ———, *Algebraic invariants of five qubits*, J. Physics A **39** (2006), no. 2, 371–377.

[182] Jean-Gabriel Luque, Jean-Yves Thibon, and Frédéric Toumazet, *Unitary invariants of qubit systems*, Mathematical Structures in Computer Science **17** (2007), no. 6, 1133–1151.

[183] Péter Lévay, *Geometry of three-qubit entanglement*, Physical Review A **71** (2005), no. 1, 12334.

[184] Yue-Chi Ma and Man-Hong Yung, *Transforming Bell's inequalities into state classifiers with machine learning*, npj Quantum Information **4** (2018), no. 1, 34.

[185] Ettore Majorana, *Atomi orientati in campo magnetico variabile*, Il Nuovo Cimento **9** (1932), no. 2, 43–50.

[186] Juan Maldacena and Leonard Susskind, *Cool horizons for entangled black holes*, Protein Science **61** (2013), no. 9, 781–811.

[187] Warren S. McCulloch and Walter Pitts, *A logical calculus of the ideas immanent in nervous activity*, Bulletin of Mathematical Biology **52** (1990), no. 4, 99–115.

[188] N. David Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states*, Phys. Rev. Lett. **65** (1990), 1838–1840.

[189] David A. Meyer and Nolan R. Wallach, *Global entanglement in multiparticle systems*, Journal of Mathematical Physics **43** (2002), no. 9, 4273–4278.

[190] Akimasa Miyake, *Classification of multipartite entangled states by multidimensional determinants*, Physical Review A **67** (2003), no. 1.

[191] Akimasa Miyake and Miki Wadati, *Multipartite entanglement and hyperdeterminants*, Quantum Information & Computation **2** (2002), no. 7, 540–555.

[192] H Mäkelä and A Messina, *N-qubit states as points on the bloch sphere*, Physica Scripta **2010** (2010), 14054.

[193] Ashley Montanaro, *Quantum algorithms : an overview*, npj Quantum Information **2** (2016), no. 1, 15023.

[194] Yonatan Most, Yishai Shimoni, and Ofer Biham, *Entanglement of periodic states, the quantum fourier transform, and shor's factoring algorithm*, Physical Review A **81** (2010), no. 5, 52306.

[195] David Mumford, John Fogarty, and Frances Kirwan, *Geometric invariant theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 2. Folge, vol. 34, Springer-Verlag Berlin Heidelberg, 1994.

[196] Jiang Nan and Lu Wei, *Quantum coherence and quantum entanglement method based on grover search algorithm*, 2018.

[197] Hendrik Poulsen Nautrup, Nicolas Delfosse, Vedran Dunjko, Hans J Briegel, and Nicolai Friis, *Optimizing quantum error correction codes with reinforcement learning*, Quantum **3** (2019), 215.

[198] John Von Neumann, *Mathematical foundations of quantum mechanics*, 1955.

[199] M. A. Nielsen, *Conditions for a class of entanglement transformations*, Physical Review Letters **83** (1999), no. 2, 436–439.

[200] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information : 10th anniversary edition*, 2011.

[201] A G Nurmiev, *Orbits and invariants of cubic matrices of order three*, Sbornik Mathematics **191** (2000), no. 5, 717–724.

[202] Luke Oeding, *Hyperdeterminants of polynomials*, Advances in Mathematics **231** (2012), no. 3, 1308 – 1326.

[203] Sung-Kwun Oh, Witold Pedrycz, and Byoung-Jun Park, *Polynomial neural networks architecture : analysis and design*, Computers & Electrical Engineering **29** (2003), no. 6, 703 – 725.

[204] Theobald Oliver, *Machine learning for absolute beginners : A plain english introduction*, Machine Learning from Scratch Series, Independently Published, 2018.

[205] P.J. Olver, P.J. Olver, C.M. Series, and J.W. Bruce, *Classical invariant theory*, Classical Invariant Theory, Cambridge University Press, 1999.

[206] Hong Choon Ong, Choon , Lim Chee Kang, and Yong Yeow Wui, *Non linear approximations using multi-layered perceptions and polynomial regressions*, Proceedings of the 2nd IMT-GT Regional Conference on Mathematics, Statistics and Applications, Universiti Sains Malaysia, Penang, June 13-15 (2006).

[207] Roman Orus and Jose I. Latorre, *Universality of entanglement and quantum computation complexity*, Physical Review A **69** (2004), no. 5, 52308.

[208] Andreas Osterloh and Jens Siewert, *Entanglement monotones and maximally entangled states in multipartite qubit systems*, International Journal of Quantum Information **4** (2006), no. 3, 531–540.

[209] Luca Pagani and Paul J. Scott, *Curvature based sampling of curves and surfaces*, Computer Aided Geometric Design **59** (2018), 32–48.

[210] Minghua Pan, Daowen Qiu, Paulo Mateus, and Jozef Gruska, *Entangling and disentangling in grover's search algorithm*, Theoretical Computer Science **773** (2019), 138–152.

[211] Minghua Pan, Daowen Qiu, and Shenggen Zheng, *Global multipartite entanglement dynamics in grover's search algorithm*, Quantum Information Processing **16** (2017), no. 9, 211.

[212] P G Parfenov, *Tensor products with finitely many orbits*, Russian Mathematical Surveys **53** (1998), no. 3, 635–636.

[213] S. Parker and M. B. Plenio, *Entanglement simulations of shor's algorithm*, Journal of Modern Optics **49** (2002), no. 8, 1325–1353.

[214] M. H. Partovi, *Universal measure of entanglement*, Physical Review Letters **92** (2004), no. 7, 77904.

[215] A. Parusiński, *Multiplicity of the dual variety*, Bulletin of the London Mathematical Society **23** (1991), no. 5, 429–436.

[216] Anirban Pathak, *Elements of quantum computation and quantum communication*, 2013.

[217] Arun K Pati and Samuel L Braunstein, *Role of entanglement in quantum computation*, Journal of the Indian Institute of Science **89** (2012), no. 3, 295–302.

[218] Benjamin Perez-Garcia, Raul I. Hernandez-Aranda, Andrew Forbes, and Thomas Konrad, *The first iteration of grover's algorithm using classical light with orbital angular momentum*, Journal of Modern Optics **65** (2018), no. 16, 1942–1948.

[219] Ri Qu, Bingjian Shang, Yanru Bao, Dawei Song, Chunming Teng, and Zhiwei Zhou, *Multipartite entanglement in grover's search algorithm*, Natural Computing **14** (2015), no. 4, 683–689.

[220] Yihui Quek, Stanislav Fort, and Hui Khoon Ng, *Adaptive quantum state tomography with neural networks*, (2018), Preprint .

[221] Mukund Rangamani and Massimiliano Rota, *Entanglement structures in qubit systems*, Journal of Physics A **48** (2015), no. 38, 385301–385301.

[222] Rohit Raturi, *Large data analysis via interpolation of functions : Interpolating polynomials vs artificial neural networks*, American Journal of Intelligent Systems **8** (2018), no. 1, 6–11.

[223] Robert Raussendorf and Hans J. Briegel, *A one-way quantum computer*, Phys. Rev. Lett. **86** (2001), 5188–5191.

[224] Patrick Rebentrost, Masoud Mohseni, and Seth Lloyd, *Quantum support vector machine for big data classification*, Phys. Rev. Lett. **113** (2014), no. 13, 130503.

[225] Alfréd Rényi, *Probability theory*, 1970.

[226] M. Rossi, D. Bruß, and C. Macchiavello, *Scale invariance of entanglement dynamics in grover's quantum search algorithm*, Physical Review A **87** (2013), no. 2, 22331.

[227] M Rossi, D Bruß, and C Macchiavello, *Hypergraph states in grover's quantum search algorithm*, Physica Scripta **2014** (2014), 14036.

[228] David E. Rumelhart, Geoffrey E. Hinton, and Ronald J. Williams, *Learning internal representations by error propagation*, Neurocomputing : foundations of research (1988), 673–695.

[229] W. Saddler, *Triple binary forms ; the complete system for a single (1, 1, 1) form with its geometrical interpretation*, Mathematical Proceedings of the Cambridge Philosophical Society **22** (1925), no. 5, 688–693.

[230] Metod Saniga, Frédéric Holweck, and Hamza Jaffali, *Taxonomy of three-qubit mermin pentagrams*, Symmetry **12** (2020), no. 4, 534.

[231] Gábor Sárosi and Péter Lévay, *Entanglement classification of three fermions with up to nine single-particle states*, Phys. Rev. A **89** (2014), 042310.

[232] J Schliemann, *Entanglement in SU(2)-invariant quantum systems : The PPT criterion and others*, Phys. Rev. A **68** (2005), no. quant-ph/0503123. 1, 012309. 7 p.

[233] D. Schlingemann and R. F. Werner, *Quantum error-correcting codes associated with graphs*, Phys. Rev. A **65** (2001), 012308.

[234] E. Schrödinger, *Die gegenwärtige situation in der quantenmechanik*, Naturwissenschaften **23** (1935), no. 50, 807–812.

[235] ———, *Discussion of probability relations between separated systems*, Mathematical Proceedings of the Cambridge Philosophical Society **31** (1935), no. 4, 555–563.

[236] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione, *The quest for a quantum neural network*, Quantum Information Processing **13** (2014), no. 11, 2567–2586.

[237] ———, *An introduction to quantum machine learning*, Contemporary Physics **56** (2015), no. 2, 172–185.

[238] L. Schwartz and J.P. Bourguignon, *Les tenseurs*, Actualités scientifiques et industrielles, Hermann, 1975.

[239] Fabio Sebastiano, Harald Homulle, Bishnu Patra, Rosario Incandela, Jeroen Dijk, Lin Song, Masoud Babaie, Andrei Vladimirescu, and E. Charbon, *Cryo-cmos electronic control for scalable quantum computing : Invited*, 06 2017, pp. 1–6.

[240] C. E. Shannon, *The mathematical theory of communication*, 1949.

[241] Yu-Bo Sheng and Lan Zhou, *Distributed secure quantum machine learning*, Science Bulletin **62** (2017), no. 14, 1025–1029.

[242] Yishai Shimoni, Daniel Shapira, and Ofer Biham, *Entangled quantum states generated by shor's factoring algorithm*, Physical Review A **72** (2005), no. 6, 62308.

[243] Y. Shin and J. Ghosh, *Approximation of multivariate functions using ridge polynomial networks*, [Proceedings 1992] IJCNN International Joint Conference on Neural Networks, vol. 2, 1992, pp. 380–385.

[244] ———, *Ridge polynomial networks*, IEEE Transactions on Neural Networks **6** (1995), no. 3, 610–622.

[245] Peter W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing **26** (1997), no. 5, 1484–1509.

[246] Jean-Claude Sidler, *Géométrie projective : Cours, exercices et problèmes corrigés*, 2ème édition ed., DUNOD, 2009.

[247] R. Simon, *Peres-horodecki separability criterion for continuous variable systems*, Phys. Rev. Lett. **84** (2000), 2726–2729.

[248] Karen E. Smith and Joel Rosenberg, *Rational and non-rational algebraic varieties : Lectures of jános kollár*, arXiv preprint arXiv :alg-geom/9707013 (1997).

[249] Julian Sonner, *Holographic schwinger effect and the geometry of entanglement*, Physical Review Letters **111** (2013), no. 21, 211603–211603.

[250] Donald F. Specht, *Generation of polynomial discriminant functions for pattern recognition*, IEEE Transactions on Electronic Computers **16** (1967), no. 3, 308–319.

[251] C. Spee, J. I. de Vicente, and B. Kraus, *The maximally entangled set of 4-qubit states*, Journal of Mathematical Physics **57** (2016), no. 5, 052201.

[252] W. M. Stuckey, Michael Silberstein, and Michael Cifone, *Reversing the arrow of explanation in the relational blockworld : Why temporal becoming, the dynamical brain and the external world are all*, Proceedings of the ZiF Interdisciplinary Research Workshop, 2005, pp. 293–316.

[253] Ilya Sutskever, James Martens, George E. Dahl, and Geoffrey E. Hinton, *On the importance of initialization and momentum in deep learning*, Proceedings of The 30th International Conference on Machine Learning, 2013, pp. 1139–1147.

[254] Hiroyasu Tajima, *Deterministic locc transformation of three-qubit pure states and entanglement transfer*, Annals of Physics **329** (2013), 1–27.

[255] Peiyuan Teng, *Accurate calculation of the geometric measure of entanglement for multipartite quantum states*, Quantum Information Processing **16** (2017), no. 7, 181.

[256] E. A. Tevelev, *Projectively dual varieties*, Journal of Mathematical Sciences **117** (2003), no. 6, 4585–4732.

[257] R. M. Thrall and J. H. Chanler, *Ternary trilinear forms in the field of complex numbers*, Duke Mathematical Journal **4** (1938), no. 4, 678–690.

[258] Denis Tolkunov, Vladimir Privman, and P. K. Aravind, *Decoherence of a measure of entanglement*, Physical Review A **71** (2005), no. 6, 60308.

[259] Constantino Tsallis, *Possible generalization of boltzmann-gibbs statistics*, Journal of Statistical Physics **52** (1988), no. 1, 479–487.

[260] V. Vedral and M. B. Plenio, *Entanglement measures and purification procedures*, Phys. Rev. A **57** (1998), 1619–1633.

[261] V. Rao Vemuri, *Artificial neural networks : concepts and control applications*, (1992).

[262] Frank Verstraete, J Dehaene, B De Moor, and Henri Verschelde, *Four qubits can be entangled in nine different ways*, Physical Review A **65** (2002), no. 5, 52112.

[263] Guifré Vidal, *Entanglement monotones*, Journal of Modern Optics **47** (2000), no. 2-3, 355–376.

[264] Guifré Vidal, *Efficient classical simulation of slightly entangled quantum computations.*, Physical Review Letters **91** (2003), no. 14, 147902–147902.

[265] Guifré Vidal and Reinhard F Werner, *Computable measure of entanglement*, Physical Review A **65** (2002), no. 3, 032314.

[266] È B Vinberg, *The weyl group of a grade lie algebra*, Mathematics of The Ussr-izvestiya **10** (1976), no. 3, 463–495.

[267] ———, *Classification of homogeneous nilpotent elements of a semisimple graded lie algebra*, TrudySem. Vektor. Tenzor. Anal. **19** (1979), 155–177.

[268] È. B. Vinberg and A. G. Èlašvili, *A classification of the three-vectors of nine-dimensional space*, Trudy Sem. Vektor. Tenzor. Anal. **18** (1978), 197–233.

[269] Bingjie Wang, *Learning to detect entanglement*, (2017), Preprint .

[270] L. Wang and D.L. Alkon, *Artificial neural networks : oscillations, chaos, and sequence processing*, Neural Networks Technology Series, IEEE Computer Society Press, 1993.

[271] Tzu-Chieh Wei and Paul M. Goldbart, *Geometric measure of entanglement and applications to bipartite and multipartite quantum states*, Phys. Rev. A **68** (2003), 042307.

[272] Jiayan Wen and Wei Cao, *Multipartite entanglement in adiabatic quantum searching algorithm*, 2012 8th International Conference on Natural Computation, 2012, pp. 893–897.

[273] R. F. Werner and M. M. Wolf, *All-multipartite bell-correlation inequalities for two dichotomic observables per site*, Phys. Rev. A **64** (2001), 032112.

[274] Jerzy Weyman and Andrei Zelevinsky, *Singularities of hyperdeterminants*, Annales de l'Institut Fourier **46** (1996), no. 3, 591–644 (en). MR 97m :14050

[275] B. Widrow and M.A. Lehr, *30 years of adaptive neural networks : perceptron, madaline, and backpropagation*, Proceedings of the IEEE **78** (1990), no. 9, 1415–1442.

[276] Nathan Wiebe, Daniel Braun, and Seth Lloyd, *Quantum algorithm for data fitting*, Phys. Rev. Lett. **109** (2012), 050505.

[277] Nathan Wiebe, Ashish Kapoor, and Krysta M. Svore, *Quantum deep learning*, Quantum Info. Comput. **16** (2016), no. 7-8, 541–587.

[278] Wikipédia, *Algorithme de grover — wikipédia, l'encyclopédie libre*, 2019, [En ligne ; Page disponible le 28-octobre-2019].

[279] ———, *Algorithmique — wikipédia, l'encyclopédie libre*, 2019, [En ligne ; Page disponible le 12-octobre-2019].

[280] ———, *Mécanique quantique — wikipédia, l'encyclopédie libre*, 2019, [En ligne ; Page disponible le 29-octobre-2019].

[281] ———, *Postulats de la mécanique quantique — wikipédia, l'encyclopédie libre*, 2019, [En ligne ; Page disponible le 9-décembre-2019].

[282] Wikipedia contributors, *Veronese surface — Wikipedia, the free encyclopedia*, 2018, [Online ; accessed 15-March-2020].

[283] Joanna Wiśniewska and Marek Sawerwain, *Detecting entanglement in quantum systems with artificial neural network*, Intelligent Information and Database Systems (Cham) (Ngoc Thanh Nguyen, Bogdan Trawiński, and Raymond Kosala, eds.), Springer International Publishing, 2015, pp. 358–367.

[284] Ian H. Witten, Eibe Frank, Mark A. Hall, and Christopher J. Pal, *Data mining, fourth edition : Practical machine learning tools and techniques*, 4th ed., Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2016.

[285] Alexander Wong and Nelson Christensen, *Potential multiparticle entanglement measure*, Phys. Rev. A **63** (2001), 044301.

[286] Leonard Wossnig and Simone Severini, *Quantum machine learning : Challenges and opportunities*, Bulletin of the American Physical Society (2019).

[287] Li Xue, Lie Wu, Gen-Chang Cai, and Nian-Quan Jiang, *Maximal entangled four-qubit state and its preparation in cavity qed system*, International Journal of Quantum Information **9** (2011), no. 3, 875–881.

[288] Mu Yang, Chang-liang Ren, Yue-chi Ma, Ya Xiao, Xiang-Jun Ye, Lu-Lu Song, Jin-Shi Xu, Man-Hong Yung, Chuan-Feng Li, and Guang-Can Guo, *Experimental simultaneous learning of multiple nonclassical correlations*, Phys. Rev. Lett. **123** (2019), no. 19, 190401.

[289] Bin Ye, Tingzhong Zhang, Liang Qiu, and Xuesong Wang, *Quantum discord and entanglement in grover search algorithm*, Central European Journal of Physics **14** (2016), no. 1, 171–176.

[290] Ye Yeo and Wee Kang Chua, *Teleportation and dense coding with genuine multipartite entanglement*, Physical Review Letters **96** (2006), no. 6, 60502.

Titre : Étude de l'Intrication dans les Algorithmes Quantiques : Approche Géométrique et Outils Dérivés

Mots clés : intrication, algorithmes quantiques, géométrie algébrique, hyperdéterminants, réseaux de neurones

Résumé : L'intrication quantique est un des phénomènes les plus intéressants et intriguant en Mécanique Quantique, et de surcroit en Théorie de l'Information Quantique. Ressource fondamentale pour le calcul quantique, son rôle dans l'efficacité et la fiabilité des protocoles ou algorithmes quantiques n'est toujours pas totalement compris. Dans cette thèse, nous étudions l'intrication quantique des états multipartites, et notamment la nature de sa présence dans les algorithmes quantiques. L'étude de l'intrication se fait d'un point de vue théorique, en utilisant principalement des outils issus de la géométrie algébrique. Nous nous intéressons alors aux algorithmes de Grover et de Shor et déterminons quelles sont les classes d'intrication présentes (ou non) dans ces algorithmes, et ceci constitue donc une étude qualitative de l'intrication. De plus, nous mesurerons l'intrication quantitativement, à l'aide de mesures algébriques et géométriques, et étudions son évolution tout au long des différentes étapes de ces algorithmes. Nous proposons également des interprétations géométriques originales de ces résultats numériques. D'autre part, nous cherchons également à développer et exploiter de nouveaux outils pour mesurer, caractériser et classifier l'intrication quantique. Ceci se fait dans un premier temps d'un point de vue mathématique en étudiant les singularités des hypersurfaces liées aux systèmes quantiques pour caractériser différentes classes d'intrication. Dans un second temps, nous proposons des candidats pour les états maximalement intriqués, notamment pour les états symétriques et fermioniques, en utilisant des polynômes invariants et une mesure géométrique de l'intrication pour quantifier l'intrication. Enfin, nous avons également adopté une approche de type Machine Learning, notamment en entrainant des réseaux de neurones artificiels de manière supervisée, afin de reconnaitre certaines variétés algébriques modélisant certains types d'intrication précis.

Title : Entanglement in quantum algorithms : geometrical approach and related tools

Keywords : entanglement, quantum algorithms, algebraic geometry, hyperdeterminants, neural networks

Abstract : Quantum entanglement is one of the most interesting phenomenon in Quantum Mechanics, and especially in Quantum Information. It is a fundamental resource in Quantum Computing, and its role in the efficiency and accuracy of quantum algorithms or protocols is not yet fully understood. In this thesis, we study quantum entanglement of multipartite states, and more precisely the nature of entanglement involved in quantum algorithms. This study is theoretical, and uses tools mainly coming from algebraic geometry. We focus on Grover's and Shor's algorithms, and determine what entanglement classes are reached (or not) by these algorithms, and this is the qualitative part of our study. Moreover, we quantitatively measure entanglement, using geometric and algebraic measures, and study its evolution through the several steps of these algorithms. We also propose original geometrical interpretations of the numerical results. On another hand, we also develop and exploit new tools for measuring, characterizing and classifying quantum entanglement. First, from a mathematical point of view, we study singularities of hypersurfaces associated to quantum states in order to characterize several entanglement classes. Secondly, we propose new candidates for maximally entangled states, especially for symmetric and fermionic systems, using polynomial invariants and geometric measure of entanglement. Finally, we use Machine Learning, more precisely the supervised approach using neural networks, to learn how to recognize algebraic varieties directly related with some entanglement classes.

UBFC UNIVERSITE BOURGOGNE FRANCHE-COMTE

Université Bourgogne Franche-Comté
32, avenue de l'Observatoire
25000 Besancon