Calcul quantique : algèbre et géométrie projective

Anne-Céline Baboin

N° d'ordre : Année 2011

THÈSE

présentée à

L'UFR DES SCIENCES ET TECHNIQUES
DE L'UNIVERSITÉ DE FRANCHE-COMTÉ

pour obtenir le

GRADE DE DOCTEUR
DE L'UNIVERSITÉ DE FRANCHE-COMTÉ
spécialité Sciences Pour l'Ingénieur

CALCUL QUANTIQUE : ALGÈBRE ET GÉOMÉTRIE PROJECTIVE

par

Anne-Céline Baboin

Soutenue le 27 Janvier 2011 devant la Commission d'Examen :

Président et Rapporteur	M. Maurice Kibler	Professeur des Universités Université Claude Bernard, Lyon 1
Rapporteur	M. Metod Saniga	Chargé de recherches Astronomical Institute, Slovak Academy of Sciences
	M. Patrick Solé	Directeur de recherche CNRS E.N.S.T. , Paris
Examinateur	M. Pascal Vairac	Professeur des Universités E.N.S.M.M. de Besançon
	M. Fabrice Bouquet	Professeur des Universités Université de Besançon
Directeur de thèse	M. Michel Planat	D.E. - Chargé de Recherche CNRS Institut FEMTO-ST, Besançon

Remerciements

Je remercie Michel Planat d'avoir été mon directeur de thèse, de m'avoir prodigué plusieurs conseils et de m'avoir expliqué dans le détail certains aspects de ses travaux. Je suis très reconnaissante à l'égard de Maurice Kibler pour sa disponibilité tant scientifique qu'humaine, pour ses nombreuses remarques pertinentes, pour avoir apporté grand nombre de corrections à cet essai. Il a vraiment été d'un bon soutien quand j'ai été obligée de terminer la rédaction de ma thèse à Lyon. Je sais gré au directeur de l'école doctorale sciences pour l'ingénieur et microtechniques (ED SPIM), Éric Lantz, d'avoir su tenir compte de circonstances particulières et de m'avoir accordé un an d'interruption de thèse. Cette démarche m'a été conseillée par Rachel Langlet et je ne la remercierai jamais assez. Merci beaucoup à Metod Saniga pour m'avoir aidée à mieux appréhender les droites projectives et pour m'avoir permis de faire un séjour en Slovaquie, séjour qui fut à la fois scientifique et culturel. Je suis également ravie que le directeur du laboratoire d'informatique de Franche-Comté, Jacques Julliand, m'ait donné la possibilité de suivre des cours d'informatique théorique en master 2 en candidat libre. J'ai également eu l'opportunité d'acquérir quelques notions en intelligence artificielle, grâce à Fabrice Bouquet et Christophe Lang, et je tiens à les citer même si ceci ne concerne pas directement l'objet de cette thèse. Philippe Jorrand me fut également d'un grand secours durant cette thèse, surtout en ce qui concerne le calcul quantique basé sur la mesure. Je remercie également Monsieur Dupont, mon professeur de physique en math spé, car il m'a transmis son amour pour la physique et Monsieur Brachet, mon professeur de mathématiques en math sup, pour des raisons similaires. C'est grâce aux travaux d'Alan Turing et au livre de Simon Singh [Sin99] que je me suis intéressée à l'informatique théorique et quantique. Pour finir, je remercie Joëlle Berthelot, la secrétaire de l'accueil, pour sa gentillesse; dans la même veine, il y a Aline Chagrot, Bernard Desmoulin qui s'occupe de la reprographie à l'ENSMM, certains thésards et, bien sûr, mes parents et mon fils Albéric, auxquels je dédie cette thèse. Sans oublier, naturellement, des remerciements anticipés au jury.

Chez toi la mesure est source de démesure,
Mécanique Quantique es-tu si diabolique ?
Dame Réalité devient une imposture
Donc sous quelle optique pourrait le scientifique

Te rendre loquace à moins que la vanité
Ou la quête de la vérité, restons juste,
Ne l'aveugle et qu'il ne mesure la beauté
De ne pouvoir percer tous les desseins qu'ajuste

La divinité. Il est de ces particules
Qui naissent plusieurs en une, sont indiscernables.
L'Amour Absolu régit-il ces corpuscules ?
Ensemble ils prennent une densité palpable.

Est-ce plutôt Passion qui pour l'individu
Est délétère ? Incapable d'exister, il
Fusionne en l'autre, se délocalise, perd son dû,
Oblitère une communion qui sur l'île

De la Félicité l'emmènerait entier.
D'autres évoluent dans un état extatique,
A plusieurs se superposent et prennent pied
Dans un monde étrange dans lequel ils ne tiquent.

Quatre postulats, une singularité,
Apportent leur magie au monde du calcul.
D'aucuns le disent froid, avec sévérité,
A tort car il est le Verbe V majuscule :

Alphabets, mots, langages, grammaires, conjugaisons,
Ses serviteurs et amis, Ses enfants bénis,
Apportent leur contribution avec raison

A l'édifice de l'union de deux génies :

l'Informatique Théorique et la Quantique.
En parallèle, ils déploient des trésors d'astuce.
Des multi-univers, des oracles s'appliquent
A satisfaire cet embryon d'octopus.

Spéciale dédicace à Albéric et à mes parents

Table des matières

Introduction générale

L'informatique quantique... Cette discipline semble au premier abord en être à ses balbutiements et c'est actuellement vrai du point de vue des réalisations concrètes. Cependant, affirmer une telle chose serait renier les bienfaits de toute la théorie qui en a découlé, car c'est ici que des domaines aussi distincts que, la théorie des nombres en mathématiques, celles de la complexité et de la calculabilité en informatique théorique, et la physique quantique, trouvent un « terrain d'entente ».

Historiquement issue de l'étude du rayonnement du corps noir (quantification de l'énergie : pour une onde de fréquence ν, les seules énergies possibles sont des multiples du quantum $h\nu$), du fait que l'électromagnétisme restait impuissant quant à expliquer ce phénomène malgré le caractère ondulatoire de la lumière (diffraction, interférences), la physique quantique joua un rôle fondamental pour la description et la compréhension des phénomènes naturels, dès que ceux-ci se produisent à une échelle atomique ou subatomique. Elle a permis d'unifier les deux concepts suivants : matière (mécanique newtonienne) et rayonnement (électromagnétisme).

Par définition, ce qui est quantique – et uniquement cela – est d'associer un corpuscule matériel d'impulsion $\mathbf{p}$ (ou quantité de mouvement) à une onde, caractérisée par une longueur d'onde λ. Cette association est décrite par la relation de Louis de Broglie : $\lambda = \frac{h}{|\mathbf{p}|}$, où h est la constante de Planck. L'évolution de la fonction d'onde, ψ, décrivant l'onde est régie par l'équation de Schrödinger, en abandonnant l'idée classique selon laquelle, en prenant l'exemple de la mécanique, on définit l'état d'un système par 6 paramètres : 3 de position et 3 de vitesse. On parlera alors de probabilité de présence de la particule et la notion de trajectoire, chère à notre intuition, n'a plus de signification.

La théorie quantique a depuis quelque temps un impact réel sur la technologie. Cela tient en partie aux éclaircissements qu'elle a apportés dans certains domaines d'application technologiquement importants tels que la chimie, la métallurgie (étude du comportement des conducteurs) ou encore l'informatique (transistors). De toute façon, tout objet physique, si on l'analyse suffisamment en détail, est un objet quantique : *« Un tournevis est un objet quantique ! »* affirme par provocation Rolf Landauer. Cela dit, dans le cas d'un ordinateur classique, ce comportement quantique est collectif : si la valeur 0 d'un bit est représentée physiquement dans un ordinateur par un condensateur non chargé, tandis que la valeur 1 l'est par le même condensateur, mais chargé, la différence entre états chargé

et non chargé se traduit par le déplacement de plusieurs millions d'électrons et le côté probabiliste des phénomènes quantiques est « camouflé ». La grande nouveauté, depuis les années 80, est la possibilité pour les physiciens de manipuler et d'observer des objets quantiques individuellement : photons, atomes, ions, ... non plus d'agir uniquement sur le comportement quantique collectif. C'est pourquoi il a été possible de commencer à parler d'information et d'informatique quantique, domaines dans lesquels ces objets quantiques élémentaires que sont les photons, atomes, ions, permettent de construire physiquement les bits quantiques ou *qubits*, homologues des bits classiques.

Plus spécifiquement, c'est dans les années 70 et 80 que les premiers ordinateurs quantiques naissent par retournement dans l'esprit de physiciens, tels que Richard Feynman, David Deutsch ou Charles Bennett : *« Au lieu de nous plaindre que la simulation des phénomènes quantiques demande des puissances énormes à nos ordinateurs actuels, utilisons la puissance de calcul des phénomènes quantiques pour faire plus puissant que nos ordinateurs actuels »* est une célèbre phrase de Feynman dans le domaine. De plus, la miniaturisation croissante des composants électroniques va trouver ses limites en raison des effets quantiques qui vont devenir prédominants en dessous de la dizaine de nanomètres, ce qui est prévu pour 2020 (loi empirique de Moore).

Avant tout définissons précisément ce qu'est la notion de qubit. Le bit – le « légo », ou encore l'atome (au sens étymologique, c'est-à-dire, l'insécable) du monde classique – est égal soit à 0, soit à 1. Le qubit – son homologue quantique – peut avoir non seulement les valeurs 0 et 1, mais également toutes les valeurs intermédiaires : on parle de *superposition linéaire d'états*. L'acte de le mesurer détruit cette superposition (sauf dans les cas où le qubit était déjà à 0 ou 1), et le qubit prend les valeurs 0 ou 1. On pourrait donc croire qu'au final – au sens littéral puisque la mesure est la finalité de toute expérience – bit et qubits sont semblables. On verra qu'il n'en est pourtant rien. La seconde grande propriété à la base de l'information quantique, et visible dès que l'on considère un système à 2 qubits, est celle d'intrication : deux objets, aussi éloignés que l'on veut l'un de l'autre, se comportent comme si ils étaient une entité indissociable. Elle sera précisément expliquée car c'est en grande partie grâce à elle que le calcul quantique est possible. L'intrication et la superposition linéaire sont à la base du parallélisme quantique massif, qui est la possibilité d'effectuer un grand nombre d'opérations en parallèle, mais de façon différente à ce que l'on peut s'attendre via un ensemble d'ordinateurs classiques mis en réseau : c'est un peu comme si les ordinateurs quantiques avaient en plus la capacité de ne former qu'un durant un petit laps de temps.

On pourrait se demander comment est-il possible d'exploiter les propriétés de la mécanique quantique, par essence probabiliste, pour faire du calcul qui se doit d'être déterministe. En fait, les calculs effectués sur les qubits sont tout ce qu'il y a de plus déterministes. Le bémol est dans l'acte d'observation lui-même, c'est-à-dire le fait de mesurer. Tout l'art relatif au calcul quantique consiste alors à s'arranger pour que les résultats soient toujours

les mêmes quelque soit la mesure effectuée. Cet arrangement est possible via des trésors d'astuce qui consistent à « forcer » un système de qubits à coup de transformations successives, afin d'obtenir une configuration adéquate pour un calcul. Jusqu'à maintenant, (à moins que cela soit devenu du ressort des services secrets), il existe deux algorithmes principaux exploitant le parallélisme quantique : l'algorithme de Shor (1994), qui permet de factoriser de grands nombres dans un temps raisonnable à l'aide d'un ordinateur quantique, ce qui est une révolution dans le monde du codage (RSA) et, celui de Grover, qui permet de trouver une entrée dans une base de données non triée. Plusieurs cas d'école en ont été la source d'inspiration et, afin d'introduire le concept d'algorithme quantique, deux d'entre eux, connus sous le nom d'oracle de Deutsch et d'oracle de Simon, seront abordés dans le chapitre 2 de la première partie. L'algorithme de Schor est assez complexe et ne sera que peu discuté, au contraire de celui de Grover, dont l'interprétation géométrique est assez simple.

Mais déjà, qu'est ce que le calcul quantique ou même un calcul classique ? Car même si cette notion est omniprésente dans notre quotidien, surtout depuis qu'il est habité par les ordinateurs, ce n'est pas une sinécure que d'en dégager une définition rigoureuse. On va donc tâcher, dans un premier temps, de définir ce qu'est le calcul classique en exposant le b-a-ba de l'informatique théorique, en espérant ainsi clarifier ce qu'est le calcul avant de s'aventurer dans les méandres de la mécanique quantique.

Une première partie de cette thèse se bornera à être une introduction, sinon exhaustive, assez complète et facile d'accès à cette notion de calcul tant classique (chapitre 1), que quantique (chapitres 2, 3).

La deuxième partie de cet essai utilise un nouveau formalisme tiré de plusieurs horizons des mathématiques et va mettre en évidence de nouvelles facettes de ce domaine fantastique qu'est le calcul quantique. Deux approches originales du calcul quantique seront abordées : la première est de nature algébrique (cf. chapitre 4), la deuxième a plutôt recours à la géométrie projective (cf. chapitre 5).

Première partie

Le calcul dans tous ses états

Chapitre 1

Excursion au sein de l'informatique théorique

Introduction

On ne peut prétendre faire du **calcul** de quelque nature que ce soit sans au moins définir ce que c'est et sans évoquer deux notions importantes : la **calculabilité** (cf. section 1.3.1) et la **complexité** (cf. section 1.3.2), qui ont leurs lettres de noblesse en informatique théorique. La première étudie le fait de savoir si un problème donné peut être résolu « de façon mécanique », c'est-à-dire algorithmiquement, la seconde traite de l'efficacité en termes de ressources (temps, espace, entropie au sens de la théorie de l'information de Claude Shannon), nécessaires au traitement du problème.

Après avoir introduit certains éléments de langage de l'informatique théorique (cf. section 1.1), on examinera des modèles de calcul dits universels, c'est-à-dire des modèles pouvant simuler toutes les fonctions dites calculables, au sens de la calculabilité. Dans le chapitre 2, les divers points fondamentaux du calcul quantique sont exposés en adoptant le modèle des circuits logiques quantiques [CN00], modèle de calcul qui s'impose de prime abord pour sa simplicité, théorique comme pratique, et sa faculté d'adaptation vis-à-vis de ses homologues classiques (circuits électroniques) ; c'est pourquoi ils seront abordés dans le détail (cf. section 1.2.2). Néanmoins, ce choix est critiquable car ce n'est pas ce modèle qui est à l'origine à proprement dit de la notion de calcul : on pourrait aborder l'information quantique et l'informatique quantique avec les yeux des machines de Turing, ce qui a d'ailleurs été fait [Per06], ainsi que via d'autres modèles [Lal06], [Per06], [HDE+05]. Ce sont des machines de Turing, automates accomplis, que découle, originellement, le concept de calcul. C'est pourquoi, même si le choix des circuits logiques quantiques pour expliquer le calcul quantique va s'imposer par la suite, afin de comprendre la notion de calcul, semble-t-il, sinon nécessaire, du moins intéressant, de s'arrêter quelques instants au moins sur les machines de Turing (cf. section 1.3).

Ce chapitre est en partie inspiré du livre de Pierre Wolper [Wol91] intitulé *Introduc-*

tion à la calculabilité ; je le conseille à tout un chacun qui veut explorer les méandres de l'informatique théorique car c'est un chef d'oeuvre de simplicité et d'exhaustivité.

1.1 Le concept de problème

Tout au long de cette section, certains mots seront mis *en italique* ; ils sont en effet très utilisés dans le langage courant mais ont une signification bien particulière quand on parle d'informatique théorique.

Quiconque s'est amusé à faire de la programmation a pu croire, du moins au début, que l'informatique relevait du bricolage. Or il n'en est rien : cette science dans une certaine mesure modélise de façon on ne peut plus rigoureuse la notion de *langage* : ainsi un poème de Lamartine est-il modélisable en terme d'*alphabets*, ensembles finis composés de caractères : ({a,b,c,d,...,z} ou {0,1} ou encore {♢, ♡, ♣, ♠}), de *mots*, qui sont des chaînes finies de ces caractères : (« mortadelle », « 100 », « ♣♣♣♣ »), d'un *langage* (ensemble fini de mots) qui devra, c'est mieux, *accepter* tous les mots du poème (« arrrrrrrrrrgh » par exemple ne sera accepté que par certains langages, mais pas par celui de Microsoft Word). Si ce langage accepte tous les mots du poème et uniquement ceux-ci, il constitue l'ensemble des *instances positives* du poème. Celles-ci sont régies par certaines *grammaires* (ici celle du Becherel) qui permettent, via un ensemble de *règles* (en l'occurrence orthographe, conjugaison), de générer tous les mots du langage... le tout exécuté (en tout cas pour ce qui est de le recopier) par des **automates** (des **programmes**), sans pour autant que le poème en perdre sa saveur ! Bien au contraire.

De façon plus précise, on peut résoudre n'importe quel **problème** soluble en se représentant les instances de celui-ci. Déterminer si un nombre naturel est pair ou non est un problème. L'alphabet associé peut être indifféremment $\{0, 1\}$ ou $\{0, 1, 2, \ldots, 9\}$ et ses mots sont l'ensemble des entiers naturels auxquels on aura fixé une borne supérieure (les mots de longueur infinie ne sont pas admis !). Les instances du problème sont l'ensemble des questions du type : « 4444 est-il pair ? », et donnent toujours lieu à une réponse : ici « oui ». Dans ce cas, il s'agit d'une instance positive. Un problème peut toujours être traduit de telle manière à ce qu'il s'applique à un ensemble d'éléments : ici $\mathbb{N}$, l'ensemble des entiers naturels.

De manière encore plus concrète, déterminer la somme de deux nombres est un problème. Les instances du problème sont l'ensemble des questions du type : « la somme $4+4$ a t-elle pour résultat 8 ? », et donnent toujours lieu à une réponse : ici « oui ».

On se limitera à la **classe** des **problèmes binaires** ou dits **de décision** (deux réponses seulement sont possibles : oui ou non). Elle permet d'appréhender de façon efficace l'ensemble de la problématique, à savoir les limites qualitatives et quantitatives de l'informatique, et nombreux sont ceux exprimables dans cette catégorie. Il est à noter qu'un programme ne définit pas le problème, il se contente de le résoudre lorsque ses instances

sont dans une représentation qui lui convient. La preuve en est qu'il peut y avoir différents programmes pour résoudre un même problème, déjà du fait qu'il existe des alphabets différents. En résumé, résoudre un problème se réduit à *reconnaître un langage*.

Concrètement, même en se limitant à une telle classe de problèmes, ceux-ci peuvent se révéler compliqués. Ainsi, usant du vieil adage « diviser pour mieux régner », utilise-t-on souvent en informatique un outil qualifié **d'oracle** : il s'agit de décomposer le problème en sous-problèmes, c'est-à-dire de décomposer une fonction (binaire en l'occurrence pour cette classe) en sous-fonctions « internes », elles-mêmes binaires. Leur fonctionnement interne, comment les construire, n'intéresse pas au préalable, mis à part leur comportement en sortie suivant l'entrée. Ce sont des « macros » en quelque sorte. Elles sont symbolisées par des « boîtes noires » qui sont des oracles : on les « questionne » en leur affectant une valeur à leur entrée et elles « répondent » en révélant une valeur de sortie, sans pour autant que l'on sache ce qui s'est passé en elles ; un peu comme l'Oracle de la Pythie de la Grèce Antique... On verra dans le chapitre 2, dans l'exemple le plus simple qui soit, que le concept d'oracle est vraiment très bien adapté au calcul quantique, du moins quand on adopte le point de vue des circuits logiques.

1.2 Les modèles de calcul

1.2.1 La machine de Turing

Son histoire :

Historiquement, le concept de la machine de Turing a émergé en réponse à une question que se posait le mathématicien Hilbert, à savoir : n'importe quel problème est-il oui ou non résoluble de façon mécanique ? Hilbert pensait que oui, jusqu'au moment où Alan Turing lui démontra qu'il n'en était rien ! Ainsi est-il des questions dont la réponse n'est ni oui ni non ! Ainsi ce que les philosophes essaient en vain (sans pour autant démériter) de démontrer, les sciences dites « dures » le démontrent rigoureusement, procurant ainsi semble-t-il de l'espérance.

Avant tout, donnons la parole à Alan Turing [Tur36] : *« Un calcul s'effectue normalement sur papier en y écrivant certains symboles. Supposons que l'on découpe la surface de ce papier en petits carrés comme pour un livre d'arithmétique pour enfant. En cours d'arithmétique élémentaire, le caractère* $2D$ *du papier est parfois exploité, mais un tel usage est parfaitement évitable et je pense que tout le monde sera d'accord avec moi pour affirmer que ce caractère n'est pas fondamental pour qui veut faire de l'informatique. C'est pourquoi, je suppose que l'on ne dispose que d'un ruban de papier, à une dimension mais infini, et constitué d'une succession de cases sur lesquelles on peut inscrire des symboles qui sont eux-mêmes en nombre limité. Si l'on permet l'utilisation d'un nombre infini de symboles, ceux-ci vont se différencier avec une précision parfois petite et de toute façon arbitraire. Cette restriction n'a pas d'effets qui méritent d'être relevés : ainsi, en représen-*

tation décimale, 99999999999999999999 est un symbole unique. Dans n'importe quel langage européen, les mots sont considérés comme des symboles uniques à part entière (même si dans la langue chinoise on a tendance à énumérer toujours plus de symboles et de fait leur nombre tend vers l'infini). De toute façon, si on considère 9999999999999999999999 et 99999999999999999999999, un premier regard ne permet pas de les différencier. Le comportement d'un ordinateur à tout instant est déterminé par des symboles qu'il observe, et « ses états d'âme » au moment où il les observe. Supposons qu'il y ait un nombre limité B de symboles ou de carrés différents que l'ordinateur puisse observer à tel moment ; si celui-ci veut observer toujours plus, il doit le faire de façon « successive ». Supposons également que ses états d'esprit soient en nombre limité. La raison d'une telle hypothèse est du même acabit que celle formulée à propos du nombre de symboles. Si on admet l'existence d'un nombre infini d'états d'esprit, certains d'entre eux vont être proches de façon arbitraire, et il sera possible de les confondre. Encore une fois, cette restriction n'a aucune importance en soi pour le calcul, puisque l'utilisation d'états d'âme « plus sophistiqués » peut être évitée en écrivant sur le ruban un nombre plus conséquent de symboles. »

Sa définition :

De façon plus rigoureuse [Wol91], une **machine de Turing** est définie par le *sept-uplet* $(\varrho, \Gamma, \Sigma, \delta, s, B, F)$, où :

- ϱ est un ensemble fini d'états
- Γ est l'alphabet de ruban (l'alphabet utilisé sur le ruban)
- $\Sigma \subseteq \Gamma$ est l'alphabet d'entrée (l'alphabet utilisé pour le mot d'entrée)
- $s \in \varrho$ est l'état initial
- $F \subseteq \varrho$ est l'ensemble des états accepteurs (états pour lesquels la machine s'arrête)
- $B \in F - \Sigma$ est le « symbole blanc », que l'on notera b
- $\delta : \varrho \times \Sigma \to \varrho \times \Gamma \times \{\Leftarrow, \Rightarrow\}$ est la fonction de transition ; $\Leftarrow$ signifie que la tête de lecture/écriture du ruban se déplace d'une case vers la gauche.

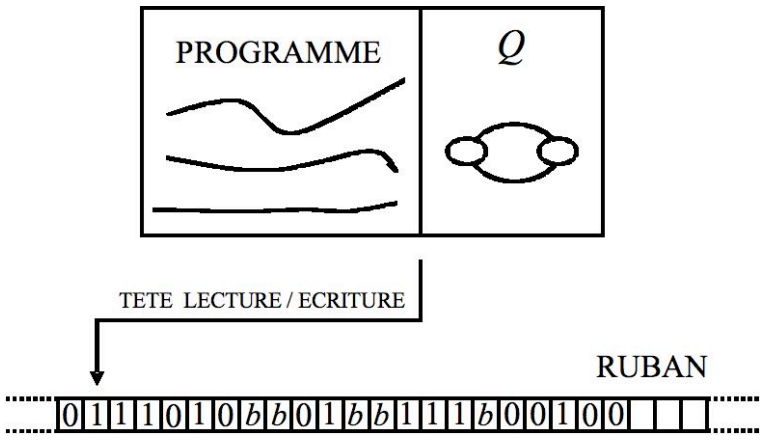


Fig. 1.1 – Machine de Turing

La figure 1.1 illustre de manière basique une machine de Turing (avec $\Gamma = \{0, 1, b\}$). Elle est constituée d'un programme (que l'on notera P pour les exemples qui suivent), pour lequel chaque ligne est une fonction de transition δ_{ij}, d'un ensemble fini d'états ϱ correspondant aux « états d'âme » de la machine qui coordonnent les étapes des opérations, d'un ruban infini jouant le rôle de mémoire en lecture/écriture, et enfin d'une tête de lecture/écriture, permettant de changer ou non les symboles figurant sur le ruban, et de savoir à chaque instant sur quelle case le calcul s'effectue. Une machine de Turing est un ensemble d'instructions simples, plus une mémoire illimitée.

Son universalité :

En tenant pour vraie la thèse de Turing-Church : *« la classe des fonctions calculables par une machine de Turing correspond exactement à la classe des fonctions calculables algorithmiquement »* [Wol91], il est possible d'associer à chaque fonction **calculable**, telle l'addition, la multiplication, une machine de Turing qui, selon ses états et la succession de ses fonctions de transition, permettra de la calculer suivant les entrées écrites au départ sur le ruban. Afin de les distinguer entre elles, on peut les indexer.

On peut démontrer l'existence d'une machine de Turing universelle et même l'écrire en une série de 0 et de 1 ! [Pen92]. Une telle machine est capable de simuler n'importe quelle machine de Turing et constitue par là même un ordinateur universel. On peut également montrer que la représentation en termes de circuits logiques est équivalente à la machine de Turing universelle [CN00].

Certes, la machine de Turing reste un modèle du fait du caractère infini de son ruban et la vitesse d'exécution d'un programme même très simple est effroyablement longue comme le montre l'exemple ci-après, mais elle a permis l'explosion d'une nouvelle discipline : l'informatique.

Un exemple simple : construire une machine de Turing qui calcule la somme de deux nombres représentés en base unaire

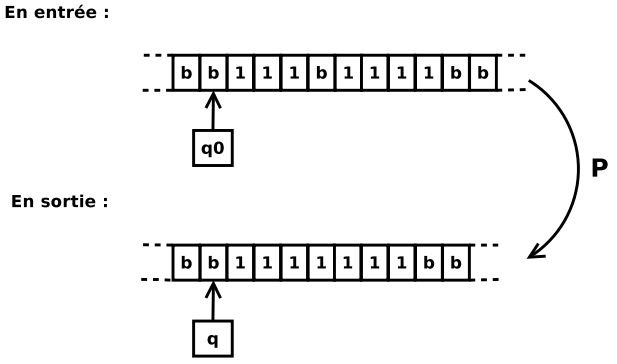


FIG. 1.2 – En entrée, on a les chiffres 3 et 4 en base unaire, séparés par le symbole « blanc » ; en sortie, après l'exécution du programme P, on a 7, soit 3+4, en base unaire.

La machine de Turing pour cet exemple est le *sept-uplet* $M=(\varrho, \Gamma, \Sigma, \delta, s, b, F)$ où

- $\varrho=\{q_0, q_1, q_2, q_3, q_4, q_5\}$,
- $\Gamma=\{1, b\}$,
- $\Sigma=\{1\}$,
- $s = q_0$,
- $F = \{q_5\}$ et
- δ contient les transitions

(1) $(q_0, b) \to (q_1, b, \Rightarrow)$

(2) $(q_1, b) \to (q_2, 1, \Leftarrow)$ $(q_1, 1) \to (q_1, 1, \Rightarrow)$ **(3)**

(4) $(q_2, b) \to (q_3, b, \Rightarrow)$ $(q_2, 1) \to (q_2, 1, \Leftarrow)$ **(5)**

(6) $(q_3, 1) \to (q_4, b, \Rightarrow)$

(7) $(q_4, 1) \to (q_5, 1, \Leftarrow)$

Illustration de l'exemple :

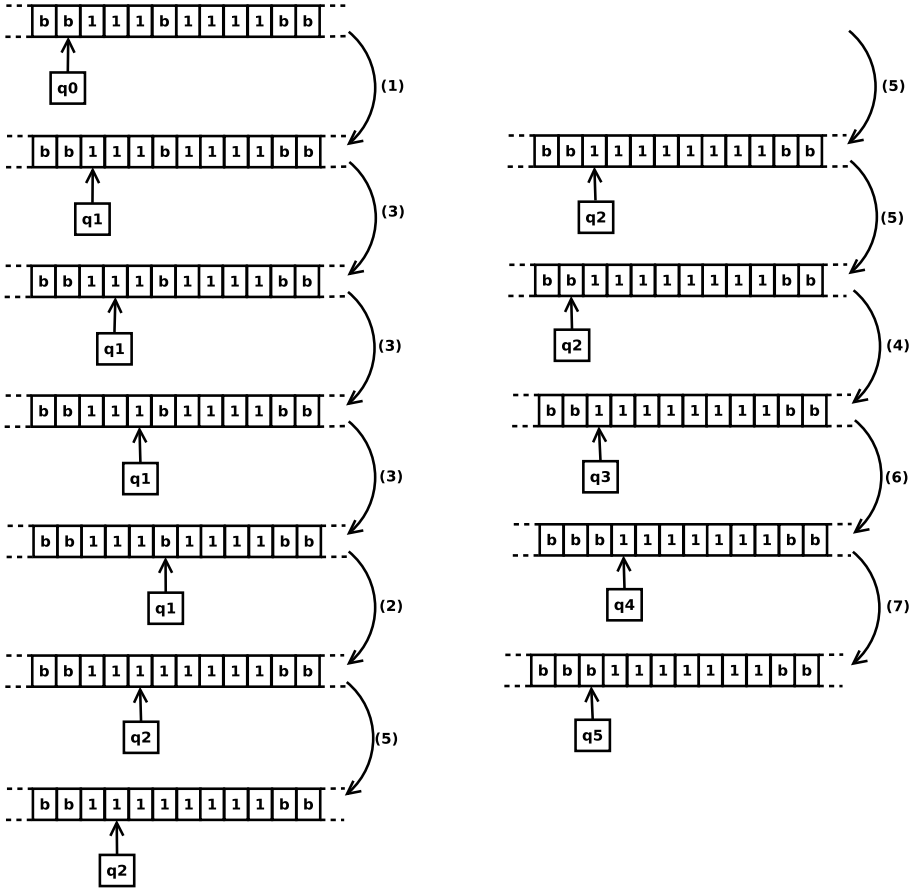


Fig. 1.3 – En entrée, on a les chiffres 3 et 4 en base unaire, séparés par le « symbole blanc » ; en sortie, après l'exécution du programme $P := (1) \to (3) \to (3) \to (3) \to (2) \to (5) \to (5) \to (5) \to (4) \to (6) \to (7)$, on a 7, soit 3+4, en base unaire.

Automate résumant le programme de l'exemple :

À première vue, l'ensemble des transitions qui caractérisent le programme pour cette machine de Turing peut sembler facile à trouver, mais ce n'est pas si trivial que cela et il y a toujours un risque d'oublier un « cas de figure ». C'est pourquoi, surtout quand les exemples se complexifient, est-il important de disposer d'un outil visuel tel que celui qui figure dans le schéma 1.4.

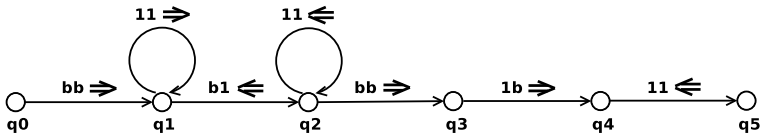


FIG. 1.4 – Automate qui permet de visualiser la fonction de transition de la machine de Turing qui exécute l'addition de deux nombres représentés en base unaire.

1.2.2 Les circuits logiques

Leur histoire :

Pourquoi parle-t-on de circuits logiques ? *A priori*, la logique relève du domaine de la pensée alors que les circuits sont des dispositifs physiques obéissant à des règles précises dont on ne perçoit aucune émanation de pensée.

Il est d'usage de vulgariser le fonctionnement des ordinateurs en disant que ce sont des machines qui représentent et traitent l'information sous forme de zéros et de uns (0/1). Aussi, si on associe respectivement à ces zéros et uns le sens de FAUX et VRAI, on peut relever un prélude de signification au mot logique dans « circuits logiques ». Mais est-ce tout ?

Les circuits logiques, que l'on appelle également circuits numériques, ne se retrouvent pas uniquement dans les ordinateurs : ils envahissent quotidiennement le domaine de la technologique jusqu'à le dominer presque intégralement.

Les termes « logique » et « numérique » puisent leurs origines dans une multitude de disciplines, telles que la philosophie, la cybernétique, les sciences cognitives, les mathématiques, etc.

La philosophie grecque fut l'une des premières à poser la problématique de la validité du raisonnement en termes systématiques. Aristote fut l'instigateur de ce projet qui consistait à établir les règles que suit le raisonnement humain. Ce faisant, Aristote énonça une partie importante des règles de la logique que l'on connaît aujourd'hui, et ces règles furent considérées valides et complètes durant plus de vingt siècles. Ce n'est qu'au début du XXe siècle que ces règles furent interrogées en profondeur, et il fallut pour cela que se mêle à la philosophie d'autres disciplines de la connaissance, principalement les mathématiques. Le lien avec les mathématiques put être établi grâce aux travaux de George Boole. À la fin du XIXe siècle, ce mathématicien britannique autodidacte propose d'écrire les propositions

logiques sous forme d'équations algébriques. Il en simplifie ainsi la manipulation et crée un heureux pont entre l'algèbre et la philosophie.

Cette algèbre de la logique, que l'on appelle depuis algèbre de Boole, remplace les valeurs VRAI et FAUX par les éléments 1 et 0 et les opérateurs logiques (ET, OU) par les opérations arithmétiques de multiplication et d'addition ($\cdot$,+). L'opérateur unaire NON, servant à la négation, est également introduit (-). Elle permet ainsi d'écrire toute proposition logique à l'aide de variables logiques (booléennes) et de manipuler de manière systématique le raisonnement par le développement d'équations mathématiques. L'algèbre de Boole n'allait cependant pas seulement outiller la philosophie d'une notation compacte, elle allait d'une part donner aux mathématiques le *corpus* dont elles allaient avoir besoin pour reconstruire leurs fondements ; et, sous forme appliquée, l'algèbre de Boole allait prendre de l'ampleur et bouleverser le XXe siècle grâce aux travaux en télécommunication de l'ingénieur américain Claude E. Shannon.

À la fin des années trente, Shannon est étudiant à la maîtrise au *Massachusetts Institute of Technology (M.I.T.)* où il travaille sur l'automatisation des circuits à relais (interrupteurs) pour les besoins grandissants de la téléphonie. Au *M.I.T.*, Shannon suit un cours de philosophie où il découvre l'algèbre de Boole, et c'est la révélation.

Aux premiers temps de la télécommunication, la téléphonie reposait sur un large réseau de relais permettant de mettre en communication les usagers. Un relais était un interrupteur qu'une opératrice raccordait suivant les besoins des clients des compagnies de téléphone pour créer les connexions. Quand le réseau commençait à s'élargir, le problème d'automatisation de ces réseaux s'est posé, et c'est Shannon qui allait y trouver une solution en apportant un cadre théorique issu de l'algèbre de Boole.

Pour ce faire, Shannon convient qu'un circuit ouvert est représenté par un 0, un circuit fermé par un 1 (cf. figure 1.5) :

Fig. 1.5 – Circuit ouvert - Circuit fermé

Shannon établit ensuite un ensemble d'opérateurs inspirés de l'algèbre de Boole (cf. figure 1.6).

Il introduit également les opérateurs de négation et d'égalité :

1. Si on dispose d'un relais X, $\overline{X}$ est un relais qui se ferme lorsque X est ouvert, et vice et versa.
2. On dit que X = Y si X et Y se ferment et s'ouvrent en même temps.

Avec ces outils en main, on comprend qu'il devenait possible de manipuler logiquement un circuit à relais, et, éventuellement, de le simplifier. La figure 1.7 illustre l'exemple d'une telle simplification, exemple où les circuits à relais **(a)** et **(b)** sont identiques.

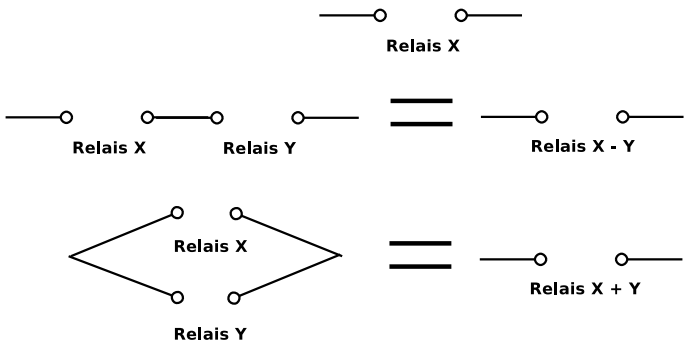


FIG. 1.6 – Opérateurs issus de l'algèbre de Boole

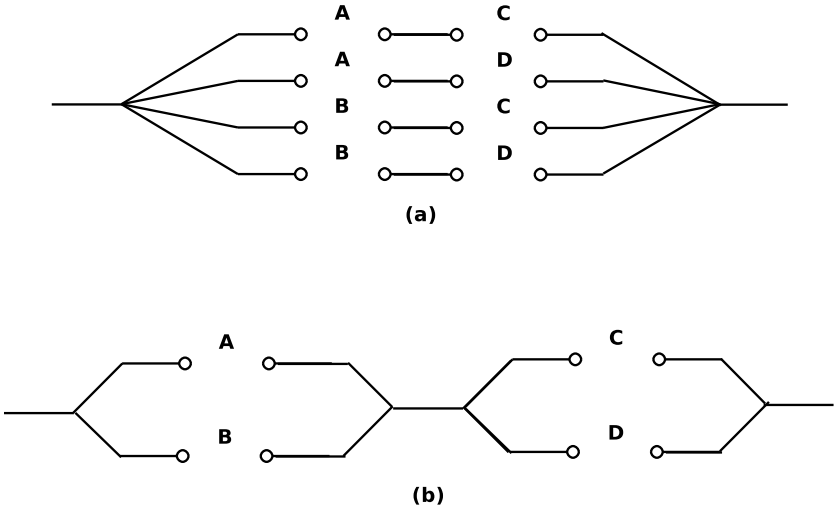


FIG. 1.7 – Ce résultat provient de l'égalité : A·C+A·D+B·C+B·D = (A+B)·(C+D).

D'abord avec les tubes électroniques, et plus profondément encore avec l'invention du transistor, l'implémentation physique de composants jouant le rôle de relais contrôlés devint possible et les circuits logiques purent prendre forme.

Leur définition :

Avec l'algèbre logique de George Boole, on sait que toute fonction logique peut être exprimée en utilisant les opérateurs **NON**, **ET** et **OU** (comme on le verra dans le prochain paragraphe consacré à l'universalité du modèle des circuits logiques).

On introduit donc des composants, appelés portes logiques, qui correspondent à ces opérateurs. La figure 1.8 donne leur forme et leur table de vérité (comportements) respectives.

La figure 1.9 illustre un circuit contrôlant un relais dont la fermeture est actionnée lorsque $(A + B)\cdot(C + D)$ est vrai.

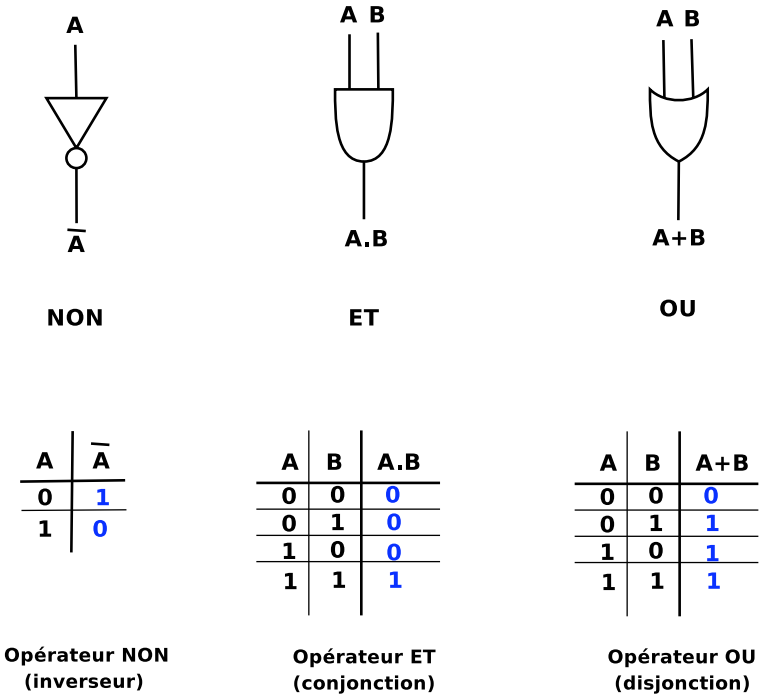


Fig. 1.8 – Par exemple, la table de vérité de l'opérateur **NON** exprime que si en entrée on a **0 / FAUX**, alors en sortie on a **1 / VRAI**, et vice-versa.

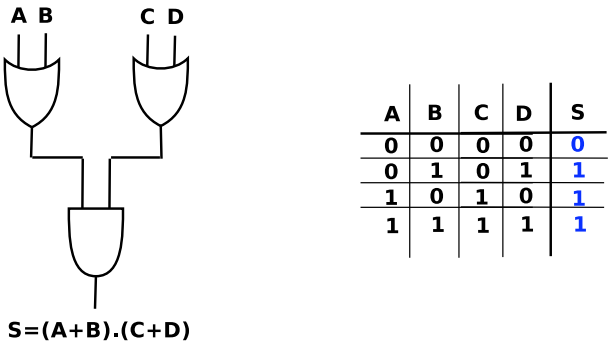


Fig. 1.9 – Un exemple de circuit

Que se passe-t-il si A=1, B=1, C=0 et D=0 ? Injectons les valeurs des variables dans l'équation $(A+B)\cdot(C+D)$:

A+B | A=1, B=1 $= 1 + 1 = 1$,

C+D | C=0, D=0 $= 0 + 0 = 0$, alors

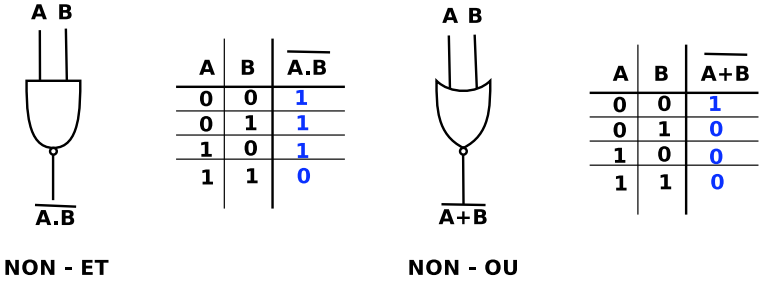
(A+B)·(C+D) | A=1, B=1, C=0, D=0 $= 1 \cdot 0 = 0$.

Dans ce cas là, le relais sera ouvert.

Comme l'exemple le montre, un circuit est fait de portes et de fils ; les uns exécutent de simples instructions de calcul, les autres transportent l'information, c'est-à-dire des **bits** (des **« 0 »** et des **« 1 »**), qui sont les « atomes » de l'information.

À ces trois portes de base, on peut en ajouter deux autres, obtenues en inversant les

portes ET et OU. Elles s'appellerons respectivement NON-ET et NON-OU. La figure 1.10 illustre leur forme et leur comportement.



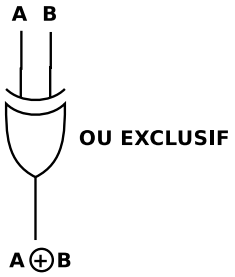
A	B	$\overline{A.B}$
0	0	1
0	1	1
1	0	1
1	1	0

A	B	$\overline{A+B}$
0	0	1
0	1	0
1	0	0
1	1	0

FIG. 1.10 – Schémas et tables de vérité des portes NON-ET et NON-OU

Un fait remarquable concerne ces deux portes : Si l'on dispose uniquement de NON-ET (respectivement NON-OU), il serait possible d'exprimer toute fonction logique à l'aide de ces portes. Le paragraphe suivant le montre pour NON-ET.

Pour la suite, on aura besoin également de la porte OU EXCLUSIF ; la figure 1.11 illustre leur forme et leur comportement.



A	B	A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

FIG. 1.11 – Schéma et table de vérité de la porte OU EXCLUSIF

Leur universalité :

De façon générale, un circuit met en scène divers bits d'information en entrée et en sortie, divers fils et diverses portes logiques. Une porte logique est une fonction

$$f : \{0,1\}^k \to \{0,1\}^l \tag{1.1}$$

pour k et l donnés, respectivement le nombre de bits d'entrée et de sortie.

Exemple : la porte NON a un bit en entrée, un bit en sortie et calcule la fonction $f(a) = 1 \oplus a$, où a est un bit et $\oplus$ est l'addition modulo 2.

On va montrer l'universalité du modèle des circuits logiques en considérant le cas où

la fonction à calculer est de la forme :

$$f : \{0,1\}^n \rightarrow \{0,1\} \tag{1.2}$$

Une telle fonction est connue sous le nom de fonction booléenne et la simplification de la démonstration qui va suivre qu'elle occasionne est similaire à se limiter à la classe des problèmes binaires (cf. section 1.1).

Preuve de l'universalité du modèle par récurrence sur n :

Pour $n = 1$, il n'y a que quatre fonctions booléennes que l'on puisse calculer :

- l'identité, qui consiste en un simple fil,
- la fonction qui change la valeur du bit d'entrée (fonction *bit flip* en anglais) ; la porte NON en permet la réalisation,
- la fonction qui remplace le bit d'entrée par un 0 ; elle peut être obtenue en utilisant la porte ET sur le bit d'entrée, et un bit auxiliaire (une entrée supplémentaire) mis à l'état 0,
- enfin, la fonction qui remplace le bit d'entrée par un 1 ; elle peut être obtenue en utilisant la porte OU sur le bit d'entrée, et un bit auxiliaire mis à l'état 1.

On suppose que toute fonction booléenne à n bits peut être calculée par un circuit. Soit f une fonction à $n+1$ bits. On définit deux fonctions booléennes à n bits, notées f_0 et f_1, telles que

$$f_0(x_1, x_2, ..., x_n) \equiv f(0, x_1, x_2, ..., x_n) \text{ et } f_1(x_1, x_2, ..., x_n) \equiv f(1, x_1, x_2, ..., x_n) \tag{1.3}$$

Par hypothèse, il existe des circuits pour f_0 et f_1. La figure 1.12 montre comment alors construire un circuit capable de calculer f. Le circuit calcule f_0 et f_1 sur les n derniers bits d'entrée. Ensuite, il donne en sortie la réponse appropriée, suivant que le premier bit d'entrée (x_1) était à **« 0 »** ou **« 1 »**.

Preuve de l'universalité de la porte NON-ET :

On va maintenant montrer - en images ! (cf. figures 1.13 et 1.14) - que la porte **NON-ET** peut être utilisée pour simuler les portes **ET**, **OU EXCLUSIF** et **NON** avec, comme ressources, des bits auxiliaires et la possibilité de dupliquer un bit (opération qui prend un bit en entrée et en donne deux copies en sortie).

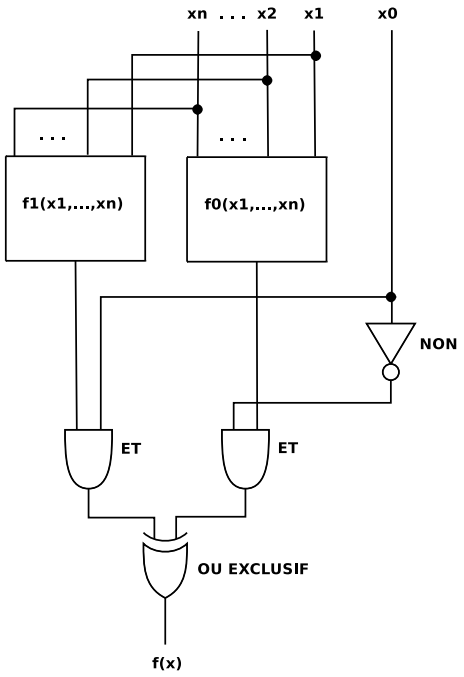
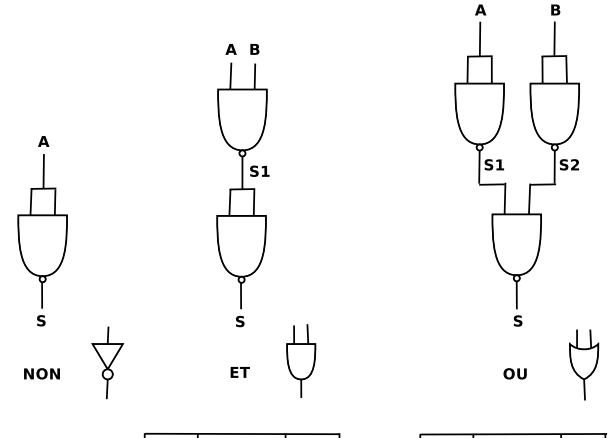


FIG. 1.12 – Circuit permettant le calcul d'une fonction arbitraire f agissant sur $n+1$ bits, sous l'hypothèse de récurrence qu'il existe des circuits capables de calculer les fonctions sur n bits f_1 et f_2.



A	S
0	1
1	0

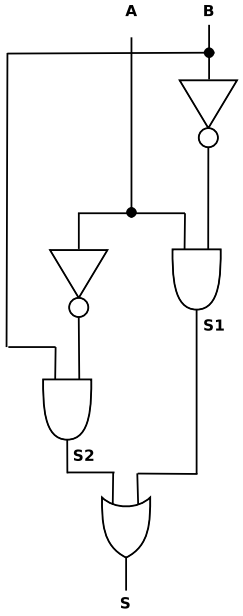
Entrées		Etat interne	Sortie
A	B	S1	S
0	0	1	0
0	1	1	0
1	0	1	0
1	1	0	1

Entrées		Etats internes		Sortie
A	B	S1	S2	S
0	0	1	1	0
0	1	1	0	1
1	0	0	1	1
1	1	0	0	1

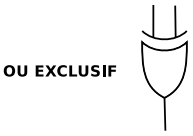
FIG. 1.13 – Expression des portes **NON**, **ET** et **OU** avec des portes **NON-ET**

On déduit directement des figures 1.13 et 1.14 que la porte **OU EXCLUSIF** peut s'écrire en terme de portes **NON-ET**

On a donc montré d'une part que le modèle est universel, d'autre part, qu'en terme de ressources, seuls des bits auxiliaires, des duplications de bits, et la porte **NON-ET** suffisent. On verra dans le chapitre 2 que **NON-ET** a un homologue quantique (C_{not}),



OU EXCLUSIF



Entrées		Etats internes		Sortie
A	B	S1	S2	S
0	0	0	0	0
0	1	0	1	1
1	0	1	0	1
1	1	0	0	0

Fig. 1.14 – Expression de la porte **OU EXCLUSIF** en fonction des portes **NON**, **ET** et **OU**

même si il ne s'agira pas de la même notion d'universalité.

1.3 Les *challenges*

1.3.1 La calculabilité

La **décidabilité** est à un ensemble mathématique ce qu'est la **calculabilité** à la fonction caractéristique de l'ensemble, c'est-à-dire une fonction qui permet de caractériser si un élément appartient ou non à l'ensemble considéré. Pour que cette fonction soit calculable, on devra entre autre pouvoir tester tous les éléments, donc pouvoir les compter (**dénombrabilité**). Dans ce propos qui n'est qu'un « clin d'oeil » à ces notions, on utilisera indifféremment les termes calculabilité (non calculabilité), décidabilité (indécidabilité) et dénombrabilité (indénombrabilité).

Étant donné que la démonstration de l'existence de problèmes indécidables, en terme de machine de Turing, demanderait une introduction un peu trop détaillée du formalisme inhérent aux langages tels qui n'ont été que brièvement évoqués (section 1.1), il est préférable d'aborder la calculabilité sous un autre angle. Heureusement, on peut constater ce phénomène étrange qu'est l'indécidabilité en termes mathématiques.

Précédemment, on a dit que les machines de Turing pouvaient être indexées (nombre de Turing [CN00]). L'ensemble des machines de Turing est donc dénombrable, c'est-à-dire : on peut les compter. Il s'agit d'établir qu'il existe une bijection entre un ensemble et un sous-ensemble de celui des entiers naturels $\mathbb{N}$, pour dire du premier qu'il est **dénombrable**. En revanche, comme on va le voir, l'ensemble de tous les langages ne l'est pas.

On considère le théorème suivant : *l'ensemble des sous-ensembles d'un ensemble infini et dénombrable (ensemble que l'on peut donc par bijection identifier à l'ensemble des entiers naturels* $\mathbb{N}$*) n'est pas dénombrable*. La démonstration de ce théorème repose sur une technique simple, mais puissante (elle est par ailleurs utilisée dans tout problème dont on veut connaître la calculabilité, si on ne peut le « réduire » à un autre dont on connaît déjà la réponse [Wol91]) : la technique de la diagonale par Cantor.

Soient un ensemble dénombrable infini $\mathcal{A} = \{a_0, a_1, a_2, ...\}$, et $\mathcal{S} = \{s_0, s_1, s_2, ...\}$, l'ensemble de ses sous-ensembles. On suppose (par l'absurde) que $\mathcal{S}$ est dénombrable et on construit le tableau suivant :

	a_0	a_1	a_2	a_3	a_4 ...
s_0	✓	✓		✓	
s_1	✓	□		✓	
s_2		✓	✓		✓
s_3	✓		✓	□	
s_4		✓		✓	□

Considérons l'ensemble $\mathcal{D} = \{a_i \mid a_i \notin s_i\}$. Graphiquement, c'est l'ensemble des □ figurant sur la diagonale du tableau ; c'est donc un sous-ensemble de $\mathcal{A}$. L'ensemble $\mathcal{D}$ existe mais n'est pas un des sous-ensembles s_i. En effet, supposons que $\exists k \mid \mathcal{D} = s_k$, or $a_k \in \mathcal{D} \Leftrightarrow a_k \notin s_k$ ce qui est absurde, ainsi l'hypothèse de départ est-elle fausse [Wol91].

L'ensemble des langages (donc des problèmes) est l'ensemble des sous-ensembles d'un ensemble dénombrable infini (l'ensemble des mots) et n'est donc pas dénombrable. Il existe donc des problèmes insolubles. Du point de vue strictement mathématique, la notion d'indécidabilité a été mise en avant par Gödel dans ses théorèmes de complétude et d'incomplétude, dont un aperçu plutôt clair peut être apprécié dans [Pen92].

1.3.2 La complexité

Après la question, plus tout à fait anodine maintenant, de savoir si oui ou non un problème est soluble, se pose la question de l'efficacité de l'algorithme associé. C'est en grande partie à cette notion que l'informatique quantique doit son émergence. L'efficacité d'un programme se mesure via trois ressources : temps, espace (mémoire), entropie. Le dernier paramètre ne sera pas abordé car il demande une connaissance profonde de la théorie de l'information, classique et quantique. De toute façon, du moins en théorie, du fait que les transformations quantiques sont réversibles (comme on le verra dans le chapitre 2), le calcul quantique l'est et donc a une entropie nulle. (En pratique, il n'en est rien mais ce paramètre n'est pas décisif, du moins quand il s'agit juste d'introduire les concepts).

Il semble au premier abord difficile de donner une définition de l'efficacité indépendamment de la technologie utilisée : des ressources déraisonnables pour un calcul manuel ne le sont pas forcément pour un calcul effectué par un ordinateur ; de plus, ce qui semble inaccessible à ces derniers, ne le sera peut-être pas pour les machines du futur. La solution

pour pallier à cette pseudo défaite est de mesurer la quantité des ressources utilisées par rapport à la taille (et non la valeur) de l'instance du problème posé (c'est-à-dire la longueur du mot qui la représente : $n \in \mathbb{N}$). On fait l'hypothèse que la frontière entre « l'acceptable » et « l'inacceptable » se situe à la limite définie entre fonctions polynomiales (n^α, n, $\alpha \in \mathbb{N}$), et non polynomiales (2^n). À partir d'un certain rang n, cette hypothèse semble intuitivement raisonnable [Wol91].

Les différentes classes de complexité qui découlent de cette distinction ont une définition rigoureuse grâce au modèle de Turing et seront définies par rapport au temps.

En effet, l'utilisation de chaque unité élémentaire de mémoire (chaque case du ruban) nécessite au moins l'exécution d'une instruction, donc la complexité en terme d'espace est toujours inférieure à celle en temps. En terme de complexité, on se place toujours dans « le pire des scénarios ».

Les premières définitions concernant l'étude de la complexité portent sur des encadrements de fonctions, puisqu'il s'agit d'une étude de comparaison entre différentes solutions algorithmiques :

$$\begin{aligned} g(n) &= O(f(n)) \text{ signifie : } \exists c, n_0 \text{ constantes telles que } \forall n > n_0, g(n) \leq cf(n) \\ g(n) &= \Omega(f(n)) \text{ signifie : } \exists c, n_0 \text{ constantes telles que } \forall n > n_0, cf(n) \leq g(n) \\ g(n) &= \Theta(f(n)) \text{ signifie : } g(n) = O(f(n)) \text{ et } g(n) = \Omega(f(n)) \end{aligned}$$

Pratiquement, on utilisera plutôt la première définition qui donne l'allure « la pire » du comportement d'un algorithme, ce qui en plus simplifie l'expression de sa complexité. Par exemple, $4n^2 + 4n = O(n^2)$ signifie qu'à partir d'un certain rang (on considère les valeurs croissantes de n), n est négligeable devant n^2.

Maintenant, il faut définir ce que l'on entend par complexité en terme de temps. Soit M une machine de Turing *déterministe* (dans certains cas, une des fonctions de transition d'une machine de Turing peut avoir divers choix ; ici on admet qu'il n'en n'est rien) et qui s'arrête toujours, la complexité en temps de M est la fonction $T_M(n)$ définie par :

$T_M(n) = \max\{m \mid \exists\ x$, mot de longueur n et l'exécution de M sur x comporte m étapes$\}$

$T_M(n)$ donne le nombre maximum (donc le cas le plus mauvais) d'étapes permettant de calculer x. La complexité sera dite **polynomiale** si $T_M(n)$ est bornée par un polynôme.

La **classe de complexité** P est la classe des langages calculables par une machine de Turing polynomiale. Elle regroupe donc l'ensemble des langages calculables de façon efficace et sa définition est indépendante de la technologie utilisée. À partir de là, se pose la question de l'existence ou non d'autres classes. Une idée, afin de démontrer qu'un langage n'appartient pas à P, serait d'utiliser la diagonalisation comme dans le cas de l'étude

de la calculabilité. Cependant, cette méthode, si elle permet de constater l'existence de problèmes indécidables, ne permet pas de montrer si certains problèmes pratiques, dont on ne connaît, du moins à ce jour, aucun algorithme polynomial, ne sont pas dans P. Par ailleurs, et c'est une des limites de la théorie de la complexité, on n'a pas encore pu établir de manière rigoureuse l'existence de tels problèmes. Peut-être est-ce du ressort de l'indécidable ? Malgré tout, il est admis qu'il y a de grandes chances pour que ce soit le cas. Par respect pour cette intuition, on va définir mais de façon intuitive une autre classe : **la classe de complexité** NP (NP pour *non polynomiale*) qui regroupe les langages calculables, mais de façon inefficace. La théorie montre que [Wol91] les problèmes de cette veine ont tous la même caractéristique : c'est le nombre de cas à explorer qui rend leur solution algorithmique inefficace, chaque cas étant en lui même soluble rapidement. Par exemple, dans le cas de la factorisation d'un nombre de longueur n en facteurs premiers, une simple succession de divisions et un temps polynomial en $O(n)$, permettent de constater si oui ou non un facteur donné (*witness* en anglais [CN00]) est une instance positive ou non du problème. En revanche, le savoir pour tous les facteurs (compris entre 2 et $n^{\frac{1}{2}}$) prendrait un temps effroyablement long. Il y a ainsi une très belle asymétrie concernant NP.

On peut démontrer, au sein de chacune de ces classes, l'existence de problèmes dits **complets** c'est-à-dire, tous les problèmes d'une même classe sont *réductibles* à un seul problème qui est alors, d'une certaine manière, plus difficile que les autres puisque le résoudre revient à les résoudre. Si on pouvait démontrer qu'un problème NP*–complet* (une démonstration du théorème de Cook, assez facile à comprendre, qui démontre la NP–complétude d'un problème connu sous le nom de SAT, peut être trouvée dans [Wol91]) admet une solution polynomiale, on aurait $P = NP$, ce qui reste, à l'heure actuelle une conjecture ! L'informatique quantique a peut-être d'ailleurs un rôle à jouer à ce propos puisque, dans le cas de la factorisation en facteurs premiers, elle a pu faire chuter la complexité de ce problème en exploitant une structure cachée de ce problème. Néanmoins, dans ce cas précis, du fait de l'existence d'une structure cachée, le problème appartiendrait à une classe intermédiaire entre P et NP : NPI. Cela reste donc à creuser.

D'autres classes de complexité peuvent être prises en compte, elles permettent de mieux appréhender le rôle du calcul quantique. Notamment, il y a la classe $PSPACE$. Les problèmes sont dans cette classe si la machine, pour les résoudre, utilise un nombre limité de bits (ressource en terme de mémoire limitée), pendant un temps illimité. De façon évidente, $P \subset PSPACE$. On a aussi $NP \subset PSPACE$: en effet, il suffit de tester tous les témoins d'un langage L appartenant à NP. Leur temps d'exécution à chacun n'excédant pas celui d'un polynôme en n, ils occuperont un espace au pire de la même taille et l'ensemble des tests, si on écrase la mémoire à la suite de chacun d'eux, peut s'effectuer sur cette même longueur d'espace, pendant un temps illimité [CN00].

Mais pourquoi considérer une classe de complexité relative à l'espace alors que l'on a

précédemment dit que le temps était un facteur plus pertinent ? Tout simplement parce que la classe des problèmes résolubles par un ordinateur quantique [CN00] forme un sous ensemble de $PSPACE$. De même que pour NP, on ne sait pas si oui ou non $PSPACE \subset P$! Et pourtant, il semblait évident que d'avoir tout le temps que l'on veut et de disposer d'une ressource spatiale polynomiale, confère plus de pouvoir que d'avoir juste une ressource temporelle polynomiale. Si jamais la dernière inclusion avait lieu d'être, l'informatique quantique ne servirait à rien ; c'est pourquoi il est clairement d'actualité d'étudier la complexité.

Conclusion

Ces modèles, d'abord très différents, sont en fait équivalents [CN00] mais pour le montrer, il faudrait rentrer plus en profondeur dans le domaine de l'informatique théorique ; ce propos se voulait simplement une introduction au concept de calcul.

Chapitre 2

Les débuts du calcul quantique

Introduction

Après avoir introduit les quelques éléments de formalisme de la mécanique quantique nécessaires à la définition, à la « compréhension », et au maniement du modèle de calcul quantique en terme de circuits logiques quantiques, on définira ce qu'est un *quantum bit* (ou *qubit*), homologue quantique du bit en informatique classique, et comment on peut s'en servir pour faire du calcul.

Les opérations autorisées $\mathcal{U}$ par la mécanique quantique sont les opérations dites *unitaires* ; elles sont décrites par des matrices que l'on peut qualifier de *portes logiques quantiques*, si on utilise le formalisme des circuits logiques quantiques, formalisme directement calqué sur celui des circuits à portes logiques en électronique et le plus facile à appréhender. C'est d'ailleurs le premier modèle de calcul quantique qui ait été envisagé.

Dans le cadre du calcul quantique, on s'intéresse surtout à des matrices 2×2 et 4×4 qui agissent respectivement sur des systèmes à 1 et 2 qubits, car il a été montré que toute porte agissant sur n qubits pouvaient se décomposer en une succession de portes sur 1 ou 2 qubits.

Un parallèle rapide entre monde classique et monde quantique montrera les similitudes et les différences entre monde classique et monde quantique et des illustrations de calcul quantique seront données : l'oracle de Deutsch qui est un cas d'école mais qui permet vraiment d'appréhender une grande partie du potentiel du calcul quantique. L'oracle de Simon, à peine plus complexe et qui permet de comprendre certains aspects de l'algorithme de Shor, sera abordé, ainsi que l'algorithme de Grover, car son interprétation géométrique le rend facile d'accès.

Ce qui suit s'est beaucoup inspiré de la « bible » de l'information et de l'informatique quantique : *Quantum Computation and Quantum information*, par Michael A. Nielsen et Isaac L. Chuang [CN00].

2.1 La mécanique quantique version informatique

Postulat 1 :

La mécanique quantique est un modèle mathématique construit par les physiciens dès le début du XXe siècle afin de rendre compte de certains comportements du monde microscopique. Ce modèle est construit de manière axiomatique à partir de postulats.

Il ne s'agit pas ici de trouver une signification profonde à chacun de ces postulats, mais plutôt de les considérer comme étant les règles de ce jeu de construction que l'on nomme mécanique quantique. Jusqu'à aujourd'hui, ces derniers n'ayant pas été mis en défaut, cette philosophie semble acceptable. De toute façon, en science(s), il ne s'agit pas de comprendre mais de constater, modéliser, valider, recommencer, jusqu'à ce que le modèle devienne obsolète.

Il existe diverses formulations équivalentes de ces postulats ; celle qui suit sert de support à cette application si particulière de la mécanique quantique : l'informatique quantique.

Les différents « êtres mathématiques » qui vont êtres mentionnés dans les postulats seront explicités et manipulés dans la prochaine section.

Enoncé du premier postulat :

L'état d'un système *fermé* est complètement décrit par une fonction d'onde associée à un vecteur d'état (ket) $|\psi\rangle$, décrit par un vecteur colonne unitaire. Ce dernier appartient à un espace vectoriel complexe muni d'un produit scalaire, connu sous le nom d'espace des états (c'est un espace de Hilbert que l'on notera $\mathcal{H}$).

On peut trouver une définition plus formelle de l'espace de Hilbert dans la section A.5 de l'annexe A.

Postulat 2 :

L'évolution d'un système quantique fermé est décrite par une transformation unitaire. Soit l'état $|\psi\rangle$ d'un système à l'instant t_1 et $|\psi\rangle'$ son état à t_2 , alors il existe une transformation unitaire $\mathcal{U}$ telle que :

$$|\psi\rangle' = \mathcal{U}\,|\psi\rangle \tag{2.1}$$

$\mathcal{U}$ est juste fonction de t_1 et t_2.

Remarque 1 : quand $\mathcal{U}$ est **hermitienne** (toutes ses valeurs propres sont réelles) alors elle est mesurable et il s'agit d'une **observable** ; sinon, seule l'appellation d'opérateur convient.

Postulat 2′ :

L'évolution du ket ou de l'opérateur (il y a équivalence) associé à un système fermé est régie par l'équation de Schrödinger :

$$i\hbar\frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle \tag{2.2}$$

L'opérateur H est le hamiltonien du système, c'est l'observable associée à l'énergie totale du système. Par ailleurs, $\hbar = \frac{h}{2\pi}$ où h est la constante de Planck.

Postulat 3 :

On considère l'équation aux valeurs propres d'une observable $\mathcal{O}$:

$$\mathcal{O}\,|\psi_n\rangle = \lambda_n\,|\psi_n\rangle \tag{2.3}$$

avec $|\psi_n\rangle$ base complète. On peut alors définir $|\psi\rangle$ sur cette base :

$$|\psi\rangle = \sum_n c_n\,|\psi_n\rangle \tag{2.4}$$

La probabilité de mesurer λ_n est $\mid c_n \mid^2$. Le résultat est *aléatoire* : λ_1, λ_2, λ_3, ... excepté dans le cas où l'état $|\psi\rangle$ est de la forme $|\psi_n\rangle$ (auquel cas, $\mid c_n \mid^2 = 1$ et la mesure donne la valeur λ_n).

Remarque 2 : Soit dit en passant, il s'agit de « vrai aléatoire » ; le monde classique, même en physique statistique, ne peut être régit que par du « pseudo-aléatoire ».

Remarque 3 : Comment la mesure d'une observable peut oui ou non influer sur une autre ? Avant que de répondre à cette question, il faut définir ce qu'est le **commutateur** : deux observables $\mathcal{A}$ et $\mathcal{B}$ commutent si et seulement si :

$$[\mathcal{A},\mathcal{B}] = \mathcal{A}\mathcal{B} - \mathcal{B}\mathcal{A} = 0 \tag{2.5}$$

Quand deux observables commutent, faire la mesure de $\mathcal{A}$, puis celle de $\mathcal{B}$ est un événement équivalent à celui d'effectuer d'abord celle de $\mathcal{B}$, puis celle de $\mathcal{A}$.

Exemple :

Soient deux états $|\psi_1\rangle = |\leftrightarrow\rangle$ et $|\psi_2\rangle = |\updownarrow\rangle$ correspondant respectivement à la polarisation horizontale ($\lambda_1 = -1$) et verticale ($\lambda_2 = +1$) d'un photon. Celui-ci sera dans cette superposition d'états : $|\psi\rangle = c_1\,|\leftrightarrow\rangle + c_2\,|\updownarrow\rangle$ avant la mesure. Excepté dans les cas $|\psi\rangle = |\leftrightarrow\rangle$ ou $|\psi\rangle = |\updownarrow\rangle$, il est impossible de connaître à l'avance le résultat de la mesure.

Postulat 4 :

L'espace des états d'un système physique composé est le produit direct des espaces des états associés aux sous-systèmes qui le composent. Techniquement, si un sous-système i est représenté par le ket $|\psi_i\rangle$, et que le système total est constitué de n kets numérotés de 1 à n, alors l'état du système est : $|\psi_1\rangle \otimes ... \otimes |\psi_i\rangle \otimes ... \otimes |\psi_n\rangle$.

Remarque 4 : un état quantique a comme représentant mathématique un vecteur, une observable, un opérateur hermitien, et une valeur de l'observable, une valeur propre de l'opérateur hermitien associé. Il est souvent d'usage d'identifier les uns avec les autres, mais si il faut distinguer, par exemple, l'observable de son opérateur, la convention est de changer de notation : on écrira l'observable, $\mathcal{A}$, et l'opérateur, A.

2.2 Système à un qubit

2.2.1 Le qubit

Avant d'aborder le formalisme inhérent à un qubit (ket de dimension 2), il faut se convaincre que celui-ci a bien une raison d'être : qu'est ce que physiquement un qubit ? Il en existe plusieurs représentations mais on évoquera seulement deux d'entre elles : la polarisation d'un photon, qui semble la plus simple à appréhender, et celle du spin 1/2, mise en évidence par l'expérience de Stern et Gerlach et dont une représentation très commode existe : la sphère de Bloch.

Pourquoi déjà le terme de *qubit* ? Un qubit (ou bit quantique) est l'analogue quantique du bit classique. C'est la « description informatique » de l'état d'une particule, système quantique élémentaire. Alors que le bit ne peut prendre qu'une seule valeur (0 ou 1), à la lumière des postulats énoncés dans la section 2.1, un qubit peut exister dans une superposition d'états. Par exemple, un électron peut occuper *simultanément* deux orbites d'un atome.

Plus formellement, en utilisant la notation de Dirac, un **qubit** est décrit de la façon suivante :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{2.6}$$

Ici α et β sont des nombres complexes, appelés les **amplitudes** des états classiques respectifs $|0\rangle$ et $|1\rangle$. Elles vérifient la condition de normalisation suivante :

$$|\,\alpha\,|^2 + |\,\beta\,|^2 = 1 \tag{2.7}$$

Quand l'état $|\psi\rangle$ est *mesuré*, on observe soit $|0\rangle$, soit $|1\rangle$, ceci avec les probabilités respectives $|\,\alpha\,|^2$ et $|\,\beta\,|^2$. Par ailleurs les mesures sont *irréversibles* : l'état du système devient $|0\rangle$ ou $|1\rangle$ et il devient impossible de remonter aux valeurs de α et β.

Exemples physiques de qubits :

Un premier modèle issu de la polarisation de la lumière :

La polarisation de la lumière a été mise en évidence pour la première fois par le chevalier Malus en 1809 grâce aux propriétés biréfringentes d'un cristal de spath d'Islande. Un tel cristal peut décomposer un rayon lumineux en deux rayons polarisés dans des directions perpendiculaires. Le phénomène de polarisation met en évidence le caractère vectoriel des vibrations lumineuses.

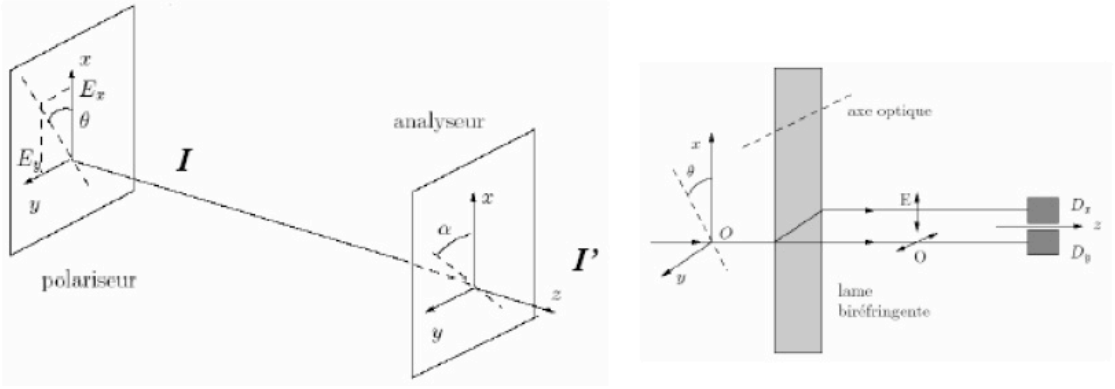


FIG. 2.1 – Description de la polarisation de la lumière

A la sortie d'un polariseur (schéma de gauche de la figure 2.1), le champ électrique est orienté suivant un angle θ dans le plan perpendiculaire à la direction de propagation (axe z). Si on analyse avec un polariseur orienté suivant α, on obtient une intensité (loi de Malus) :

$$I' = I \times \cos^2(\theta - \alpha) \tag{2.8}$$

Considérons maintenant le schéma de droite de la figure 2.1. Dans le cas d'un champ classique (N photons avec N grand) d'intensité I, les détecteurs mesurent (loi de Malus) :

$$D_x = I \times \cos^2(\theta) \text{ et } D_y = I \times \sin^2(\theta) \tag{2.9}$$

Dans le cas d'un champ quantique (les photons « arrivent 1 par 1 »), les détecteurs ne clignent jamais simultanément et le font successivement avec les probabilités suivantes :

$$P(D_x, clic) = \cos^2(\theta) \text{ et } P(D_y, clic) = \sin^2(\theta) \tag{2.10}$$

Où il est enfin question de mécanique quantique...

On ne peut pas prévoir, pour un photon donné, s'il va déclencher D_x ou D_y. Si on recombine les deux faisceaux de la première lame biréfringente (schéma de droite de la figure 2.1) en utilisant une seconde lame qui lui est symétrique, on obtient alors l'entrée et la sortie du système du schéma de gauche de la figure 2.1.

Pour traverser l'analyseur, un photon quelconque peut choisir le trajet $x(y)$ avec une probabilité $\cos^2(\theta)$ ($\sin^2(\theta)$) de traverser l'analyseur, soit une probabilité totale de traverser, pour le choix du trajet $x(y)$, égale à :

$$\cos^2(\theta)\cos^2(\alpha)\ (\sin^2(\theta)\sin^2(\alpha)) \tag{2.11}$$

La probabilité totale s'obtient en additionnant les probabilités des deux trajets possibles :

$$\cos^2(\theta)\cos^2(\alpha) + \sin^2(\theta)\sin^2(\alpha), \tag{2.12}$$

ce qui est faux par rapport à la loi de Malus et le résultat correct (confirmé par l'expérience) est :

$$\cos^2(\theta - \alpha). \tag{2.13}$$

Afin d'être cohérent avec les résultats de l'optique ondulatoire classique, il faut introduire en physique quantique la notion d'amplitude de probabilité dont le module élevé au carré donne la probabilité :

$$a(\theta \to x) = \cos(\theta)\ ,\ a(\theta \to y) = \sin(\theta)\ ,\ a(x \to \alpha) = \cos(\alpha)\ ,\ a(y \to \alpha) = \sin(\alpha) \tag{2.14}$$

On additionne les amplitudes pour des trajets indiscernables et le carré donne :

$$\cos^2(\theta - \alpha). \tag{2.15}$$

Tout se passe donc comme si le photon empruntait les deux chemins à la fois ! [Bel05].

Le qubit : polarisation d'un photon

On choisit une base pour mesurer la polarisation (x, y) (axes de la lame biréfringente) :

- $|0\rangle_{xy} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{xy}$ correspond à un photon polarisé selon x
- $|1\rangle_{xy} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_{xy}$ correspond à un photon polarisé selon y

Remarque : les valeurs assignées à $|0\rangle_{xy}$ et $|1\rangle_{xy}$ le sont de façon arbitraire, on aurait pu aussi bien choisir une autre convention.

Si on choisit une base $(x'y')$, tournée de θ par rapport à (x, y), on définit :

- $|0\rangle_{x'y'} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{x'y'}$ correspond à un photon polarisé selon x'
- $|1\rangle_{x'y'} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_{x'y'}$ correspond à un photon polarisé selon y'

On a alors :

$$|0\rangle_{x'y'} = \cos(\theta)\,|0\rangle_{xy} + \sin(\theta)\,|1\rangle_{xy} \text{ et } |1\rangle_{x'y'} = -\sin(\theta)\,|0\rangle_{xy} + \cos(\theta)\,|1\rangle_{xy}$$

On a bien par exemple $\cos^2(\theta)+\sin^2(\theta) = 1$ qui correspond aux probabilités respectives pour $|0\rangle_{x'y'}$ d'être dans les états $|0\rangle_{xy}$ ou $|1\rangle_{xy}$.

Les coefficients attachés aux kets sont réels car on a considéré des polarisations rectilignes. Le cas général est la polarisation elliptique qui est décrite par un vecteur complexe unitaire dans un espace de Hilbert $\mathcal{H}$ de dimension 2, de composantes : $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ où $\{|0\rangle, |1\rangle\}$ est une base orthonormale de $\mathcal{H}$. Ici, $\alpha = \cos\theta e^{i\phi}$ et $\beta = \sin\theta$ sont tels que $|\,\alpha\,|^2 + |\,\beta\,|^2 = 1$.

Le vecteur $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ est ainsi une superposition linéaire d'un photon polarisé selon x et d'un photon polarisé selon y. À ce titre, un qubit est une entité beaucoup plus riche qu'un bit ordinaire car il peut prendre toutes les valeurs intermédiaires entre 0 et 1 et contient donc une infinité d'information. Cependant c'est sans compter la mesure du qubit qui ne peut donner que « 0 » ou « 1 ». Heureusement, on peut exploiter « l'information cachée » (à savoir $e^{i\phi}$) dans la superposition linéaire avec de l'astuce (cf. section 2.3).

Un deuxième modèle : la notion de spin 1/2

Une autre réalisation importante du qubit est le spin 1/2. C'est d'ailleurs à celle-ci qu'on s'intéressera plus particulièrement.

Imaginez une petite aiguille aimantée qui constitue ce que les physiciens appellent un dipôle magnétique. Il est caractérisé par un moment (dipolaire) magnétique, noté $\vec{\mu}$. Placé dans un champ magnétique $\vec{B}$, cette aiguille s'aligne dans la direction du champ, similairement à l'aiguille d'une boussole dans le champ magnétique terrestre.

La raison de cet alignement est régie par la relation $E = -\vec{\mu}.\vec{B}$, où E est l'énergie du dipôle magnétique dans le champ $\vec{B}$. La position d'énergie minimale est donc celle pour laquelle $\vec{\mu}$ et $\vec{B}$ sont parallèles. Lorsque $\vec{B}$ n'est pas uniforme, le dipôle se déplace vers la région où le champ est le plus grand en valeur absolue, de façon à minimiser son énergie. En clair, le dipôle est soumis à un couple qui tend à l'aligner avec le champ et à une force qui tend à le faire bouger sous l'influence d'un gradient de champ. Il existe également un moment angulaire propre comme l'a mis en évidence l'expérience de Stern et Gerlach.

C'est cette dernière [Bel05] qui, à l'aube des années 20, a permis de mettre en évidence la notion de spin en utilisant des atomes d'argent, chauffés à blanc dans un four, puis soumis à un champ magnétique. Ces atomes ont une structure relativement compliquée et il est plus simple de considérer des atomes d'hydrogène. Chacun d'entre eux possède un proton et un électron en orbite. On peut considérer ce dernier comme un petit courant électrique. Ce courant est à l'origine du champ magnétique de l'atome c'est-à-dire son moment dipolaire magnétique. Ainsi chaque atome se comporte-t-il comme un aimant

dont l'axe d'orientation est le même que celui autour duquel l'électron tourne. On soumet ensuite ces « aimants » à un champ magnétique constant et de manière à ce que l'atome ne dévie que selon une des composantes de son moment dipolaire magnétique. Les résultats sont spectaculaires : au lieu d'obtenir une distribution continue d'angles représentant le côté aléatoire de l'orientation du moment dipolaire des atomes sortant du four, on obtient un ensemble discret d'angles : le moment dipolaire magnétique est quantifié. Les atomes d'hydrogène utilisés dans l'expérience sont tels que leur moment dipolaire magnétique est nul : classiquement cela signifie que l'électron n'a pas de mouvement orbital autour du noyau mais à l'époque les connaissances en mécanique quantique permettaient de comprendre un tel résultat. La véritable originalité de l'expérience réside dans le fait suivant : au lieu d'observer un seul « rayon d'atomes » en sortie du four et non dévié par le champ magnétique du fait de l'absence d'un moment dipolaire magnétique, on constate l'existence de deux rayons déviés par le champ magnétique, l'un vers le haut, l'autre vers le bas : naquit ainsi la notion de spin. Heisenberg fut le premier à défendre l'idée que le spin et le mouvement orbital de l'électron sont deux contributions distinctes au moment dipolaire magnétique. C'est pourquoi on parle de spin pour l'électron.

Au premier abord, on pourrait visualiser le spin d'un électron comme un simple bit classique indiquant si l'atome d'hydrogène est « dirigé vers le haut (valeur 0) ou vers le bas (valeur 1) », selon sa « valeur » : $\frac{1}{2}$ ou $-\frac{1}{2}$, mais en mettant deux dispositifs de Stern et Gerlach en cascade et en bloquant un des rayons issus du premier système, on observe en sortie du second encore deux rayons, et ceci en ayant pris le soin d'orienter le deuxième champ magnétique dans une direction orthogonale à celle du premier. Comme dans le premier cas, si le spin se comportait vraiment comme un bit classique, on aurait dû observer un seul rayon, celui correspondant au moment dipolaire magnétique orienté selon la direction du premier champ magnétique ! [CN00]

La notion de spin est de fait très difficile à visualiser et fait appel à des outils mathématiques très perfectionnés qui ont abouti à une représentation très fidèle du spin 1/2 : la sphère de Bloch (le photon ayant un spin 1, on lui associerait une autre sphère, celle de Poincaré). Formellement, cette sphère décrit l'ensemble des valeurs que peut prendre un vecteur associé au spin 1/2 et toutes les transformations licites (c'est-à-dire unitaires, comme ce sera expliqué bientôt) auxquelles il peut être soumis, peuvent être décrites visuellement grâce à cette sphère. Sans rentrer dans les détails mais afin de mettre l'accent sur le fait que cette sphère n'en a en fait que le nom, cet ensemble est la projection stéréographique de l'ensemble des rotations de dimension 3 [Alt05]. Pour schématiser, on peut considérer la sphère de Bloch comme étant une sphère dont les trois axes ont la même direction que pour une sphère classique, mais possédant deux sens : par exemple, l'axe Nord/Sud a « deux flèches ». Avant d'aborder cette représentation, il est nécessaire d'introduire les opérations agissant sur un qubit.

2.2.2 Manipulations sur 1 qubit

Des transformations unitaires

Avant de visualiser la sphère de Bloch, il est nécessaire d'introduire un peu de formalisme.

On considère un espace de Hilbert $\mathcal{H}$ de dimension 2 muni d'une base orthonormale $\{|0\rangle, |1\rangle\}$. Cette base doit être orthogonale afin que les états soient distinguables lors de la mesure : par exemple, la base $\{|0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}\}$ poserait des problèmes une fois sur deux, mais on aurait pu choisir la base $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. La base est également normalisée puisque les kets le sont. Il est évident, d'apès la dimension de $\mathcal{H}$, que les opérations qui vont être effectuées sur ses éléments sont modélisables en matrices 2×2.

Soient $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|\psi\rangle' = \alpha'|0\rangle + \beta'|1\rangle$ tels que $|\psi\rangle' = U|\psi\rangle$, ce qui revient à écrire : $\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

En vertu du fait que la somme des probabilités (condition de normalisation des amplitudes) doit toujours être égale à 1, on doit avoir :

$$|\alpha|^2 + |\beta|^2 = |\alpha'|^2 + |\beta'|^2 = 1.$$

C'est la seule condition à remplir et elle correspond à U **unitaire**, soit, par définition, telle que :

$$U^\dagger U = U U^\dagger = I_2 \tag{2.16}$$

où I_2 est la matrice unité 2×2. Cette condition implique que toute transformation unitaire est réversible donc que tout calcul, en l'absence de mesures, est réversible. Une des conséquences est que le déterminant de U est égal à $e^{i\alpha}$ où $\alpha \in \mathbb{R}$, ce qui simplifie grandement l'ensemble des transformations à considérer.

Pour décrire un spin 1/2 et les transformations qui agissent dessus, on peut utiliser la représentation dite de Bloch [CN00] (cf. section 2.2.2), c'est la manière la plus simple de visualiser un spin 1/2. Les transformations unitaires qui « fonctionnent bien » avec cette représentation sont connues sous le nom de matrices de Pauli. Elles constituent la famille suivante :

$$\left\{ I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

Exemple : $\sigma_x|0\rangle = |1\rangle$ pour $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Remarque : dans certaines littératures, ces matrices sont également notées X, Y et Z. C'est la « base » (en ce sens qu'à partir de cette famille on retrouve toutes les opérations quantiques) la plus connue car la plus simple (présence de I_2), et la plus naturelle : les deux matrices σ_x et σ_z sont également surnommées respectivement opérateurs *shift* et *clock*. Le premier échange la valeur des qubits, opération des plus simples mais déjà indispensable pour des registres de bits classiques, le deuxième introduit un retard de phase.

Des opérateurs rotations :

On définit une fonction f agissant sur une matrice A de la manière suivante : si A est un opérateur normal, c'est-à-dire si il vérifie $AA^\dagger = A^\dagger A$, alors, d'après le théorème de décomposition spectrale [CN00], on a :

$$A = \sum_a a \left|a\right\rangle \left\langle a\right| \tag{2.17}$$

Il en découle :

$$f(A) = \sum_a f(a) \left|a\right\rangle \left\langle a\right| \tag{2.18}$$

Si, de plus, f peut être mise sous la forme d'une série de puissance de la manière suivante :

$$f(x) = \sum_{i=0}^{\infty} c_i x^i, \tag{2.19}$$

on a alors :

$$f(A) = c_0 I + c_1 A + c_2 A^2 + c_3 A^3 + ... \tag{2.20}$$

et en particulier :

$$e^A = I + A + \frac{A^2}{2!} + \frac{A^3}{3!} + ... \tag{2.21}$$

On définit l'opérateur rotation d'un opérateur A comme $e^{i\theta A}$; si, par ailleurs, A vérifie $A^2 = I$ (ce qui est le cas pour les matrices de Pauli), on a :

$$e^{i\theta A} = \cos(\theta) I + i \sin(\theta) A \tag{2.22}$$

De manière générale, on définit ainsi l'opérateur rotation rattaché à la sphère de Bloch :

$$R_n(\theta) = e^{i\frac{\theta n.\sigma}{2}} = \cos(\frac{\theta}{2}) I_2 - i \sin(\frac{\theta}{2})(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z) \tag{2.23}$$

où n est un vecteur unitaire de composantes (n_x, n_y, n_z), lesquelles composantes sont sur les axes de la sphère de Bloch et où $\sigma = (\sigma_x, \sigma_y, \sigma_z)$.

Considérons l'état quantique suivant :

$$\left|\psi\right\rangle = \alpha \left|0\right\rangle + \beta \left|1\right\rangle \tag{2.24}$$

où $\alpha, \beta \in \mathcal{C}$ tels que $\mid \alpha \mid^2 + \mid \beta \mid^2 = 1$. On peut se convaincre facilement [Gle05] qu'il décrit la sphère de Bloch. Une autre façon d'exprimer cet état, sans perdre en généralité, lorsqu'on considère le qubit en terme de spin 1/2 est :

$$|\psi\rangle = e^{i\alpha}[\cos(\frac{\theta}{2})\,|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})\,|1\rangle] \tag{2.25}$$

Avec $\theta, \alpha, \phi \in \mathbb{R}$. Au final, on a :

$$|\psi\rangle = \cos(\frac{\theta}{2})\,|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})\,|1\rangle \tag{2.26}$$

car, lors de la mesure, la phase globale disparaît. « L'information cachée » mentionnée précédemment se situe au niveau de la phase relative.

Supposons que $|\psi\rangle$ soit décrit sur la sphère de Bloch par un vecteur, dit de Bloch, noté $\vec{\lambda}$. L'effet de l'opérateur $R_n(\theta)$ est de faire subir à $|\psi\rangle$ une rotation d'angle θ autour de l'axe n.

Exemple : $R_x(\theta) = e^{-i\frac{\theta X}{2}} = \cos(\frac{\theta}{2})I_2 - i\sin(\frac{\theta}{2})X = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$

Soit U une transformation unitaire. À ce titre, elle peut être mise sous la forme (décomposition d'Euler [CN00]) :

$$U = \begin{pmatrix} e^{i(\alpha-\frac{\beta}{2}-\frac{\delta}{2})}\cos(\frac{\gamma}{2}) & -e^{i(\alpha-\frac{\beta}{2}+\frac{\delta}{2})}\sin(\frac{\gamma}{2}) \\ e^{i(\alpha+\frac{\beta}{2}-\frac{\delta}{2})}\sin(\frac{\gamma}{2}) & e^{i(\alpha+\frac{\beta}{2}+\frac{\delta}{2})}\cos(\frac{\gamma}{2}) \end{pmatrix} \text{ soit } U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) \tag{2.27}$$

Appliquer U à $|\psi\rangle$ revient à faire faire à celui-ci une rotation d'angle δ autour de l'axe z de la sphère de Bloch, suivie d'une rotation d'angle γ autour de l'axe y, puis d'une rotation d'angle β autour de l'axe z. Pour finir, on fait subir un déphasage global de α au nouvel état. Cette succession de rotations est compréhensible en observant les valeurs des vecteurs propres des matrices de Pauli et la sphère de Bloch (cf. figure 2.2) :

- σ_z a pour vecteurs propres $|0\rangle$ et $|1\rangle$; ils sont situés respectivement au « Nord » et au « Sud » de la sphère de Bloch (axe z).
- σ_x a pour vecteurs propres $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ et $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$; ils sont situés respectivement en « avant » et en « arrière » de la sphère de Bloch (axe x).
- σ_y a pour vecteurs propres $\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$ et $\frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$; ils sont situés respectivement à « droite » et à « gauche » de la sphère de Bloch (axe y).

Pour conclure, toute opération sur un qubit peut être vue comme une succession de rotations : voilà un miracle du formalisme.

La porte de Hadamard :

L'exemple le plus important de ces transformations unitaires est la **porte de Hadamard**, car c'est grâce à elle que l'on peut exploiter les superpositions quantiques. Elle est

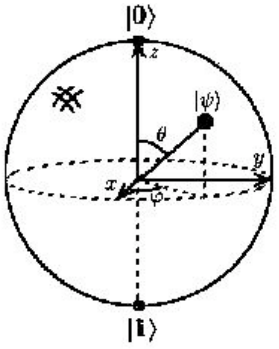


Fig. 2.2 – L'état quantique $|\psi\rangle$ décrit la sphère de Bloch.

définie de la façon suivante :

$$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Cette porte permet de faire rentrer un état quantique connu (par exemple $|0\rangle$ qui sera une polarisation horizontale dans le cas du photon) dans une superposition d'états (propriété connue sous le nom de « pile ou face quantique », (cf. figure 2.3), et pour lequel il est impossible de tricher !). Elle permet également, si on l'applique deux fois ($H^2 = I_2$), de conserver n'importe quel état.

Le pile ou face quantique :

Afin d'illustrer ce qu'est un circuit quantique, la figure 2.3 donne la représentation du **pile ou face quantique**. Le registre d'entrée est constitué d'un qubit dans l'état $|0\rangle$. Le temps s'écoule de gauche à droite. Les lignes simples transportent de l'information quantique, les doubles de la classique, $\mathcal{M}$ est un système de mesure (par exemple un détecteur de photons).

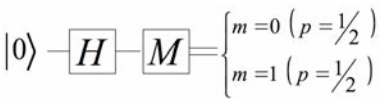


Fig. 2.3 – Action de H en « vision circuit » et en terme de « pile ou face » quantique

Dans cet exemple plutôt simple, on applique la porte H à l'état $|0\rangle$, ce qui conduit à l'état $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. La mesure donne comme résultat soit 0 soit 1, ceci avec une probabilité p de $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$, et l'état devient un état observable et classique, nommément 0 ou 1.

On définira, de manière naturelle puisque directement copié sur le calcul classique, un calcul quantique de la façon suivante : on dispose d'un *registre d'entrée* de n qubits, le calcul à proprement parlé est une succession de transformations unitaires qui aboutit à un *registre de sortie* de nature, soit quantique (exemple : protocole de la téléportation, cf.

section 3.2 du chapitre 3), soit classique (exemple : algorithme de Deutsch, cf. section 2.3). Dans l'exemple du pile ou face quantique, on a $n = 1$ et la sortie est de nature classique.

2.2.3 Systèmes à 2 qubits

Formalisme et intrication :

Une propriété fondamentale et purement quantique fait son apparition sous certaines conditions dès que l'on considère un système à 2 qubits : **l'intrication**. Le quatrième postulat de la mécanique quantique permet de définir le formalisme suivant : soient deux espaces de Hilbert $\mathcal{A}$ et $\mathcal{B}$ distincts à 1 qubit, munis de deux bases orthonormales « commodes » : $H_{\mathcal{A}} = \{|0_{\mathcal{A}}\rangle, |1_{\mathcal{A}}\rangle\}$ et $H_{\mathcal{B}} = \{|0_{\mathcal{B}}\rangle, |1_{\mathcal{B}}\rangle\}$. Le premier est régit par l'observateur « Alice », le second par « Bob ». Le système total est alors - avec abus de notation - $\{Alice\} \otimes \{Bob\}$, constitué de la base $\{|0_{\mathcal{A}}\rangle \otimes |0_{\mathcal{B}}\rangle, |0_{\mathcal{A}}\rangle \otimes |1_{\mathcal{B}}\rangle, |1_{\mathcal{A}}\rangle \otimes |0_{\mathcal{B}}\rangle, |1_{\mathcal{A}}\rangle \otimes |1_{\mathcal{B}}\rangle\}$ soit, en allégeant les notations, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

On aura besoin, pour la suite, de définir de façon pratique l'opération produit tensoriel entre matrices : soient $M_{\mathcal{A}}$ et $M_{\mathcal{B}}$ deux matrices agissant respectivement sur $\{Alice\}$ et $\{Bob\}$, alors :

$$M_{\mathcal{A}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } M_{\mathcal{B}} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \Longrightarrow M_{\mathcal{A}} \otimes M_{\mathcal{B}} = \begin{pmatrix} aM_{\mathcal{B}} & bM_{\mathcal{B}} \\ cM_{\mathcal{B}} & dM_{\mathcal{B}} \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta & b\alpha & b\beta \\ a\gamma & a\delta & b\gamma & b\delta \\ c\alpha & c\beta & d\alpha & d\beta \\ c\gamma & c\delta & d\gamma & d\delta \end{pmatrix}$$

De la même façon, on aura :

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Le quatrième postulat semble impliquer que l'on pourrait *a priori* décomposer un système quantique très grand, complexe, en produits tensoriels de sous-systèmes plus petits, plus simples. Cependant c'est loin d'être toujours le cas et ceci dès que l'on considère deux qubits : soient $|\psi_{\mathcal{A}}\rangle$ et $|\psi_{\mathcal{B}}\rangle$ deux qubits, un état quantique à deux qubits est dit **intriqué** si *il n'est pas* de la forme $|\psi_{\mathcal{A}}\rangle \otimes |\psi_{\mathcal{B}}\rangle$. L'exemple le plus célèbre est celui des **états de Bell**, qui sont les suivants :

$$\begin{aligned} |B_0\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |B_1\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |B_2\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |B_3\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

Physiquement, cela signifie que les 2 qubits sont corrélés de façon maximale, maximale

en ce sens que la corrélation ne dépend de rien. Dans le cas classique, lorsque deux valeurs sont corrélées, la fonction de corrélation qui leur est associée dépend de divers paramètres, par exemple certaines décroissent lorsque la distance entre deux grandeurs augmentent. En revanche, dans le cas quantique, la corrélation ne dépend d'aucun paramètre. Cette propriété est des plus étonnantes car si Alice mesure $|\psi_{\mathcal{A}}\rangle$ et trouve par exemple la valeur « 0 », tout se passe comme si $|\psi_{\mathcal{B}}\rangle$ « savait » que son « collègue » avait pris cette valeur pour basculer instantanément dans le même état, et ceci même si il se trouve à des millions d'années-lumière ! Autrement dit et même de façon plus forte, ce phénomène est *non local*. Comme on va le voir, l'intrication (mais pas son caractère non local) est un ingrédient indispensable pour faire du calcul quantique.

La porte $Cnot$ **:**

Maintenant, voyons à proprement parler les manipulations possibles sur 2 qubits. Même si de manière générale, toute matrice unitaire de dimension 4×4 peut être une transformation unitaire sur deux qubits, les opérations unitaires sur 2 qubits découlent le plus souvent de la question suivante : « si A alors B ». En effet, comme celle-ci revêtait une grande importance en logique classique, l'idée est venue d'en définir un homologue quantique, connu sous l'appellation **« Controlled–U »**, et notée C_U. Son action est la suivante : on considère un qubit de contrôle, $|c\rangle$, et un qubit-cible, $|t\rangle$. Si le qubit de contrôle est à « 0 » (c'est-à-dire dans l'état $|0\rangle$), le qubit-cible conserve son état ; dans le cas contraire ($|1\rangle$), l'opération U est appliquée au qubit-cible. L'exemple pertinent pour ce qui est de la compréhension basique des propriétés du calcul quantique (à savoir découvrir ce qu'est formellement l'intrication) est $C_U = C_{\sigma_x}$, transformation plus connue sous le nom de C_{not}, dont voici la caractérisation :

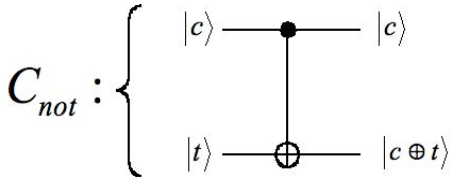


Table de vérité de C_{not} ***:***

$|00\rangle \mapsto |00\rangle$
$|01\rangle \mapsto |01\rangle$
$|10\rangle \mapsto |11\rangle$
$|11\rangle \mapsto |10\rangle$

Fig. 2.4 – C_{not} en « vision circuit »

Ainsi que l'on peut le constater sur la figure 2.5 , c'est une des opérations sur deux qubits qui permet de créer de l'intrication :

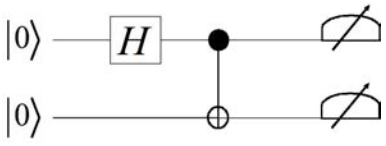


Fig. 2.5 – Création d'une paire intriquée en « vision circuit »

Cette figure permet l'opération suivante, qui peut se « lire » de deux façon différentes :

– $|0\rangle$ – $\boxed{H}\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$ – $\boxed{C_{not}}\rightarrow \frac{|00\rangle+|11\rangle}{\sqrt{2}} = B_0$

– $(C_{not} \times (H \otimes I_2))\,|00\rangle = B_0$

2.2.4 Généralisation / famille universelle de portes logiques

Les systèmes comportant plus de 2 qubits ne sont guère plus compliqués à étudier avec le modèle des circuits logiques quantiques, du moins du point de vue conceptuel. On définit comme précédemment, pour un nombre $(n + k)$ de qubits donné, des portes « $controlled - U$ », notées C_U^n, vérifiant l'équation suivante :

$$C_U^n\,|x_1x_2...x_n\rangle\,|\psi\rangle = |x_1x_2...x_n\rangle\,U^{x_1x_2...x_n}\,|\psi\rangle \tag{2.28}$$

où $x_1x_2...x_n$ est le produit des bits $x_1x_2...x_n$ et $|\psi\rangle$ est un système de k qubits. Cela signifie que l'opérateur U est appliqué sur les k qubits-cible si et seulement si les n qubits de contrôle sont à « 1 », sinon il ne se passe rien.

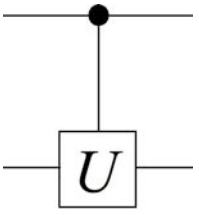


FIG. 2.6 – C_U en « vision circuit » pour le cas des 2 qubits

On démontre [CN00], ainsi que c'est exprimé sur la figure 2.7 ci-dessous pour le cas $n + k = 3$ avec $n = 2$ et $k = 1$, que n'importe quelle opération unitaire agissant sur n qubits peut être implantée exactement par des portes logiques à 1 qubit et des C_{not}.

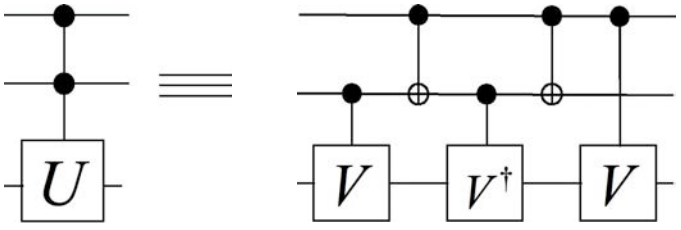


FIG. 2.7 – Construction de C_U^2 via l'opération sur 1 qubit V vérifiant $V^2 = U$ et C_{not}.

Un tel résultat se démontre facilement en considérant le produit de matrices suivant :

$$\begin{pmatrix} I_2 & 0 & 0 & 0 \\ 0 & I_2 & 0 & 0 \\ 0 & 0 & V & 0 \\ 0 & 0 & 0 & V \end{pmatrix} (C_{not} \otimes I_2)(I_2 \otimes V^\dagger)(C_{not} \otimes I_2)(I_2 \otimes V) = \begin{pmatrix} I_2 & 0 & 0 & 0 \\ 0 & I_2 & 0 & 0 \\ 0 & 0 & I_2 & 0 \\ 0 & 0 & 0 & V^2 \end{pmatrix} = C^2(U)$$

On démontre également [CN00] que la famille composée des portes logiques quantiques à 1 qubit suivante :

$$\left\{ H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} ; S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} ; T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \right\}$$

respectivement la porte de Hadamard, la porte de « phase », la porte « $\frac{\pi}{8}$ », munie de la porte C_{not}, constitue une famille universelle approchée pour le calcul quantique, approchée en ce sens que n'importe quelle opération unitaire agissant sur n qubits peut être approximée, avec une précision arbitraire, par un circuit logique quantique construit uniquement avec ces portes.

Une première conclusion : Classique versus Quantique

Il ne s'agit pas là d'exposer de façon exhaustive les propriétés respectives des mondes classique et quantique mais plutôt, tout en faisant un parallèle entre ces deux là, de résumer et de se focaliser sur leurs différences essentielles dans le cadre si particulier qu'est le calcul et / ou l'information. Cette prise de conscience permettra de mieux cibler les propriétés du calcul quantique. Ce distinguo est issu d'un des séminaires de Philippe Jorrand.

Physique classique :

- À tout instant t, un système physique S est dans un seul état à la fois (série de 0 et/ou de 1) : un registre de 3 bits donnera la valeur 0, 1, 2, 3, 4, 5, 6 ou 7 (en notation décimale).
- Les transformations qui modélisent l'évolution de l'état de S ne sont pas, en général, réversibles : si on considère, par exemple, la porte $NAND$ en logique classique, il n'est pas possible de savoir, dans le cas où sa sortie est à 1, si les 2 bits d'entrée étaient à 01, 10 ou 00. Dans le cas de NOT, en revanche, si la sortie est à 0, on en déduit que l'entrée était à 1, et vice-versa.
- L'observation (ou la mesure) de S dans un état E ne modifie pas E : si le registre à 3 bits était à 7, l'observateur mesurera la valeur 7.
- La mesure est déterministe : elle fournit la même information pour des systèmes identiques qui sont dans un même état E.
- On peut cloner un système : $FANOUT$ est une opération, en logique classique, à une entrée et à plusieurs sorties qui sont autant de duplications de l'entrée.
- L'état d'un système physique composé de n sous-systèmes peut se traduire en un n-uplet des états de ces sous-systèmes. En clair, le fait de mesurer un de ces sous-systèmes n'interférera pas sur le résultat d'un des autres sous-systèmes.

Physique quantique :

- À tout instant t, un système physique S peut être dans une superposition d'états (à la fois « 0 » et « 1 ») : un registre de 3 qubits aura donc les valeurs 0, 1, 2, 3, 4, 5, 6 et 7 à la fois.
- Les transformations qui modélisent l'évolution de l'état d'un système isolé et inobservé sont réversibles et déterministes.
- L'observation de S dans un état E modifie E de façon irréversible.
- La mesure est probabiliste : elle peut fournir une information différente pour des systèmes identiques qui sont dans un même état E. Le registre de 3 qubits sera dans l'état 0, 1, 2, 3, 4, 5, 6 ou 7, avec la probabilité qui leur est à chacun attachée.
- On ne peut pas cloner un système (linéarité de la mécanique quantique).
- L'état d'un système quantique composé de n sous-systèmes ne peut pas, en général, se traduire en un n–uplet des états de ces sous-systèmes (intrication).

2.3 Exemples de calcul quantique par requête à un oracle

2.3.1 Définition

On a vu dans la section 1.1 que tout problème calculable est traduisible en terme de problème de décision c'est-à-dire que, pour une instance donnée de ce problème, on obtient la réponse « oui » si elle est positive, « non » si elle est négative. Afin de bien pouvoir modéliser des problèmes en apparence complexe, les questions peuvent être aussi élaborées que possible et les réponses apportées par l'algorithme associé peuvent être « raisonnablement » longues. Les questions et les réponses font souvent appel à des bits auxiliaires (*ancilla bits*) : ce sont des entrées et/ou des sorties supplémentaires qui ne seront d'aucune utilité pour la réponse du calcul elle-même, mais qui constituent un « espace de travail ». L'étude des algorithmes en terme d'oracle convient parfaitement à l'ordinateur quantique car la sortie d'un calcul quantique est probabiliste. Le but du jeu est donc de s'arranger pour obtenir une probabilité égale à 1 pour le « bon » résultat et quelques trésors d'astuce vont être dévoilés afin de montrer que l'on peut, dans certains cas, mener l'entreprise à bien. Mais, avant toute chose, voici la définition d'un oracle quantique, devancée par une illustration : la figure 2.8.

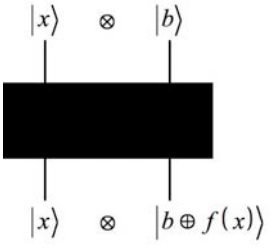


Fig. 2.8 – Forme de base d'un oracle quantique

La « boîte noire » contient une fonction $f : \{0,1\}^n \to \{0,1\}$; elle répond à une question par « oui » ou « non ».
Remarque 1 : le contexte exige parfois $f : \{0,1\}^n \to \{0,1\}^m$.

On a vu qu'il était possible d'implanter (du moins théoriquement) n'importe quelle opération unitaire (cf. section 2.2), il existe donc des constituants pour la « boîte noire ».

En classique, on a besoin, en terme de complexité, « d'appeler » $O(f(n))$ la fonction f (soit $O(f(n))$ requêtes en langage d'informaticien) ; en quantique, le plus souvent il y aura une seule requête (parfois n). Le parallèle entre classique et quantique sera mieux explicité dans le paragraphe qui suit.
Remarque 2 : la construction de la « boîte noire » exige parfois un coût en terme de complexité plus conséquent en quantique, qu'en classique.

2.3.2 Exemples

L'oracle de Deutsch :

C'est le point de départ du calcul quantique en ce sens qu'il est le plus simple et, de fait, rend compte de façon presque immédiate des vertus de la mécanique quantique en terme d'efficacité de calcul. Cet exemple pourra sembler au premier abord trivial mais, d'ores et déjà naît la difficulté de faire le distinguo entre les différents rôles joués par les interférences, les superpositions et l'intrication quantiques. On peut même aller jusqu'à dire que leurs rôles sont sacrément intriqués !

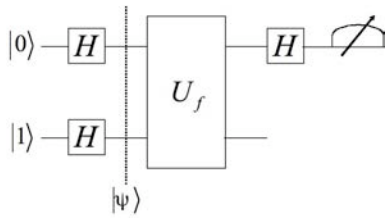


Fig. 2.9 – Oracle de Deutsch

La fonction $f : \{0,1\}^n \to \{0,1\}$ est supposée soit constante ($f(0) = f(1)$), soit balancée ($f(0) \neq f(1)$).

Classiquement, il faudrait effectuer deux requêtes à l'oracle qui calculerait les deux valeurs à comparer.

Quantiquement, une seule requête suffit ainsi que l'on va le constater.

Le circuit de la figure 2.9 se traduit de la façon suivante :

$$|\psi\rangle = (H|0\rangle) \otimes (H|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = \left(\frac{1}{2}\sum_{x=0}^{1}|x\rangle\right) \otimes (|0\rangle - |1\rangle)$$

Rappel : $U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle$
À ce stade là, deux posssibilités :

1. $f(x) = 0 \Longrightarrow (\left|0\right\rangle - \left|1\right\rangle) \rightarrow (\left|0\right\rangle - \left|1\right\rangle)$
2. $f(x) = 1 \Longrightarrow (\left|0\right\rangle - \left|1\right\rangle) \rightarrow (\left|1\right\rangle - \left|0\right\rangle) \rightarrow -(\left|0\right\rangle - \left|1\right\rangle)$

De façon plus compacte, on a : $(\left|0\right\rangle - \left|1\right\rangle) \rightarrow (-1)^{f(x)}(\left|0\right\rangle - \left|1\right\rangle)$
Par suite, $U_f \left|\psi\right\rangle = \left(\frac{1}{2}\sum_{x=0}^{1}(-1)^{f(x)} \left|x\right\rangle\right) \otimes (\left|0\right\rangle - \left|1\right\rangle) = \left|\phi\right\rangle \otimes \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)$,
où $\left|\phi\right\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}\left|0\right\rangle + (-1)^{f(1)}\left|1\right\rangle\right)$ est le registre dit de données et $(\left|0\right\rangle - \left|1\right\rangle)$, le registre–cible.
Finalement, on applique H à $\left|\phi\right\rangle$:

$$\begin{aligned} H\left|\phi\right\rangle &= \tfrac{1}{2}\left[(-1)^{f(0)}(\left|0\right\rangle + \left|1\right\rangle) + (-1)^{f(1)}(\left|0\right\rangle - \left|1\right\rangle)\right] \\ &= \tfrac{1}{2}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)\left|0\right\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)\left|1\right\rangle\right] \end{aligned}$$

Après mesure, si on obtient $\left|0\right\rangle$, cela signifie qu'il y a 100% de chance pour que f soit constante ; sinon $(\left|1\right\rangle)$, toujours avec 100% de chance, f est balancée.

À partir de là, une remarque s'impose : la question au préalable était juste de savoir si f était constante ou balancée, non pas de connaître les valeurs respectives de $f(0)$ et $f(1)$. À ce jour, l'algorithme classique connu calcule systématiquement ces deux valeurs, ce qui en soi est un surplus d'information par rapport à la problématique, surplus qui nécessite deux requêtes à l'oracle, soit deux séquences d'opérations permettant de calculer une valeur de f ; de tels calculs peuvent se révéler fastidieux en terme de complexité de calcul. En revanche, dans le cas quantique, on a exactement ce que l'on veut et ceci en faisant appel à l'oracle qu'une seule fois, ainsi que cela a été exprimé ci-dessus ; l'astuce ici étant que l'obtient toujours, après avoir mesuré le système, une probabilité égale à 1.

Analysons de façon plus précise cet algorithme. Il s'agit là bien sûr d'un cas d'école mais il donne déjà une bonne petite idée de ce que l'on peut accomplir en exploitant le parallélisme quantique. Qu'elle est la nature véritable du parallélisme quantique ? Car, après tout, dans le monde classique, on peut très bien faire agir deux ordinateurs en parallèle ! Il est également possible de simuler classiquement une superposition d'états. Cependant, dans le cas classique, les deux processeurs ne travailleront jamais de façon vraiment simultanée. C'est la mise en superposition d'états, suivie de l'action d'intriquer qui permettent de faire en sorte que les deux « processeurs quantiques » (ici à 1 qubit) agissent pleinement de concert puis, lorsqu'on les fait interférer, c'est un petit peu comme si on prenait de l'information sur le premier processeur en acceptant d'en perdre sur le deuxième pour obtenir une réponse.

Par ailleurs, le fait de pouvoir ajouter de l'intrication aux superpositions quantiques fait chuter la complexité en terme de calcul : admettons que l'on décide de construire classiquement une superposition de 2^n états car c'est aussi une caractéristique des systèmes

classiques linéaires. On a besoin d'un *unique* système physique capable de supporter chaque état, par exemple en considérant les 2^n modes de vibration d'une onde vibrante. Ces modes vont correspondre à des niveaux de plus en plus hauts d'une ressource physique quelconque, par exemple l'énergie de l'onde vibrante. Une superposition de ces 2^n modes requiert une quantité exponentielle (en n) de cette grandeur physique pour la représenter. En revanche, dans le monde quantique, on peut représenter une telle superposition en utilisant seulement n (complexité linéaire en n) systèmes à 2 niveaux, ceci grâce au phénomène de l'intrication. Ainsi, bien qu'il puisse y avoir des superpositions dans le monde classique, le phénomène d'intrication permet-il un gain exponentiel en terme de ressources physiques nécessaires à la représentation de grandes superpositions.

En gros les superpositions quantiques, plus l'intrication, permettent de « construire » avec une complexité linéaire un nombre exponentiel « d'univers » à vases communicants.

Pour résumer, il y a trois ingrédients de base pour le calcul quantique qui sont : superpositions, intrication, interférences. Ingrédients – de base – en ce sens que ces trois-ci sont déjà nécessaires dans le cas de l'oracle de Deutsch.

L'oracle de Deutsch-Jozsa :

Il s'agit d'une généralisation de l'oracle de Deutsch avec, cette fois-ci, $f : \{0,1\}^n \to \{0,1\}$. La fonction f possède donc 2^n antécédents et 2 images. Dans ce cas, f est dite *balancée* si $f = 0$ pour la moitié de ses entrées et 1 pour les restantes.

Classiquement, il faut, au pire, $2^{\frac{n}{2}} + 1$ requêtes, soit une complexité exponentielle en $O\left(2^{\frac{n}{2}}\right)$. En effet, l'émetteur qui s'occupe de l'entrée, Alice, sélectionne un nombre x tel que $0 \leq x \leq 2^n - 1$ dont elle envoie la valeur à Bob, chargé de la sortie. Celui-ci calcule $f(x)$ et lui répond en lui envoyant la valeur 0 ou 1. Dans le pire des scénarios, Bob va toujours trouver la même valeur, arbitrairement 0, pour la moitié des entrées soit après $2^{\frac{n}{2}}$ requêtes, plus une afin d'achever le calcul.

Quantiquement, une requête suffit !

L'oracle de Bernstein-Vazirani :

Il s'agit de l'oracle le plus simple qui étudie la périodicité a d'une fonction $f : \{0,1\}^n \to \{0,1\}^n$. La fonction f est telle que $f(x) = ax$, où $a \in \{0,1\}^n$. La question qui se pose alors est : quelle est la valeur de a ? Classiquement, il faut, au pire, 2^n requêtes, plus la résolution d'un système linéaire à n équations, soit une complexité en $O(2^n)$.

Quantiquement... une requête !

La Transformée de Fourier Quantique (TFQ) :

Avant d'aborder l'oracle de Simon et *a fortiori* celui de Shor, il est nécessaire de savoir calculer la période d'une fonction. La transformée de Fourier en physique classique a la propriété de décomposer une fonction du temps et de l'espace en une somme ou série de

fonctions élémentaires sinusoïdales, donc de périodes constantes. De façon plus imagée, elle donne la relation entre la représentation spatio-temporelle d'un signal et sa représentation en « bâtonnets » plus ou moins longs, qui constituent son spectre, c'est-à-dire l'ensemble des harmoniques du signal, donnant accès facilement à l'ensemble de ses périodes. L'idée alors d'utiliser la transformée de Fourier pour l'oracle de Simon ne semble plus dénuée de sens.

Comme on pourra le constater par la suite, les algorithmes dits « quantiques » le sont pour certaines étapes, les restantes utilisant les artifices classiques. Cela vient du fait que le gain en terme de complexité, du moins à ce jour, s'obtient au niveau du nombre de requêtes à l'oracle. L'hypothèse selon laquelle il faut continuer à exploiter les astuces de l'algorithmique classique semble raisonnable quand on voit toute l'ingéniosité qui a été requise pour l'étude du « design » des algorithmes classiques, et aussi du fait qu'un algorithme quantique doit impérativement être plus efficace que son homologue classique.

Le fait que la solution quantique est bien plus efficace réside dans les propriétés de ce que l'on appelle la transformée de Fourier quantique (TFQ) dont on a va considérer les grandes lignes. Il est à noter que la transformée de Fourier classique ou quantique est caractérisée de façon optimale grâce à la théorie des groupes en mathématiques ! En particulier, pour l'étude des oracles de Simon et de Shor, on considère les deux groupes additifs suivants : $\mathbb{F}_2^n$ et $\mathbb{Z}_n$.

Par définition, on a :

- $\mathbb{F}_2^n = \{0,1\}^n$: c'est un ensemble de 2^n éléments de la forme $x = \{x_1, x_2, ..., x_n\}$. Ce sont des n-uplets qui sont tels que $\forall i, x_i \in \{0,1\}$.
- $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ est le groupe additif des entiers relatifs modulo n, muni de l'addition modulo n.

Exemple : $\mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$ est le groupe additif des entiers modulo 4, muni de l'addition modulo 4.

Dans le premier et le deuxième cas, pour un système de n qubits, la transformée de Fourier quantique est respectivement linéaire et quadratique en n, au détriment d'une complexité exponentielle dans le cas classique !

Ces propriétés découlent directement du parallélisme quantique : la transformée de Fourier quantique associée à $\mathbb{F}_2^n$ est tout bonnement :

$$H^{\otimes n} = H \otimes H \otimes ... \otimes H, \; n \text{ fois.} \tag{2.29}$$

La transformée de Fourier associée à $\mathbb{Z}_n$ est l'opération suivante

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{i\frac{2\pi xy}{2^n}} |y\rangle \tag{2.30}$$

On peut montrer que :

$$\sum_{y=0}^{2^n-1} e^{i\frac{2\pi xy}{2^n}} |y\rangle = (|0\rangle + e^{i\frac{\pi xy}{2^0}} |1\rangle)(|0\rangle + e^{i\frac{\pi xy}{2^1}} |1\rangle)...(|0\rangle + e^{i\frac{\pi xy}{2^{n-1}}} |1\rangle) \tag{2.31}$$

On retrouve bien la notion de parallélisme quantique.

La transformée de Fourier quantique, associée à $\mathbb{Z}_n$, est réalisable via des portes d'Hadamard, de C_{not}, et de $Controlled - U$, où U représente des rotations d'angles $\frac{\pi}{2^k}$, avec $k \in \mathbb{N}\backslash\{0\}$ [CN00].

L'oracle de Simon, un pas décisif pour l'algorithme de Shor :

Enoncé :

Soit $f : \{0,1\}^n \to \{0,1\}$, f est telle que $f(x) = f(y) \Leftrightarrow x = y$ ou $x = x \oplus r$ (addition modulo 2) avec $r \in \{0,1\}^n$; la question est de savoir ce que vaut r. Classiquement, on a une complexité $> 2^{\frac{n}{2}}$; quantiquement, il faudra n itérations d'un algorithme mettant en scène la transformée de Fourier quantique qui, pour le cas présent, est en $O(n)$, soit, au total, une complexité quadratique $O(n^2)$.

Protocole :

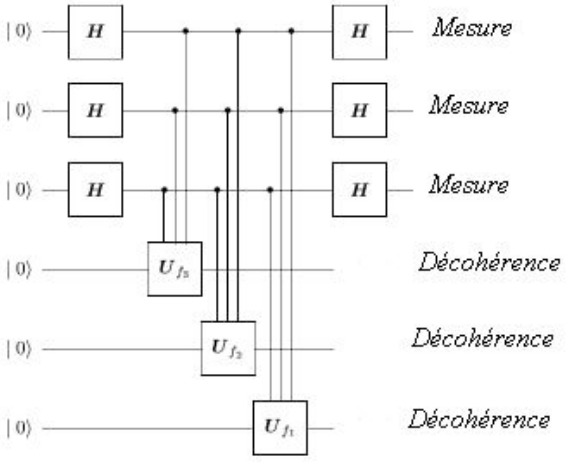


Fig. 2.10 – Oracle de Simon

Dans le cas général, le protocole comprend n « lignes » « au sommet » (cf. figure 2.10), semblables à celles des autres oracles mentionnés : dans le cas de celui de Deutsch, par exemple, $n = 1$. Les n « lignes » « du bas » ont chacune pour rôle d'implanter la sous-fonction $f_i : \{0,1\}^n \to \{0,1\}$. L'ensemble constitué par ces sous-fonctions correspond aux critères de la fonction f de l'oracle de Simon.

Les « boîtes » U_{f_i} dotées d'un « fil » représentent des portes $C_{U_{f_i}}$ dont le comportement est régi par $f_i(x)$.

En bref, l'oracle de Simon teste une fonction $f : \{0,1\}^n \to \{0,1\}^n$, fonction que l'on peut décrire grâce à n fonctions f_i à valeurs scalaires : 1 ou 0, soit « oui » ou « non ». La fonction f doit vérifier les deux conditions suivantes :

1. f est « deux en un », c'est-à-dire : $\forall y = f(x)$, $\exists x_1, x_2$ tels que $x_1 \neq x_2$ et $f(x_1) = f(x_2)$.
2. f est périodique : $\exists r \in \{0,1\}^n$ tel que $f(x \oplus r) = f(x)$ où $\oplus$ est l'addition modulo 2 (bit à bit).

Remarque : si au bout d'un certain temps une mesure n'a pas été effectuée sur un état quantique, celui-ci perd ses propriétés et adopte un comportement classique. Ce phénomène se nomme *décohérence*.

Étude pour $f : \{0,1\}^n \to \{0,1\}^n$:

1. On applique la porte de Hadamard sur les n premières lignes ($TFQ_{\mathbb{F}_2^n}$) :
   $\to \frac{1}{2^{\frac{n}{2}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) \otimes |0\rangle^{\otimes n}$ pour le registre des $2n$ qubits, initialisés à 0, c'est-à-dire qu'ils sont dans l'état $|0\rangle$.
2. On applique ensuite les portes U_{f_i} qui font passer les n premières lignes de l'état $|0\rangle$ à l'état $|0 \oplus f_i(x)\rangle = |f_i(x)\rangle \mapsto \frac{1}{2^{\frac{n}{2}}} \left(\sum_{x=0}^{2^n-1} |x\rangle \right) \otimes f(x)$.
3. Après décohérence des n dernières lignes, on obtient quelque valeur qui correspond soit à $f(x_0)$, soit à $f(x_0 \oplus r)$. Les n premières lignes sont donc sous la forme $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus r\rangle)$ (intrication).
   L'ordinateur est alors dans l'état $\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus r\rangle) \otimes f(x_0)$.
4. En appliquant H aux n premières lignes, on obtient :
   $\frac{1}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y=0}^{2^n-1} \left((-1)^{x_0.y} + (-1)^{(x_0 \oplus r).y} \right) |y\rangle \right) \otimes |f(x_0)\rangle$, où . est le produit bit à bit.
   Le vecteur y est tel que $y.r = 0$ ou $y.r = 1$.
   Dans le second cas, on a $(-1)^{x_0.y} - (-1)^{x_0.y} = 0$ donc seuls les vecteurs y orthogonaux à r vont rester.
   Par suite, le registre est : $\frac{2}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y.r=0} (-1)^{x_0.y} |y\rangle \right) \otimes f(x_0)$.

Mesurer les n premières lignes donnent ainsi toujours un vecteur y orthogonal à r. Il faut ensuite répéter le procédé un nombre suffisant de fois (complexité linéaire en n), afin d'obtenir n vecteurs y_i différents, vecteurs qui permettront de résoudre de façon classique un système linéaire à n équations, d'inconnu r, de la forme : $y_1.r = 0, y_2.r = 0, ..., y_n.r = 0$.

En résumé, on applique l'opération $H^{\otimes n}$ sur les n premières lignes initialisées à $|0\rangle$, lignes qui constituent le registre des données, afin d'obtenir pour ce registre une superposition de tous les nombres possibles, compris entre 0 et 2^{n-1}. Ceci étant, on le couple par

intrication avec le registre dit « cible », registre chargé d'évaluer la fonction f pour tous ses antécédents possibles en même temps.

Classiquement, il faudrait 2^{n-1} évaluations de f, soit le même nombre de requêtes à l'oracle de f, pour remplacer ce seul calcul quantique. C'est l'utilisation de portes $C_{U_{f_i}}$ qui fait que le calculateur quantique tout entier est dans un état intriqué. Lors de la décohérence des n dernières lignes, les n premières restent intriquées avec les dernières et sont forcées d'être dans la superposition :

$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus r\rangle) \tag{2.32}$$

Ainsi r est-il déjà présent dans le registre des données même si il reste assujetti à x_0. Il reste donc à éliminer l'indésirable, ce qui est possible en effectuant des rotations sur chaque qubit, avec pour résultat l'obtention d'un vecteur y orthogonal à r. On répète le processus au minimum n fois afin d'obtenir n y différents. Dans le pire des scénarios, la complexité reste linéaire en n.

Autant l'oracle de Deutsch passe pour un « cas d'école », autant on s'aperçoit que cela se corse pour celui de Simon, même si l'on peut éviter le « bagage » mathématique sous-jacent en considérant juste $H^{\otimes n}$ en tant que telle, et pas en tant que la TFQ rattachée à $\mathbb{F}_2^n$.

Cependant, il ne faut pas se réjouir trop tôt car l'oracle de Simon n'a pas d'utilité concrète, du moins sous la forme présentée. Il permet juste d'introduire l'oracle de Shor dont la propriété - ô combien troublante pour les créateurs et les briseurs de code - est de permettre la décomposition en facteurs premiers d'un nombre de longueur arbitraire n (nombre de bits représentant le nombre), c'est-à-dire de le factoriser, via un algorithme de complexité polynomiale en n, au lieu du $O\left(2^{n^{\frac{1}{3}}log(n)^{\frac{1}{3}}}\right)$ de son homologue classique, le plus efficace connu à ce jour, l'algorithme général crible pour les nombres (*General Number Field Sieve* en anglais). L'engouement provoqué par l'informatique quantique trouve son origine dans cet algorithme capable de briser le code RSA resté jusqu'alors incassable (du moins de façon efficace) avant cette découverte. Le code RSA exploite le caractère non réversible des fonctions modulo [Sin99] et est surtout exploité par les organismes qui veulent une sécurité fiable dans le cryptage de leurs informations.

L'algorithme de Shor met en scène la TFQ de $\mathbb{Z}_n$, la procédure d'estimation de phase (soit un opérateur unitaire U dont un vecteur propre u a pour valeur propre inconnue $e^{2i\pi\phi}$, le but du jeu est d'estimer ϕ). Entre également en considération le fait de pouvoir rendre équivalent le problème de l'ordre (soient x, N deux nombres entiers positifs tels que $x \leq N$, on cherche le plus petit entier positif r tel que $x^r = 1 mod[N]$) et celui de factorisation, lui même similaire à la recherche de la période d'une fonction. Pour cela il faut bien comprendre l'arithmétique et plus particulièrement l'arithmétique modulaire [CN00]. On exploite également dans certains cas l'algorithme des fractions continues [CN00].

2.4 État de l'art en terme d'algorithmes quantiques

Ingrédients essentiels et récurrents :

Un algorithme quantique est un procédé physique quelconque qui utilise des effets quantiques afin d'effectuer des calculs utiles. C'est toujours plus facile d'expliquer un concept en faisant un parallèle avec ce qui est déjà plus ou moins connu : à savoir le calcul classique. Les bits de mémoire d'un ordinateur quantique, comme il a déjà été spécifié, sont des qubits plutôt que des bits et les opérations élémentaires décrivant le calcul quantique sont des transformations unitaires, agissant sur un nombre fixé à l'avance de qubits ; elles remplacent les opérations de logique booléenne du calcul classique.

Voici les étapes basiques de la partie quantique d'un algorithme dont l'essentiel se traduit en terme d'oracle :

$\rightarrow |0\rangle^{\otimes n} |1\rangle \leftrightharpoons$ État initial

$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \leftrightharpoons$ Superposition d'états pour le registre de données et/ou le registre cible

$\rightarrow$ Application d'une porte U_f vérifiant $|x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$

$\rightarrow$ Application sur le registre de données de portes H ou autres (TFQ : transformée de Fourier quantique, G : itération de Grover)

$\rightarrow$ Mesure du registre de données

Mis à part les oracles mentionnés ci-dessus qui restent des cas d'école, les deux « vrais » algorithmes quantiques connus à ce jour sont l'algorithme de factorisation de Shor (on « passe » d'une complexité classique en $O\left(2^{n^{\frac{1}{3}} \log n^{\frac{1}{3}}}\right)$ à une complexité quantique en $O(n)$), et l'algorithme de recherche de Grover (de $O(2^n)$ à $O\left(\sqrt{2^n}\right)$).

Dans le cas de Shor, tout se passe comme si la « boîte noire » avait la capacité de reconnaître la période d'une fonction. Dans celui de Grover, la « boîte noire » reconnaît la ou les solutions à un problème de recherche. Ce raisonnement en terme d'oracles dont on ne connaît aucunement le fonctionnement peut sembler, au premier abord, singulier et de toute façon abstrait. Dans l'exemple de Grover, il semblerait que l'oracle « sache » déjà la réponse au problème de recherche posé. Comment exploiter un algorithme de recherche basé sur les consultations d'un tel oracle ? ! Tout simplement en faisant la distinction entre le fait de « savoir » et la capacité de « reconnaître » : il est possible d'être rompu à la seconde sans être tributaire du premier.

L'algorithme de Grover :

Posons, à des fins d'illustration, le problème pour Grover : supposons qu'un voyageur de commerce ait la tâche harassante de devoir passer par n villes données, séparées chacune

d'une distance d_{ij} et, afin d'être en accord avec le principe de Fermat qui montre que n'importe quelle particule n'est heureuse que si elle en fait le moins possible (la lumière choisit toujours le chemin le plus court, les atomes s'adonnent à la relaxation), doit les parcourir dans un ordre tel que la distance totale d' qu'il aura parcouru soit plus petite qu'une distance d donnée. Ce problème est NP–complet et se traduit aussi bien en terme de problème de recherche, à savoir trouver le circuit le plus court parmi les 2^n possibilités, qu'en terme de problème de décision : existe t-il un circuit de distance d' tel que $d' \leq d$ pour un d donné ? Afin d'établir une manière très générale de traiter les problèmes de recherche et d'en avoir eu *a posteriori* une vision géométrique très simple, on pose le problème en terme d'oracle.

Soit un espace de recherche à $N = 2^n$ éléments que l'on indexe par x, entier compris entre 0 et $N-1$, le problème de recherche associé possède M solutions, avec $1 \leq M \leq N$.

Une instance de ce problème peut être décrite par une fonction f caractérisée de la façon suivante : $f(x) = 1$ si x est solution du problème, $f(x) = 0$ sinon.

On considère alors l'oracle suivant :

$$O : |x\rangle\,|q\rangle \mapsto |x\rangle\,|q \oplus f(x)\rangle\,. \tag{2.33}$$

Le vecteur $|q\rangle$ est le qubit–oracle, qui change de valeur si et seulement si $f(x) = 1$, l'opérateur O est bien unitaire. On peut ainsi vérifier si x est solution en appliquant O à $|x\rangle\,|0\rangle$.

Pour l'algorithme quantique en lui-même, on applique O à $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, comme cela a été fait dans le cas de l'oracle de Deutsch : si x n'est pas solution, q reste inchangé, sinon, $|q\rangle$ devient $\frac{|1\rangle - |0\rangle}{\sqrt{2}}$, soit $-\,|x\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

En résumé, on a :

$$O : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \mapsto (-1)^{f(x)}\,|x\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{2.34}$$

soit :

$$O : |x\rangle \mapsto (-1)^{f(x)}\,|x\rangle\,. \tag{2.35}$$

Le génie de Grover a été de construire ce que l'on appelle l'itération de Grover, notée G, qui a la forme suivante :

$$G = (2\,|\Psi\rangle\,\langle\Psi| - I_2)O \text{ où } |\Psi\rangle = \frac{1}{N^{\frac{1}{2}}}\sum_{x=0}^{N-1}|x\rangle. \tag{2.36}$$

Dans les grandes lignes, il s'agit d'appliquer G un certain nombre de fois $\left(O\left(\sqrt{N}\right)\right)$ sur le registre de données, dont les n premiers qubits sont en superposition d'états $|\Psi\rangle$ par l'entremise de $H^{\otimes n}$, et le $(n+1)^{\text{ième}}$ dans l'état $|q\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ par l'opération HX.

Un certain nombre de qubits supplémentaires est nécessaire pour « l'espace de travail » de l'oracle ; celui-ci reste cependant négligeable devant n et n'influe donc pas en terme de

complexité.

L'aplomb de la géométrie :

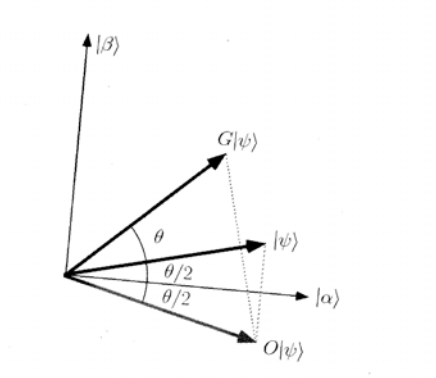


FIG. 2.11 – Action de l'itération de Grover

L'itération de Grover peut être vue comme une rotation dans l'espace engendré par les deux vecteurs suivants :

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x |x\rangle \text{ et } |\beta\rangle = \frac{1}{\sqrt{M}} \sum_x |x\rangle \text{ avec } M = 1. \tag{2.37}$$

Le vecteur $|\alpha\rangle$ représente la somme sur laquelle les x ne sont pas solutions et $|\beta\rangle$, celle où ils sont solutions.

On considère le cas $M = 1$, c'est-à-dire le cas où on ne recherche qu'une solution car c'est le plus simple à appréhender et les autres cas ne sont que des généralisations de ce qui va être abordé.

On constate assez facilement que l'état initial $|\Psi\rangle$ devient :

$$|\Psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle . \tag{2.38}$$

Si on reconsidère O, on s'aperçoit que :

$$O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle , \tag{2.39}$$

ce qui constitue une réflexion par rapport à l'axe $|\alpha\rangle$ dans la base $\{|\alpha\rangle, |\beta\rangle\}$. L'opérateur $2|\Psi\rangle\langle\Psi| - I_2$ est également une réflexion, dans le même plan, par rapport à $|\Psi\rangle$. Or le produit de deux réflexions donne une rotation et on peut montrer que dans la base $\{|\alpha\rangle, |\beta\rangle\}$, G peut s'écrire [CN00] :

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} . \tag{2.40}$$

En effet, on a :

$$O = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } 2\left|\Psi\right\rangle\left\langle\Psi\right| - I_2 = 2\begin{pmatrix} \sqrt{\frac{N-M}{N}} \\ \sqrt{\frac{M}{N}} \end{pmatrix}\begin{pmatrix} \sqrt{\frac{N-M}{N}} & \sqrt{\frac{M}{N}} \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$2\left|\Psi\right\rangle\left\langle\Psi\right| - I_2 = \begin{pmatrix} 2\frac{N-M}{N} - 1 & 2\sqrt{\frac{M}{N}\frac{N-M}{N}} \\ 2\sqrt{\frac{M}{N}\frac{N-M}{N}} & 2\frac{M}{N} - 1 \end{pmatrix} = \begin{pmatrix} 2\cos^2\frac{\theta}{2} - 1 & 2\cos\frac{\theta}{2}\sin\frac{\theta}{2} \\ 2\cos\frac{\theta}{2}\sin\frac{\theta}{2} & 2\sin^2\frac{\theta}{2} - 1 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

Par suite,

$$G = 2\left|\Psi\right\rangle\left\langle\Psi\right| - I_2 \times O = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Les entiers M et N remplissent les bonnes conditions pour définir le cosinus et le sinus d'un angle.

Au regard de la définition de θ, on a : $\left|\Psi\right\rangle = \cos\frac{\theta}{2}\left|\alpha\right\rangle + \sin\frac{\theta}{2}\left|\beta\right\rangle$, après k itérations de G :

$$G^k\left|\Psi\right\rangle = \cos\left(\frac{2k+1}{2}\theta\right)\left|\alpha\right\rangle + \sin\left(\frac{2k+1}{2}\theta\right)\left|\beta\right\rangle. \tag{2.41}$$

Si on répète un certain nombre de fois G, $\left|\Psi\right\rangle$ s'approche avec une « dangereuse certitude » de $\left|\beta\right\rangle$. Il en découle que la mesure qui sera effectuée sur $\left|\Psi\right\rangle$ donnera $\left|\beta\right\rangle$ avec une probabilité aussi proche que l'on veut de 1, ce qui est le but recherché !

L'algorithme de Grover a des applications très larges dans le domaine du calcul du fait qu'il traite un problème *NP-complet*. De plus, on peut très bien voir le problème de factorisation sous un angle permettant de l'exploiter : supposons que pour un n donné on sache qu'il existe deux facteurs premiers p et q. Une façon de les déterminer est de rechercher parmi tous les nombres compris entre 2 et $n^{\frac{1}{2}}$ le plus petit satisfaisant cette condition. L'algorithme de Grover permet d'augmenter la rapidité du processus. On peut également le découvrir en terme de simulations de systèmes physiques quantiques.

On peut démontrer [CN00] que l'algorithme de Grover est optimal, ce qui signifie que l'on peut considérer que l'étude du domaine de l'algorithmique quantique confinant aux problèmes de recherche est terminée. Malheureusement, cela signifie également que l'on ne peut plus en diminuer la complexité.

Pourquoi « si peu » de résultats, c'est-à-dire deux algorithmes plus quelques cas particuliers et quelques généralisations ? Tout simplement parce que les algorithmes quantiques doivent être plus efficaces que leurs homologues classiques : exploiter les phénomènes quantiques n'est pas une sinécure et, pour les problèmes réputés difficiles, déjà dans le domaine classique et ceci depuis plusieurs décennies, des centaines d'informaticiens planchent sur diverses solutions permettant de diminuer la complexité de tel ou tel problème, et obtiennent des résultats qui restent meilleurs que des solutions quantiques.

2.5 « Concrètement »...

Le stockage et le traitement de l'information quantique exigent des systèmes physiques obéissant aux conditions suivantes [Bel05] :

1. Une représentation du qubit robuste et bien définie
2. Des systèmes extrapolables à un nombre suffisant de qubits
3. Des qubits pouvant être initialisés dans un état connu (par exemple : $|0\rangle$)
4. Des qubits portés par des états physiques de vie moyenne assez longue afin d'assurer la cohérence des états quantiques tout au long du calcul
5. Un ensembles de portes quantiques universelles : rotations des qubits individuelles et porte C_{not}
6. Une procédure efficace de mesure des qubits à la fin du calcul

Ces conditions sont difficiles à réaliser simultanément et on en est encore aux premiers balbutiements des réalisations physiques d'ordinateurs quantiques. L'*ennemi n°1* de l'ordinateur quantique est l'interaction avec l'environnement, qui conduit au phénomène de décohérence, dont une conséquence est la perte de la phase dans la superposition linéaire des qubits. Les calculs doivent donc être effectués en un temps inférieur à celui de la décohérence (entre $10^{-10}s$ et $10^{-8}s$). Dans certains cas, ce temps peut sembler effroyablement court mais il faut aussi tenir compte, pour chacun des dispositifs, du temps que prend une opération élémentaire (une porte logique) sur un qubit (entre $10^{-14}s$ et $10^{-3}s$).

Voici quelques dispositifs imaginés jusqu'à présent [Bel05] :

- L'ordinateur quantique photonique exploitant l'effet Kerr issu de l'optique non linéaire (effet en χ 3)
- Les cavités optiques résonantes
- Les cavités micro-ondes résonantes
- La RMN (résonance magnétique nucléaire)
- Les jonctions Josephson dans les circuits supraconducteurs
- Les points quantiques
- Les ions piégés

Historiquement, l'ordinateur photonique a été le premier imaginé, directement inspiré de la théorie sur les oscillateurs harmoniques et il réunissait toutes les conditions mentionnées ci-dessus, toutes sauf une, l'effet Kerr nécessaire à l'élaboration de C_{not} s'étant révélé trop faible [CN00]. Aucun des dispositifs à ce jour ne fonctionnent vraiment car il y a toujours une ou des conditions qui pêchent et il s'agit encore d'une histoire de compromis. Les différentes solutions exposées ont, à ce jour, au mieux, concerné 2 qubits, à l'exception

de la RMN qui est allée jusqu'à 7 (et où il est possible de factoriser 15 [CN00]) ! Ceci dit, du moins *a priori*, aucune d'elles n'est l'avenir de l'ordinateur quantique.

Conclusion :

On a parlé d'universalité dans ces deux premiers chapitres mais cette notion n'est pas identique en classique et en quantique et il est très important de bien la distinguer selon le contexte.

Dans le monde classique, quand un modèle est dit universel, cela signifie qu'il est capable théoriquement de résoudre n'importe quel problème décidable. En quantique, on démontre [NC97] qu'il n'existe pas d'ordinateur quantique capable de résoudre n'importe quel algorithme quantique : le calculateur quantique qui résoudra l'algorithme de Shor n'aura pas la même structure que celui qui exécutera celui de Grover. En revanche, l'universalité des familles de portes logiques développée précédemment signifie que ces deux calculateurs les utiliseront ; c'est pourquoi on parle d'universalité malgré tout.

On a dressé, tout au long de ce chapitre, un diaporama de ce qu'est le calcul quantique avec la « vision » des circuits logiques quantiques. Pourquoi ce choix ? Et bien pour des raisons historiques et de simplicité d'appréhension puisque ce modèle est directement calqué sur le calcul classique. Cependant, il serait par trop réducteur que de s'y conformer car certains aspects du calcul quantique sont camouflés. C'est pourquoi on s'intéressera, dans le chapitre suivant, à d'autres formalismes de calcul.

Chapitre 3

Le calcul quantique revisité

Préambule

L'idée de l'ordinateur quantique est née avec cette réflexion de Feynman : **plutôt** que de désespérer de ne pouvoir simuler, c'est-à-dire, calculer l'évolution d'un système quantique sur un ordinateur classique, **pourquoi** ne pas utiliser les propriétés du système pour effectuer la simulation sur un nouveau support, nécessairement, du moins en partie, de nature quantique ? À partir de là, puisqu'il s'agit de calcul finalement, beaucoup de scientifiques se sont basés sur des modèles de calcul classique (machine de Turing, circuits logiques, algèbre de processus, marches aléatoires) pour formuler des homologues quantiques afin de pouvoir, d'une part accélérer des calculs dits compliqués (classes de complexité autres que **P**) et, d'autre part, comprendre plus en profondeur les propriétés quantiques, à savoir l'intrication, les superpositions linéaires et les interférences. Le modèle le plus simple à appréhender et qui a été le plus développé est celui des portes logiques quantiques (cf. chapitre 2), mais il est très difficile à implanter car une évolution unitaire est très fragile. C'est pourquoi : **plutôt** que de désespérer sur le fait que l'homologue quantique des circuits de calcul classique (en terme de portes NAND) est difficilement implantable à cause de la nature destructive des mesures en mécanique quantique, **pourquoi** ne pas exploiter les propriétés de ces dernières ? De plus, non seulement le postulat de la mesure en physique quantique constitue pour beaucoup de scientifiques la principale « bête noire » en terme de compréhension, mais un modèle quantique non calqué sur le monde classique ne peut que se révéler intéressant. Ainsi est-il devenu crucial d'élaborer une nouvelle modélisation de calcul quantique et le seul à ce jour qui ne possède pas d'homologue classique est le calcul quantique basé sur la mesure que l'on va aborder dans ce chapitre. D'autres modèles calqués sur des modèles classiques [Per06, Lal06, Kem03] (pour ne citer qu'eux), différents des circuits logiques quantiques existent, mais ils ne seront pas abordés.

Un premier modèle basé sur la mesure a été introduit par Briegel et Raussendorf [Rau03] : le *One-Way Quantum Computing*. En bref, il s'agit d'intriquer des particules de spin 1/2 grâce à l'interaction d'Ising. Ce « cluster » de qubits constitue l'état initial. On

lui applique ensuite une succession de rotations définissant le calcul voulu, ce qui revient à les projeter dans une succession de bases de l'espace de Hilbert de dimension 2, pour enfin obtenir le résultat du calcul.

Un deuxième modèle, proposé par Nielsen [Nie03], n'utilise, lui, que des mesures projectives, moins générales et plus pratiques que pour le modèle précédent et sans la nécessité de disposer au départ d'états intriqués. Ce dernier modèle fut largement amélioré ensuite [Leu04] en terme de ressources (nombre de qubits auxiliaires, nombre des différentes mesures projectives) pour déboucher sur des optimisations (ressources minimales) du modèle [Per06, Per05] *via* la notion de *transfert d'état*. Par exemple, les mesures les plus complexes alors à effectuer se réduisent à un unique produit tensoriel de deux observables bien définies ! Même si cette amélioration suscite la perte de la non localité en terme de téléportation, l'implantation physique de ce produit tensoriel, ainsi qu'une meilleure compréhension théorique de celui-ci, constituent des défis très intéressants.

Les deux modèles de calcul évoqués ci-dessus se sont révélés par la suite équivalents [Joz05] et ont été décortiqués afin de mieux comprendre ce qu'est le calcul quantique, en allant au-delà de ce que permettait les circuits logiques quantiques.

Avant de rentrer un peu plus dans les détails de ces deux modèles, il est important de mentionner que la démarche des divers acteurs impliqués a été de considérer que montrer l'universalité d'un nouveau modèle de calcul était équivalent à montrer sa capacité à simuler une famille universelle de transformations unitaires, notamment $\{SU(2), C_{not}\}$ pour l'universalité exacte [CN00], et $\{H, T, C_{not}\}$ pour l'universalité approchée [CN00] (approchée en ce sens que l'on peut approximer une transformation unitaire avec une précision arbitraire). En plus d'être universel, un modèle de calcul, pour être pertinent, doit être valable quelque soit la taille de la donnée à traiter et être tolérant vis-à-vis des erreurs.

Pour finir avec ce préambule, il n'est pas inutile de rappeler ce qu'est le postulat de la mesure en mécanique quantique et certains cas particuliers de mesures :

Énoncé : soit $\{M_m\}$ une famille d'opérateurs tels que $\sum_m M_m^\dagger M_m = I$, soit $|\psi\rangle$ l'état avant la mesure, la probabilité d'avoir le résultat m est $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$ et l'état $|\psi\rangle$ devient après la mesure : $\left|\psi'\right\rangle = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}$.

Cas particuliers :

-Mesures projectives (ou mesures de Von Neumann) :

Une telle mesure est définie par une observable (opérateur hermitien) $M = \sum_m mP_m$ (décomposition spectrale : les P_m sont des projecteurs) ; on a donc $p(m) = \langle\psi| P_m |\psi\rangle$ et $\left|\psi'\right\rangle = \frac{P_m|\psi\rangle}{\sqrt{p(m)}}$.

Remarque 1 : mesurer $M = \sum_m mP_m$ revient à choisir $\{P_m\}$ tel que $\sum_m P_m = I$ et $P_m P_{m'} = \delta_{mm'} P_{m'}$.

Remarque 2 : « mesurer dans la base orthonormale $\{|m\rangle\}$ » signifie effectuer la mesure projective avec les $P_m = |m\rangle \langle m|$.

Remarque 3 : historiquement, « mesurer le spin le long de l'axe $\overrightarrow{v}$ » signifie mesurer l'observable $\overrightarrow{v}.\overrightarrow{\sigma} = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3$, où les v_i sont les composantes d'un vecteur réel unitaire, associées aux matrices de Pauli (excepté I).

-2 types de mesures dégénérées pour les 2 qubits :

- Mesure projective ne tenant compte que des 2 projecteurs suivant (au lieu de 4) : $|\psi\phi\rangle \langle\psi\phi|$, $I - |\psi\phi\rangle \langle\psi\phi|$.
- Projection sur l'espace orthonormal *« intriqué »* de dimension 2 : $\{|B_0\rangle + |B_3\rangle , |B_1\rangle + |B_2\rangle\}$, où les B_i sont les états de Bell.

3.1 Le « one-way quantum computer » *(1WQC)*

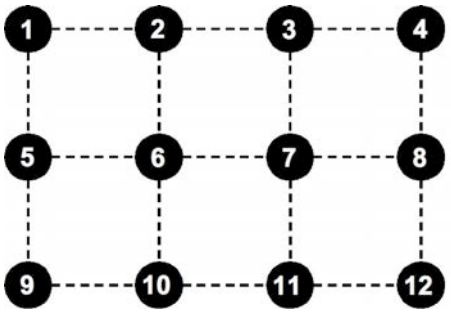
3.1.1 Les ressources utilisées

Un état initial appelé « cluster » :

Pour fabriquer un *cluster* (un ensemble), on procède de la façon suivante :

1. On dispose initialement de la ressource : $|\psi\rangle = \bigotimes_i |+\rangle_i$ où $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$
2. Les qubits sont intriqués deux à deux via une interaction d'Ising, uniforme

et accordable : $\mathcal{C}_Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$



– Un rond correspond à 1 qubit dans l'état $|+\rangle$.
– Une ligne correspond à une interaction d'Ising.

FIG. 3.1 – Cluster 2D

L'ensemble des qubits est intriqué simultanément (complexité temporelle en $O(1)$) car les matrices décrivant ces interactions commutent entre elles. Par ailleurs, cette préparation s'effectue avant le calcul proprement dit (préparation *off-line*). Ensuite, la simulation d'une première transformation $\mathcal{U}_{in}$ permettra celle de l'état du registre d'entrée voulu : $|\psi_{in}\rangle$.

Remarque 1 : le cluster peut se définir également comme l'unique état vérifiant :

$$\mathcal{K}^{(a)} |\psi\rangle_C = |\psi\rangle_C \text{ où } \mathcal{K}^{(a)} = \sigma_x^a \bigotimes_{b \in \mathcal{N}(a)} \sigma_z^b \tag{3.1}$$

L'opérateur $\mathcal{K}^{(a)}$ décrit les corrélations quantiques entre les divers qubits, $\mathcal{N}(a)$ est le voisinage du qubit a. Cette définition du cluster, plus compacte, (issue du formalisme des stabilisateurs) permet de démontrer [Rau03] comment via ce modèle de calcul on peut simuler, par exemple, la famille universelle $\{SU(2), C_{not}\}$.

Remarque 2 : un cluster 2D est une ressource universelle pour le calcul quantique, contrairement au cluster 1D comme cela a été démontré, entre autre, par Josza dans [Joz05].

Des mesures sur 1 qubit (donc locales) :

Des mesures (bases à définir) sur 1 qubit, successives (notion d'ordre), sur divers regroupements (caractère cliffordien ou non des transformations simulées) de qubits constituent le calcul. Entre les diverses séries de mesures, il faudra corriger d'éventuelles erreurs.

On considère 2 types de mesures :

-mesure du spin par rapport à l'observable Z : (c'est-à-dire selon l'axe (Oz))

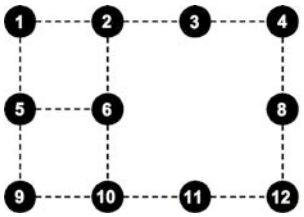


Fig. 3.2 – Figure 3.1 après la mesure du qubit 7 selon l'axe (Oz)

Elle a pour effet de « gommer » le qubit correspondant : il se projette dans un plan perpendiculaire au plan du cluster. Par exemple, si on mesure le qubit 7, le cluster de la figure 3.1 changera de forme, conformément à la figure 3.2.

Cette mesure permet d'imprimer une structure de circuit logique qui, on le verra, n'est pas indispensable.

-mesure du spin par rapport à l'observable $\cos(\phi)\sigma_x + \sin(\phi)\sigma_y$:
Elle a pour effet de faire faire une rotation quelconque au qubit correspondant. Grâce à une telle mesure, on peut implanter toutes les transformations souhaitées.

Un registre de sortie :

Le résultat du calcul se lit via un état final : les qubits qui n'ont pas été mesurés constituent l'état final $|\psi_{out}\rangle$; ils sont dans un état dépendant du calcul voulu.

Comme cela a déjà été mentionné dans le chapitre 2, un calcul quantique, en tant que tel, aura une sortie classique mais, dans certains cas, comme c'est expliqué dans la section 3.2 dédiée au calcul quantique basé sur la téléportation, on considérera parfois une sortie quantique qui constituera l'entrée de la séquence de calcul suivante. Les étapes de correction ne seront alors plus nécessaires car une simple ré-interprétation des résultats suffira. Bien sûr, au final, on aura une sortie classique qu'il sera nécessaire de corriger.

3.1.2 Un modèle universel

Théorème : *on simule [Rau03]* $\{SU(2), C_{not}\}$*, de la façon suivante :*

1. simulation de $\mathcal{C}_{not}$:

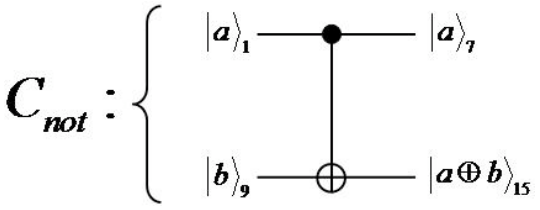


Table de vérité de C_{not} ***:***

$|00\rangle \mapsto |00\rangle$
$|01\rangle \mapsto |01\rangle$
$|10\rangle \mapsto |11\rangle$
$|11\rangle \mapsto |10\rangle$

FIG. 3.3 – Rappel : C_{not} en « vision circuit »

   (a) Préparation de l'état $|\psi_{in}\rangle_{C_{15}} = |\psi_{in}\rangle_{1,9} \otimes \left(\bigotimes_{i \in C_{15}\setminus\{1,9\}} |+\rangle_i \right)$, les qubits a et b de la figure 3.3 correspondent respectivement aux qubits 1 et 9 de la figure 3.4.

   (b) Intrication des 15 qubits via une interaction d'Ising

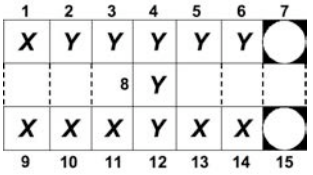


FIG. 3.4 – C_{not} en « vision 1WQC »

Remarque : comme il s'agit de la simulation d'une porte logique, on a préféré imprimer directement la structure de circuit dans le cluster en ne considérant que 15 qubits, mais

on aurait pu tout aussi bien considérer un cluster de 21 qubits (ce qui est généralement le cas ; les lignes pointillées de la figure 3.4 représentant, dans ce cas, les interactions d'Ising supplémentaires) et appliquer les mesures selon Z appropriées, avec une modification sans importance du point de vue conceptuel car locale de l'opérateur erreur $U_{\Sigma,C_{not}}$, défini dans l'équation 3.2.

(c) Mesure de tous les qubits excepté les numéros 7 et 15 :

Les mesures peuvent être effectuées toutes à la fois comme expliqué ci-dessous. Les qubits 1, 9, 10, 11, 13 et 14 sont mesurés dans la base de σ_x, les qubits 2 à 6, 8 et 12 dans celle de σ_y. Soit s_i le résultat de la mesure du qubit i, la porte logique simulée est alors :

$$U'_{C_{not}} = U_{\Sigma,C_{not}} C_{not}(a,b) \text{ où } U_{\Sigma,C_{not}} = {\sigma_x^{(a)}}^{\gamma_x^{(a)}} {\sigma_x^{(b)}}^{\gamma_x^{(b)}} {\sigma_z^{(a)}}^{\gamma_z^{(a)}} {\sigma_z^{(b)}}^{\gamma_z^{(b)}} \tag{3.2}$$

avec :
$$\begin{cases} \gamma_x^{(a)} &= s_2 + s_3 + s_5 + s_6 \\ \gamma_x^{(b)} &= s_2 + s_3 + s_8 + s_{10} + s_{12} + s_{14} \\ \gamma_z^{(a)} &= s_1 + s_3 + s_4 + s_5 + s_8 + s_9 + s_{11} + 1 \\ \gamma_z^{(b)} &= s_9 + s_{11} + s_{13} \end{cases} \tag{3.3}$$

L'opérateur $U_{\Sigma,C_{not}}$ décrit les erreurs de à corriger, il appartient au groupe de Pauli.

Ô miracle, cette porte est simulable en une étape ! En effet, C_{not} appartient à un groupe particulier, le groupe de Clifford, qui est le normalisateur du groupe de Pauli dans le groupe unitaire. Cela signifie en particulier que : $U_{\Sigma,C_{not}} C_{not} = C_{not} U'_{\Sigma,C_{not}}$. Pratiquement, on peut propager toutes les erreurs vers « le registre de sortie » de C_{not} (c'est-à-dire vers les qubits 7 et 15) sans modifier cette dernière. Quant à l'opérateur d'erreur, qu'il change ou non n'a guère d'importance. Le « registre de sortie » correspond au « registre d'entrée » de la transformation suivante, éventuelle à simuler. Ainsi peut-on effectuer toutes les mesures à la fois et ne corriger qu'à la fin. Pourquoi les guillemets ? On a exprimé les conséquences du caractère cliffordien de C_{not} dans une vision « circuit de portes logiques » qui a sa raison d'être uniquement pour démontrer l'universalité du modèle de Briegel et Raussendorf. En effet, admettons par exemple que l'on veuille simuler deux portes cliffordiennes, puis une qui ne l'est pas, et, pour finir, une dernière porte cliffordienne. Une première série de mesures permettra de simuler les 3 portes cliffordiennes à la fois, ce qui signifie qu'on simulera la dernière porte avant l'avant dernière ! Il faudra ensuite simuler la porte non cliffordienne qui demande une correction éventuelle au cours du calcul, cette porte pouvant être dépendante du résultat d'une série de mesures antérieures (cf. la simulation de $\mathcal{U} \in SU(2)$, figure 3.5, pour un exemple concret). Cette possibilité d'effectuer ainsi des calculs de façon ***non purement*** séquentielle en ce sens que l'on peut effectuer des opérations avant qu'elles « n'apparaissent », contrairement à l'ordre exigé d'apparitions des portes dans le modèle basé sur les circuits logiques quantiques, et pouvoir le faire en parallèle, n'a pas lieu chez les homologues

quantiques des modèles classiques ; ce qui est très intéressant déjà du point de vue conceptuel.

2. simulation de $\mathcal{U} \in SU(2)$:

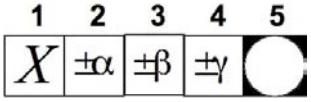


FIG. 3.5 – U en « vision 1WQC »

D'après la décomposition en angles d'Euler, on a : $U = R_x[\theta]R_z[\beta]R_x[\gamma]$. Les rotations autour des axes x et z sont respectivement $R_x[\theta] = \exp(-i\theta\frac{\sigma_x}{2})$ et $R_z[\theta] = \exp(-i\theta\frac{\sigma_z}{2})$.

(a) Préparation de l'état $|\psi_{in}\rangle_{C_5} = |\psi_{in}\rangle_1 \otimes \left(\bigotimes_{i \in C_{5\setminus\{1\}}} |+\rangle_i\right)$

(b) Intrication des 15 qubits via une interaction d'Ising

(c) Mesure de tous les qubits excepté le numéro 5 dans une base appropriée :

Soit la base de mesure suivante : $B_j(\phi_j) = \{\frac{|0\rangle_j + e^{i\phi_j}|1\rangle_j}{\sqrt{2}}, \frac{|0\rangle_j - e^{i\phi_j}|1\rangle_j}{\sqrt{2}}\}$, on applique la procédure suivante :

- Mesure du qubit 1 dans la base $B_1(0)$
- Mesure du qubit 2 dans la base $B_2(-\alpha(-1)^{s_1}))$
- Mesure du qubit 3 dans la base $B_3(-\beta(-1)^{s_2}))$
- Mesure du qubit 4 dans la base $B_4(-\gamma(-1)^{s_1+s_3}))$

On obtient alors : $U' = U_{\Sigma,U}U$ avec $U_{\Sigma,U} = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}$ l'opérateur d'erreurs, éventuelles (on peut avoir s_1=s_2=s_3=s_4=0 mais c'est rare) et/ou éventuellement à corriger (c'est-à-dire, quand l'étape de correction peut être remplacée par une ré-interprétation de résultats classiques comme cela sera expliqué dans la section 3.2). La transformation U n'est pas (en général) cliffordienne, c'est pourquoi les mesures ne peuvent pas se faire en même temps : elles dépendent du résultat de la mesure antérieure. De plus, il faudra corriger le registre de sortie de U si nécessaire.

3.2 Le calcul quantique basé sur la téléportation

3.2.1 Étape 0 : la téléportation pour 1 qubit (Bennett et Brassard)

a) D'abord une petite histoire :

La petite histoire qui va suivre, issue d'un des séminaires de Philippe Jorrand, met bien en scène d'une part, tous les ingrédients et d'autre part, de façon ludique donc marquante, toute la puissance du protocole de la téléportation quantique :

Il était une fois ...

... Alice prit un qubit et Bob prit l'autre qubit provenant de la même paire EPR (état de Bell) : $|EPR\rangle$. Une fois ce partage effectué, Bob s'envola à destination d'une lointaine, très lointaine et secrète galaxie.

Quelque temps plus tard ...

... un qubit dans un état inconnu : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ arrive chez Alice avec la mission suivante pour Alice (si, si, elle l'accepta !) : transmettre $|\psi\rangle$ à Bob.

Mais c'était au-dessus des forces d'Alice que de ...

... transmettre directement $|\psi\rangle$ à Bob (pour cela il lui faudrait l'observer donc le perturber)

... copier $|\psi\rangle$ pour obtenir beaucoup de qubits et leur faire prendre leur envol à travers l'univers (théorème du non clonage : cf. remarque ci-dessous)

... obtenir les valeurs respectives de α et β pour les transmettre à Bob par radio à travers l'espace intergalactique ($|\psi\rangle$ contient potentiellement une infinité d'informations puisque sa description la plus connue en tant que spin, la sphère de Bloch, est un ensemble continu ; il faudrait donc l'éternité à Alice pour transmettre toute l'information).

Remarque : étant donné que la démonstration du théorème de non clonage peut s'effectuer en 4 lignes, en exploitant le fait que la mécanique quantique est linéaire, il serait dommage de résister à la tentation. Pour ce faire, on effectue un raisonnement par l'absurde : soient M_C l'opérateur « machine à cloner », $|\psi\rangle$ le qubit que l'on veut cloner, et $|page\rangle$ la « page blanche ». Donc $M_C(|\psi\rangle|page\rangle)$ doit vérifier par la nature même de M_C :

$$M_C(|\psi\rangle|page\rangle) = |\psi\rangle|\psi\rangle$$

On a d'une part :

$$M_C(|\psi\rangle|page\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$$

D'autre part, comme la mécanique quantique est linéaire, on a :

$$\begin{aligned} M_C(|\psi\rangle|page\rangle) &= \alpha M_C(|0\rangle|page\rangle) + \beta M_C(|1\rangle|page\rangle) \\ &= \alpha|00\rangle + \beta|11\rangle \end{aligned}$$

ce qui n'est pas du tout la même chose. Conclusion, on ne peut pas cloner un qubit ! Sauf si $\alpha^2 = \alpha$, $\beta^2 = \beta$, et $\alpha\beta = 0$, conditions qui correspondent aux cas $(\alpha = 0, \beta = 1)$ et $(\alpha = 1, \beta = 0)$. Encore faut-il savoir au préalable qu'il est dans un de ces deux états !

Malgré tout, ni Alice ni Bob ne renoncèrent. Ainsi que l'on va le constater de façon plus formelle.

b) Le protocole :

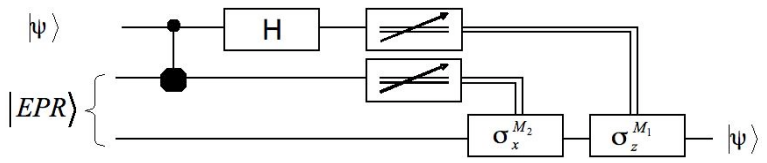


FIG. 3.6 – Protocole de téléportation, « en vision circuit », pour 1 qubit $|\psi\rangle$

Légende : – Les traits simples correspondent à des voies par lesquelles transite un qubit.
– Les traits doubles correspondent à des canaux par lesquels transitent des bits.

On peut lire la figure de la manière suivante :

$$\longmapsto \quad |\psi\rangle\,|EPR\rangle \tag{1}$$
$$= \quad (\alpha\,|0\rangle + \beta\,|1\rangle)(\frac{|00\rangle + |11\rangle}{\sqrt{2}}) \tag{2}$$
$$\longmapsto \quad \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle)(|00\rangle + |11\rangle)] \tag{3}$$
$$\longmapsto \quad \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle)(|10\rangle + |01\rangle)] \tag{4}$$
$$\longmapsto \quad \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \tag{5}$$
$$\longmapsto \quad \frac{1}{2}[|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)] \tag{6}$$
$$= \quad \frac{1}{2}[|B_0\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |B_1\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |B_2\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |B_3\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)] \tag{7}$$

NB1 : On peut ré-exprimer l'avant dernière ligne du calcul dans la base de Bell (dernière ligne), ce qui se révèle utile pour la compréhension du modèle de calcul quantique basé sur la téléportation. Par ailleurs, historiquement, c'est ainsi que Bennett et Brassard ont explicité leur protocole.

c) Mesure d'Alice :

Alice effectue sa mesure et obtient une fois sur quatre 00, 01, 10 ou 11, soit deux bits classiques. Voici alors ce qui se passe suivant les cas, en se référant à (6) et au postulat de la mesure :

$$\begin{aligned} 00 \longmapsto |\psi\rangle_{Bob} &= \alpha\,|0\rangle + \beta\,|1\rangle \\ 01 \longmapsto |\psi\rangle_{Bob} &= \alpha\,|1\rangle + \beta\,|0\rangle \\ 10 \longmapsto |\psi\rangle_{Bob} &= \alpha\,|0\rangle - \beta\,|1\rangle \\ 11 \longmapsto |\psi\rangle_{Bob} &= \alpha\,|1\rangle - \beta\,|0\rangle \end{aligned} \tag{3.4}$$

NB2 : Alice effectue sa mesure soit dans la base de calcul standard comme exprimé ci-dessus, soit dans la base de Bell (NB1).

Alice transmet le résultat de sa mesure à Bob *via* un canal classique, par exemple en l'émettant par radio, et ceci dans toutes les directions puisqu'elle ne sait pas à quel endroit Bob s'est réfugié.

d) Mesure de Bob :

Suivant la teneur de l'information reçue d'Alice, Bob va devoir appliquer telle transformation unitaire sur son qubit de départ afin d'obtenir $|\psi\rangle$. Puisque $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle, Z|0\rangle = |0\rangle$ et $Z|1\rangle = -|1\rangle$, d'après l'expression (3.4), Bob va appliquer la transformation suivante : $Z^{M_1}X^{M_2}$, où M_1 et M_2 prennent respectivement les valeurs du premier et du second bit d'Alice.

Exemple : Bob reçoit l'information 01, son qubit est alors dans la configuration $\alpha|1\rangle + \beta|0\rangle$ et $M_1 = 0$, $M_2 = 1$. Bob appliquera donc l'opération $Z^0X^1 = X$.

e) Remarque importante vis-à-vis du calcul quantique :

Le point clef de ce protocole est le fait qu'Alice, l'émetteur, peut diviser la totalité de l'information encodée dans l'état $|\psi\rangle$ en deux parties : une purement classique et l'autre purement quantique, et les faire parvenir à Bob *via* deux voies de communication différentes.

Cette distinction parfaite entre classique et quantique permet, ainsi qu'on le verra, de faire la même différenciation pour un algorithme quantique, traduit en terme de calcul basé sur la téléportation. Ceci n'est pas le cas pour le calcul quantique dit traditionnel qui exige la préparation d'un état initial, l'application d'une succession de transformations unitaires et des mesures finales, trois étapes dans lesquelles les mondes classique et quantique restent mélangés. Un algorithme quantique contient toujours un traitement classique et il s'agira ainsi de minimiser la partie quantique, ainsi que de comprendre toujours plus en profondeur le véritable rôle de la mécanique quantique dans la diminution de la complexité d'un calcul.

3.2.2 Étape 1 – M. Nielsen

Téléportation traduite uniquement en terme de mesures et interprétée en terme de simulation de la porte logique identité, à un opérateur de Pauli près [Nie03] :

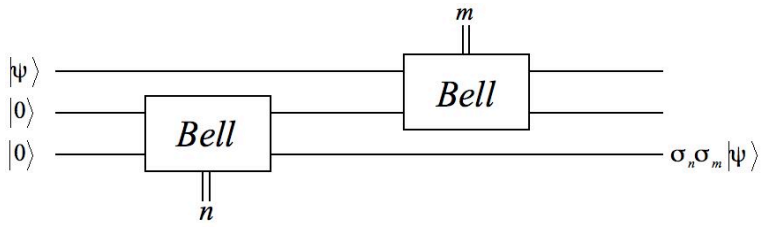


FIG. 3.7 – Protocole de téléportation traduit en terme de mesures

Légende : $\boxed{Bell} \Longrightarrow$ Base de mesures projectives sur 2 qubits : $\{|B_n\rangle \langle B_n|\}_{n\in\{0,1,2,3\}}$
D'où : $|00\rangle$–$\boxed{Bell}\rightarrow |B_n\rangle$, puis, $|\psi\rangle$ + la paire EPR $|B_n\rangle$ –$\boxed{Bell}\rightarrow \sigma_n\sigma_m |\psi\rangle$

Nielsen a eu la bonne idée de traduire le protocole défini ci-dessus juste en terme de mesures. Ce, grâce à une base de mesure intelligemment choisie : la base dite de Bell. Selon le résultat m de la mesure ***simultanée*** des 2 qubits du registre d'entrée, l'état sortant de la première « boîte Bell » sera l'un des états de Bell qui correspond à la paire EPR partagée par Alice et Bob dans le protocole d'origine (ce n'est pas grave si ce n'est pas B_0 car l'éventuelle correction (de Pauli) à appliquer sera locale). La deuxième mesure de Bell correspond à celle d'Alice. De fait, $|\psi\rangle$ a bien été téléporté, à une correction locale près.

Remarque : on considère que la téléportation, sous cette forme, exprime des mesures projectives NON DESTRUCTIVES : le vecteur $|\psi\rangle$ ne se porte en effet pas si mal.

Nielsen a montré que l'on peut effectuer du calcul quantique universel en utilisant seulement des mesures projectives :

Simulation de $\{U \in SU(2), V \in SU(4)\}$ **,** ***a fortiori*** **de** $\{U \in SU(2), C_{not}\}$ **:**

- Projection « off-line » de $|00\rangle$ sur $\{|U_j\rangle = (I \otimes U\sigma_j)\,|B\rangle_0\}$:

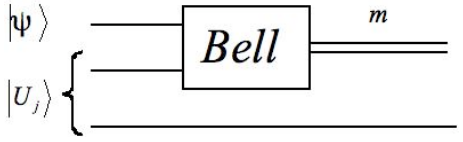


FIG. 3.8 – Simulation de $U \in SU(2)$, « à la Nielsen »

Comme $\boxed{Bell}$ et $U\sigma_j$ commutent, la figure 3.8 équivaut à :

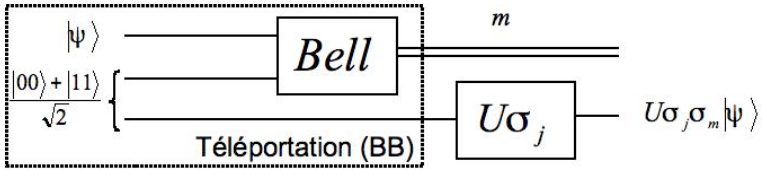


FIG. 3.9 – Simulation de $U \in SU(2)$ en terme de téléportation, « à la Nielsen »

- Projection « off-line » de $|0000\rangle$ sur $\{|V_{jk}\rangle = (I_{12} \otimes (V(\sigma_j \otimes \sigma_k))_{34}) |B_0\rangle_{13} |B_0\rangle_{24}\}$:

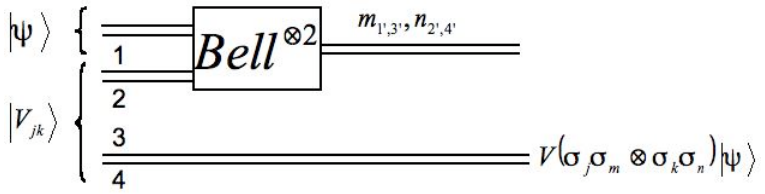


Fig. 3.10 – Simulation de $V \in SU(4)$, « à la Nielsen »

Il s'agit ici de faire une mesure dans « la bonne base » d'un état initial quelconque avant tout calcul préalable (« off-line »), puis d'effectuer une succession de mesures dites de Bell telles que décrites plus haut.

Ainsi qu'on le constate, un tel modèle nécessite non seulement 4 qubits auxiliaires (pour simuler une porte à 2 qubits on a besoin d'un état initial à 6 qubits ; 1, 2, 3 et 4 étant ces qubits supplémentaires), mais également de pouvoir mesurer 4 qubits à la fois ce qui est difficile à réaliser expérimentalement.

Il est important de s'intéresser au nombre de qubits auxiliaires puisque c'est un des paramètres décrivant la complexité d'un algorithme quantique.

Deux astuces sont à mettre au compte de D. Leung tant qualitatif (étape 3), que quantitatif (étape 4) [Leu04].

3.2.3 Étape 2 – D. Leung / Concept

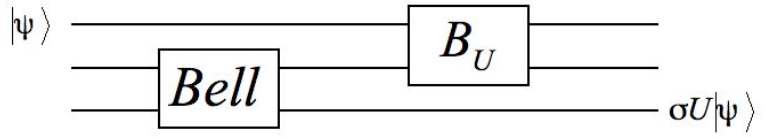


Fig. 3.11 – Simulation de $U \in SU(2)$, « à la Leung »

Où $B_U = \{(U^\dagger \otimes I_2) |B_n\rangle \langle B_n| (U \otimes I_2)\}_{n \in \{0,1,2,3\}}$ est une base de mesures projectives.

Ce qui équivaut à :

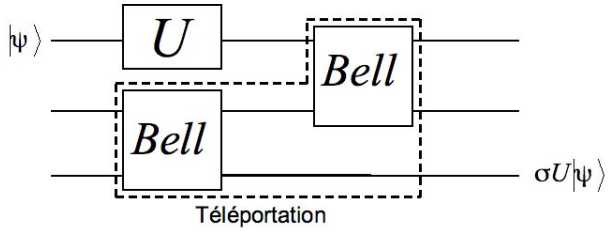


Fig. 3.12 – Simulation de $U \in SU(2)$ en terme de téléportation, « à la Leung »

Le modèle de Nielsen équivaut à la téléportation de $|\psi\rangle$ puis à l'application de U, alors que celui de Leung, c'est réaliser U puis téléporter $|\psi\rangle$.

Cela peut sembler anodin à première vue mais pas si l'on considère que les mesures en mécanique quantique le plus souvent nécessitent une étape de correction. C'est plutôt difficile chez Nielsen [Nie03], tandis que grâce à Leung [Leu02], les opérateurs de correction ne sont plus que des produits tensoriels d'opérateurs de Pauli. C'est ainsi que [JP03] dans le cadre du calcul quantique qui se termine par des mesures dans la base de calcul standard (c'est-à-dire une « sortie » classique), comme il s'agit d'un produit tensoriel d'opérateurs de Pauli, il suffit juste de ré-interpréter les résultats des mesures. Plus d'étapes de correction ! Mais plutôt des étapes de ré-interprétation, contrôlées de façon classique : par exemple, si l'opérateur de correction à appliquer est σ_x, on inverse les rôles des résultats classiques « 0 » et « 1 ». L'intérêt d'un tel raisonnement, mis à part qu'il évite l'étape de correction, réside dans le fait que le modèle devient déterministe car, dans le pire des cas, une étape de correction peut ne jamais se terminer (du moins si on reste dans le cadre du calcul quantique uniquement basé sur la mesure) et, dans tous les cas, on ne sait jamais de toute façon quand celle-ci se termine. En revanche, si on désire une « sortie » quantique bien spécifique, comme dans le cas du protocole de la téléportation originel qui a une toute autre application que le calcul, il y a une étape de correction comme cela a été déjà explicité.

3.2.4 Étape 3 – D. Leung / Ressources

C'est en exploitant le fait qu'en mécanique quantique on puisse faire des mesures dites dégénérées que Leung a montré [Leu02] qu'il suffisait de pouvoir faire des mesures projectives sur au maximum 2 qubits ; c'est un optimum car il faut des interactions sur au moins 2 qubits pour exploiter les propriétés de la mécanique quantique (intrication).

Le travail de D. Leung [Leu02] a donné également lieu à un important théorème dont voici l'énoncé : $\{Z, X, X \otimes X, Z \otimes Z, X \otimes Z, \frac{X+Y}{\sqrt{2}} \otimes X\}$ est une famille d'observables approximativement universelle en disposant de 4 qubits auxiliaires.

Constat : pour l'universalité approchée, on a un ensemble discret d'observables sur 1 et 2 qubits. L'idée de la démonstration est la suivante : appliquer la base de mesure B_U définie ci-dessus dans les cas particuliers où $U = \{H, T, C_{not}\}$ et $B_U = Bell$.

Halte 1 ! Soit $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ en tant qu'opérateur (décrivant une opération), il est hermitien donc on peut lui associer une observable X.
On a alors :

$|0\rangle \,/\, |1\rangle$ — $\boxed{\sigma_x} \longrightarrow |1\rangle \,/\, |0\rangle$

$|\psi\rangle$ — $\boxed{\text{X}} \longrightarrow sortie = + \Longrightarrow |\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ ou $sortie = - \Longrightarrow |\psi\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

Halte 2 ! Le symbole « $\otimes$ » signifie simultanéité (au sens détection de « bonnes » corrélations ou anti-décorrélations) de la mesure (ce symbole a donc une signification bien différente de celui que l'on trouve dans le postulat traitant de la séparabilité d'un système en sous-systèmes).

Comment simplifier encore plus le modèle ? Intuitivement, c'est fait pour le type de mesures puisque l'interaction entre deux qubits est nécessaire et suffisante pour exploiter l'intrication. En revanche, ça ne l'est pas pour le nombre de qubits auxiliaires : simuler une transformation unitaire avec une mesure destructive nécessite au moins 1 qubit auxiliaire et jusqu'ici il y en a 4. Se pose également la question de savoir si on peut diminuer le nombre d'observables sur 1 et 2 qubits. Dans cette optique, S. Perdrix a introduit un nouveau concept : le transfert d'état.

3.2.5 Étape 4 – S. Perdrix

Le transfert d'état [Per05] :

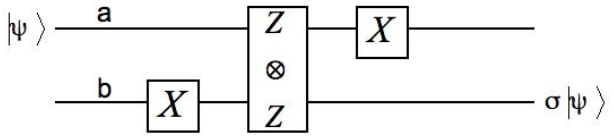


Fig. 3.13 – Le transfert d'état

Preuve :

1. mesure par rapport à $X^{(b)}$:

$\rightarrow$ mesure du qubit du registre d'entrée b dans la base projective $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$
$\rightarrow$ résultat de la mesure : $j \in \{1,-1\} \Rightarrow |\psi_1\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\sigma_z^{\frac{1-j}{2}}(\frac{|0\rangle+|1\rangle}{\sqrt{2}}))$
soit : $|\psi_1\rangle = \frac{1}{\sqrt{2}}(I \otimes \sigma_z^{\frac{1-j}{2}})(\alpha|00\rangle + \alpha|01\rangle + \beta|10\rangle + \beta|11\rangle)$

2. mesure par rapport à $Z^{(a)} \otimes Z^{(b)}$:

$\rightarrow$ mesure projective sur 2 qubits : soit $k \in \{-1,1\}$ le résultat
$\Rightarrow |\psi_2\rangle = (\sigma_z^{\frac{1-j}{2}} \otimes \sigma_x^{\frac{1-k}{2}})(\alpha|00\rangle + \beta|11\rangle)$

3. mesure par rapport à $X^{(a)}$ avec comme résultat : $m \in \{-1,1\}$

$\Rightarrow |\psi_3\rangle = (\sigma_z^{\frac{1-m}{2}} \otimes \sigma_z^{\frac{1-j.m}{2}} \sigma_x^{\frac{1-k}{2}})(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \alpha|0\rangle + \beta|1\rangle)$
$|\psi\rangle$ a bien été transféré du registre a au registre b, à $\sigma = \sigma_z^{\frac{1-j.m}{2}} \sigma_x^{\frac{1-k}{2}}$ près.

Contrairement à la téléportation, il n'y a pas de notion de *non localité* chez le transfert d'état. Après tout, pour du calcul à proprement dit, on n'a pas besoin d'une telle notion. Le transfert d'état par définition transfert l'état $|\psi\rangle$ d'un registre à un autre (au sens de la machine de Turing), à un opérateur de Pauli près. Autrement dit, il simule l'opérateur

I à un terme correctif près. De façon imagée, il conserve ce qu'il faut d'intrication pour le calcul. Cela peut paraître choquant à première vue car l'intrication est par nature non locale mais, du point de vue du calcul, ce qui est intéressant est de faire « interférer les registres entre eux » de façon parfaite (contrairement à ce qui se passe dans le monde classique) et ce, pas forcément à des années-lumière. Le gain encouru : on n'a besoin d'un seul qubit auxiliaire pour la simulation d'une transformation unitaire sur un qubit, au lieu des deux nécessaires pour le protocole de téléportation d'un qubit.

Décortiquons un peu plus cette merveille. Tout comme dans le théorème de Leung, au lieu de considérer une mesure complète dans la base de Bell, on ne se contente que de mesures sur 2 qubits dégénérées. La mesure de Bell, complète, est traduisible de la façon suivante : mesurer selon l'observable $Z \otimes Z$ (c'est-à-dire la mesure dégénérée : $\{|B_0\rangle + |B_3\rangle, |B_1\rangle + |B_3\rangle\}$), puis selon $X \otimes X$ ($\{P^{(1)}_{X\otimes X} + P^{(-1)}_{X\otimes X}, P^{(1)}_{X\otimes X} - P^{(-1)}_{X\otimes X} / P^{(\lambda)}_{X\otimes X} = \frac{I+\lambda X\otimes X}{2}\}$).

Ces deux observables nécessairement commutent, partageant ainsi des vecteurs propres communs et formant une base dans l'espace de Hilbert de dimension 4. Ceci lève par définition le caractère dégénéré de la mesure. Intuitivement, même dans un contexte de non localité, les mesures dégénérées suffisent pour du calcul car peu importe que 2 qubits aient le « choix » de se projeter sur 4 états de Bell (mesure de Bell) ou 2 : tout ce que l'on désire, c'est qu'ils soient intriqués.

En allant plus loin, cette dégénérescence est nécessaire au transfert d'état qui n'utilise qu'un seul qubit auxiliaire : on souhaite conserver l'état $|\psi\rangle$ malgré le fait que la mesure soit destructive. Le fait que la mesure soit dégénérée fait que ce dernier a « deux fois moins de chance d'être détruit », puis on ramène cette chance à zéro « au détriment » du qubit auxiliaire.

Remarque 1 : le transfert se fait entre registres voisins : la simplicité par excellence.

Remarque 2 : si on conservait le même registre (sur la figure 3.13, $|\psi\rangle$ et le qubit auxiliaire resteraient sur « la même ligne »), il n'y aurait transfert que d'opérateurs de Pauli.

Le transfert d'état généralisé :

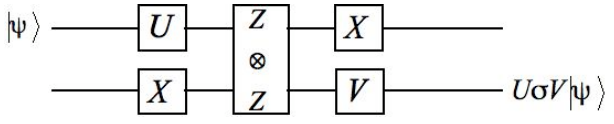


FIG. 3.14 – Le transfert d'état généralisé

Du fait qu'appliquer U puis mesurer selon l'observable O est équivalent à mesurer par rapport à l'observable $U^\dagger OU$ puis appliquer U [Per06], le transfert d'état généralisé peut se traduire uniquement en terme de bases de mesures :

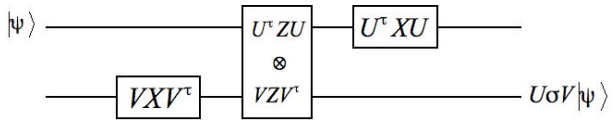


Fig. 3.15 – Le transfert d'état généralisé traduit en terme de mesures

Ainsi le transfert d'état généralisé simule-t-il UV à un opérateur de Pauli près. Et si on considère la famille approximativement universelle $\{H, HT, C_{not}\}$ qui simule de façon évidente, $\{H, T, C_{not}\}$, on a :

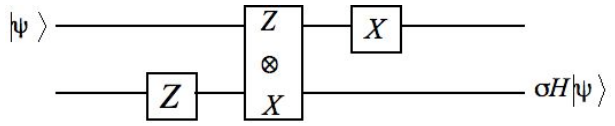


Fig. 3.16 – Le transfert d'état généralisé : simulation de H en posant $U = I$ et $V = H$

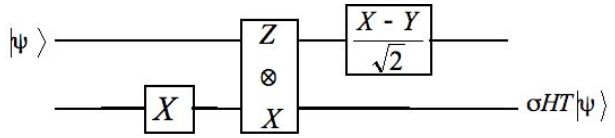


Fig. 3.17 – Le transfert d'état généralisé : simulation de H en posant $U = I$ et $V = HT$

En ce qui concerne la simulation de C_{not}, la démarche est un peu différente mais on peut vérifier que l'on a :

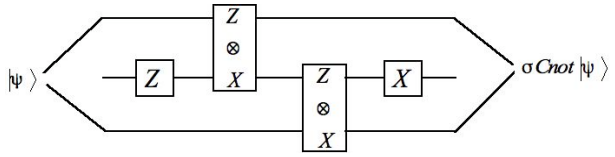


Fig. 3.18 – Le transfert d'état généralisé : simulation de C_{not}

Il en découle le théorème suivant : $\{Z \otimes X, Z, X, \frac{X-Y}{\sqrt{2}}\}$ est approximativement universelle en utilisant un seul qubit auxilaire.

L'optimum est atteint en terme de nombre d'observables par rapport à 2 qubits et nombre de qubits auxiliaires. Reste à savoir si on peut diminuer le nombre d'observables par rapport à 1 qubit.

En ce qui concerne l'universalité exacte vis-à-vis de la famille $\{U \in SU(2), C_{not}\}$, a été démontré le théorème suivant : $\{Z \otimes X, Z, \cos\theta X + \sin\theta Y, \theta \in [0, \pi]\}$ est universelle avec un seul qubit auxiliaire.

Remarque : il est évident que pour l'universalité exacte il faille une infinité d'observables

puisqu'il y a une infinité d'opérations unitaires. Il a été montré [CN00] qu'en y rajoutant C_{not}, cela suffisait pour l'universalité exacte : intuitivement, du moment que ça intrique, on peut modéliser toute transformation unitaire portant sur n qubits.

Conclusion

A priori les deux modèles semblent très différents. Il n'en est rien. Plusieurs approches ont été suivies afin de démontrer leur équivalence [CLN05, JP04] mais celles-ci demeurent, malgré leur pertinence, moins satisfaisantes [Joz05] que celle de F. Verstraete [VC04]. Ce dernier est le premier à avoir eu l'idée, s'inspirant de la physique du solide, d'introduire la notion **d'état à liaisons de valence** (*VBS* pour *valence bond state*) dans ce contexte si particulier qu'est le calcul quantique. Grâce à cette notion chaque mesure locale sur 1 qubit va pouvoir être interprétée comme une téléportation, un article très complet sur le sujet est [Cla06].

Ce chapitre termine un état de l'art concernant le calcul quantique qui s'est voulu, sinon complet, simple d'accès.

Deuxième partie

Approches algébriques et géométriques du calcul quantique

Chapitre 4

Approche algébrique

Introduction

On a vu dans la première partie de cet essai que le calcul en règle générale est avant tout un problème de langage et de modélisation. La seconde partie va explorer certains aspects du calcul quantique *via* la géométrie projective, les graphes et l'algèbre. L'utilisation de ces trois « langages » va permettre de mettre en évidence des liens entre quelques facettes du calcul quantique et les trois domaines des mathématiques mentionnés à l'instant. Beaucoup des travaux de mon directeur de thèse, Michel Planat, [SPR04], [PR05], [PSK06], [SP07b], [SPP08], [SPKP07], [SPK06], [SP07a], [PS08], [PBS07], [PB07], [Pla10b], [Pla09], [PS09], [PK10], [PJ08], [Pla10a], [Pla11], abondent dans ce sens et c'est à partir d'eux que j'ai effectué mes recherches. Les paradoxes apparents de la mécanique quantique induisent grand nombre de questions et Michel Planat a voulu lever le voile sur certains d'entre eux en interrogeant les mathématiques. Ce chapitre a pour vocation d'introduire les résultats du dernier chapitre mais uniquement du point de vue de l'algèbre. L'annexe A définit les quelques notions d'algèbre utilisées dans ce chapitre.

La surprenante efficacité mathématique pour la physique sera illustrée, sur le thème des observables de la physique quantique et du paradoxe d'Einstein, Podolsky et Rosen (appelé paradoxe EPR) de 1935 [EPR35]. Les travaux de Michel Planat établissent un lien fort entre, d'une part, la démonstration de Kochen et Specker [KS67] ayant donné lieu à un théorème de physique (revue et rendue simple d'accès par les travaux de Peres et Mermin en 1993 [Mer93]) sur l'impossibilité des variables cachées contextuelles, et d'autre part, la machinerie mathématique de la théorie de Galois [Art98], en particulier ses corps et ses anneaux (cf. sections A.2, A.3, A.3.2). La principale caractéristique des corps de Galois est qu'ils sont finis et de dimension puissance d'un nombre premier. Par extension, la notion d'anneaux de Galois a été introduite par le mathématicien W. Krull en 1924. Il s'agit [Alb06] des anneaux finis dont les diviseurs de 0 forment un idéal principal (cf. section A.2.2) de cardinal (cf. section A.1.3) p où p est un nombre premier. La structure d'un anneau de Galois est décrite par la caractéristique (cf. équation A.4) de l'anneau qui

est une puissance du nombre premier p, et son nombre d'éléments qui est une puissance de sa caractéristique. Comme pour les corps de Galois, on peut donner une construction polynomiale des anneaux de Galois (cf. section A.3.2 pour le cas des corps).

4.1 Le contexte

4.1.1 Historique et discussion

La mécanique quantique est *non déterministe*, dans le sens où elle ne peut pas prédire avec certitude le résultat d'une mesure. Elle ne peut prédire que les probabilités des résultats d'une mesure (postulat de la mécanique quantique concernant la mesure, cf. section 2.1). Cela conduit à une situation où la mesure d'une certaine propriété sur deux systèmes formellement identiques peut conduire à deux résultats différents. La question se pose inévitablement de savoir s'il peut exister un niveau de réalité plus profond, qui pourrait être formalisé par une théorie plus fondamentale que la mécanique quantique, et pourrait prédire avec certitude le résultat de la mesure.

Max Born publia en 1926 deux articles [AE88] proposant l'interprétation du carré du coefficient complexe d'un état comme étant la probabilité de mesurer cet état. Selon cette interprétation, il fallait accepter qu'un paramètre physique ne possède pas une valeur déterminée avant qu'il ne soit mesuré. Cela marqua le point de départ d'une opposition à cette interprétation, principalement menée par Albert Einstein, Erwin Schrödinger et Louis de Broglie. Ces physiciens étaient attachés à une vision dite *réaliste* de la physique, selon laquelle la physique se doit de décrire le comportement d'entités physiques réelles, et non se contenter de prédire des résultats. Dans ce cadre, accepter un indéterminisme fondamental est difficile, ce que Einstein a traduit par sa célèbre phrase : *« Dieu ne joue pas aux dés »* [AE88].

Environ dix ans plus tard, dans un des articles les plus cités du vingtième siècle [EPR35], Einstein, Podolsky et Rosen s'interrogent sur la complétude de la théorie quantique et répondent par la négative, ouvrant ainsi la voie aux théories dites *à variables cachées* : *« dans une théorie complète [EPR35], il y a un élément correspondant à chaque élément de réalité. Une condition suffisante pour la réalité d'une quantité physique est la possibilité de la prédire avec certitude, sans perturber le système. En mécanique quantique, pour deux quantités physiques décrites par des opérateurs qui ne commutent pas, la connaissance de l'une exclut la connaissance de l'autre. Alors soit la description de la réalité de la fonction d'onde en mécanique quantique n'est pas complète* (1)*, soit ces deux quantités n'ont pas de réalité simultanée* (2)*. Réaliser des prédictions pour un système, sur la base de mesures faites pour un autre système ayant interagi auparavant, conduit au résultat que si* (1) *est faux, alors* (2) *est faux. On doit donc en conclure que la description donnée par la fonction d'onde est incomplète ».*

La contribution la plus connue, qui sans pour autant clore la discussion a fait pencher

la balance en faveur de la mécanique quantique, est celle de John Bell avec ses fameux *no-go* théorèmes [Bel66], connus également sous le nom d'inégalités de Bell [CN00]. C'est en 1964 que John Bell établit ses célèbres inégalités, inégalités qui doivent être vérifiées si des variables cachées - au sens défini par Einstein - existent, et violées si elles n'existent pas. Les expériences visant à vérifier les inégalités de Bell purent être menées au début des années 1980 par Alain Aspect et *al* [AGR82], [ADR82], et aboutirent à une violation des inégalités, invalidant la possibilité d'existence de variables cachées au sens défini par Einstein (c'est-à-dire des variables dites *locales*, respectant le principe de causalité, principe qui stipule que si un phénomène (nommé cause) produit un autre phénomène (nommé effet), alors l'effet ne peut pas précéder la cause).

Une autre contribution, datant de 1967, longtemps laissée aux oubliettes car très complexe à appréhender, connue sous le nom du théorème de Kochen et Specker ([KS67], [Mer93]), que l'on notera (KS), a refait surface bien plus tard, en 1993, grâce à Peres et Mermin qui ont simplifié considérablement le problème [Mer93].

Le théorème (KS) démontre que toute théorie à variables cachées rendant compte des résultats des expériences de physique quantique est *contextualiste*, c'est-à-dire que les valeurs mesurées des paramètres physiques dépendent nécessairement du contexte expérimental, et non des entités physiques seules. Ce théorème porte un autre coup à la vision réaliste d'Einstein, qui supposait que chaque entité physique a une existence objective, indépendante de son environnement et de l'observation. Cela revient à dire qu'il est impossible d'attribuer aux observables décrivant un système individuel quantique une valeur définie, lorsque celles-ci ne commutent pas (cf. section 2.1, équation 2.5).

En bref, le théorème (KS) démontre que les mesures ne révèlent pas des valeurs préexistantes. Toute théorie déterministe qui prétend assigner un résultat défini à chaque mesure quantique, et conforme aux résultats statistiques de la théorie quantique, doit nécessairement être contextuelle : elle dépend de l'endroit où se trouve l'observateur, du type d'appareil de mesure.

Toutefois, ce théorème ne met pas tout à fait un terme aux espoirs d'une certaine forme de réalisme (toutefois assez éloigné du réalisme classique selon Einstein) car il est toujours possible d'imaginer que l'entité « réelle » - possédant toutes les caractéristiques déterminant le résultat de la mesure - ne soit plus constituée des particules seules, mais des particules ET leur contexte, globalement (ce qui est envisageable dans le cadre de variables cachées non locales). Cette forme de réalisme est parfois nommée *ontologie contextuelle* [Str08].

En 2003, Anthony Leggett établit des inégalités [Leg03], semblables à celles de Bell, qui doivent être vérifiées par toute théorie à variables cachées non locales vérifiant certains

pré-requis raisonnables. La violation de ces inégalités rendraient donc un ensemble important de théories à variables cachées, mais cette fois-ci non locales, incompatibles avec l'expérience.

En 2007, Anton Zeilinger réussit à tester ces inégalités [GPK$^+$07], qui s'avèrent violées. Ainsi semble-t-il difficile de maintenir des théories à variables cachées, locales ou non, car les hypothèses retenues par Legget pour bâtir le modèle aboutissant à ses inégalités sont raisonnables [Leg03]. Toutefois, selon Alain Aspect [Asp07], la violation avérée des inégalités de Legett ne remet pas en cause le modèle à variables cachées non locales de Bohm.

En ce qui concerne cette dernière théorie, elle est remise en cause [Sua07] non par les inégalités de Leggett, mais notamment par un type d'expériences, nommée *before-before experiment*, effectuées en 2002 [SZGS02], qui mettent en jeu un dispositif du genre expérience d'Aspect, mais avec des polariseurs en mouvement.

Ces résultats - encore récents - doivent être pris avec prudence, mais peu de physiciens doutent de la validité de ces résultats expérimentaux. Dans l'état actuel des choses, même l'ontologie contextuelle devient difficile à défendre en l'absence de variables cachées non-locales, et il semble (en tout cas telle est la conclusion de Zeilinger et de son équipe) qu'il faille abandonner toute forme de réalisme, dans le sens où le résultat d'une mesure quantique ne dépend pas (entièrement) des propriétés objectives du système quantique mesuré.

Ce débat quelque peu ésotérique, mais primordial si on veut tenter de comprendre une théorie (et non pas seulement appliquer ses postulats comme les règles d'un jeu), à propos de la définition de la réalité physique, s'est mué en une argumentation mathématique non triviale qui illustre la nature parfois ambiguë des rapports entre mathématiques et physique. De plus, du point de vue de l'informatique quantique, c'est l'un des apanages du scientifique qui s'intéresse à cette discipline que d'explorer différents formalismes, différents modèles, pour arriver à de nouvelles constructions algorithmiques. L'algèbre, avec ces structures, en l'occurrence plus particulièrement ses groupes, corps et anneaux de Galois, est une vision qui peut se révéler intéressante.

Par ailleurs, même si les théorèmes de Bell et le théorème (KS) sont de très bons arguments, le débat est-il pour autant clos ? C'est là ce que Michel Planat a voulu explorer, comme on va le voir dans la suite des événements. Il montre entre autre que ces notions de non déterminisme et de non prédiction en physique quantique ont une structure de corps et d'anneaux de Galois sous-jacente, [LN97], [Con], pour finalement évoluer vers une formulation mathématique de la complémentarité quantique. Deux observables sont dites **complémentaires** (cf. section 4.3) si une connaissance précise de l'une implique que les valeurs possibles, issues de mesures sur l'autre observable, ont la même probabilité d'être obtenues (sont également incertaines).

4.1.2 Le théorème de Kochen et Specker et les travaux de Peres et Mermin

Le théorème de Kochen et Specker :

Avant d'énoncer le théorème (KS), il ne semble pas inutile d'expliciter les deux hypothèses liées à l'idée, au premier abord anodine, de *réalisme scientifique*, idée chère aux partisans d'une théorie quantique à variables cachées (cf. la référence [oP00] qui constitue une très bonne introduction aux tenants et aux aboutissants du théorème (KS)) :

1. **(VD)** Toutes les observables décrivant un système quantique ont une valeur définie à chaque instant [oP00].

Cette hypothèse dite de la *valeur définie* est motivée par le principe qui semblait acquis jusqu'à maintenant que ce qui existe dans la nature est indépendant des mesures que l'on pourrait effectuer dessus, mesures qui ne servent qu'à nous donner des informations. Puisque la mesure d'observables en mécanique quantique donne des valeurs plus ou moins précises, il y a de bonnes raisons de penser que de telles valeurs existent indépendamment des mesures, ce qui amène à supposer l'énoncé (VD) vrai. (Il est à noter que l'on a pas besoin de supposer ici que les valeurs soient révélées de manière exacte par une mesure quelconque, mais seulement qu'elles existent !) On peut compléter l'hypothèse d'un réalisme scientifique par cette deuxième hypothèse, plus concrète, hypothèse dite de *non contextualité* :

2. **(NC)** Si un système quantique possède une propriété (la valeur d'une observable), celle-ci doit être indépendante d'un quelconque contexte de mesure, c'est-à-dire indépendante du *comment* cette valeur a été mesurée [oP00].

Cela signifie que si un système possède une propriété donnée, c'est de manière indépendante à l'éventualité d'avoir obtenu d'autres valeurs par d'autres moyens. Les hypothèses (VD) et (NC) expriment l'idée de l'indépendance de la réalité physique par rapport à d'éventuelles mesures.

Le théorème (KS) établit une contradiction entre (VD)+(NC) et la mécanique quantique. Donc accepter la mécanique quantique comme théorie complète, c'est renoncer à (VD) ou (NC).

Plus concrètement, supposons, par exemple, que A, B et C soient des opérateurs hermitiens (cf. chapitre 2, section 2.1), dont les commutateurs satisfont $[A, B] = [A, C] = 0$ et $[B, C] \neq 0$. L'hypothèse de non contextualité dit que la valeur, prédite dans une mesure de l'observable $\mathcal{A}$, ne dépend pas du fait que les observables $\mathcal{B}$ et $\mathcal{C}$ aient été mesurées simultanément. Le théorème (KS) montre qu'un modèle de physique quantique à variables cachées, qui est non contextuel dans ce sens, est impossible à obtenir pour un espace de Hilbert de dimension $x \geq 3$. Dans l'hypothèse où B et C commutent, cela n'a donc pas de sens de se poser la question de la contextualité.

La théorie quantique requiert que le résultat de la mesure d'une observable $\mathcal{A}$ est l'une des valeurs propres $v(A)$ de l'opérateur. Supposons qu'il existe une relation fonctionnelle $f(\mathcal{A}, \mathcal{B}, \mathcal{C}, \dots) = 0$ entre les observables, dont toutes ne commutent pas entre elles. Alors, on s'attend à ce qu'une relation algébrique similaire soit satisfaite par les valeurs propres, soit $f(v(A), v(B), v(C), \dots) = 0$. Cependant, il est possible de construire des contre-exemples à cette stratégie, ce qui nie l'existence de variables cachées non contextuelles.

Énoncé du théorème (KS) **[oP00] :**

Soit $\mathcal{H}$ un espace de Hilbert de dimension $x \geq 3$, il existe un ensemble $\mathcal{M}$ d'observables, contenant y éléments, tels que les deux hypothèses suivantes sont contradictoires :

1. (KS_1) Tous les éléments y de $\mathcal{M}$ ont simultanément des valeurs, c'est-à-dire qu'on peut les identifier sans ambiguïté à des nombres réels, notés $v(\mathcal{A})$, $v(\mathcal{B})$, $v(\mathcal{C})$,... pour les observables $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$,...
2. (KS_2) Les valeurs des observables vérifient :
   - (a) Si $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$,... commutent deux à deux et si $\mathcal{C} = \mathcal{A} + \mathcal{B}$,... alors $v(\mathcal{C}) = v(\mathcal{A}) + v(\mathcal{B})$,...
   - (b) Si $\mathcal{A}, \mathcal{B}, \mathcal{C}$,... commutent deux à deux et si $\mathcal{C} = \mathcal{A}.\mathcal{B}$,... alors $v(\mathcal{C}) = v(\mathcal{A}).v(\mathcal{B})$,...

L'hypothèse (KS_1) correspond à (VD). Il est plus difficile de relier (KS_2) à (NC). Les énoncés (a) et (b) sont connus dans la littérature comme respectivement la règle de somme (*Sum Rule*) et la règle de produit (*Product Rule*). Ils sont conséquence d'un principe appelé principe de composition fonctionnelle qui est lui même une conséquence de (NC) [oP00].

Si on considère les contraposées (au sens logique, c'est-à-dire si la proposition A implique la proposition B, la négation de B implique la négation de A) de (KS_1) et de (KS_2), cela revient à dire qu'il est impossible d'attribuer aux observables décrivant un système individuel quantique une valeur définie ou qu'il est impossible qu'elles ne dépendent pas d'un contexte d'expérimentation, lorsque celles-ci ne commutent pas.

La première preuve de ce théorème (KS) date de 1967 [KS67] et a été formulée pour un espace de dimension $x = 3$, représentant les états de spin d'une particule de spin 1, à partir de $y = 117$ observables, associées au carré des composantes du moment angulaire, le long des 117 directions. Il est un fait que les carrés des composantes, le long des directions orthogonales, sont des opérateurs qui commutent et possèdent des valeurs propres 0 ou 1, satisfaisant à la règle quantique $v(\mathcal{A})+v(\mathcal{B})+v(\mathcal{C}) = 2$, quelque soit le triplet d'observables $(\mathcal{A}, \mathcal{B}, \mathcal{C})$. Or on montre, par un argument géométrique assez compliqué [Mer93], que cette condition est impossible à satisfaire pour le système ci-dessus.

Plusieurs démonstrations ont par la suite simplifié le problème en impliquant moins d'observables : Mermin en 1990 [Mer90b],[Mer90a], Peres en 1991 [Per91], Kernaghan en 1994 [Ker94], [KP95], Cabello et *al* en 1997 [Cab97], [CEA97] pour ne citer qu'eux, avec,

pour apothéose en terme de simplicité, les travaux de Peres et Mermin de 1993 [Mer93] que l'on va maintenant évoquer.

Les travaux de Peres et Mermin

Peres et Mermin ont exhibé de leur étude de (KS) [Mer93] un système de neuf observables, représentant l'interaction de deux particules de spin 1/2, c'est-à-dire interagissant dans un espace de Hilbert de dimension $q = 4$.

Les opérateurs du système de Peres et Mermin sont représentés dans le tableau 4.1 :

$I_2 \otimes \sigma_z$	$\sigma_z \otimes I_2$	$\sigma_z \otimes \sigma_z$
$\sigma_x \otimes I_2$	$I_2 \otimes \sigma_x$	$\sigma_x \otimes \sigma_x$
$\sigma_x \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$

TAB. 4.1 – Le carré magique de Peres et Mermin pour la preuve (KS)

Les matrices intervenant sont les matrices de Pauli, dites également opérateurs de Pauli (cf. chapitre 2, section 2.2.2). Le symbole « $\otimes$ » représente ici le produit tensoriel (dernier postulat de la mécanique quantique, chapitre 2, section 2.1).

On observe que chacune des lignes ou des colonnes du tableau 4.1 est constituée d'un triplet d'opérateurs qui commutent entre eux. D'autre part, chacun des opérateurs possèdent des valeurs propres $+1$ ou -1. En multipliant entre elles toutes les lignes et toutes les colonnes, puisque chacun des opérateurs intervient 2 fois, le produit des valeurs propres est 1. Au niveau des opérateurs, le produit des opérateurs dans un triplet est toujours $I_2 \otimes I_2 = I_4$, sauf pour la dernière colonne où le produit est $-I_4$. Il y a donc contradiction entre la règle algébrique pour les opérateurs et celle pour les valeurs propres correspondantes, ce qui démontre le théorème (KS) pour ce système. Cette contradiction vient du fait que les opérateurs sur des lignes ou colonnes distinctes ne commutent pas nécessairement. (cf. la table de multiplication des 16 opérateurs intervenant dans l'interaction de deux spins 1/2, explicitée dans la section 4.3.1 du présent chapitre).

Concrètement, on verra dans la section 4.3 que les travaux de Peres et Mermin [Mer93] ont permis d'évoluer vers une formulation mathématique de la complémentarité quantique très simplifiée et entre autre, par ce biais, de re-démontrer le théorème (KS) ; certes, pour des cas particuliers, mais de façon très simple et, de toute façon, un seul contre-exemple montrant qu'une théorie quantique à variables cachées est fausse suffit dans l'absolu.

4.2 Un ingrédient mathématique

4.2.1 Le corps fini à 4 éléments ou plus : $\mathbb{F}_4$

De manière générale, le corps de Galois (cf. annexe A, section A.3.2) $\mathbb{F}_q$, à q éléments, où $q = p^n$ avec p premier et $n \in \mathbb{N}\backslash\{0\}$, est représenté par des classes de polynômes $\mathbb{F}_p[x]$, à

coefficients dans un corps de base $\mathbb{F}_p$, le corps des entiers modulo p, obtenues en effectuant les calculs modulo un polynôme irréductible sur le corps de base (cf. section A.3.2).

Par exemple, pour $p = 2$, le polynôme $1 + x + x^2$ est irréductible dans $\mathbb{F}_2[X]$ (c'est d'ailleurs l'unique polynôme irréductible de degré 2). Le corps de base est $\mathbb{F}_2 = \mathbb{Z}_2$, le corps à 2 éléments 0 et 1. L'extension correspondante est un corps noté $\mathbb{F}_4$ (cf. section A.3.3). Ce corps a exactement 4 éléments qui sont 0, 1, et les deux racines, x et $x + 1$, du polynôme $1 + x + x^2$. Ses lois sont données dans les tableaux, 4.2 pour la loi additive, 4.3 pour la loi multiplicative (cf. section A.3.2).

Le groupe additif de $\mathbb{F}_4$:

La table du groupe est la suivante :

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

Tab. 4.2 – Addition dans $\mathbb{F}_4$

Le groupe multiplcatif de $\mathbb{F}_4$

La table du groupe est la suivante :

.	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

Tab. 4.3 – Multiplication dans $\mathbb{F}_4$

4.2.2 Un hiéroglyphe découvert : la table de Pauli

$*$	I_2	σ_x	σ_y	σ_z
I_2	I_2	σ_x	σ_y	σ_z
σ_x	σ_x	I_2	$i\sigma_z$	$-i\sigma_y$
σ_y	σ_y	$-i\sigma_z$	I_2	$i\sigma_x$
σ_z	σ_z	$i\sigma_y$	$-i\sigma_x$	I_2

Tab. 4.4 – Multiplication des matrices de Pauli

Avec

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ et } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{4.1}$$

Il s'agit des matrices de Pauli. L'opération $*$ est la multiplication des matrices.

Si on identifie : 0 et I_2 à « A », 1 et σ_x à « B », x et σ_y à « C », $x+1$ et σ_z à « D », les tableaux 4.2 et 4.4 deviennent :

$+$	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

TAB 4.a - Table d'addition du groupe $\mathbb{F}_4$ avec la nouvelle notation

$*$	A	B	C	D
A	A	B	C	D
B	B	A	iD	$-iC$
C	C	$-iD$	A	iB
D	D	iC	$-iB$	A

TAB 4.b - Multiplication des matrices de Pauli avec la nouvelle notation

On note que les tableaux 4.a et 4.b ont une structure similaire, au symbole multiplicatif près, i ou $-i$ (ce qui n'est pas dérangeant du point de vue de la physique puisqu'il s'agit d'une phase globale donc non mesurable ; dans le chapitre 2, à la section 2.2.1, a été évoquée l'information cachée dans la description d'un qubit).

On a déjà vu que les matrices de Pauli sont les attributs naturels des habitants de l'espace de Hilbert H_2, les qubits (cf. chapitre 2, section 2.2.1), et qu'elles permettent de faire les opérations les plus élémentaires de calcul quantique (cf. chapitre 2, section 2.2.2).

A la vue des tableaux 4.a et 4.b, il semble y avoir un lien entre le groupe additif $\mathbb{F}_4$ (cf. tableau 4.2) et la loi de multiplication des matrices de Pauli (cf. tableau 4.4).

4.3 Formulation mathématique de la complémentarité quantique

4.3.1 Un outil : la table de multiplication des 16 opérateurs intervenant dans l'interaction de deux spins 1/2

On utilise pour le tableau 4.5 ci-après la notation suivante :

$$\begin{aligned} &0 = I_4, 1 = I_2 \otimes \sigma_z, 2 = \sigma_z \otimes I_2, 3 = \sigma_z \otimes \sigma_z, \\ &4 = \sigma_x \otimes I_2, 5 = I_2 \otimes \sigma_y, 6 = \sigma_x \otimes \sigma_y, 7 = \sigma_x \otimes \sigma_z, \\ &8 = \sigma_z \otimes \sigma_x, 9 = \sigma_y \otimes \sigma_y, 10 = I_2 \otimes \sigma_x, 11 = \sigma_y \otimes I_2, \\ &12 = \sigma_y \otimes \sigma_x, 13 = \sigma_y \otimes \sigma_z, 14 = \sigma_x \otimes \sigma_x, 15 = \sigma_z \otimes \sigma_y \end{aligned}$$

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	7	-i10	-i14	4	i15	-i12	i5	i3	i9	11	i6	-i8
2	2	3	0	1	i11	15	i9	i13	10	-i6	8	-i4	-i14	-i7	i12	5
3	3	2	1	0	i13	-i8	12	i11	i5	-14	i15	-i7	6	-i4	-9	-i10
4	4	7	-i11	-i13	0	6	5	1	-i12	i15	14	i2	i8	i3	10	-i9
5	5	i10	15	i8	6	0	4	i14	-i3	11	-i1	9	-i13	i12	-i7	2
6	6	i14	-i9	1é	5	4	0	i10	-13	i2	-i7	i15	3	-8	-i1	-i11
7	7	4	-i13	-i11	1	-i14	-i10	0	9	8	i6	i3	-15	i2	i5	-12
8	8	-i15	10	-i5	i12	i3	-13	9	0	7	2	-i14	-i4	-6	-i11	i1
9	9	i12	i6	-14	-i15	11	-i2	8	7	0	-i13	5	-i1	i10	-3	i4
10	10	-i5	8	-i15	14	i1	i7	-i6	2	i13	0	12	11	-i9	4	i3
11	11	13	i4	i7	-i2	9	-i15	-i3	i14	5	12	0	10	1	-i8	i6
12	12	-i9	i14	6	-i8	i13	3	-15	i4	i1	11	10	0	-i5	i2	-7
13	13	11	i7	i4	-i3	-i12	-8	-i2	-6	-i10	i9	1	i5	0	15	14
14	14	-i6	-i12	-9	10	i7	i1	i5	i11	-3	4	i8	-i2	15	0	13
15	15	i8	5	i10	i9	2	i11	-12	-i1	-i4	-i3	-i6	-7	14	13	0

Tab. 4.5 – Table de multiplication des 16 opérateurs généralisés de Pauli intervenant dans l'interaction de deux particules de spin 1/2.

Le tableau 4.5 permet de lire directement si les opérateurs concernés commutent ou pas. En l'occurrence, il s'agit des opérateurs de Pauli généralisés sur 2 qubits. Ils sont dits **généralisés** en ce sens qu'ils ne s'appliquent plus seulement sur 1 qubit. Ce tableau va être utile pour la suite et permettra également de construire la matrice d'adjacence du graphe de Pauli pour les 2 qubits défini dans le chapitre 5.

4.3.2 Structure cachée dans le carré de Peres et Mermin

On définit une notation condensée telle que les 3 éléments d'une ligne ou d'une colonne du tableau 4.1 s'écrivent $X_1(i)$, $X_2(i)$ et $X_3(i)$ pour $i \in \{1,2,3,4,5,6\}$. Par exemple, on aura pour la ligne 1 :

$$X_1(1) = I_2 \otimes \sigma_z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, X_2(1) = \sigma_z \otimes I_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$X_3(1) = \sigma_z \otimes \sigma_z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

et $i = 2$ fera référence à la deuxième ligne, $i = 3$ à la troisième, $i = 4$ à la première colonne, $i = 5$ à la deuxième et enfin $i = 6$ à la troisième.

Considérons l'ensemble $Y(j) = \{I_4, X_1(j), X_2(j), X_3(j)\}_{j=1..5}$, constitué de la matrice unité et d'un triplet d'opérateurs du tableau 4.1 correspondant aux lignes 1 à 3 ou aux colonnes 1 et 2. Pour chacun des $Y(j)$, on observe les relations algébriques suivantes :

$*$	I_4	X_1	X_2	X_3
I_4	I_4	X_1	X_2	X_3
X_1	X_1	I_4	X_3	X_2
X_2	X_2	X_3	I_4	X_1
X_3	X_3	X_2	X_1	I_4

TAB. 4.6 – Structure de groupe caché du carré magique de Peres et Mermin

Par exemple, pour la ligne 1 du tableau 4.1, on vérifie aisément que :

$$X_1(1)X_2(1) = X_3(1), X_1(1)X_3(1) = X_2(1), X_2(1)X_3(1) = X_1(1), \text{ etc.} \tag{4.2}$$

On montre par des calculs plutôt simples (cf. equation 4.2) que le tableau 4.6 est vérifié également pour $j = 2, 3, 4$ et 5, mais qu'en revanche ce n'est pas le cas pour la colonne 3 du tableau 4.1.

En utilisant la notation condensée X_1, X_2 et X_3 et en identifiant respectivement I_4 et 0 à A, X_1 et 1 à B, X_2 et x à C et enfin X_3 et $x+1$ à D, les tableaux 4.2 et 4.6 deviennent le tableau 4.7 :

opération	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

TAB. 4.7 – Les tableaux 4.2 et 4.6 dans la nouvelle notation

Le tableau 4.6 est ainsi similaire au tableau 4.2. On peut dire que la multiplication des opérateurs de l'espace de Hilbert de dimension 4, présents dans les lignes 1 à 3 et colonnes 1 et 2 du carré de Peres et Mermin (opérateurs du tableau 4.1 auxquels on adjoint l'unité I_4), est isomorphe (cf. section A.4) à l'addition du corps fini à 4 éléments $\mathbb{F}_4$.

On peut donc en conclure que la démonstration du théorème (KS) par le carré magique de Peres et Mermin est intimement liée aux propriétés du groupe additif dans le corps $\mathbb{F}_4$.

Reste que la règle de multiplication des lignes 1 à 3, et colonnes 1 et 2 du carré de Peres et Mermin (cf. tableau 4.6), est aussi très similaire à la règle de multiplication des matrices de Pauli (cf. tableau 4.4), pour peu que l'on ignore le symbole multiplicatif i ou $-i$.

4.3.3 Bases mutuellement non biaisées (*MUBs* pour *Mutually Unbiased Bases*)

Définition

Deux bases de l'espace de Hilbert considéré/deux observables (on étudie leurs vecteurs propres et, pour rappel, leurs valeurs propres sont réelles, caractéristique qui leur confère leur caractère mesurable) sont dites **mutuellement non biaisées** (ou maximalement incompatibles, ou maximalement décorrélés, ou encore complémentaires) si une mesure précise effectuée *via* l'une/sur l'une, laisse attendre des résultats tout à fait aléatoires (parmi les résultats équiprobables prévus par le postulat de la mesure) pour une autre mesure qui serait effectuée ultérieurement *via* l'autre/sur l'autre (et réciproquement).

De façon plus formelle, deux bases orthonormales $\mathcal{A}$ et $\mathcal{B}$ d'un espace de Hilbert de dimension d, noté H_d, sont dites **mutuellement non biaisées** si et seulement si [CN00] :

$$\forall a \in \mathcal{A}, b \in \mathcal{B}, |< a \mid b >| = \frac{1}{\sqrt{d}} \tag{4.3}$$

Exemple

Pour 1 qubit, deux *MUBs* sont celles respectivement définies par les vecteurs propres de σ_x et σ_z ; autrement dit, les deux bases de l'espace de Hilbert de dimension 2, H_2, suivantes : $\{|0\rangle, |1\rangle\}$ et $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ sont des *MUBs*. C'est pourquoi, dans le chapitre 1, à la section 2.2, a été dit que la base $\{|0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}\}$ poserait « un problème une fois sur 2 ». Il s'agit juste d'une reformulation des choses.

Remarque : cette propriété est très importante et purement quantique ; elle intervient plus ou moins de façon implicite, autant dans les protocoles quantiques (téléportation et cryptographie quantiques par exemple), qu'en calcul quantique.

Application

Faisons maintenant apparaître un nouveau carré d'opérateurs qui se distingue de celui du tableau 4.1 par les éléments en colonne 2 et 3 de la deuxième ligne.

$I_2 \otimes \sigma_z$	$\sigma_z \otimes I_2$	$\sigma_z \otimes \sigma_z$
$\sigma_x \otimes I_2$	$I_2 \otimes \sigma_y$	$\sigma_x \otimes \sigma_y$
$\sigma_x \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$

Tab. 4.8 – 3 bases mutuellement non biaisées

Ses nouvelles propriétés sont les suivantes :

1. Contrairement au tableau 4.1 les opérateurs d'une même colonne ne commutent pas tous, les deux contre-exemples étant :

$$[(I_2 \otimes \sigma_y), (\sigma_z \otimes \sigma_x)] \neq 0 \text{ et } [(\sigma_x \otimes \sigma_y), (\sigma_y \otimes \sigma_y)] \neq 0$$

2. Les opérateurs sur chacune des lignes possèdent les mêmes valeurs propres (cette propriété est partagée par le tableau 4.1).
3. Le produit des opérateurs d'un ligne ou d'une colonne vaut I_4 : on ne retrouve pas la contradiction (KS) (explicitée pour un espace de Hilbert de dimension 4 dans le tableau 4.1).
4. Entre deux lignes distinctes, les observables sont mutuellement non biaisés. On dira encore que les observables d'une ligne sont complémentaires des observables d'une autre ligne (ce n'était pas le cas pour le tableau 4.1 à cause de sa deuxième ligne).

Cette propriété de complémentarité vaut en fait pour un ensemble complet de 5 lignes, représenté dans le tableau 4.9, ci-dessous [LBZ02].

$I_2 \otimes \sigma_z$	$\sigma_z \otimes I_2$	$\sigma_z \otimes \sigma_z$
$\sigma_x \otimes I_2$	$I_2 \otimes \sigma_y$	$\sigma_x \otimes \sigma_y$
$\sigma_x \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$
$I_2 \otimes \sigma_x$	$\sigma_y \otimes I_2$	$\sigma_y \otimes \sigma_x$
$\sigma_y \otimes \sigma_z$	$\sigma_x \otimes \sigma_x$	$\sigma_z \otimes \sigma_y$

TAB. 4.9 – Ensemble complet de 5 bases mutuellement non biaisées

5. Considérons l'ensemble $\{I_4, X_1(j), X_2(j), X_3(j)\}_{j=1..5}$, constitué de la matrice unité et d'une triade d'opérateurs du tableau 4.9, correspondant aux lignes 1 à 5. On retrouve les relations algébriques du tableau 4.6. La multiplication des opérateurs de l'espace de Hilbert de dimension 4, présents au sein des lignes 1 à 5 (auxquels on adjoint l'unité I_4), est isomorphe à l'addition du corps fini à 4 éléments $\mathbb{F}_4$.

4.4 Corps de Galois cachés

4.4.1 Le groupe multiplicatif de $\mathbb{F}_4^*$

.	1	x	x+1
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

TAB. 4.10 – Multiplication dans $\mathbb{F}_4^*$

Le corps privé de l'élément zéro $\mathbb{F}_4^* = \mathbb{F}_4 \backslash \{0\}$ est un groupe multiplicatif d'ordre 3 (cf. section A.1.3), généré par l'élément x (puisqu'à partir de $x \in \mathbb{F}_4^*$, on a $x^2 = x + 1$, $x^3 = 1$, $x^4 = x$, $x^5 = x + 1$, etc.).

4.4.2 Les 2 qubits

Le groupe $\mathbb{F}_4^*$ introduit un ordre naturel des éléments du corps, qui peut être utilisé [KSSdG05] pour indicer les éléments d'une base de l'espace quadridimensionnel de Hilbert $H_4 : \{|0\rangle, |x\rangle, |x^2\rangle, |x^3\rangle\}$ où

$$|0\rangle = (1,0,0,0), |x\rangle = (0,1,0,0), |x^2\rangle = (0,0,1,0) \text{ et } |x^3\rangle = (0,0,0,1) \tag{4.4}$$

4.4.3 La fonction trace et les caractères additifs sur $\mathbb{F}_4$

La fonction trace :

La trace est un outil utilisé dans de nombreuses branches des mathématiques. Dans le cadre des représentations d'un groupe fini, elle est à la base de la définition du caractère, elle permet de mieux comprendre la structure d'un groupe.

On définit la trace d'un élément g de $\mathbb{F}_4$ par :

$$g \in \mathbb{F}_4 \longmapsto tr(g) = g + g^2 \in \mathbb{F}_2$$

La fonction trace est une application de $\mathbb{F}_4$ vers le corps $\mathbb{F}_2$, composé des bits 0 et 1.

Les caractères additifs :

Un caractère est un morphisme d'un groupe (cf. section A.4 de l'annexe A pour la définition d'un morphisme) dans le groupe multiplicatif constitué des éléments non nuls des nombres complexes $(\mathbb{C}\backslash\{0\},\cdot)$. Cette notion de caractère permet de représenter de façon la plus simple possible les groupes finis et ainsi de plus facilement les manipuler, les partitionner, les comparer, les classifier, etc.

On définit les caractères additifs de $\mathbb{F}_4$ (c'est-à-dire du groupe additif de $\mathbb{F}_4$) par :

$$g \in \mathbb{F}_4 \longmapsto \kappa(g) = e^{i\pi tr(g)}$$

qui satisfont, entre autre, aux relations suivantes :

$$\forall g_1, g_2 \in \mathbb{F}_4, \kappa(g_1)\kappa(g_2) = \kappa(g_1 + g_2) \text{ et } \sum_{g \in \mathbb{F}_4} \kappa(g) = 0$$

Leur action sur les éléments de $\mathbb{F}_4^*$ est $\kappa(0) = 1, \kappa(x) = -1, \kappa(x^2) = -1$ et $\kappa(x^3) = 1$.

4.4.4 Les opérateurs généralisés de Pauli

Le tableau 4.9 utilise une règle de construction [KSSdG05] dont les briques de base sont les opérateurs de décalage X_r et les opérateurs de phase Z_m. Ceci est une généralisation des opérateurs de Pauli, d'erreur de bit σ_x, et d'erreur de phase σ_z. Les actions respectives des opérateurs X_r et Z_m sur les kets $|x^k\rangle$ sont :

$$X_r\,|x^k\rangle = |x^k + x^r\rangle \text{ et } Z_m\,|x^k\rangle = \kappa(x^{m+k})\,|x^k\rangle \text{ pour : } k = 0...3 \text{ et } m, r = 0...2$$

Ces opérateurs forment des ensembles :

$$\{Z_m\}_{m=0...2}, \{X_m\}_{m=0...2} \text{ et } \{X_m Z_{m+r}\}_{m,r=0...2} \text{ avec } r \text{ fixé}$$

qui ont la propriété d'être disjoints et pour lesquels chaque élément d'un ensemble (pour r choisi) commute avec tous les autres éléments.

Numérotons de 1 à 15 les éléments du tableau 4.9, numérotation qui correspond à celle des opérateurs du tableau 4.5. Avec les mêmes notations, les bases prévues par la représentation dite de Galois [KSSdG05] s'écrivent :

3	1	2
14	10	4
9	5	11
6	8	13
12	15	7

TAB. 4.11 – Construction de Galois d'un ensemble complet de 5 *MUBs*

On parle de représentation de Galois [KSSdG05] car par construction le tableau 4.11 s'écrit également comme suit (cf. tableau 4.12) :

- la première ligne ne concerne que les opérateurs en « Z »,
- la deuxième ligne ne concerne que les opérateurs en « X »,
- les troisième, quatrième et cinquième lignes correspondent respectivement à $r = 0$, $r = 1$ et $r = 2$,
- les première, deuxième et troisième colonnes correspondent respectivement à $m = 0$, $m = 1$ et $m = 2$.

Z_0	Z_1	Z_2
X_0	X_1	X_2
X_0Z_0	X_1Z_1	X_2Z_2
X_0Z_1	X_1Z_2	X_2Z_3
X_0Z_2	X_1Z_3	X_2Z_4

TAB. 4.12 – Construction de Galois explicitée de l'ensemble complet de 5 *MUBs* du tableau 4.11

Le tableau 4.11 est tout à fait équivalent au tableau 4.9 (à des permutations près) et possède par construction les mêmes propriétés.

Avec les mêmes notations que celles utilisées pour le tableau 4.11, le carré de Peres et Mermin s'écrit :

1	2	3
4	10	14
7	8	9

Tab. 4.13 – Le carré magique de Peres et Mermin du tableau 4.1 dans les mêmes notations que le tableau 4.11

Sous cette forme, d'après le tableau 4.11 (mais cela était aussi visible d'après le tableau 4.9), il apparaît facilement que les opérateurs sur deux lignes distinctes du carré de Peres et Mermin sont aussi mutuellement non biaisés. Mais des opérateurs ont été permutés au sein d'une même ligne.

On peut aisément observer depuis le tableau 4.13 que :

$$3 = 1 * 2, 14 = 4 * 10, 9 = 7 * 8, 7 = 1 * 4 \text{ et } 8 = 2 * 10,$$

mais qu'en revanche :

$$3 * 14 = -9.$$

Explicitons la contradiction :

$$7 * 8 = (1 * 4) * (2 * 10) = 1 * (4 * 2) * 10,$$

tandis que :

$$3 * 14 = 1 * (2 * 4) * 10.$$

Or,

$$2 * 4 = -i11,$$

tandis que :

$$4 * 2 = i11.$$

La contradiction révélée par le carré de Peres et Mermin provient de la non commutativité des opérateurs 2 et 4.

Il est aisé, par cette méthode, d'exhiber d'autres carrés « à la Peres et Mermin » possédant la même propriété d'obstruction, comme le montre le tableau 4.14 à titre d'exemple.

1	2	3
4	5	6
7	15	12

TAB. 4.14 – Un autre carré magique de Peres et Mermin dans les mêmes notations que 4.11

Revenons au tableau 4.13. Dans la représentation de Galois, on a $2 * 4 = Z_2 * X_2$. L'action de ces opérateurs est :

$$X_2 \left|x^k\right\rangle = \left|x^k + x^2\right\rangle \text{ et } Z_2 \left|x^k\right\rangle = \kappa(x^{k+2}) \left|x^k\right\rangle, \tag{4.5}$$

l'action du commutateur est :

$$(X_2 Z_2 - Z_2 X_2) \left|x^k\right\rangle = (\kappa(x^{k+2}) - 1) \left|x^k + x^2\right\rangle. \tag{4.6}$$

Ainsi, l'opération n'est-elle commutative que lorsque $x = 0$ (action sur l'état $|0\rangle$ de H_4) ou $k = 1$, puisque $\kappa(x^3) = \kappa(1) = 1$ (action sur l'état $|1\rangle$ de H_4). Dans les cas contraires, pour $k = 0$ ou k=2 (actions sur les états $|x^3\rangle$ et $|x + 1\rangle$), il y a une action du commutateur.

Il paraît donc clair que les caractères additifs du corps de Galois $\mathbb{F}_4$ sont intimement liés au théorème de Kochen et Specker en dimension 4.

4.5 Anneaux de Galois cachés

4.5.1 L'anneau de Galois $\mathbb{R}_{4^2}$

La démonstration du théorème de Kochen et Specker en dimension 4 s'est appuyée sur la contradiction entre une relation algébrique pour les observables et celle pour les valeurs propres (cf. section 4.1.2).

Or ces mêmes valeurs propres sont aussi les caractères additifs du corps $\mathbb{F}_4$. On va poursuivre et montrer désormais que les vecteurs propres sont les caractères additifs d'un anneau noté $\mathbb{R}_{4^2}$.

De même que $\mathbb{F}_4$ possède pour corps de base $\mathbb{F}_2 = \mathbb{Z}_2$, constitué des bits 0 et 1, l'anneau $\mathbb{R}_{4^2}$ possède pour anneau de base $\mathbb{Z}_4$, l'ensemble des entiers modulo 4.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tab. 4.15 – Addition dans $\mathbb{Z}_4$

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tab. 4.16 – Multiplication dans $\mathbb{Z}_4$

En observant les tables de $\mathbb{Z}_4$ ci-dessus, on peut noter la différence avec l'addition et la multiplication dans $\mathbb{F}_4$, dont les tableaux sont 4.2 et 4.3 respectivement. En particulier $2 * 2 = 0$ ou, en d'autres termes, l'anneau possède 2 pour diviseur de zéro (non trivial).

Dans la section 4.2.1, on a introduit les polynômes $\mathbb{F}_2[x]$, à coefficients dans le corps de base $\mathbb{F}_2 = \mathbb{Z}_2$, et définit le corps $\mathbb{F}_4$ comme l'ensemble des classes de polynômes obtenues en effectuant les opérations modulo le polynôme irréductible $x^2 + x + 1$.

Désormais, on introduit les polynômes $\mathbb{Z}_4[x]$, à coefficients dans l'anneau de base $\mathbb{Z}_4$, et on définit l'anneau $\mathbb{R}_{4^2}$ comme l'ensemble des classes de polynômes obtenues en effectuant les opérations modulo le même polynôme irréductible $x^2 + x + 1$ (une classification des anneaux d'ordre plus élevé que $\mathbb{Z}_4$ se trouve dans [PR05]).

Il est aisé de montrer que tout élément y de l'anneau $\mathbb{Z}_4$ s'écrit :

$$y = a + 2.b \text{ avec } a, b \in \mathbb{Z}_2,$$

où les opérations + et . ont lieu dans $\mathbb{Z}_4$.

La même relation s'applique à la décomposition de tout élément y de l'anneau $\mathbb{R}_{4^2}$, à partir de l'ensemble $T = \{0, 1, x, x^2 = 3 + 3.x\}$:

$$y = a + 2.b, y \in \mathbb{R}_{4^2} \text{ et } a, b \in T,$$

où les opérations + et . (ainsi que le carré) sont dans l'ensemble T. Cela étant dit, il y a une ressemblance entre T et $\mathbb{F}_4 = \{0, 1, x, x^2 = x + 1\}$.

La décomposition ci-dessus permet d'exprimer les éléments de l'anneau $\mathbb{R}_{4^2}$ par le tableau 4.17.

+2.	0	1	x	3x+3
0	0	2	2x	2x+2
1	1	3	2x+1	2x+3
x	x	x+2	3x	3x+2
3x+3	3x+3	3x+1	x+3	x+1

TAB. 4.17 – Synthèse des éléments de $\mathbb{R}_{4^2}$ par l'opération +2.

Dans le tableau 4.17, +2. indique qu'un élément de la table est la somme $a + 2.b$ de l'élément a de la ligne et de 2 fois l'élément b de la colonne (on a omis pour simplifier la forme du tableau 4.17 de mettre le symbole +2. pour les éléments de $\mathbb{R}_{4^2}$).

4.5.2 Les caractères additifs de l'anneau $\mathbb{R}_{4^2}$

La section 4.4 a permis d'élucider le plan de montage des valeurs propres pour les observables du carré de Peres et Mermin (et des *MUBs*), à partir des caractères additifs du corps $\mathbb{F}_4$. Le même type d'approche s'applique aux vecteurs propres communs aux observables d'une ligne, pour peu que l'on exhibe les caractères additifs de l'anneau $\mathbb{R}_{4^2}$.

Dans le cas présent, la trace d'un élément g de $\mathbb{R}_{4^2}$, sur l'anneau de base $\mathbb{Z}_4$, s'écrit :

$$g \in \mathbb{R}_{4^2} \longmapsto tr(g) = +\sigma(g) \text{ où } \sigma(g) = a^2 + 2.b^2$$

Grâce à cela, on obtient le caractère additif d'un élément de l'anneau :

$$g \in \mathbb{R}_{4^2} \longmapsto \kappa(g) = e^{\frac{2i\pi}{4} tr(g)} = i^{tr(g)}$$

4.5.3 Les vecteurs propres communs des *MUBs*

Les vecteurs propres $\Theta^a_{b,l}$ communs à chacune des lignes $a = 0...4$ de l'ensemble complet de *MUBs*, c'est-à-dire aussi aux 2 dernières lignes du carré de Peres et Mermin, résultent immédiatement de la définition du caractère additif de $\mathbb{R}_{4^2}$. Dans cette notation du vecteur propre, $b = 0...3$ désigne l'index du vecteur, et $l = 0...3$ désigne l'index de la composante du vecteur.

Les *MUBs* sont constituées de la base de calcul :

$$B_1 = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\},$$

et des 4 suivantes qui, pour $a = 0...3$, comprennent les vecteurs propres :

$\{\Theta^a_{b,l} = \frac{1}{2}\kappa[(a+2.b).l]\}_{b,l=0\ldots3}$; soit, de façon explicite :

$$\begin{aligned}
B_2 &= \tfrac{1}{2}\{(1,1,1,1),(1,1,-1,-1),(1,-1,-1,1),(1,-1,1,-1)\}\\
B_3 &= \tfrac{1}{2}\{(1,-1,-i,-i),(1,-1,i,i),(1,1,i,-i),(1,1,-i,i)\}\\
B_4 &= \tfrac{1}{2}\{(1,-i,-i,-1),(1,-i,i,1),(1,i,i,-1),(1,i,-i,1)\}\\
B_5 &= \tfrac{1}{2}\{(1,-i,-1,-i),(1,-i,1,i),(1,i,1,-i),(1,i,-1,i)\}
\end{aligned}$$

Les expressions de ces bases sont en accord avec les résultats de la référence [Kib10], résultats obtenus à partir d'une décomposition polaire de l'algèbre de Lie de $SU(2)$.

Comme on pouvait s'y attendre, le produit scalaire (cf. section A.5.2) entre les vecteurs $|\Theta^a_b\rangle = \sum_{l=0}^{3} \Theta^a_{b,l}$ d'une base (orthogonale), et le vecteur $|\Theta^c_d\rangle$ ($c \neq d$), d'une autre base, est constant en module, égal à $\langle \Theta^a_b \mid \Theta^c_d \rangle$. Cela vaut aussi pour le produit scalaire d'un vecteur $|\Theta^a_b\rangle$, avec ceux de la base de calcul.

Notons que cette théorie lève une partie de la dégénérescence : les valeurs propres appartiennent en commun aux 15 opérateurs du tableau 4.11, tandis que les vecteurs propres sont partagés seulement par les opérateurs au sein d'une base. Le passage des caractères additifs du corps $\mathbb{F}_4$ (à 4 éléments) à ceux de l'anneau $\mathbb{R}_{4^2}$ (à 16 éléments) a permis ce dévoilement. Si une levée complète de la dégénérescence est possible, on pourra peut-être considérer que l'on a à faire, avec les structures de Galois, à une réelle théorie à variables cachées qu'Einstein appelait de ses vœux. C'est dans ce but premier que Michel Planat a eu l'idée d'intégrer certains éléments de l'algèbre à la mécanique quantique.

Conclusion

On a vu qu'en partant de l'analyse de théorèmes liés à la complétude de la théorie quantique, l'algèbre permettait d'établir des liens entre quelques unes de ses structures (corps et anneaux de Galois) et des facettes du calcul quantique comme les matrices de Pauli et la complémentarité quantique. Cependant cette vision reste trop générique et, pour vraiment comprendre, pour aller plus en profondeur dans cette démarche, il semble intéressant d'étudier des cas plus particuliers pour ensuite si possible revenir à des généralisations. Cette démarche va être celle du dernier chapitre de cet essai.

Chapitre 5

Un formalisme original des relations de commutation : approche géométrique

Introduction

Une importante question théorique en mécanique quantique pour des espaces de Hilbert de dimension finie est partiellement restée en suspens : celle de trouver des ensembles complets (c'est-à-dire maximaux) de bases mutuellement non biaisées (de *MUBs*), quelque soit la dimension. Cela provient, entre autre, de la question de la complémentarité quantique et du *no-go* théorème de Kochen et Specker (cf. chapitre 4). Quant à la définition des *MUBs*, elle a déjà été donnée dans le chapitre 4 (cf. équation 4.3).

Par ailleurs, le comportement des *MUBs* est intimement lié aux protocoles d'information quantique (la téléportation quantique [BB84], par exemple) et au calcul quantique (cf. chapitres 2, 3).

On sait par construction [BBRV02] que, pour une dimension d de l'espace de Hilbert considéré puissance d'un nombre premier, on aura $d+1$ MUBs et $d+1$ ensembles maximalement commutant disjoints de cardinal $d-1$. Cela signifie que l'on peut réunir un maximum de $d-1$ opérateurs qui commutent les uns avec les autres, et qu'il y a $d+1$ réunions de ce type. Pour d quelconque, le nombre de MUBs est au maximum égal à $d+1$ [KSSdG05].

Exemple : pour 2 qubits, $d=4$. On a $d^2-1 = 4^2-1 = (2^2-1)\times(2^2+1)$, ce qui signifie qu'il y a 5 *MUBs* et 5 ensembles maximaux disjoints d'opérateurs qui commutent, de cardinal 3, explicités dans le tableau 5.1.

$I_2 \otimes \sigma_z$	$\sigma_z \otimes I_2$	$\sigma_z \otimes \sigma_z$
$\sigma_x \otimes I_2$	$I_2 \otimes \sigma_y$	$\sigma_x \otimes \sigma_y$
$\sigma_x \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$
$I_2 \otimes \sigma_x$	$\sigma_y \otimes I_2$	$\sigma_y \otimes \sigma_x$
$\sigma_y \otimes \sigma_z$	$\sigma_x \otimes \sigma_x$	$\sigma_z \otimes \sigma_y$

Tab. 5.1 – Un ensemble complet de 5 bases mutuellement non biaisées pour 2 qubits

Cela signifie déjà qu'une base pour 2 qubits est totalement caractérisée par les vecteurs propres communs de 3 opérateurs.

Entre deux lignes distinctes, ces observables (il s'agit des opérateurs de Pauli généralisés pour les 2 qubits, déjà abordés dans le chapitre 4) sont mutuellement non biaisées. Ainsi, une mesure précise effectuée grâce aux observables d'une ligne laisse-t-elle attendre des résultats tout à fait aléatoires pour une autre mesure, qui serait effectuée ultérieurement sur les observables d'une autre ligne.

Quant aux lignes prises deux à deux, elles forment des *MUBs*. Pour le voir, on cherche les vecteurs propres communs sur chacune des lignes du tableau 5.1 et on constate d'une part, qu'ils sont chacun non biaisés avec tous ceux des autres lignes et d'autre part, que l'ensemble des vecteurs d'une ligne constitue une base pour l'espace de Hilbert de dimension 4, H_4.

Une idée naturelle pour l'étude des *MUBs* est ainsi d'étudier les propriétés de commutation/non commutation entre les opérateurs de Pauli généralisés.

Afin d'en faciliter l'étude on peut tâcher d'en « dessiner » les propriétés et, de toute façon, commencer par le cas le plus simple et non trivial : les 2 qubits. Les 2 qubits constituent un cas particulier car ainsi que l'on va le voir, toutes les propriétés et les différentes partitions de leur graphe de Pauli, définies dans la section 5.1, sont englobées dans la géométrie du quadrangle généralisé d'ordre 2 (cf. section B.3.1). Une généralisation à n qubits a été depuis lors étudiée et sera abordée dans la section 5.2, de manière succincte du fait que la méthodologie employée ne diffère pas fondamentalement. La section 5.1 est principalement une explication détaillée de [PS08], pour ensuite aborder, dans la section 5.3, les cas particuliers auxquels je me suis intéressée [PBS07, PB07].

Beaucoup d'éléments vont être évoqués durant ce chapitre et proviennent de divers horizons. Les annexes A, B et C donnent les notions de base respectivement en algèbre, en géométrie projective et en théorie des graphes.

5.1 Cas des 2 qubits

5.1.1 Le graphe de Pauli pour 2 qubits

On définit le **graphe de Pauli pour 2 qubits**, que l'on notera $P[2,2]$, de la manière suivante : chaque sommet est un produit tensoriel de 2 matrices de Pauli, soit 15 sommets différents en excluant I_4, que l'on numérote de la façon suivante :

$$0 = I_2 \otimes I_2, 1 = I_2 \otimes \sigma_x, 2 = I_2 \otimes \sigma_y, 3 = I_2 \otimes \sigma_z,$$
$$a = \sigma_x \otimes I_2, 4 = \sigma_x \otimes \sigma_x, 5 = \sigma_x \otimes \sigma_y, 6 = \sigma_x \otimes \sigma_z,$$
$$b = \sigma_y \otimes I_2, 7 = \sigma_y \otimes \sigma_x, 8 = \sigma_y \otimes \sigma_y, 9 = \sigma_y \otimes \sigma_z,$$
$$c = \sigma_z \otimes I_2, 10 = \sigma_z \otimes \sigma_x, 11 = \sigma_z \otimes \sigma_y, 12 = \sigma_z \otimes \sigma_z$$

Remarque : Ces notations sont différentes de celles utilisées dans le tableau 4.5 du chapitre 4, leur pertinence va se révéler au cours de cette section.

On va observer où conduit le fait de partitionner de diverses manières un tel graphe. Sa matrice d'adjacence est donnée par le tableau 5.2, en vertu de sa définition (cf. section C.1.2). On peut la déduire directement du tableau 4.5 du chapitre 4 mais de fait elle a été calculée grâce au logiciel de calcul MATHEMATICA, qui a été d'une grande aide pour la plupart des résultats obtenus.

	1	2	3	a	4	5	6	b	7	8	9	c	10	11	12
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0
2	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0
3	0	0	0	1	0	0	1	1	0	0	1	1	0	0	1
a	1	1	1	0	1	1	1	0	0	0	0	0	0	0	0
4	1	0	0	1	0	0	0	0	0	1	1	0	0	1	1
5	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1
6	0	0	1	1	0	0	0	0	1	1	0	0	1	1	0
b	1	1	1	0	0	0	0	0	1	1	1	0	0	0	0
7	1	1	1	0	0	0	0	0	1	1	1	0	0	0	0
8	0	1	0	0	1	0	1	1	0	0	0	0	1	0	1
9	0	0	1	0	1	1	0	1	0	0	0	0	1	1	0
c	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
10	1	0	0	0	0	1	1	0	0	1	1	1	0	0	0
11	0	1	0	0	1	0	1	0	1	0	1	1	0	0	0
12	0	0	1	0	1	1	0	0	1	1	0	1	0	0	0

TAB. 5.2 – Matrice d'adjacence de $P[2, 2]$

NB : On « met des 0 » sur la diagonale de cette matrice, bien que chaque opérateur commute avec lui-même, afin d'avoir à faire à un graphe **simple** : aucun sommet n'a d'arête sur lui-même. Les points a, b et c sont des *points de référence*. Le choix de tels points peut sembler arbitraire mais il n'en est rien : les partitions du graphe de Pauli que l'on va expliciter en découlent immédiatement.

Au préalable, on remarque que la matrice d'incidence de $P[2, 2]$ a une structure de la forme du tableau 5.3, à ceci près que l'on a supprimé les points de référence a, b et c. On a posé : $0 = 0_3$ et $A = I_3$. La matrice $\hat{A}$ est le **complément** de A, au sens de la théorie des graphes (on intervertit les 0 et les 1 dans la matrice d'adjacence).

0	A	A	A
A	0	$\hat{A}$	$\hat{A}$
A	$\hat{A}$	0	$\hat{A}$
A	$\hat{A}$	$\hat{A}$	0

Tab. 5.3 – Structure « mise en abyme » de la matrice d'adjacence de $P[2,2]$

Le « sous-tableau » en bas à droite du tableau 5.3 est en fait un carré de Peres et Mermin (cf. section 4.1.2 du chapitre 4) ; on aura l'occasion, après l'avoir explicitée, de faire un petit arrêt sur la partition du graphe de Pauli qu'il constitue en partie.

De la matrice d'incidence, on déduit immédiatement que $P[2,2]$ est régulier, de degré 6 (cf. section C.1.3) et, de ce fait, pourrait être intimement lié au graphe complet d'ordre 6 (cf. section C.2.2), noté K_6. En fait, on a exactement $P[2,2] \equiv \hat{L}(K_6)$. Pour rappel des notations, cela signifie que $P[2,2]$ est isomorphe au complément du graphe d'incidence de K_6 (cf. section C.2.3). Si on calcule le recouvrement minimum des sommets de $P[2,2]$ (cf. section C.2.1), on retrouve le graphe dit de Petersen (cf. section C.2.2). Par ailleurs, le graphe de Petersen est isomorphe à $\hat{L}(K_5)$ (cf. section C.1.5). Le complément du graphe de Petersen peut également être vu comme une configuration de Desargues (cf. section B.2.3). Le graphe $P[2,2]$ est également isomorphe au recouvrement minimum des sommets de $\hat{L}(K_7)$ (cf. section C.2.1).

5.1.2 Trois partitions du graphe de Pauli

Il découle de tout ceci trois partitions – tout en figure ! – qui sont les suivantes :

1. Un pinceau de lignes dans le plan de Fano (PF) (cf. section B.2.2) et un cube (C)

Partition (PF) – (C) :

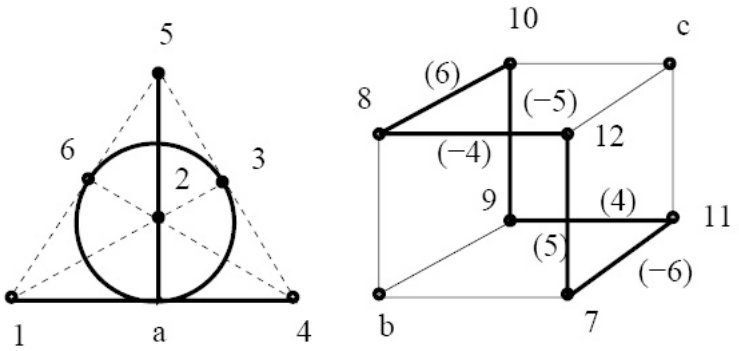


Fig. 5.1 – Partition (PF) – (C)

Légende : – *Trait plein : « commutent »*
– *Trait pointillé : « ne commutent pas »*

Pour ce choix particulier, c'est-à-dire 1 sommet particulier du graphe de Pauli, les lignes de (PF) représentent les bases à 2 qubits non intriquées.

Remarques :
- $1 \times a = 4$, $2 \times a = 5$ et $3 \times a = 6$: chaque paire d'opérateurs d'une même ligne conduit au $3^{\text{ième}}$.
- 4, 5, et 6 partagent une base commune, de dimension 4.
- $8 \times 10 = 6$ et $8 \times 12 = -4$: il y a une application entre (PF) et (C), explicitée pour le cycle intriqué caractérisant les 6 bases intriquées suivantes : $(7, 11)$, $(7, 12)$, $(12, 8)$, $(8, 10)$, $(10, 9)$ et $(9, 11)$. On les définit via 2 opérateurs au lieu de 3, puisque le dernier ce déduit automatiquement des 2 autres : $8 \times 10 = 6$, par exemple.

Ce découpage provient de l'étude des droites projectives (cf. annexe B) sur les anneaux finis (cf. section A.2) du type $\mathbb{Z}_2^{\times n}$ (où $n = 2, 3, 4$), lors de travaux antérieurs [PSK06].

2. Un graphe bipartite (cf. section C.2.2) (GB) et un carré de Peres et Mermin (PM)

Partition (GB) – (PM) :

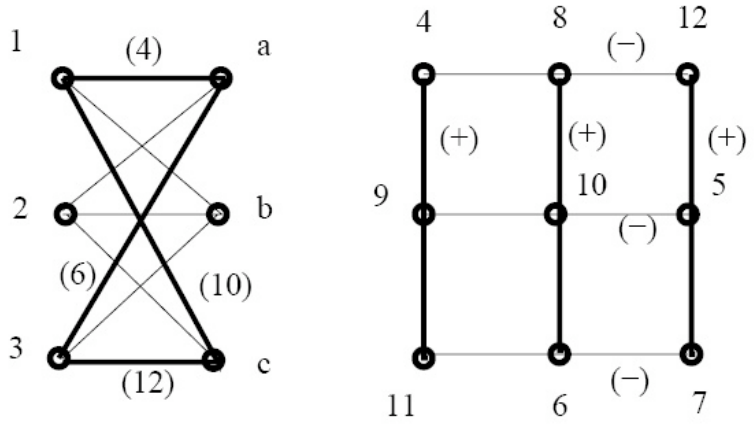


FIG. 5.2 – Partition (GB) – (PM)

Remarques :
- Une des remarques précédentes, faite dans le cadre de la partition (PF)-(C), s'applique à (PM), à savoir que chaque paire d'opérateurs d'une même ligne conduit au $3^{\text{ième}}$.
- Les bases définies par 2 opérateurs de (GB) qui commutent ne sont pas intriquées, (GB) est « la partie non intriquée » du graphe de Pauli.
- Il y a une application de (GB) à (PM).
- Le carré (PM) est constitué de 3 lignes et de 3 colonnes, l'ensemble correspond à 6 MUBs intriquées : (PM) est « la partie intriquée » du graphe de Pauli.

3. Le graphe de Petersen (GP) et un ensemble indépendant (I)

Partition (GP) – (I) :

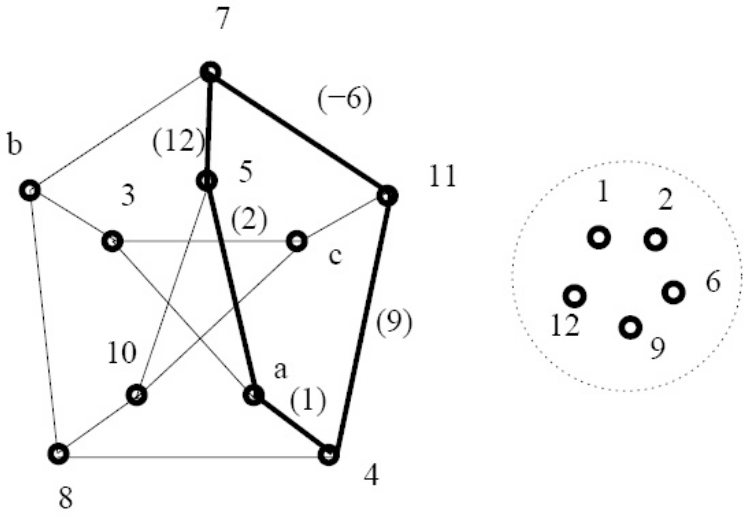


Fig. 5.3 – Partition (GP) – (I)

Remarques :
- Le graphe (GP) admet une application reliant ses arêtes aux sommets de (I).
- Le complément de (GP) peut être vu comme une configuration de Desargues (10_3) (cf. section B.2.3).

Ces trois factorisations proviennent naturellement du fait que le quadrangle $W(2)$ possède des hyperplans géométriques de 3 types distincts (cf. section B.3.1) ; ils seront explicités à travers la figure 5.4, mais voici déjà leur nom :

- le premier est du type, ensemble perpendiculaire de points,
- le deuxième, du type grille,

– le troisième, du type ovoïde.

Ces factorisations seront également expliquées du point de vue de l'algèbre, via la notion de droites projectives sur des anneaux finis.

Petit Arrêt sur la partition (PM) – (GB)

En substance, comme on l'a déjà signalé, (PM) caractérise la partie intrication et (GB), celle non intriquée du système formé des 15 opérateurs que constitue le graphe de Pauli. C'est pourquoi, personnellement, me parait-elle la plus intéressante du point de vue de l'information quantique. D'après les notations utilisées dans le tableau 4.5 du chapitre 4 et sur la figure 5.2, on a : $(PM) = \{4, 5, 6, 8, 9, 10, 11, 12\}$ et $(GB) = \{1, 2, 3, a, b, c\}$. On a vu que l'on pouvait directement « extraire » (PM) du tableau 5.3 (c'est également vrai pour (GB), après rajout des points de référence). C'est par de telles extractions que l'on a pu révéler les diverses partitions.

Remarque : il y a d'autres choix possibles concernant la grille de 9 points et 6 lignes qui constitue (PM) mais ils sont, de toute manière, tous englobés dans la structure de $W(2)$. En revanche, chacune de ces grilles ne constituera pas forcément un carré de Peres et Mermin, au sens de la contradiction (KS) (cf. chapitre 4).

Par ailleurs, (PM) peut être vu comme :

– un graphe régulier de degré 4,
– une « sous »-configuration de Pappus (cf. section B.2.3),
– une configuration projective (cf. section B.2.3), notée $(9_2, 6_3)$; du point de vue de la théorie des graphes, cela signifie qu'il est égal à son complément,
– la droite projective sur l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_2$ si on identifie, et les deux ensembles des points, et les relations de graphe « opérateurs qui commutent »/« points mutuellement distants » qui les régissent respectivement ; c'est d'ailleurs ceci qui a motivé une étude plus approfondie des droites projectives [SPKP07, SPK06] et qui a abouti à des liens révélateurs entre la géométrie projective et la structure de systèmes à plusieurs qubits [PSK06, SPP08]. L'article [PS08] est un survol de ces travaux antérieurs.

Remarque : l'annexe B donne la définition d'une droite projective et l'illustre par divers exemples. Il fournit également la définition de la structure de graphe à laquelle on rattache une droite projective. À chaque fois que l'on parlera de droites projectives, même si on omet de le mentionner, elles seront implicitement munies de cette structure.

Afin de compléter l'étude du graphe de Pauli $P[2, 2]$, quelques uns de ses invariants

sont répertoriés dans le tableau 5.6, tableau qui les listent également pour certains de ses sous graphes remarquables à titre de comparaison [SPP08] :

G	$P[2,2]$	GP	PM	GB	PF	C
s	15	10	9	6	7	8
a	45	15	18	9	9	12
$sp(G)$	$\{-3^5, 1^9, 6\}$	$\{-2^4, 1^5, 3\}$	$\{-2^4, 1^4, 4\}$	$\{-3, 0^4, 3\}$	$\{-2, -1^3, 1^2, 3\}$	$\{-3, -1^3, 1^3, 3\}$
$g(G)$	3	5	3	4	3	3
$\kappa(G)$	4	3	3	2	3	2

Tab. 5.4 – Principaux invariants de $P[2,2]$ et de quelques uns de ses sous graphes

Les symboles s, a, $sp(G)$, $g(C)$ et $\kappa(G)$ représentent respectivement, pour un graphe G, son nombre de sommets, son nombre d'arêtes, son spectre, sa circonférence et son nombre chromatique (cf. sections C.1.4, C.1.6).

5.1.3 Unification des trois partitions

Pour aller plus loin dans cette étude géométrique des opérateurs de Pauli pour 2 qubits, on identifie cette fois-ci les opérateurs avec des points, et les ensembles maximaux d'opérateurs qui commutent, avec des lignes (de façon plus prosaïque, on recherche les *cliques* maximaux, c'est-à-dire les plus grands sous graphes complets, de $P[2,2]$; en l'occurence, des triangles). Les sommets seront reliés si les opérateurs correspondant commutent (dans le langage $W(2)$-*ien*, on dit que les points sont **colinéaires**, cf. section B.3.1). Ainsi fait, découvre-t-on que la structure géométrique englobant les 2 qubits est le quadrangle généralisée d'ordre 2 (cf. section B.3.1), $W(2)$, représenté sur la figure 5.4.

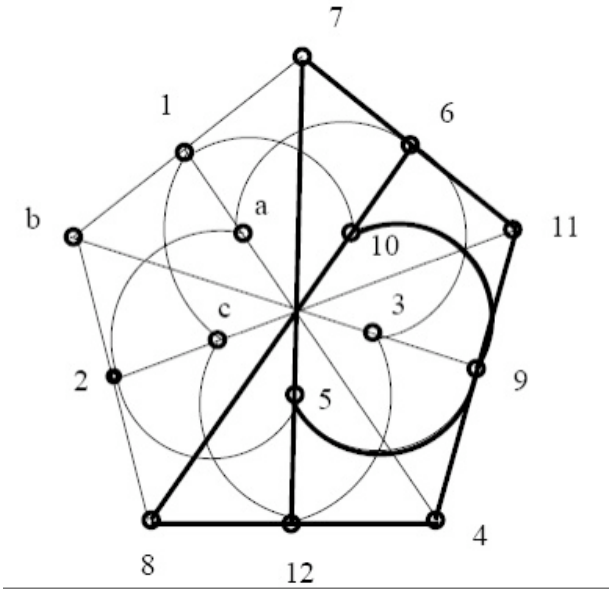


Fig. 5.4 – Quadrangle généralisé d'ordre 2 : $W(2)$

Chacune des lignes de $W(2)$ correspond à un ensemble maximalement commutant ; en

voici la liste exhaustive : $\{1, a, 4\}$, $\{2, a, 5\}$, $\{3, a, 6\}$, $\{1, b, 7\}$, $\{2, b, 8\}$, $\{3, b, 9\}$, $\{1, c, 10\}$, $\{2, c, 11\}$, $\{3, c, 12\}$, $\{4, 8, 12\}$, $\{5, 7, 12\}$, $\{6, 7, 11\}$, $\{4, 9, 11\}$, $\{5, 9, 10\}$ et $\{6, 8, 10\}$.

Comme cela a déjà été mentionné, $W(2)$ possède 3 types d'hyperplans, correspondant au 3 différentes partitions ; ce fait semble justifier qu'il soit la géométrie sous-jacente de $P[2, 2]$. Il découle des définitions de $W(2)$, et de ce qu'est un hyperplan géométrique (cf. annexe B), qu'il y a :

- 15 ensembles de 7 points colinéaires avec un point donné inclus, appelés ensembles perpendiculaires (*perp-set*). Du point de vue des opérateurs associés, cela signifie qu'il y en a 6 qui commutent avec un opérateur donné. On a comme ensemble perpendiculaire, par exemple : $\{1, a, 4, 2, 3, 5, 6\}$, c'est-à-dire (PF). Ils sont au nombre de 15 car $W(2)$ possède 15 sommets.
- 10 grilles de 9 points sur 6 lignes (*grid*) ; par exemple $\{4, 8, 12, 9, 10, 5, 11, 6, 7\}$, c'est-à-dire (PM). Il y en a 10 car le graphe de Petersen a 10 sommets.
- 6 ovoïdes (*ovoïd*) de 5 points. Du point de vue des opérateurs associés, cela signifie qu'ils ne commutent pas ensemble. On a comme ovoïde, par exemple : $\{1, 2, 6, 9, 12\}$, c'est-à-dire l'ensemble indépendant (I). Les 6 ovoïdes correspondent aux 6 configurations possibles d'un ensemble complet de *MUBs*.

La dualité de $W(2)$ s'applique à chacun de ses hyperplans. En particulier, le dual d'un ovoïde, appelé un **drapeau** (*spread*), est un ensemble de 5 lignes contenant 3 points, deux à deux disjointes, un drapeau contient donc tous les sommets du quadrangle. Chacun des 6 différents drapeaux est un ensemble de 5 sous ensembles maximaux d'opérateurs qui commutent. On a ainsi une façon (ce n'est pas la seule) de recouvrir les 6 ensembles complets de 5 MUBs pour 2 qubits, dont l'un est référé dans le tableau 5.1 .

Une grille duale (grille de 9 lignes à 3 points), quant à elle, a la propriété suivante : chaque triplet d'opérateurs sur une même ligne partage une base d'états non intriqués. Partage signifie ici qu'ils possèdent les mêmes vecteurs propres. En l'occurrence, ils décrivent tous un état à 2 qubits non intriqués et l'ensemble constitue une base pour l'espace de Hilbert de dimension 4.

Pour finir sur l'étude géométrique de $W(2)$, puisque ce dernier est de degré 6 et fortement régulier, une idée a été de chercher si il avait un lien avec le graphe complet à 6 éléments, K_6. On peut constater que : $W(2) \equiv \hat{L}(K_6)$ ($W(2)$ est isomorphe au complément du graphe d'incidence de K_6). Le groupe des automorphismes de $W(2)$ (concrètement, ses symétries) est $\mathbb{S}_6$ (groupe symétrique d'ordre 6, soit l'ensemble des permutations à 6 éléments, ou encore les transformations laissant un hexagone invariant).

5.1.4 Autre description du graphe de Pauli

On peut également formuler $P[2,2]$ en terme de droite projective sur un anneau fini et ainsi connecter la théorie des nombres à la géométrie. Le quadrangle $W(2)$ peut être associé à la droite projective définie sur l'anneau $\mathbb{Z}_2^{2\times 2}$ des matrices 2×2 à coefficients dans $\mathbb{Z}_2$; c'est-à-dire, l'anneau défini de la manière suivante :

$$\mathbb{Z}_2^{2\times 2} = \{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} | \alpha,\beta,\gamma,\delta \in \mathbb{Z}_2\}.$$

Dans une telle optique, on note les 16 éléments du susdit anneau de la façon suivante :

$$\begin{aligned}
1' &\equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, 2' \equiv \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, 3' \equiv \begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}, 4' \equiv \begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}\\
5' &\equiv \begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}, 6' \equiv \begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix}, 7' \equiv \begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}, 8' \equiv \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\\
9' &\equiv \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, 10' \equiv \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, 11' \equiv \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, 12' \equiv \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\\
13' &\equiv \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}, 14' \equiv \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}, 15' \equiv \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, 0' \equiv \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}
\end{aligned}$$

On observe que $U = \{1', 2', 9', 11', 12', 13'\}$ constitue l'ensemble des unités de $\mathbb{Z}_2^{2\times 2}$ (les matrices inversibles) et $\Theta = \{0', 3', 4', 5', 6', 7', 8', 10', 14', 15'\}$, celui des diviseurs de 0.

On applique la définition de la droite projective : après avoir vérifié l'admissibilité de chaque paire (a,b), on élimine celles qui ne le serait pas ; puis, on cherche à quelle classe d'équivalence, de la forme (qa,qb) pour $q \in U$, chacune d'entre elles appartient.

Exemple : $(3',4')_{q=1'} \equiv (3',7')_{q=2'} \equiv (4',3')_{q=9'} \equiv (7',4')_{q=11'} \equiv (7',3')_{q=12'} \equiv (4',7')_{q=13'}$.

On ne conservera que $(3',4')_{q=1'}$ par exemple, soit l'un des représentants de la classe définie par $q = 1'$.

On trouve, après des calculs simples mais très longs [SPKP07, SP07b] que d'une part, la droite projective sur l'anneau $\mathbb{Z}_2^{2\times 2}$ est unique et n'existe « qu'à gauche » (l'anneau n'est pas commutatif et la non existence à droite a été vérifiée à la main ; c'est pourquoi on a « testé » non pas (aq,ab), mais (qa,qb)), d'autre part, que celle-ci est constituée des 35

points suivants :

$$
\begin{array}{lll}
(1',1') & , & (1',2'),(1',9'),(1',11'),(1',12'),(1',13') \\
(1',0') & , & (1',3'),(1',4'),(1',5'),(1',6'),(1',7'),(1',8'),(1',10'),(1',14'),(1',15') \\
(0',1') & , & (3',1'),(4',1'),(5',1'),(6',1'),(7',1'),(8',1'),(10',1'),(14',1'),(15',1') \\
(3',4') & , & (3',10'),(3',14'),(5',4'),(5',10'),(5',14'),(6',4'),(6',10'),(6',14')
\end{array}
$$

Le classement des points sur 4 lignes n'est pas fortuit : sur la 1ère ligne, par exemple, les deux composantes sont des unités ; les trois autres traitent des 3 cas restants.

Entre autre, en utilisant la relation voisin/distant, la partition graphe bipartite-carré de Peres et Mermin devient un sous ensemble de la droite projective et on s'aperçoit que les diviseurs de 0 semblent jouer un rôle important dans la « partie intrication » :

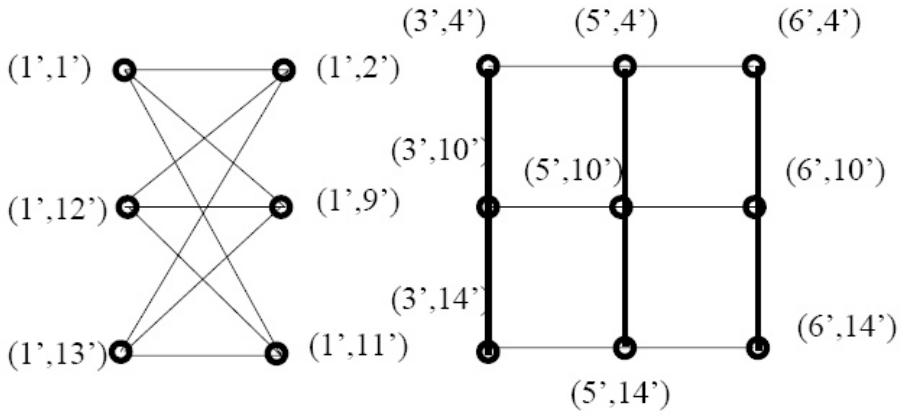


FIG. 5.5 – Points de la droite projective sur la partition PM – GB

On peut montrer que les 3 types d'hyperplans de $W(2)$ ont une explication algébrique : l'anneau $\mathbb{Z}_2^{2\times 2}$ a, entre autre, 3 sous anneaux d'ordre 4 et de caractéristique 2 [SPP08] :

$P[2,2]$	Ensemble de 5 opérateurs ne commutant pas mutuellement	Ensemble de 6 opérateurs commutant avec un des 6 donné	9 opérateurs d'un carré de Peres-Mermin
$W(2)$	Ovoïde	Ensemble perpendiculaire de point de référence l'opérateur donné	Grille
Droites projectives sur :	$\mathbb{F}_4 \equiv \mathbb{Z}_2[x]/ < x^2+x+1 >$	$\mathbb{Z}_2[x]/ < x^2 >$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2[x]/\langle x\,(x+1)\rangle$

TAB. 5.5 – Résumé des différentes correspondances

Il a été établi [Tha71] qu'il y avait une bijection entre les points de la droite projective

sur $\mathbb{Z}_2^{2\times 2}$ et les lignes de $PG(3,2)$, qui est le plus simple espace projectif (tous ses hyperplans sont des plans de Fano). Les 15 points de $PG(3,2)$ correspondent aux 15 opérateurs. Chacune des 35 lignes de $PG(3,2)$ correspondent à un triplet d'opérateurs $(\sigma_k, \sigma_l, \sigma_m)$ vérifiant, pour $k \neq l \neq m$, $\sigma_k \times \sigma_l = \mu\sigma_m$, où $\mu = \{1, -1, i, -i\}$. Les opérateurs situés sur les 15 lignes totalement isotropes de $PG(3,2)$ appartiennent à $W(2)$ (quand $\mu = \{1, -1\}$). Mathématiquement, on dit que l'on *plonge* $W(2)$ dans $PG(3,2)$.

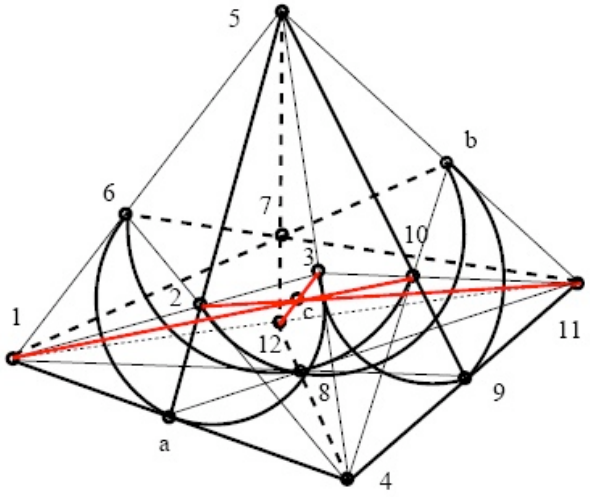


Fig. 5.6 – W_2 est plongé dans $PG(3,2)$; les 15 points de $PG(3,2)$ correspondent aux 15 opérateurs de Pauli.

Pour conclure, la particularité des systèmes à 2 qubits provient du fait qu'il existe une parfaite dualité entre les sommets (opérateurs) et les arêtes (ensembles maximalement commutant), dualité perdue dès l'étude de systèmes quantiques de niveau supérieur à 4. Cela n'a pas été démontré pour le cas général mais l'étude des dimensions 6, 8 et 9 [PS08] abonde dans ce sens. Le cas des dimensions supérieures exige une puissance de calcul supérieure à celle des ordinateurs disponibles, ou alors faudrait-il changer de méthode au niveau de la recherche des ensembles maximalement commutant puisque c'est un problème NP-complet. En effet, ce qui en physique équivaut à la recherche de *MUBs*, en théorie des graphes, il s'agit de celle des sous graphes complets maximaux du graphe de Pauli (ou cliques maximaux), et ce problème est équivalent à celui du voyageur de commerce, mentionné dans le chapitre 2.

5.2 Généralisation à N qubits

5.2.1 Les 3 qubits

Le graphe de Pauli pour 3 qubits sera lui constitué de $4^3 - 1 = 63$ sommets correspondant aux opérateurs de Pauli généralisés de la forme $(\sigma_j \otimes \sigma_k \otimes \sigma_l)$, tels que $i, j, k \in \{1, 2, 3, 4\}$ et $(i, j, k) \neq (1, 1, 1)$.

En explicitant sa matrice d'adjacence, on s'aperçoit que l'on a affaire à un graphe, noté $P[3,2]$, de degré 30 et de spectre : $\{-5^{27}, 3^{35}, 30\}$. Sa matrice d'adjacence peut être compactée en une forme **tripartite** (cf. section C.2.2), après avoir omis les 3 points de référence :

$$a_3 = \sigma_x \otimes I_2 \otimes I_2, b_3 = \sigma_y \otimes I_2 \otimes I_2 \text{ et } c_3 = \sigma_z \otimes I_2 \otimes I_2,$$

comme exprimé dans le tableau 5.6.

0_3	A_3	A_3	A_3
A_3	0_3	$\hat{A}_3$	$\hat{A}_3$
A_3	$\hat{A}_3$	0_3	$\hat{A}_3$
A_3	$\hat{A}_3$	$\hat{A}_3$	0_3

TAB. 5.6 – Structure « mise en abyme » de la matrice d'adjacence de $P[3,2]$

La matrice 0_3 est la matrice d'adjacence de $P[2,2]$, $A_3 = 0_3 + I_8$, et $\hat{A}_3$ est le complémentaire de A_3. Cette propriété « fractale » reste vérifiée pour les N qubits, quelque soit N. Malgré cela, il n'y a plus de partitions simples. En revanche, quelque soit N, le graphe de Pauli des N qubits reste fortement régulier [PS08] ; et, comme on va le constater, cette caractéristique se révèle intéressante pour une généralisation en terme de géométrie.

Dans le cas des deux qubits, on a vu qu'il y avait un lien entre la théorie des graphes (cliques maximaux) et la physique (*MUBs*). Quelle physique peut bien se cacher derrière cette propriété de fortement régulier ? La prochaine section met en évidence, pour le cas des N qubits, une géométrie sous jacente pour leur graphe de Pauli, faisant intervenir les espaces polaires symplectiques et les géométries partielles (cf. section 5.2.2) mais, jusqu'à maintenant, n'a pas été distingué le sens physique qui pourrait éventuellement y être caché.

5.2.2 Les N qubits

Les espaces polaires symplectiques

A partir de $N > 2$, les N qubits ne sont plus caractérisés par un quadrangle généralisé d'ordre N mais sont reliés [SP07a, Tha07, Hav07] à une structure plus générique du fait que l'on a perdu la dualité : les espaces polaires symplectiques (cf. section B.2.5), notés $W_{2N-1}(q)$. Ces derniers constituent en effet, ainsi qu'on va le voir, la géométrie sous-jacente au graphe de Pauli pour les N qubits.

Cette idée d'avoir tenté et réussi à relier les N qubits à de tels objets provient du fait que $W(2)$ est le plus petit représentant (en terme de rang) de la famille constituée par ces derniers.

Pour rappel, un **espace polaire symplectique** est un espace vectoriel de dimension d sur le corps de Galois F_q, noté $V(d,q)$, muni en plus d'une forme bilinéaire alternée non dégénérée.

Un tel espace, noté $W_{d-1}(q)$, existe si et seulement si $d = 2N$, où N est son **rang** (ou

ordre). Un sous espace de $V(d,q)$ est dit **totalement isotrope** si la forme associée est la fonction nulle. L'espace $W_{d-1}(q)$ peut alors être vu comme l'espace des sous espaces totalement isotropes de $PG(2N-1,q)$, tout en tenant compte de la forme symplectique [PS08]. Les plus grands sous espaces totalement isotropes en sont les générateurs.

Pour $q=2$, cet espace polaire contient :

$$\mid W_{2N-1}(2) \mid = \mid PG(2N-1,2) \mid = 2^{2N}-1 = 4^N-1 \text{ points.} \tag{5.1}$$

$$(2+1)(2^2+1)...(2^N+1) \text{ générateurs } G. \tag{5.2}$$

Un **drapeau** (*spread*) S de $W_{2N-1}(2)$ est un ensemble de générateurs constituant une partition des points de $W_{2N-1}(2)$, les cardinaux d'un drapeau et d'un générateur de $W_{2N-1}(2)$ sont respectivement :

$$\mid S \mid = 2^N+1 \text{ et } \mid G \mid = 2^N-1 \tag{5.3}$$

Par ailleurs, deux points distincts de $W_{2N-1}(q)$ sont dits **perpendiculaires** si ils sont reliés par une ligne ; pour $q=2$, il y en a :

$$2^{2N-1} \tag{5.4}$$

A la lumière de tout ceci, on peut faire correspondre :

- le nombre de points de $W_{2N-1}(2)$, au nombre d'opérateurs de Pauli généralisés (équation 5.1),
- le concept de deux opérateurs qui commutent, avec celui de deux points perpendiculaires,
- suite à l'identification entre les deux concepts, l'ensemble des points d'un générateur G, avec un ensemble maximalement commutant. L'ensemble S reconstitue la partition évoquée tout au début de ce chapitre : pour une dimension de l'espace de Hilbert considéré, puissance d'un nombre premier d, on aura $d+1$ *MUBs* et $d+1$ ensembles maximalement commutant de cardinal $d-1$ (équation 5.2),
- le nombre total de générateurs de $W_{2N-1}(2)$, au nombre des ensembles maximalement commutant (disjoints ou non).

De plus, l'équation 5.4 indique qu'il y a 2^{2N-1} opérateurs qui ne commutent pas avec un opérateur donné. Certes, le fait est que cela reste une conjecture que de dire que la géométrie cachée du graphe de Pauli pour les N qubits – qui sera noté par la suite $P[2,N]$ – est $W_{2N-1}(2)$. Cependant, il y a beaucoup de coïncidences : notamment, la propriété issue de l'équation 5.4 a été vérifiée indépendamment par Koen Thas [Tha07]. De façon pratique, cela a été calculé pour les cas des 2, 3, et 4 qubits (voir le tableau 5.7 en fin de

section) ; et en soi, vu de quoi il retourne, il n'y a pas, du moins *a priori*, tellement de raisons pour que l'hypothèse se révèle fausse.

C'est pourquoi on va considérer que $W_{2N-1}(2)$ est la bonne géométrie cachée de $P[2, N]$. Cette dernière cependant est une géométrie « multi-ligne » (au sens où un point peut appartenir à deux lignes par exemple) ; mais on va voir que, du fait que le graphe de Pauli pour les N qubits soit fortement régulier, des relations entre $W_{2N-1}(2)$ et les géométries partielles, définies plus loin, permettent de retrouver toutes les propriétés de $P[2, N]$. L'intérêt en est que les géométries partielles sont des espaces presque linéaires (cf. section B.2.4) qui vont « lisser » la structure géométrique sous-jacente de $P[2, N]$.

Les géométries partielles :

On sait [Cle02] que la matrice d'adjacence, notée A, d'un graphe fortement régulier vérifie les équations suivantes :

$$AJ = DJ \text{ et } A^2 + (\mu - \lambda)A + (\mu - D)I = \mu J \tag{5.5}$$

où J est la matrice ne contenant que des 1, I, la matrice identité, D, son degré tel que deux sommets adjacents sont tous les deux adjacents avec le même nombre λ de sommets, et tel que deux sommets non adjacents sont tous les deux adjacents avec le même nombre μ de sommets. On notera le graphe fortement régulier correspondant de la façon suivante : $gfr(v, D, \lambda, \mu)$

La matrice A a ainsi comme valeur propre D avec une multiplicité 1 (D n'apparaît qu'une fois dans son spectre) ; ses autres valeurs propres sont r (>0) et l (<0), reliées de la manière suivante :

$$r + l = \lambda - \mu \text{ et } rl = \mu - D \tag{5.6}$$

Les graphes fortement réguliers ont de multiples propriétés [Cle02] ; en particulier, les deux valeurs propres r et l sont (excepté pour les graphes connus sous le nom de graphes de conférence [Cle02]) des entiers dont les multiplicités respectives, f et g, vérifient les relations suivantes :

$$f = \frac{-D(l+1)(D-l)}{(D+rl)(r-l)} \text{ et } g = \frac{D(r+1)(D-r)}{(D+rl)(r-l)} \tag{5.7}$$

Le graphe de Pauli pour les N qubits, étant fortement régulier, vérifie les propriétés évoquées ci-dessus qui vont permettre de relier les espaces polaires symplectiques avec les géométries partielles.

Une **géométrie partielle**, notée $gp(s, t, \alpha)$ [Bat97], est un objet plus générique qu'un quadrangle généralisé fini. C'est un espace presque linéaire $\{P, L\}$ tel que, pour tout point P n'appartenant pas à une ligne L, on ait :

– Le nombre de points de L reliés à P par une ligne est α
– Chaque ligne a $s+1$ points
– Chaque point est sur $t+1$ lignes

Le graphe de $gp(s,t,\alpha)$ est constitué de $(s+1)\frac{st+\alpha}{\alpha}$ sommets et de $(t+1)\frac{st+\alpha}{\alpha}$ lignes ; il est fortement régulier, du type :

$$gfr\left((s+1)\frac{st+\alpha}{\alpha}, s(t+1), s-1+t(\alpha-1), \alpha(t+1)\right) \tag{5.8}$$

Par ailleurs, si le spectre d'un graphe fortement régulier est de la même forme que celui d'une géométrie partielle, un tel graphe est dit **pseudo-géométrique**. Les graphes associés aux espaces polaires symplectiques $W_{2N-1}(q)$ sont pseudo-géométriques [Cle02], et sont de la forme :

$$pseudo-g\left(q\frac{q^{N-1}-1}{q-1}, q^{N-1}, \frac{q^{N-1}-1}{q-1}\right) \tag{5.9}$$

Par suite, le graphe de Pauli pour N qubits est du type décrit par l'équation 5.9.

Exemples :

Afin de fixer un peu mieux les idées, voici un exemple détaillé pour $N=3$. La section 5.2.1 donne le graphe de Pauli des 3 qubits et quelques unes de ses caractéristiques. Du spectre de ce dernier, $\{-5^{27}, 3^{35}, 30\}$, puis grâce à l'équation 5.6 (calcul de λ et μ), il découle que $P[3,2]$ est, avec les notations du paragraphe précédent, le graphe :

$$gfr(63, 30, 13, 15)$$

On va en déduire la géométrie partielle associée :

$$\begin{aligned} gfr(v, D, \lambda, \mu) &= gfr\left((s+1)\frac{st+\alpha}{\alpha}, s(t+1), s-1+t(\alpha-1), \alpha(t+1)\right) \\ &\Longrightarrow gp(s,t,\alpha)? \end{aligned}$$

L'expression ci-dessus est issue de l'équation 5.8 et des notations concernant les graphes fortement régulier, du paragraphe précédent. On ne recherche finalement que 3 paramètres, nommément s, t et α, et on dispose de 4 relations comme exprimé ci-dessus. Eh bien qu'à cela ne tienne ! On utilise les 3 équations les plus simples ; la plus compliquée, à savoir celle qui contient une fraction, on s'en contentera comme vérification. Par identification, on a :

$$D = s(t+1)\ ,\ \lambda = s-1+t(\alpha-1) \text{ et } \mu = \alpha(t+1)$$

Ainsi, dans le cas des 3 qubits, obtient-on la géométrie partielle $gp(6, 4, 3)$.

A titre d'exemples, le tableau 5.7 regroupe les caractéristiques des graphes de Pauli des N qubits, pour les cas $N = 2$, $N = 3$ et $N = 4$.

N	v	e	D	r	l	λ	μ	s	t	α
2	15	15	6	1	−3	1	3	2	2	1
3	63	45	30	3	−5	13	15	6	4	3
4	255	153	126	7	−9	6	63	14	8	7

TAB. 5.7 – Invariants des graphes de Pauli $P[2, N]$ pour $N \in \{2, 3, 4\}$

Les invariants des graphes de Pauli mentionnés dans le tableau 5.7 ont été calculés « à la main », mais *a posteriori* ils découlent directement des propriétés des espaces polaires symplectiques d'ordre 2 et de rang N.

On a, en règle générale :

- le nombre de sommets du graphe : $v = 4^N - 1$,
- le degré du graphe : $D = v - 1 - 2^{2N-1}$,
- $s = 2\frac{2^{N-1}-1}{2-1}$,
- $t = 2^{N-1}$,
- $\alpha = \frac{2^{N-1}-1}{2-1}$,
- $\mu = \alpha(t + 1) = rl + D$,
- $\lambda = s - 1 + t(\alpha - 1) = \mu + r + l$,
- le fait que le nombre d'arêtes du graphe e puisse se déduire de α, s et t ; c'est également un autre moyen de retrouver v (cf. la constitution du graphe de $gp(s, t, \alpha)$).

Quel pourrait être l'intérêt véritable des géométries partielles ? Eh bien, il s'agit d'une autre partition du graphe de Pauli, « moins complexe » au sens géométrique puisque c'est un espace presque linéaire, et qu'elle possède moins de lignes que l'espace symplectique associé. Par exemple, dans le cas des 3 qubits, l'espace polaire symplectique associé au graphe de Pauli possède 135 lignes, tandis que la géométrie partielle, elle, « seulement » 45 ($45 \times 3 = 135$). Peut-être – cela reste une question ouverte – que les 45 ensembles d'opérateurs de Pauli généralisés disjoints, « révélés » et organisés en partition par ces 45 lignes, ont un sens physique particulier du fait de leur particularité, comme ce fut le cas pour la géométrie des 2 qubits, qui « révéla » les ensembles maximalement commutant.

5.3 Les systèmes composites

5.3.1 Motivations

5.3.1.1 Les espaces de Hilbert composites

Une idée naturelle, à la suite de la généralisation de la section précédente, est d'étudier les cas composites, caractérisés par un autre type d'opérateurs de Pauli généralisés. Le cas le plus simple est celui de l'alliance qubit-qutrit.

Un **qutrit** est un système à trois niveaux, au sens de la mécanique quantique et il s'écrira comme un vecteur colonne unitaire à 3 composantes.

De manière générale, on appellera **qudit** le vecteur d'état décrivant un système quantique attaché à un espace de Hilbert de dimension d, $\mathcal{H}_d$.

Pour d une dimension égale à un nombre premier p, une manière de caractériser les systèmes composites est la suivante : on construit [BBRV02] une base orthonormée d'un espace de Hilbert de dimension p en utilisant les opérateurs de Pauli X et Z, nommés également opérateurs *shift* et *clock*. Leurs actions respectives sont :

$$X\left|n\right\rangle = \left|n+1\right\rangle \text{ et } Z\left|n\right\rangle = \omega_p^n \left|n\right\rangle \text{ avec } \omega_p = e^{\frac{2i\pi}{p}} \text{ (racine } p^{\text{ième}} \text{ de l'unité)} \tag{5.10}$$

La base associée (il s'agit de la base des opérateurs de Pauli généralisés) sera alors sous la forme [BBRV02, KSSdG05] :

$$\{Z^k\}; k = 1, ..., p-1 \text{ et } \{(XZ^m)^k\}\,;\, k = 1, ..., p-1\ ,\ m = 0, ..., p-1 \tag{5.11}$$

Ses composantes sont regroupées en $p+1$ classes disjointes contenant chacune $p-1$ opérateurs qui commutent deux à deux. On a au total p^2-1 opérateurs, plus l'opérateur identité, la matrice I_p, que l'on ne fait pas toujours intervenir du fait de son action triviale. De telles classes sont maximales en terme de cardinal. Les vecteurs propres communs de différentes classes forment différents ensembles complets de *MUBs* [BBRV02, KSSdG05].

Le cas le plus simple ($p = 2$) correspond au qubit et il s'agit des 4 matrices de Pauli habituelles.

Le cas suivant ($p = 3$) correspond à un système physique à 3 niveaux : le qutrit. Une base orthonormale d'opérateurs pour un tel système sera [Law04] :

$$\sigma_I = \{I_3, Z, X, Y, Z^2, X^2, Y^2, V, V^2\} \text{ pour } I = 1, 2, ..., 9 \text{ avec}$$

$$X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \text{ où } \omega = e^{\frac{2i\pi}{3}}, Y = XZ \text{ et } V = XZ^2$$

Comment caractériser un système de dimension composite ? Eh bien en utilisant le

dernier postulat de la mécanique quantique : par exemple, pour un système à 6 niveaux, on effectue le produit tensoriel entre les opérateurs de Pauli pour 1 qubit, et ceux pour 1 qutrit. On aurait pu également définir une base pour un espace de Hilbert de dimension 6 directement à partir de *shift* et *clock*, bien que ces opérateurs aient une forme un peu différente des matrices de Pauli originelles [Kib08], puisque 6 n'est pas un nombre premier, mais le choix a été fait de séparer le système à deux niveaux de celui à trois. En effet, il s'agit d'une étude des relations de commutation et de la complémentarité quantique, et ce choix permet de mieux appréhender le rôle des *MUBs* des différents systèmes les unes par rapport aux autres.

5.3.1.2 Les systèmes composites par l'algèbre

Dans cette section, on aura à faire à une dimension d, où d est un produit de nombres premiers *distincts*. Quand on parlera de groupe de Pauli et d'opérateurs X et Z en dimension d, on utilisera implicitement la représentation du groupe de Pauli issue de produits tensoriels entre les opérateurs X et Z qui ont déjà été présentés dans la section 5.3.1.1.

Munis de la loi de multiplication, les opérateurs X et Z génèrent le groupe de Pauli G (non commutatif) à partir de la relation [HS07] :

$$ZX = \omega XZ$$

A partir de là a été montré [Vou07, HS07] que les éléments de G pouvaient être mis sous la forme suivante :

$$\omega^a X^b Z^c \text{ où } a, b, c \in \mathbb{Z}_d$$

On peut réduire le nombre d'éléments du groupe de Pauli, nombre égal à d^3, à d^2 en considérant le quotient de G par son centre G' : G/G' (cf. section A.1.3).

La référence [HS07] décrit les relations de commutation entre les opérateurs de G et de G/G', d'une part en utilisant les vecteurs (b, c) appartenant à $\mathbb{Z}_d^2$ et en considérant leur sous module cyclique (cf. section A.2.3), défini comme suit :

$$\mathbb{Z}_d(b, c) = \{(ub, uc), u \in \mathbb{Z}_d\},$$

et d'autre part, en mettant à contribution les points de la droite projective :

$$\mathcal{P}_1(\mathbb{Z}_d) = \{\mathbb{Z}_d(b, c), (b, c) \text{ est admissible}\}.$$

Pour rappel, un vecteur admissible (b, c) est tel que :

$$\exists (x, y) \in \mathbb{Z}_d^2, \begin{pmatrix} b & c \\ x & y \end{pmatrix} \text{ est inversible,}$$

ce qui pour une matrice à coefficients dans un anneau commutatif est équivalent à avoir un déterminant égal à l'une des unités de cet anneau.

Une classe d'équivalence de (b, c) est un sous module cyclique libre $\mathbb{Z}_d(b, c)$, d'ordre d, et aussi un point de la droite projective $\mathcal{P}_1(\mathbb{Z}_d)$.

On rappelle (afin de pouvoir faire un parallèle avec le paragraphe suivant concernant la définition d'un ensemble perpendiculaire) la structure de graphe de la droite projective $\mathcal{P}_1(\mathbb{Z}_d)$: deux points distincts $\mathbb{Z}_d(b, c)$ et $\mathbb{Z}_d(b', c')$ sont dits **distants** si

$$det \left| \begin{pmatrix} b & c \\ b' & c' \end{pmatrix} \right| \text{ est égal à une unité de } \mathbb{Z}_d,$$

sinon ils sont dits **voisins**.

Un autre concept intéressant permet de répartir les vecteurs appartenant à $\mathbb{Z}_d^2$ différemment : on définit un ensemble perpendiculaire (à ne pas confondre avec l'hyperplan du même nom d'un quadrangle) $(b, c)^\perp$ comme suit :

$$(b, c)^\perp = \{(u, v) \in \mathbb{Z}_d^2, (b, c) \perp (u, v)\} \text{ où} (b, c) \perp (u, v) \text{ si } det \left| \begin{pmatrix} b & c \\ u & v \end{pmatrix} \right| = 0$$

On note [PB07] d'ores et déjà que deux vecteurs appartenant au sous module cyclique libre sont mutuellement perpendiculaires. Selon [HS07], les opérateurs de G qui commutent avec un opérateur fixé constituent un ensemble perpendiculaire. En utilisant cette analogie, on peut identifier les éléments d'un sous module cyclique libre qui sont mutuellement perpendiculaires, avec les ensembles maximaux d'opérateurs de Pauli qui commutent, comme cela a déjà d'ailleurs été fait implicitement dans [PBS07]. *A posteriori* on ne devrait pas être surpris que la droite projective $\mathcal{P}_1(\mathbb{Z}_6)$ corresponde à la structure d'incidence des ensembles maximaux commutant du système qubit-qutrit (cf. section 5.3.2). Pour compléter cette vision géométrique des relations de commutation, il faut identifier les vecteurs (pas nécessairement admissibles) de $\mathbb{Z}_d^2$ avec les d^2 opérateurs de Pauli.

Le théorème 1 de la référence [HS07] énonce qu'un sous module cyclique libre $\mathbb{Z}_d(b', c')$ contenant un vecteur (b, c) appartient à l'ensemble perpendiculaire $(b, c)^\perp$. Seulement si (b, c) est admissible, le dit module est égal à $(b, c)^\perp$.

Cela va dans le sens de l'interprétation [PB07] selon laquelle les ensembles maximaux d'opérateurs qui commutent (qui correspondent à $\mathbb{Z}_d(b, c)$) définissent également une base d'opérateurs (correspondant à $(b, c)^\perp$).

Une conséquence immédiate concerne l'application aux *MUBs*. Deux vecteurs d'une bases seront perpendiculaires tandis que deux vecteurs de deux *MUBs* distinctes ne le seront pas. En utilisant deux vecteurs distincts non nuls et admissibles (b, c) et (b', c'), les deux ensembles de vecteurs :

$$\mathbb{Z}_d(b, c)\backslash\{(0, 0)\} = \{(ub, uc), u \in \mathbb{Z}_d\backslash\{0\}\} \text{ et } \mathbb{Z}_d(b', c')\backslash\{(0, 0)\} = \{(vb', vc'), v \in \mathbb{Z}_d\backslash\{0\}\}$$

sont disjoints seulement si :

$$uv(bc' - cb') \neq 0$$

c'est-à-dire si

$$uv \neq 0 \text{ et } (b, c), (b', c') \text{ ne sont pas perpendiculaires}$$

On ne peut pas « partitionner » en termes d'ensembles maximaux commutant car il n'y en a pas du fait que l'anneau $\mathbb{Z}_d$ possède des diviseurs de 0, qui est donc tel que u et v peuvent être des diviseurs de 0. Le nombre maximum de *MUBs* en dimension composite pourrait ainsi être reformulé comme étant le nombre maximum de tels ensembles de vecteurs disjoints dans l'anneau associé à la dimension en question [PB07].

Si la dimension d est la puissance de nombres premiers distincts p_k, le théorème 2 de la référence [HS07] produit des résultats quantitatifs à propos de :

- le nombre de points, noté n_d, de la droite projective $P_1(\mathbb{Z}_d)$ contenant tout vecteur (b, c)
- le partitionnement de $(b, c)^\perp$ comme étant l'union (au sens de la théorie des ensembles) de ces points
- la cardinalité de $(b, c)^\perp$

On a en effet d'après ce théorème :

$$n_d = \prod_{k \in \mathcal{K}} (p_k + 1) \text{ et } \left|(b, c)^\perp\right| = \prod_{k \in \mathcal{K}} p_k \tag{5.12}$$

où $\mathcal{K}$ est un l'ensemble des indices relatives à la décomposition des composantes de (b, c) en ses idéaux principaux.

On va maintenant aborder dans le détail des cas particuliers de systèmes composites. Selon les systèmes, on privilégiera les aspects les plus pertinents.

5.3.2 Le système qubit-qutrit

Rien est véritablement ressorti de l'étude de la géométrie du graphe de Pauli associé : le graphe de Pauli n'étant pas fortement régulier dans ce cas-ci, on ne peut pas lui associer de géométries partielles ou d'espaces polaires symplectiques comme cela avait été le cas pour les qubits, *a fortiori* une géométrie plus simple comme cela a été fait dans le cas particulier des 2 qubits. C'est pourquoi, on a directement considéré son dual [PS08] : les sommets deviennent les ensembles maximalement commutant (au nombre de 12), reliés si les 2 ensembles considérés ont au moins un opérateur en commun. Le graphe obtenu pour la dimension 6 (les résultats obtenus sont également valables pour le cas qutrit-qubit) est une grille 3×4 et donne lieu à une géométrie « multi-ligne », contrairement au cas des 2 qubits pour lesquels les graphes sont simples (simples, au sens de la théorie des graphes). En revanche, cette grille se révèle être la droite projective sur l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$, munie de la structure définie précédemment pour les qubits, dans lesquels cas on obtenait

seulement des « tronçons » de droites projectives ; il en va de même pour les 2 qutrits. On va maintenant voir tout cela un peu plus dans le détail [PBS07].

Sa géométrie « multi-ligne » :

Pour un système quantique de dimension $d = 6$, il y a 35 $(6^2 - 1)$ opérateurs de Pauli généralisés :

$$\sum_{(i,j)} = \sigma_i \otimes \sigma_j, i \in \{0, ..., 3\}, j \in \{0, ..., 8\}, (i, j) \neq (0, 0) \tag{5.13}$$

On les notera de manière plus compacte de la façon suivante :

$$\begin{aligned} 1 &= I_2 \otimes \sigma_1,\ 2 = I_2 \otimes \sigma_2, ..., 8 = I_2 \otimes \sigma_8 \\ a &= \sigma_z \otimes I_3,\ 9 = \sigma_z \otimes \sigma_1,\ 10 = \sigma_z \otimes \sigma_2, ... \\ b &= \sigma_x \otimes I_3,\ 17 = \sigma_x \otimes \sigma_1, ... \\ c &= \sigma_y \otimes I_3,\ 25 = \sigma_y \otimes \sigma_1, ..., 32 = \sigma_y \otimes \sigma_8 \end{aligned}$$

On a calculé la matrice d'adjacence du graphe de Pauli $P[6]$ et déduit de celle-ci 12 ensembles maximaux d'opérateurs qui commutent (comme expliqué dans le cas des 2 qubits, on cherche les sous graphes complets) :

$$\begin{aligned} L_1 &= \{1, 5, a, 9, 13\}, & L_2 &= \{2, 6, a, 10, 14\} \\ L_3 &= \{3, 7, a, 11, 15\}, & L_4 &= \{4, 8, a, 12, 16\} \\ M_1 &= \{1, 5, b, 17, 21\}, & M_2 &= \{2, 6, b, 18, 22\} \\ M_3 &= \{3, 7, b, 19, 23\}, & M_4 &= \{4, 8, b, 19, 24\} \\ N_1 &= \{1, 5, c, 25, 29\}, & N_2 &= \{2, 6, c, 26, 30\} \\ N_3 &= \{3, 7, c, 27, 31\}, & N_4 &= \{4, 8, c, 28, 32\} \end{aligned}$$

On considère ces ensembles comme des lignes au sens de la géométrie projective. Si on identifie chacune de ces lignes, respectivement deux lignes concourantes, à un sommet, respectivement à une arête du graphe dual de $P[6]$, noté $W[6]$, on obtient la structure de graphe de type grille 3×4 représentée à droite de la figure 5.7. Ce graphe correspond à $L[K(4, 3)]$, c'est-à-dire le graphe d'incidence du graphe bipartite $K(4, 3)$ représenté à gauche de la figure 5.7.

Les lignes L_i (ainsi que les lignes M_i et N_i) prises deux par deux ont un unique point d'intersection, tandis que les lignes L_i et M_I (idem pour L_i et N_i, M_i et N_i) possèdent deux points en commun. Cela signifie que les arêtes du graphe $W[6]$ ont deux « poids » possibles : « 1 » ou « 2 » (les arêtes de poids « 2 » sont indiquées sur la figure 5.7).

Le graphe $L[K(4, 3)]$ est régulier et de spectre $\{-2^6, 1^3, 2^2, 5\}$. Les *MUBs* correspondent aux lignes du graphe de Pauli $P[6]$ qui ne sont pas concourantes, c'est-à-dire, ici, aux sommets de $L[K(4, 3)]$ qui ne sont pas adjacents. Si on considère la partie de droite de la figure 5.7, on en trouve au maximum trois, comme cela a déjà pu être constaté dans d'autres travaux [Gra06].

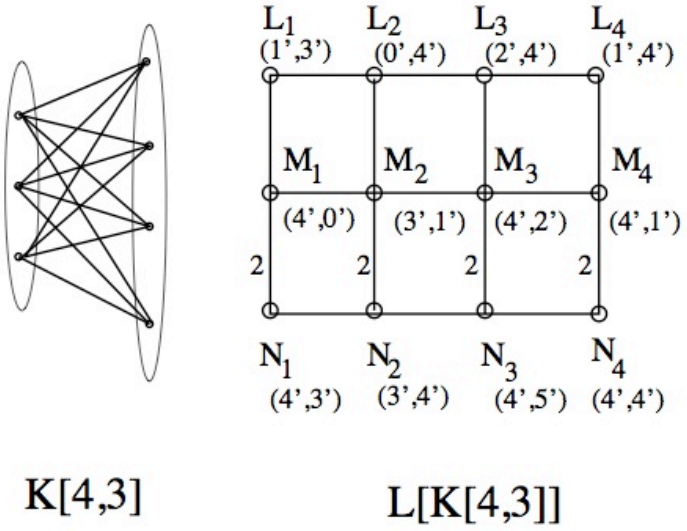


FIG. 5.7 – Le dual du graphe de Pauli pour $d = 6$, $W[6]$, est le graphe $L[K(4,3)]$.

Jusqu'à maintenant on a considéré le dual du graphe de Pauli mais qu'en est-il de celui-ci ? En étudiant de plus près sa matrice d'adjacence et en gardant la même numérotation que précédemment, on a pu caractériser sa géométrie sous-jacente. Avant d'aller plus loin, on a besoin de la définition d'une figure de la géométrie projective dite géométrie finie (0,1), c'est-à-dire une géométrie vérifiant les deux axiomes suivants :

- deux points distincts sont reliés par au maximum une ligne,
- pour une ligne donnée et un point n'appartenant pas à la ligne (un anti-drapeau), soit aucune ligne, soit une ligne passe par ce point et est concourante avec la ligne donnée,

La géométrie de $P[6]$ possède des lignes qui partagent plus d'un point et ainsi viole-t-elle le premier axiome. Cela donne lieu à une géométrie « multi-ligne ». En revanche, la géométrie de $P[6]$ respecte le deuxième axiome. Ainsi peut-on « partitionner » (partition analogue au fait de considérer les hyperplans de la géométrie (0,1)) la géométrie du graphe de Pauli en considérant les sous ensembles de ses points tels que si deux points appartiennent à une ligne alors cette ligne appartient à l'ensemble. Ces ensembles, notés S_i, que par abus de langage on nommera hyperplans, sont explicités dans l'équation 5.14 et l'un d'entre eux, S_1, est représenté dans la figure 5.8.

$$S_i = \{L_i, M_i, N_i\},\ i \in \{1,2,3,4\} \tag{5.14}$$

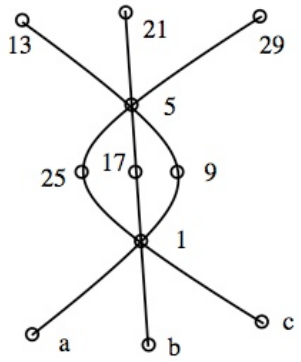


Fig. 5.8 – Structure de $S_1 = \{L_1, M_1, N_1\}$

Sa droite projective :

Dans le cas des 2 qubits, le carré de Peres et Mermin (cf. chapitre 4) peut être vu comme la droite projective définie sur l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_2$, et la géométrie des 2 qubits est englobée par la droite projective définie sur le plus petit anneau constitué des matrices 2×2 à valeurs 0 ou 1, noté $\mathbb{Z}_2^{2\times2}$ [PSK06]. On va montrer que le graphe $W[6]$ peut également être vu comme la droite projective sur l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$.

On note les éléments de l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$ de la manière suivante :

$$0' = (0,0)\ ,\ 1' = (0,1)\ ,\ 2' = (0,2)\ ,\ 3' = (1,0)\ ,\ 4' = (1,1) \text{ et } 5' = (1,2)$$

Ces tables d'addition et de multiplication sont respectivement les tableaux 5.8 et 5.9

+	0'	1'	2'	3'	4'	5'
0'	0'	1'	2'	3'	4'	5'
1'	1'	2'	0'	4'	5'	3'
2'	2'	0'	1'	5'	3'	4'
3'	3'	4'	5'	0'	1'	2'
4'	4'	5'	3'	1'	2'	0'
5'	5'	3'	4'	2'	0'	1'

Tab. 5.8 – La table d'addition de l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$

×	0'	1'	2'	3'	4'	5'
0'	0'	0'	0'	0'	0'	0'
1'	0'	1'	2'	0'	1'	2'
2'	0'	2'	1'	0'	2'	1'
3'	0'	0'	0'	3'	3'	3'
4'	0'	1'	2'	3'	4'	5'
5'	0'	2'	1'	3'	5'	4'

Tab. 5.9 – La table de multiplication de l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$

On constate d'après ces tables que l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$ possède :

– 4 diviseurs de 0 : $0'$, $1'$, $2'$ et $3'$,

– 2 unités : $4'$ et $5'$.

En usant de la définition d'une droite projective (cf. annexe B), on calcule qu'elle est constituée des 12 points suivants :

– $(4',0')$, $(4',1')$, $(4',2')$, $(4',3')$, $(0',4')$, $(1',4')$, $(2',4')$ et $(3',4')$: 8 d'entre eux possèdent une unité

– $(4',4')$ et $(4',5')$: deux d'entre eux possèdent deux unités

– $(1',3')$ et $(3',1')$: deux d'entre eux possèdent deux diviseurs de 0

Ces points munis de la structure de graphe coïncident avec la structure du graphe $L[K(4,3)]$ de la figure 5.7 dans laquelle ils ont d'ailleurs été explicités. Le graphe $W[6]$ peut donc bien être vu comme la droite projective sur l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Illustration

Illustrons les relations entre le graphe de Pauli pour le système qubit-qutrit et la structure de graphe de la droite projective $\mathcal{P}_1(\mathbb{Z}_6)$. Les opérateurs x appartenant aux ensembles maximaux sont de 3 types [PB07] :

– x est un des points de référence : a_0, b_0 ou c_0, il appartient à 4 ensembles et le nombre de points qui commutent avec lui est $\left|x^{\perp}\right| = 18$ points de type (i)),

– $x \in \{1,2,3,4,5,6,7,8\}$ appartient à 3 ensembles et $\left|x^{\perp}\right| = 12$ (points de type (ii)),

– sinon x appartient à un seul ensemble et $\left|x^{\perp}\right| = 6$ (points de type (iii))

Remarque : un ensemble perpendiculaire $\left(x^{\perp}\right)$ inclut l'opérateur x lui-même et l'opérateur unité [HS07] mais pour les ensembles maximaux commutant il est d'usage d'ignorer l'opérateur unité car il commute avec tous les opérateurs [PS08, BBRV02].

Ces résultats sont en accord avec l'expression de l'équation 5.12 avec $d = 6$, $p_1 = 2$ et $p_2 = 3$.

Un ensemble perpendiculaire $\left(x^{\perp}\right)$ attaché aux points de type (ii) est représenté par la figure 5.8. La structure complète comprend 4 ensembles similaires (les S_i) ayant les opérateurs a_0, b_0 et c_0 en commun.

5.3.3 Le système qutrit-qutrit

Suite à l'étude du cas composite le plus simple et des constats qui ont été faits, il est naturel de s'intéresser au cas des 2 qutrits (d=9), bien qu'il ne soit pas un système composite à proprement parler puisqu'il fait intervenir deux particules de même nature, pour mieux cerner à quel niveau le cas qubit-qutrit diffère tant de celui des 2 qubits.

Pour un système quantique de dimension $d = 9$, il y a 80 opérateurs de Pauli générali-

sés :

$$\sum_{(i,j)} = \sigma_i \otimes \sigma_j, i \in \{0,...,8\}, j \in \{0,...,8\}, (i,j) \neq (0,0) \tag{5.15}$$

On les notera de manière plus compacte de la façon suivante :

$$\begin{aligned}
1 &= I_3 \otimes \sigma_1,\ 2 = I_3 \otimes \sigma_2, ..., 8 = I_3 \otimes \sigma_8 \\
a &= \sigma_1 \otimes I_3,\ 9 = \sigma_1 \otimes \sigma_1,\ 10 = \sigma_1 \otimes \sigma_2, ... \\
b &= \sigma_2 \otimes I_3,\ 17 = \sigma_2 \otimes \sigma_1, ... \\
c &= \sigma_3 \otimes I_3,\ 25 = \sigma_3 \otimes \sigma_1, ..., 32 = \sigma_3 \otimes \sigma_8 \\
d &= \sigma_4 \otimes I_3, ..., h = \sigma_8 \otimes I_3, 64 = \sigma_8 \otimes \sigma_1, ..., 72 = \sigma_8 \otimes \sigma_8
\end{aligned}$$

En calculant le spectre du graphe $P[9] : \{-7^{15}, -1^{40}, 5^{24}, 25\}$, on constate que le graphe est régulier, de degré 25, mais pas fortement régulier. Il est plus difficile d'identifier des sous graphes pertinents comme ce fut le cas pour les 2 qubits, donc, afin de tenter de trouver la géométrie sous jacente du système, on va considérer le dual de $P[9]$ (comme pour le cas qubit-qutrit), c'est-à-dire le graphe dont les sommets sont les ensembles maximaux d'opérateurs qui commutent, en voici la liste :

$$\begin{aligned}
L_1 &= \{1,5,a,9,13,e,41,45\}, & L_2 &= \{2,6,a,10,14,e,42,46\} \\
L_3 &= \{3,7,a,11,15,e,43,47\}, & L_4 &= \{4,8,a,12,16,e,44,48\} \\
M_1 &= \{1,5,b,17,21,f,49,53\}, & M_2 &= \{2,6,b,18,22,f,50,54\} \\
M_3 &= \{3,7,b,19,23,f,51,55\}, & M_4 &= \{4,8,b,20,24,f,52,56\} \\
N_1 &= \{1,5,c,25,29,g,57,61\}, & N_2 &= \{2,6,c,26,30,g,58,62\} \\
N_3 &= \{3,7,c,27,31,g,59,63\}, & N_4 &= \{4,8,c,28,32,g,60,64\} \\
P_1 &= \{1,5,d,33,37,h,65,69\}, & P_2 &= \{2,6,d,34,38,h,66,70\} \\
P_3 &= \{3,7,d,35,39,h,67,71\}, & P_4 &= \{4,8,d,36,40,h,68,72\} \\
X_1 &= \{9,22,32,39,45,50,60,67\}, & X_2 &= \{10,17,27,40,46,53,63,68\} \\
X_3 &= \{11,20,30,33,47,56,58,69\}, & X_4 &= \{12,23,25,34,48,51,61,70\} \\
X_5 &= \{13,18,28,35,41,54,64,71\}, & X_6 &= \{14,21,31,36,42,49,59,72\} \\
X_7 &= \{15,24,26,37,43,52,62,65\}, & X_8 &= \{16,19,29,38,44,55,57,66\} \\
Y_1 &= \{9,23,30,40,45,51,58,68\}, & Y_2 &= \{10,19,32,33,46,55,60,69\} \\
Y_3 &= \{11,22,25,36,47,50,61,72\}, & Y_4 &= \{12,17,26,39,48,53,62,67\} \\
Y_5 &= \{13,20,27,34,41,56,63,70\}, & Y_6 &= \{14,23,28,37,42,51,64,65\} \\
Y_7 &= \{15,18,29,40,43,54,57,68\}, & Y_8 &= \{16,21,30,35,44,49,58,71\} \\
Z_1 &= \{9,24,31,38,45,52,59,66\}, & Z_2 &= \{10,24,25,35,46,52,61,71\} \\
Z_3 &= \{11,17,28,38,47,53,64,66\}, & Z_4 &= \{12,18,31,33,48,54,59,69\} \\
Z_5 &= \{13,19,26,36,41,55,62,72\}, & Z_6 &= \{14,20,29,39,42,56,57,67\} \\
Z_7 &= \{15,21,32,34,43,49,60,70\}, & Z_8 &= \{16,22,27,37,44,50,63,65\}
\end{aligned}$$

Afin de trouver une « partition » pertinente pour ces 40 bases de $P[9]$, comme cela a été fait pour le cas des 2 qubits (mais directement sur le graphe de Pauli associé, cf.

section 5.1.3), on a cherché à utiliser les hyperplans du quadrangle généralisé d'ordre 3, $Q(4,3)$. Ce quadrangle est formé des points et des lignes d'une quadrique parabolique dans l'espace projectif $PG(4,3)$ [PBS07] (c'est-à-dire l'espace projectif de dimension 4, défini sur le corps de Galois à 3 éléments $\mathbb{Z}_3$).

On a vu que le quadrangle généralisée d'ordre 2, $W(2)$, possède 3 types d'hyperplans ; il en va de même pour le quadrangle $Q(4,3)$ (cf. section B.3.1).

Où des hyperplans révèlent une géométrie « multi-ligne » :

On observe directement que les 16 lignes L_i, M_i, N_i et P_i (pour $i \in \{1,2,3,4\}$) ont deux points communs deux à deux et forment ainsi une grille 4×4 d'ordre (3,1). Une grille de $W[9]$ est représentée à titre d'exemple sur la figure 5.9a. Chaque ensemble $\{i\}$ des points caractérisé par :

$$S_i = \{L_i, M_i, N_i, P_i\}, i \in \{1,2,3,4\} \tag{5.16}$$

représente un hyperplan « multi-ligne » de la géométrie associée au graphe de Pauli $P[9]$. Toutes les arêtes de la grille sont de « poids » 2. La figure 5.9b explicite l'hyperplan en question pour i=1 (pour chaque hyperplan i, on doit rajouter outre les points des lignes concernés, les 8 points de référence a, b,..., h).

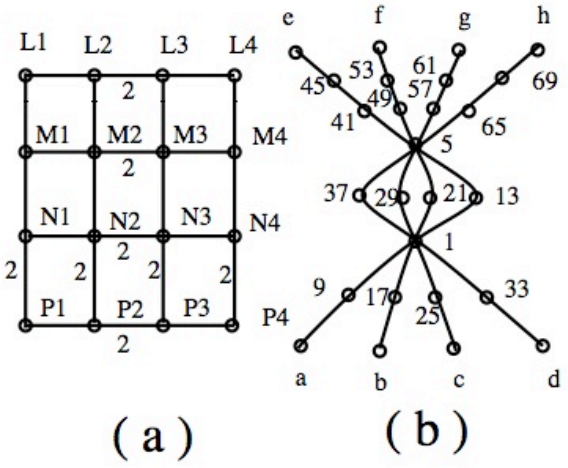


FIG. 5.9 – Une grille de $W[9]$ et la géométrie correspondante chez $P[9]$ pour i=1

La figure 5.10 montre un ovoïde constitué de 10 points (c'est-à-dire un ensemble de 10 points non colinéaires deux à deux de $W[9]$ (a) et ce à quoi il correspond dans la géométrie de $P[9]$ (b) : un ensemble de 10 lignes parallèles, ou encore dites disjointes ; les bases associées aux opérateurs sur deux lignes distinctes sont des *MUB's*, ensemble, elles forment un ensemble complet de *MUB's* pour cette dimension.

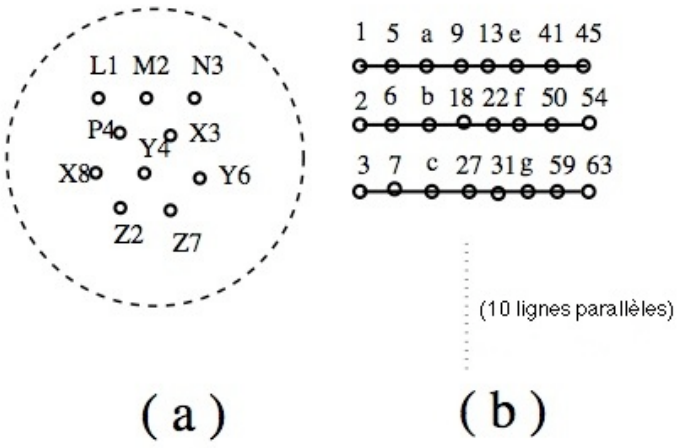


Fig. 5.10 – Un ovoïde de $W[9]$ et la géométrie correspondante chez $P[9]$

La figure 5.11 donne un exemple d'ensembles perpendiculaires de $W[9]$ (a) ainsi que la géométrie « multi-ligne » qui en découle pour $P[9]$ (b). La figure 5.11b ne montre le détail que de la ligne $\{L_1, N_4, M_2, P_3\}$ et comme on le voit c'est déjà assez complexe.

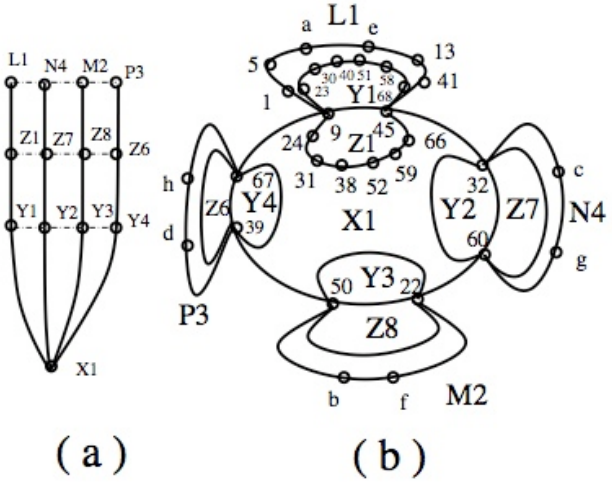


Fig. 5.11 – Un ensemble perpendiculaire de $W[9]$ et la géométrie correspondante chez $P[9]$ pour la ligne $\{L_1, N_4, M_2, P_3\}$

La droite projective pour les 2 qutrits :

Une étude [aMS07] a permis de déterminer que les 2 qutrits étaient caractérisés de façon partielle (on a parlé de « tronçons » au tout début de cette section) par la droite projective sur l'anneau $\mathbb{Z}_2^{\times 3}$.

5.3.4 Les qudits en dimension 12

Pour un système quantique de dimension $d = 2^2 \times 3 = 12$, les opérateurs de Pauli généralisés sont de la forme :

$$\sigma_i \otimes \sigma_j \otimes \sigma_k \text{ où } i, j \in \{0, ..., 3\}, k \in \{0, ..., 8\} \text{ et } (i, j, k) \neq (0, 0, 0) \tag{5.17}$$

Comme pour les autres cas, on détermine le graphe de Pauli correspondant et on extrait ces sous-graphes complets maximaux. On constate que la matrice d'incidence des ensembles maximaux commutant correspondant correspond à la droite projective définie sur l'anneau $\mathcal{R} = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{F}_{q^2}$, d'ordre $|\mathcal{R}| = (p_1 + 1)(p_2 + 1)(q^2 + 1)$, pour lequel $p_1 = q = 2$ et $p_2 = 3$.

Les opérateurs x appartenant aux ensembles maximaux sont de 3 types :

1. x est un des points de référence (son produit tensoriel inclut I_3), il appartient à $(p_1 + 1)(p_2 + 1) = 12$ ensembles et $\left|x^\perp\right| = dp_1p_2 = 72$ (points de même type (i) que pour le cas qubit-qutrit),
2. x inclut $I_2 \otimes I_2$ dans sa décomposition en produit tensoriel et appartient à $(p_1 + 1)(q^2 + 1) = 15$ ensembles et $\left|x^\perp\right| = dp_1q = 48$ (points de type (ii)),
3. sinon x appartient à $p_1 + 1 = 3$ ensembles et $\left|x^\perp\right| = p_1d = 24$ (points de type (iii))

5.3.5 Les qudits en dimension 18

Pour un système quantique de dimension $d = 2 \times 3^2 = 18$, les opérateurs de Pauli généralisés sont de la forme :

$$\sigma_i \otimes \sigma_j \otimes \sigma_k \text{ où } i \in \{0, ..., 3\}, j, k \in \{0, ..., 8\} \text{ et } (i, j, k) \neq (0, 0, 0) \tag{5.18}$$

Encore une fois, on détermine le graphe de Pauli correspondant et on extrait ces sous-graphes complets maximaux. On constate que la matrice d'incidence des ensembles maximaux commutant correspondant correspond à la droite projective définie sur l'anneau $\mathcal{R} = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_2}$, d'ordre $|\mathcal{R}| = (p_1 + 1)(p_2 + 1)^2$, pour lequel $p_1 = 2$ et $p_2 = 3$.

Les opérateurs x appartenant aux ensembles maximaux sont de 5 types :

1. x est un des 3 points de référence contenant $I_3 \otimes I_3$ dans sa décomposition en produit tensoriel, il appartient à $(p_2 + 1)^2 = 16$ ensembles et $\left|x^\perp\right| = dp_2^2 = 162$ (points de type (i)),
2. x appartient à $(p_1 + 1)(p_2 + 1) = 12$ ensembles et $\left|x^\perp\right| = dp_1p_2 = 108$ (points de type (ii)),
3. x appartient à $p_2 + 1 = 4$ ensembles et $\left|x^\perp\right| = dp_2 = 24$ (points de type (iii))
4. x appartient à $p_1 + 1 = 3$ ensembles et $\left|x^\perp\right| = dp_1p_2 = 108$ (points de type (iv))
5. sinon x appartient à un seul ensemble et $\left|x^\perp\right| = dp_2 = 24$ (points de type (v))

5.3.6 Généralisation et discussion

De manière générale, dans le cas des dimensions autres que 2^N, la géométrie associée est plus complexe car « multi-ligne » (en terme de théorie des graphes, le graphe de Pauli n'est plus fortement régulier, et il n'y a plus de possibilité de « lissage » comme dans le cas des N qubits). Pour les dimensions composites (par exemple ce n'est pas vrai pour les 2 qutrits qui sont deux systèmes physiques « de même nature »), il ***semble*** (cela n'a été démontré que pour des cas particuliers [PBS07, PB07]) que tout devient très simple en terme de droites projectives, ce qui n'est pas vrai pour l'ensemble des autres dimensions puisque les droites projectives sur les anneaux respectifs ne caractérisent à chaque fois qu'un « morceau » de la partition, comme cela a été vu dans le détail pour les 2 qubits. L'hypothèse actuelle dans l'optique de généraliser est la suivante : on considère la décomposition en facteurs premiers des nombres qui représentent des dimensions composites, par exemple :

$$6 = 2 \times 3; 10 = 2 \times 5; 12 = 2^2 \times 3; 14 = 2 \times 7; 15 = 3 \times 5; 18 = 2 \times 3^2$$

On va considérer et les diviseurs premiers, et la totalité des diviseurs : par exemple, pour « 12 », on prendra en compte « 2 », « 4 » et « 3 », pas uniquement « 2 » et « 3 ». On aura alors une droite projective, pour les dimensions ci-dessus, sur, respectivement, les anneaux suivants :

$$\mathbb{Z}_2 \times \mathbb{Z}_3; \mathbb{Z}_2 \times \mathbb{Z}_5; \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3; \mathbb{Z}_2 \times \mathbb{Z}_7; \mathbb{Z}_3 \times \mathbb{Z}_5; \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \tag{5.19}$$

On a trouvé en parallèle que les opérateurs qui commutent associés aux qudits, correspondent à des vecteurs perpendiculaires appartenant au module $\mathbb{Z}_d^2$. Les ensembles maximaux commutant ont une structure similaire à celles des sous modules libres cycliques définis sur un anneau commutatif $\mathcal{R}$, qui n'est pas systématiquement l'anneau $\mathbb{Z}_d$ dès que d contient des carrés dans sa décomposition en nombres premiers. Un vecteur admissible, qui définit un tel sous module, est de deux types [SPKP07] :

1. au moins une de ses composantes est une unité de l'anneau $\mathcal{R}$
2. les deux composantes sont des diviseurs de 0 qui n'appartiennent pas au même idéal maximal de $\mathcal{R}$

Ainsi les idéaux maximaux sont-il à la base du lien entre les droites projectives et la structure des matrices d'adjacence qui décrivent les relations de commutation des opérateurs de Pauli généralisés pour les qudits.

La figure 5.12 représente les idéaux maximaux des anneaux associés aux cas composites qui ont été abordés sous forme d'ellipses. Leurs intersections sont représentées par de petits ronds, le rond noir représente l'élément 0 de l'anneau.

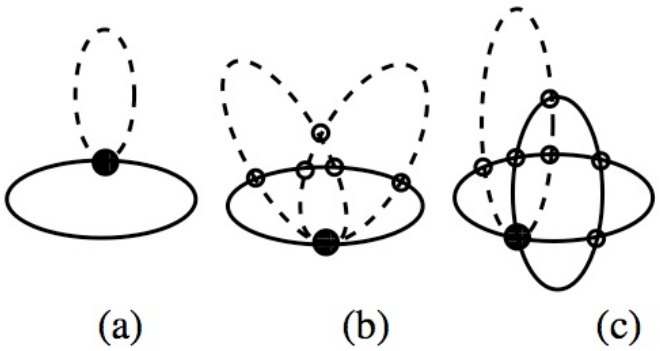


FIG. 5.12 – (a) Représentation des idéaux maximaux de l'anneau $\mathbb{Z}_2 \times \mathbb{Z}_3$ illustrant la structure d'adjacence du système composite qubit-qutrit. (b) Celle de $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ pour les 2 qubits-qutrit (c) Celle de $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{F}_4$

Dans une certaine mesure, on peut identifier les facteurs du système composite avec les idéaux maximaux, et les opérations d'union et d'intersection particulières à la théorie des ensembles régissant ces idéaux semblent correspondre avec la structure d'adjacence des relations de commutation au sein des systèmes composites associés. Les idéaux eux-même ont une structure d'anneau. Par exemple, les 3 idéaux du cas (c) représenté sur la figure 5.12 sont des sous ensembles isomorphes à $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{F}_4$ et $\mathbb{Z}_3 \times \mathbb{F}_4$ respectivement. Les droites projectives correspondantes sont des grilles 3×4, 3×5 et 4×5. La dernière grille exhibe un nombre maximum de 4 points distants, ce qui correspond au nombre maximum de *MUBs* trouvées en dimension 12.

Un nouveau travail pourrait clarifier si un anneau $\mathcal{R}$ est toujours associé à un quelconque système composite. Cela pourrait avoir entre autre une application au problème du sous groupe caché non abélien qui a déjà donné lieu à des algorithmes quantiques.

Conclusion

Pour les n qubits, l'exploration en terme de géométrie a révélé une structure connue : un quadrangle généralisé d'ordre 2 pour la dimension 4 et, au-delà, une structure d'espace symplectique (ce qui n'est pas si étonnant que cela puisque les formes symplectiques sont intimement liées au crochet de Poisson qui n'est d'autre que l'analogue classique du fameux commutateur utilisé en mécanique quantique). Pour les dimensions composites, il semblerait que l'on ait à faire à une géométrie « multi-lignes » que l'on ne puisse pas « exploiter » avec les géométries partielles, comme c'est le cas pour les N qubits, même si cela n'a été exploré que pour des exemples.

Par ailleurs, pour les dimensions composites, on a utilisé les idéaux maximaux d'un anneau $\mathcal{R}$ donné (qui peut être différent de l'anneau $\mathbb{Z}_d$) comme constituants des relations de commutations. On a vu que l'incidence (cf. figure 5.7) entre les 12 lignes du système qubit-qutrit correspond exactement à la structure de graphe associée à la droite projec-

tive définie sur l'anneau $\mathbb{Z}_6$, et obtenu des résultats similaires dans d'autres dimensions composites plus grandes : pour $d = 2 \times 5 = 10$, $d = 3 \times 5 = 15$, $d = 2 \times 3^2 = 18$ et $d = 2^2 \times 3 = 12$, l'incidence des ensembles maximaux correspondant sont similaires aux graphes des droites projectives définies respectivement sur les anneaux : $\mathbb{Z}_{10}$, $\mathbb{Z}_{15}$, $\mathbb{Z}_6 \times \mathbb{Z}_3$ et $\mathbb{Z}_6 \times \mathbb{F}_4$. L'irruption inattendue du corps de Galois à 4 éléments $\mathbb{F}_4$ au sein du modèle projectif du système 2 qubits-qutrit semble interdire une généralisation de ce modèle pour n'importe quelle dimension d, malgré tout, une étude plus poussée des droites projectives semble prometteuse.

Conclusion générale - Perspectives

Il est clair que l'on n'a pas établi dans ce travail de lien direct entre le calcul quantique tel qu'il a été présenté en partie I et les résultats de la partie II. On n'a pas su exploiter l'algèbre et la géométrie projective, telles qu'elles ont été abordées, pour construire de nouveaux algorithmes ou pour simplifier ceux qui existent, manque de temps ou tout simplement parce que c'est peut-être impossible. Pourtant l'idée de faire intervenir la théorie des graphes, une branche importante de l'informatique théorique, dans l'optique particulière qui fut la nôtre, se voulait pleine de promesses.

Malgré cela, l'étude de certains aspects de la mécanique quantique, qui interviennent de façon plus ou moins implicite dans le formalisme des différents modèles de calcul quantique, ont permis de mettre en évidence des analogies entre des concepts issus de différents domaines. Il est vrai que « travailler sur des analogies » peut se révéler dangereux : il arrive souvent qu'il ne s'agisse que de coïncidences. Mais il me semble que certaines d'entre elles qui sont apparues au cours de ce travail de thèse sont pertinentes. Par exemple, le constat que l'intrication soit liée à l'existence de diviseurs de zéros non triviaux présents au sein d'anneaux bien précis, diviseurs en rapport étroit avec une dégénérescence des valeurs propres, dégénérescence mise en évidence par les travaux de Peres et Mermin et leur fameux carré [Mer93], me semble une vision intéressante.

On a également établi des correspondances entre les bases mutuellement non biaisées, les MUBs, et des éléments d'algèbre et de géométrie projective. La notion de MUBs est fondamentale dans tous les protocoles quantiques et omniprésente dans deux des postulats de la mécanique quantique : le postulat de la mesure et celui décrivant la décomposition d'un système quantique en sous systèmes. S'il fallait vraiment prouver l'utilité de l'étude de ces bases, si cela n'a pas déjà été fait, il suffirait de constater qu'au sein de la communauté scientifique, nombreux sont ceux qui s'intéressent à leurs diverses applications ([BBRV02], [Gra06], [Law04], [LBZ02], [KSSdG05], [SPR04], [PR05], et bien d'autres). Il ne s'agit pas d'avoir l'instinct grégaire : on a déjà pu remarquer que, plusieurs fois par le passé, bon nombre de scientifiques avait traité d'une même idée au même moment. [1]

À propos des MUBs et comme résultat essentiel, on a vu dans le chapitre 4 qu'il y avait

[1] Ce fait est si bien avéré que les Grecs croyaient en l'existence d'une *noosphère*, littéralement une sphère des idées, dans laquelle les habitants, quelque soit leur lieu de villégiature, pouvait « piocher » en même temps.

une association possible entre les vecteurs propres communs d'opérateurs qui commutent générant des MUBs et les caractères additifs des anneaux de Galois.

Le chapitre 5 a mis en évidence la particularité des systèmes à 2 qubits. Ils possèdent une sorte de dualité que l'on perd dès que l'on s'intéresse à des systèmes quantique habitant des espaces de Hilbert de dimension supérieure à 4. La géométrie associée au 2 qubits est assez simple et, de ce point de vue, on a quand même pu généraliser ces résultats pour les systèmes à n qubits. En revanche, du point de vue des droites projectives liées à une structure de graphe et rattachées à des anneaux, l'étude n'a pas été concluante, même si elles interviennent de façon morcelée.

Quant aux systèmes composites, c'est sous une forme « sympatique », même si cela n'a été constaté que sur des exemples, qu'ils font leur apparition quand on aborde les droites projectives. La géométrie qu'on a voulu en dégager n'a par contre rien donné de réellement satisfaisant.

Pour conclure sur les chapitres 4 et 5, on a montré qu'il était possible d' « extraire » de nouvelles propriétés « d'êtres quantiques » par un formalisme fourni par la géométrie et l'algèbre. Mais cela reste très général et les travaux qui ont suivi, [Pla10b], [Pla09], [PS09], [PK10], [PJ08], [Pla10a], ont appliqué la même démarche sur des éléments plus ciblés. Il a semblé pertinent de considérer en premier lieu les opérations de Clifford (cf. section 3.1.2 du chapitre 3), puisqu'elles mettent en évidence ce qu'il y a de classique en calcul quantique. Ainsi cela pourrait-il permettre de mettre en relief ce qu'il y a de purement quantique en informatique quantique, comme cela a déjà été fait par le passé d'une autre façon (cf. chapitre 3).

Plus généralement, ces travaux se sont intéressés à la possibilité d'utiliser des concepts de la théorie des groupes tels que les commutateurs, les sous groupes normaux, les groupes d'automorphismes, les courtes séquences exactes, les produits couronnés, les extensions de groupes, etc. Ces concepts permettent de décrire ces opérations quantiques particulières que sont les matrices cliffordiennes, ainsi que des phénomènes quantiques, tels que la cohérence, afin de mieux les comprendre. Par exemple, les extensions sur les groupes finis offrent la possibilité de décrire de façon très compacte les aspects « cliffordiens » du calcul quantique. En bref, il s'agit de décrire l'action d'un ordinateur quantique en considérant deux groupes finis de portes quantiques. Le premier groupe englobe les portes décrivant les erreurs qu'il faudra corriger après l'action du calculateur, ce groupe provient du groupe général (en ce sens que l'on n'explicite plus le nombre de qubits auquel il se rattache) de Pauli $\mathcal{P}$. Le deuxième groupe de portes concerne les portes dites de Clifford qui découlent d'une extension du groupe général de Clifford $\mathcal{C}$. Les propriétés du groupe de Clifford sur 1 et 2 qubits en particulier ont déjà été détaillées dans [Pla09], [PS09], [PJ08], [Pla10a].

L'article [Pla11] constitue un bon résumé des travaux évoqués dans la partie II et dans la conclusion générale de cette thèse, et produit une généralisation de l'étude du graphe de Pauli pour les qudits. Tous ces travaux finalement s'intéressent à l'algèbre et à

la géométrie sous jacente de systèmes quantiques de dimension quelconque d et il serait intéressant de simplifier et d'englober ces résultats en les reliant si possible au calcul topologique quantique [Col06] qui, comme son nom l'indique, est un formalisme très inspiré des mathématiques et en particulier de la géométrie, plus que les autres modèles déjà mentionnés.

Une autre de mes perspectives est la suivante. L'approche algébrique qui a été évoquée dans le chapitre 4 permettrait d'aborder le problème d'existence des MUBs exposé dans le chapitre 5 sous un autre angle. Pour rappel, on ne connaît pas à l'heure actuelle le nombre maximum de MUBs pour un espace de Hilbert de dimension d quelconque, on sait seulement qu'il est égal au maximum à $d + 1$. De très nombreuses méthodes algébriques, géométriques, ou relevant de la théorie des graphes ([BBRV02], [Gra06], [Law04], [SPR04], [PS08], [PB07], [LBZ02], [Kib10], [Kib09], [KABW10], etc.) ont été utilisées pour la détermination des MUBs. On a abordé dans les chapitres 4 et 5 le problème du calcul des MUBs *via* les corps et anneaux de Galois, la géométrie projective et la théorie des graphes. Récemment, ce problème a été abordé via l'introduction d'une transformée de Fourier discrète **quadratique** [Kib10]. Or, une telle transformation fait apparaître des termes quadratiques qui ont des analogues en terme de caractères de corps et d'anneaux de Galois. Il serait donc intéressant d'établir un lien entre l'approche des références [Kib10], [Kib09], [KABW10], et une description plus poussée de l'approche algébrique du chapitre 4.

D'un point de vue plus personnel, en ce sens que cette perspective ne découle pas directement de mes travaux de thèse, je souhaite m'intéresser aux liens possibles entre calcul quantique et intelligence artificielle ([BF02], [SG04], [ABG06], [ABG07]).

Pour résumer, voici la liste de perspectives possibles pour cette thèse, ainsi que les miennes propres :

- continuer l'étude algébrique et géométrique du calcul quantique pour des éléments plus ciblés / dans le cadre d'une généralisation,
- relier les approches algébrique et géométrique du calcul quantique au calcul topologique,
- considérer le problème d'existence des MUBs en construisant un pont entre la transformée de Fourier discrète quadratique et les structures algébriques de Galois,
- faire (si possible) un post-doc en intelligence artificielle pour ensuite revenir à mes premières amours : le calcul quantique !

sans oublier d'avoir toujours à l'esprit que le questionnement est une des plus belles quêtes de l'aventure humaine.

ANNEXES

Annexe A

Un peu d'algèbre

A l'origine...

Au fur et à mesure que l'être humain apprend à manipuler des nombres, les problèmes se formalisent d'une manière plus abstraite. On a d'abord appris à résoudre tel ou tel problème particulier composé d'un ensemble de nombres et d'opérations bien déterminées (d'abord l'addition, la soustraction, puis la multiplication et la division). En voulant généraliser les méthodes de résolution, on est venu vers le Moyen Âge à abstraire l'inconnue (aujourd'hui le fameux x), c'est-à-dire à formuler des solutions de plus en plus génériques, pour un ensemble d'objets mathématiques de plus en plus large. Progressivement, les opérations elles-mêmes ont été abstraites et ont été identifiées à des **structures algébriques** (groupes, anneaux, corps, espaces vectoriels, ...). Ceci a permis de dégager des propriétés plus universelles encore. L'intérêt de ces structures algébriques est toujours le même : généraliser des méthodes de résolution de problèmes.

Dans le même souci d'efficacité, il est apparu intéressant de pouvoir passer d'une structure algébrique à une autre pour pouvoir transposer les propriétés. Les outils qui servent à réaliser ceci sont les **bijections**, qui garantissent la même structure (on parle d'**isomorphismes**), et les **surjections** (respectivement **injections**) qui permettent de passer d'une structure à son « modèle réduit » (respectivement agrandi). On parle de **morphismes** ou d'**homomorphismes** (littéralement « même structure »).

On étudie donc des objets de différents types : des points, des nombres, des vecteurs, etc. Ces objets, nommés encore **éléments**, forment, en vertu de certaines propriétés, un **ensemble**. Les éléments d'un ensemble sont susceptibles d'avoir entre eux ou avec ceux d'un autre ensemble, certaines **relations** (par exemple, la relation d'appartenance : un élément e appartient à un ensemble E, relation notée $e \in E$, etc.).

A.1 Les groupes

A.1.1 Définition

Un **groupe** G est un ensemble muni d'une loi de composition interne $\circ$ qui possède certaines propriétés. La propriété fondamentale d'un groupe, c'est le fait que la loi soit fermée sur cet ensemble : toutes les combinaisons possibles des éléments de G avec la loi $\circ$ donne un autre élément de G. C'est cette propriété que Galois a identifiée dans son mémoire. Ce n'est que plus tard que Cayley vit la propriété d'associativité.

Au delà des définitions, il est donc important de comprendre qu'un groupe est un ensemble d'objets que l'on peut combiner entre eux par le biais d'une transformation (ou opération) pour donner un autre objet appartenant lui aussi à l'ensemble de départ. Aujourd'hui et afin d'étendre la définition d'un groupe à des ensembles infinis, on définit un groupe par quatre propriétés :

- la loi est interne
- la loi est associative
- il existe un élément neutre
- tout élément admet un unique symétrique (ou inverse)

De façon plus formelle, un **groupe** G est un ensemble muni d'une loi $\circ$ caractérisé par les quatre axiomes suivants :

$\rightarrow$ $\circ$ est une loi de composition interne, c'est-à-dire une application de $G \times G$ dans G.

Remarque : une **application** est une relation entre deux ensembles pour laquelle chaque élément du premier (appelé ensemble de départ ou source) est relié à un *unique* élément du second (l'ensemble d'arrivée ou but).

$\rightarrow$ La loi est associative : $\forall g,\, g',\, g'' \in G,\, g \circ (g' \circ g'') = (g \circ g') \circ g''$.
$\rightarrow$ Il existe un élément neutre : $\exists e \in G \mid \forall g \in G, g \circ e = e \circ g = g$.
$\rightarrow$ Tout élément admet un unique symétrique : $\exists!\ g' \in G \mid \forall g \in G, g' \circ g = g \circ g' = e$.

La loi interne n'est pas forcément commutative, si c'est le cas elle vérifie :

$$\forall g, g' \in G, g \circ g' = g' \circ g. \tag{A.1}$$

Le groupe est alors dit commutatif ou **abélien** (en référence à Niels Henrik Abel). Quand le groupe ne contient pas trop d'éléments, on peut le représenter par sa table de « multiplication » qui donne la composition de chaque couple d'éléments de l'ensemble par la loi interne. C'est une visualisation simple des propriétés du groupe (cf. section A.1.2).

La notion de sous groupe :

Soit $(G, \circ)$ un groupe, H est un **sous-groupe** du groupe G si et seulement si il est non vide et stable pour les produits et les inverses. C'est-à-dire, H induit un sous-groupe de G si et seulement si il est non vide, inclus dans G et :

$$\forall (x, y) \in H^2, x \circ y^{-1} \in H \tag{A.2}$$

A.1.2 Exemple de table

Le groupe $\mathbb{Z}_2 \times \mathbb{Z}_2$:

Le groupe $\mathbb{Z}_2 \times \mathbb{Z}_2$ possède quatre éléments : $(0,0)$, $(0,1)$, $(1,0)$ et $(1,1)$, que l'on notera respectivement 1, A, B et C

$\circ$	1	A	B	C
1	1	A	B	C
A	A	1	C	B
B	B	C	1	A
C	C	B	A	1

TAB. A.1 – Table de « multiplication » de $\mathbb{Z}_2 \times \mathbb{Z}_2$

Il est aisé de vérifier que cette table correspond à une loi de composition interne. De même, il est facile de repérer un élément neutre (qui reproduit à l'identique la liste des éléments sur une ligne et une colonne). Ensuite, on peut vérifier que cet élément neutre figure une fois et une seule sur chaque ligne et chaque colonne de la table, ce qui traduit l'existence d'un élément symétrique pour chaque élément du groupe.

Seule l'associativité est beaucoup moins évidente à lire sur la table : elle se caractérise par le fait que l'on peut passer de la case d'un élément donné par une autre case remplie par le même élément toujours par le même « mouvement » (par exemple, un déplacement similaire à celui du cavalier aux échecs). Pour vérifier cette dernière propriété, on considérera que les limites de la table de multiplication ne sont en fait qu'arbitraires (car l'ordre d'apparition des éléments dans la table est lui même arbitraire). Par conséquent, si l'on « sort » par un côté, on « rentre » par le côté opposé. Ainsi peut-on constater que l'associativité est vérifiable sur la table, même si il est vrai que cette propriété ne saute pas aux yeux.

Pour les groupes commutatifs, on peut visualiser une symétrie par rapport à la première diagonale qui dans la table A.1 est « composée de 1 », symétrie qui caractérise leur commutativité.

A.1.3 Quelques remarques sur les groupes

La notion d'ordre :

En théorie des groupes, le mot **ordre** est utilisé dans deux sens, intimement liés :

1. L'ordre d'un groupe est son nombre d'éléments (ou son **cardinal**) si ce groupe est fini, et l'infini sinon.
2. L'ordre (ou la période) d'un élément a d'un groupe est le plus petit nombre entier positif m tel que $a^m = e$ (où e désigne l'élément neutre du groupe, et où a^m désigne le produit de m éléments égaux à a). Si aucun m de la sorte n'existe, a est dit d'ordre infini.

Le centre d'un groupe :

On appelle **centre d'un groupe** G l'ensemble des éléments qui commutent avec tous les autres.

Plus formellement, soit (G,∘) un groupe, muni de la loi multiplicative ∘, le centre de G, noté Z_G, est définit comme suit :

$$Z_G = \{z \in G \mid \forall g \in G, g \circ z = z \circ g\} \tag{A.3}$$

Une des propriétés de Z_G est qu'il est un sous-groupe de G.

Le groupe quotient :

Un **groupe quotient** (ou groupe facteur) est un groupe obtenu en identifiant les éléments d'un grand groupe en utilisant une relation d'équivalence. Par exemple, le groupe cyclique des entiers relatifs modulo n peut « se diviser » (on parle en fait de partition) en identifiant les éléments qui diffèrent par un multiple de n et de définir une structure de groupe qui fonctionne sur chacune de ces classes (appelé classe de congruence) comme une entité unique. Cette opération se notera dans ce cas $\mathbb{Z}/n\mathbb{Z}$. Si on considère le quotient d'un groupe G avec son centre $Z(G)$, on parle du **quotient central** de G

Les groupes normaux :

Un **sous-groupe normal** ou **sous-groupe distingué** ou **sous-groupe invariant** H d'un groupe G est un sous-groupe globalement stable par l'action de G sur lui-même par conjugaison. Les sous-groupes normaux sont importants en ce sens qu'ils partitionnent les groupes qui leurs sont associés, ce qui est très intéressant quand ces derniers sont trop complexes pour un étude globale.

Deux sous-groupes A et B de $(G, \circ)$ sont dits **conjugués** si :

$$\exists g \in G \mid A = g \circ B \circ g^{-1}.$$

Étant donné H un sous-groupe de G, le **normalisateur** de H, noté $N_G(H)$, est l'ensemble :

$$N_G(H) = \{g \in G \mid g \circ H \circ g^{-1} = H\}.$$

Un sous-groupe N de G est **normal** si :

$$\forall g \in G, g \circ N \circ g^{-1} = N.$$

Un groupe est dit simple si ses seuls sous-groupes distingués sont $\{e\}$ et G.

Remarque : le normalisateur de H « fait » de H un sous groupe normal, au sens où H est normal dans son normalisateur. En fait, le normalisateur est le plus grand sous-groupe contenant H, dans lequel H est distingué.

Une façon équivalente de définir un sous-groupe distingué est de dire que les classes résiduelles à droite et à gauche de H dans G coïncident, c'est-à-dire :

$$\forall x \in G, xH = Hx.$$

A.2 Les anneaux

A.2.1 Définition

Un **anneau** A est un ensemble muni de deux lois de composition interne, par exemple $+$ et $\times$, vérifiant les propriétés suivantes :
→ l'ensemble muni de la première loi interne (ici l'addition) est un groupe abélien,
→ la seconde loi (ici la multiplication) est associative,
→ la multiplication est distributive par rapport à l'addition (à droite et à gauche) :
$\forall a, a', a'' \in A, (a + a') \times a'' = a \times a'' + a' \times a''$ et $a'' \times (a + a') = a'' \times a + a'' \times a'$.

Anneau unitaire, anneau intègre :

Un anneau est dit **unitaire** s'il possède un élément neutre pour la multiplication et **commutatif** si la multiplication l'est. Un anneau unitaire et commutatif est dit **intègre** si il est sans diviseur de zéro. **Sans diviseur de zéro** signifie qu'un produit nul nécessite qu'un de ses facteurs soit nul.

En effet, il existe des anneaux qui ne sont pas intègres. Par exemple, l'anneau des matrices carrées d'ordre 2 (muni de l'addition et de la multiplication des matrices) est un anneau non commutatif et avec diviseur de zéro :

$$\begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ -4 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Caractéristique d'un anneau :

La **caractéristique** d'un anneau A, dont les éléments neutres pour la multiplication et l'addition seront notés respectivement 1_A et 0_A, est le premier entier naturel $n_A > 0$ tel que :

$$1_A + 1_A + ... + 1_A = 0_A \text{ (n_A termes égaux à } 1_A) \tag{A.4}$$

Quand aucun entier naturel ne vérifie l'équation A.4, on dit que A est de caractéristique nulle.

A.2.2 Notion d'idéal

Dans le cadre des anneaux commutatifs, on introduit la notion d'idéal. Un **idéal** I d'un anneau A est un sous groupe additif de $(A, +)$, stable pour la multiplication, c'est-à-dire :

$$\forall x \in I, \forall y \in A, x \times y \in I$$

Idéal principal :

Un idéal qui peut s'écrire xA est appelé **idéal principal** engendré par x. Un idéal principal est donc un idéal engendré par un unique élément.

Le concept d'idéal est fondamental pour la théorie des nombres et permet de partitionner l'anneau. Par exemple, un idéal de l'anneau des entiers relatifs $\mathbb{Z}$ est le sous ensemble de $\mathbb{Z}$ constitué des multiples de l'entier relatif n, noté $n\mathbb{Z}$.

A.2.3 Notion de module

Soient A un anneau (unitaire) et $(M, +)$ un groupe commutatif, M sera un module de A à gauche si il est muni d'une loi de composition externe $\circ$ de $A \times M$ dans M, vérifiant, pour tout élément a, b de A et tout élément x, y de M, les propriétés suivantes :

- $a \circ (x + y) = a \circ x + a \circ y$ (distributivité de $\circ$ par rapport à l'addition dans M)
- $(a + b) \circ x = a \circ x + b \circ x$ (distributivité de $\circ$ par rapport à l'addition dans A)
  Remarque : la loi + du membre de gauche est celle de l'anneau A et la loi + du membre de droite est celle du groupe M.
- $(ab) \circ x = a \circ (b \circ x)$
- $1 \circ x = x$

Ce qui a été défini ici est un module de A à gauche car, dans la loi externe, les éléments de A sont placés à gauche. On pourra définir de même un module de A à droite.

Il est important de remarquer que les structures de module à gauche et à droite ne diffèrent pas uniquement par leur écriture : si les deux premiers axiomes sont les mêmes, le troisième s'écrit : $x \circ (ba) = (x \circ b) \circ a$. Si l'on transcrivait naïvement cette égalité en écrivant les éléments de A à gauche, on obtiendrait $(ba) \circ x = a \circ (b \circ x)$, ce qui, si A n'est

pas commutatif, ne revient pas au même que l'axiome qui donne la structure de module à gauche.

En revanche, le petit raisonnement ci-dessus montre que si l'on « inverse » la loi de A, un module à droite peut être vu comme un module à gauche. Plus précisément, notons A^{op} l'anneau « opposé » à A, c'est-à-dire le groupe abélien A muni de la multiplication définie par $a^{op} \circ b^{op} = b \circ a$, où a^{op} et b^{op} désignent a et b vus comme éléments de A^{op}. Alors, si M est un module à gauche de A, M peut être vu comme un module à droite de A^{op}, où l'action de A^{op} est définie par $a \circ m = m \circ a^{op}$. Ceci justifie que l'on puisse se restreindre à l'étude des modules à gauche.

En bref, un module est à un anneau A ce qu'un $\mathbb{K}$ - espace vectoriel E est à son corps $\mathbb{K}$. La notion de module sur un anneau généralise donc celle d'espace vectoriel sur un corps ; la notion de module généralise également celle d'idéal d'un anneau.

Dans un espace vectoriel l'ensemble des scalaires forme un corps tandis que dans un module, ceux-ci sont de manière plus générale munis d'une structure d'anneau (non nécessairement commutatif).

Module libre, module cyclique :

Certaines propriétés, vraies pour les espaces vectoriels, ne le sont plus pour les modules. Par exemple, l'existence d'une base n'y est plus assurée mais, si c'est le cas, on parlera de **module libre**.

Un **module cyclique** est un module engendé par un seul élément.

Notion de sous module :

Soit E un module de A à gauche et M une **partie** de E (tous les éléments de M appartiennent à E). On dit que M est un **sous module** (à gauche) de A si il vérifie les conditions suivantes :

- M est un sous-groupe de $(E, +)$,
- $\forall a \in A, x \in M, a \cdot x \in M$.

A.3 Les corps

A.3.1 Définition

Un **corps** est un anneau tel que la seconde loi (la multiplication) possède, en plus, la propriété suivante : tout élément (différent de l'élément neutre de la première loi) a un inverse pour cette seconde loi. Un corps est donc un ensemble qui a une structure de groupe pour l'addition et pour la multiplication, à condition de considérer l'ensemble privé de l'élément neutre dans le cas de la multiplication. Un corps est dit commutatif si la seconde loi (la multiplication) est commutative.

A.3.2 Les corps de Galois

Dans ce qui nous occupe, on va s'intéresser au cas particulier des corps finis ou dits **corps de Galois** [Art98], notés $\mathbb{F}_n$ (pour corps fini à n éléments) ou encore $\mathbb{GF}_n$ (*Galois Field* : corps de Galois à n éléments). On peut démontrer que le **cardinal** d'un corps fini est nécessairement un nombre premier ou la puissance d'un nombre premier. On peut également montrer que tous les corps finis qui ont le même nombre d'éléments sont **isomorphes** (c'est-à-dire équivalents, cf. section A.4), ce qui en simplifie considérablement l'étude (ce n'est pas aussi simple pour les groupes finis ou dits de Galois comme pour les corps). Cela signifie entre autre que pour toute puissance n d'un nombre premier p, il existe un unique corps $\mathbb{F}_q$ (à un isomorphisme près). Voilà en quoi l'algèbre, classification intelligente par excellence des abstractions mathématiques, est-elle si importante et si jolie !

Les corps finis $\mathbb{F}_p$ pour tous les nombres premiers p sont notés $(\mathbb{Z}_p, +, \times)$, ils forment les ensembles des entiers relatifs modulo p.

Décomposition polynomiale :

Pour toutes les puissances d'un nombre premier : $q = p^n$, il y a un corps $\mathbb{F}_q$ à $q = p^n$ éléments. Par analogie avec l'existence et l'unicité de la décomposition en facteurs premiers des entiers, on peut définir une décomposition dans l'anneau des polynômes $\mathbb{F}_p[x]$. On dira qu'un polynôme est **irréductible** sur le corps $\mathbb{F}_p$ si on ne peut pas le factoriser en polynôme de **degré** (la valeur de sa plus petite puissance en x, cf. équation A.5) moindre dont les coefficients appartiennent au corps $\mathbb{F}_p$.

Plus formellement, soit $p(x)$ un polynôme unitaire de degré n à coefficients dans $\mathbb{F}_p$ et irréductible. Les restes des polynômes à coefficients dans $\mathbb{F}_p$ dans la division euclidienne par $p(x)$ forment un système de représentants de $\mathbb{F}_q$ (c'est-à-dire qu'ils caractérisent de façon non équivoque $\mathbb{F}_q$) :

$$\mathbb{F}_q \cong \mathbb{F}_p[x]/\langle p(x)\rangle \cong \{a_0 + a_1 x + ... + a_{n-1}x^{n-1}; a_0, a_1, ..., a_{n-1} \in \mathbb{F}_p\} \tag{A.5}$$

On constate que $\mathbb{F}_q$ est un espace vectoriel (cf. définition en section A.5) sur $\mathbb{F}_p$, avec pour base $\{1, x, ..., x^{n-1}\}$, et que l'on peut identifier $\mathbb{F}_p$ au sous ensemble de $\mathbb{F}_q$ formé des éléments pour lesquels $a_1 = ... = a_{n-1} = 0$. Le polynôme $p(x)$ peut donc être également considéré comme un polynôme de $\mathbb{F}_q[x]$.

Le **corps de base** d'un polynôme est le corps engendré par les coefficients d'un polynôme ou un corps le contenant.

Il est à noter que la notion de décomposition spectrale s'étend à des corps autres que les corps de Galois, mais ces cas-ci ne seront pas abordés.

Exemple : décomposition polynomiale de $\mathbb{F}_2$

Soit $\mathbb{F}_2 = \{0, 1\}$, $(\mathbb{F}_2, +, \times)$ est un corps dont voici les tables d'addition et de multiplication :

$+$	0	1
0	0	1
1	1	0

TAB A.2 (a) - Addition dans $\mathbb{F}_2$

$\times$	0	1
0	0	0
1	0	1

TAB A.2 (b) - Multiplication dans $\mathbb{F}_2$

On note $\mathbb{F}_2[x]$ l'anneau des polynômes qui ont leurs coefficients dans $\mathbb{F}_2$. Certains polynômes sont réductibles sur $\mathbb{F}_2$. Ce sont, pour le premier degré, x et $x + 1$. On peut ensuite générer d'autres polynômes en multipliant ceux-ci. Si l'on s'arrête au second degré, on obtient les polynômes réductibles suivants : x^2, $x^2 + x$ et $x^2 + 1 = (x + 1)^2$. En revanche, $x^2 + x + 1$ est irréductible.

Soit $\alpha \in \mathbb{F}_2$ une solution de $x^2 + x + 1$, α, par définition, vérifie l'équation :

$$\alpha^2 + \alpha + 1 = 0 \Longrightarrow \alpha^2 = \alpha + 1$$

Si on adjoint (cf. section A.3.3) α à $\mathbb{F}_2$, on obtient

$$\mathbb{F}_2[\alpha] = \{0, 1, \alpha, \alpha^2\} = \{0, 1, \alpha, \alpha + 1\}$$

Le corps $\mathbb{F}_2[\alpha]$ est un corps à $4 = 2^2$ éléments (on a vu qu'il existait un unique corps à p^q éléments à un isomorphisme près pour chaque nombre premier p et chaque entier q). Voici les tables d'addition et de multiplication de ce corps :

$+$	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

TAB A.3 (a) - Addition dans $\mathbb{F}_2[\alpha]$

$\times$	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

TAB A.3 (b) - Multiplication dans $\mathbb{F}_2[\alpha]$

On peut remarquer que $\alpha + 1$ est la seconde racine du polynôme $x^2 + x = 1$. Ainsi α et $\alpha + 1$ sont-ils conjugués sur $\mathbb{F}_2$.

A.3.3 Extension de corps

Soit K un corps, si on ajoute un élément algébrique α sur K (on dit alors que l'on **adjoint** α à K), on obtient une **extension de corps**, notée $K[\alpha]$. En effet, on démontre

que $K[\alpha]$ est aussi un corps. On parle parfois de **sur corps** pour $K[\alpha]$.

Soient K un corps et L une extension du corps K, pratiquement, on peut considérer L comme un espace vectoriel sur K.

A.4 Les morphismes

A.4.1 Définitions

Soient $(G, \circ)$ et $(G', \circ')$ deux groupes. On dit qu'il y a un **homomorphisme** de G dans G' si et seulement si il existe une application f telle que :

$$f : G \to G' \text{ telle que } \forall x, y \in G, f(x \circ y) = f(x) \circ f(y).$$

Exemples : • $f : (\mathbb{R}, +) \to (\mathbb{R}^*, \times)$ telle que $f(x) = exp(x)$.

L'addition sur $\mathbb{R}$ est ainsi transposée en une multiplication sur $\mathbb{R}$ car :

$$f(a + b) = exp(a + b) = exp(a) \times exp(b).$$

• $f : (\mathbb{R}^*, \times) \to (\mathbb{R}, +)$ telle que $f(x) = ln(x)$.

La multiplication sur $\mathbb{R}\backslash\{0\}$ est ainsi transposée en une addition sur $\mathbb{R}$ car :

$$f(a \times b) = ln(a \times b) = ln(a) + ln(b).$$

L'homomorphisme peut être surjectif, injectif ou bijectif (cf. section A.4.2). Si $G = G'$, l'homomorphisme est appelé **endomorphisme**. Dans le cas d'une bijection, on parle d'**isomorphisme**. Si f est une bijection et si $G = G'$, on parle d'**automorphisme**.

Un automorphisme de G induit par la conjugaison d'un élément g de G, c'est-à-dire un automorphisme f vérifiant :

$$\forall x \in G, f(x) = gxg^{-1},$$

est appelé **automorphisme intérieur** ; sinon il s'agit d'un **automorphisme extérieur**.

L'ensemble de tous les automorphismes d'un groupe G, muni de la loi de composition des fonctions, forme un groupe noté $Aut(G)$. Les automorphismes intérieurs forment un sous groupe normal de $Aut(G)$, noté $Inn(G)$. Le groupe $Inn(G)$ est isomorphe au quotient central (cf. section A.1.3) de G. Par ailleurs, le quotient $Out(G) = Aut(G)/Inn(G)$ est appelé le groupe des automorphismes extérieurs.

Les notions de morphismes s'étendent pour les autres structures algébriques (homomorphismes d'anneaux, de corps). Dans ce cas, ce sont les deux lois qui doivent être transposées d'un ensemble à l'autre.

A.4.2 Surjection, injection, bijection

Une **surjection** ou application surjective est une application pour laquelle tout élément de l'ensemble d'arrivée a *au moins* un antécédent, c'est-à-dire est image d'au moins un élément de l'ensemble de départ. De façon plus formelle, une application f de E dans F est surjective signifie :

$$\forall y \in F, \exists x \in E \text{ tel que } f(x) = y.$$

Une **injection** ou application injective est une application telle que pour tout élément de l'ensemble d'arrivée, il existe *au plus* un antécédent. De façon équivalente et plus formelle, une application f de E dans F est injective signifie :

$$\forall x, x' \in E, f(x) = f(x') \Longrightarrow x = x'.$$

Une **bijection** ou application bijective est une application telle que tout élément de son ensemble d'arrivée a *un et un seul* antécédent, c'est-à-dire est image d'exactement un élément de son ensemble de départ. En bref, c'est une application à la fois injective et surjective.

A.5 Les espaces vectoriels

A.5.1 Définition

En algèbre linéaire, un espace vectoriel est un ensemble muni d'une structure permettant d'effectuer des combinaisons linéaires.

Étant donné un corps K, un espace vectoriel E sur K est un groupe commutatif (dont la loi est notée $+$) munie d'une action compatible de K (voir dans le paragraphe qui suit la définition formelle de E). Les éléments de E sont appelés des **vecteurs**, et les éléments de K des **scalaires**. Très souvent en physique, K est le corps des réels $\mathbb{R}$ ou le corps des complexes $\mathbb{C}$.

Plus formellement : soient $(K, +, .)$ un corps, E un ensemble, f l'application qui va de $K \times E$ dans E telle que :

$$\forall (\alpha, x) \in K \times E, f\left((\alpha, x)\right) = \alpha \times x$$

L'application f se nomme **loi de composition externe**. On appelle espace vectoriel sur K (ou encore K - espace vectoriel), tout ensemble muni d'une loi de composition interne $+$ et d'une loi de composition externe $\times$, tel que :

- $(E,+)$ est un groupe commutatif
- $\forall \alpha, \beta \in K, \forall x, y \in E$:
  - $\alpha \times (x + y) = \alpha \times x + \alpha \times y$
  - $(\alpha + \beta) \times x = \alpha \times x + \beta \times x$

– $(\alpha.\beta) \times x = \alpha \times (\beta \times x)$
– $1 \times x = x$

A.5.2 Espaces vectoriels remarquables

Au préalable :

Une **valeur absolue** sur un corps K est une application qui à tout élément x de K fait correspondre un nombre réel positif noté $Abs(x)$ de telle sorte que :

1. $\forall x \in K, Abs(x) = 0 \Leftrightarrow x = 0$ (séparation),
2. $\forall (x, y) \in K^2, Abs(x + y) \leq Abs(x) + Abs(y)$ (inégalité triangulaire),
3. $\forall (x, y) \in K^2, Abs(xy) = Abs(x)Abs(y)$.

S'il n'y a pas de risque d'ambiguïté, la valeur absolue d'un élément x est notée $\mid x \mid$.

Une **norme** est une application

$$\mathcal{N} : E \to \mathbb{R}^+,$$

satisfaisant les axiomes suivants :

1. $\forall x \in E, \mathcal{N}(x) = 0 \Rightarrow x = 0_E$ (séparation),
2. $\forall (\lambda, x) \in K \times E, \mathcal{N}(\lambda x) = \mid \lambda \mid \mathcal{N}(x)$ (homogénéité),
3. $\forall (x, y) \in E^2, \mathcal{N}(x + y) \leq \mathcal{N}(x) + \mathcal{N}(y)$ (inégalité triangulaire).

S'il n'y a pas de risque d'ambiguïté, la norme d'un élément x est notée $|| x ||$.

Une **distance** est une application qui formalise l'idée intuitive de distance, c'est-à-dire la longueur qui sépare deux points. Plus formellement, on appelle distance sur un ensemble E une application :

$$d : \mathrm{E} \times \mathrm{E} \to \mathbb{R}^+,$$

vérifiant les axiomes suivants :

1. $\forall x, y \in \mathrm{E}, d(x, y) = d(y, x)$ (symétrie),
2. $\forall x, y \in \mathrm{E}, d(x, y) = 0 \Leftrightarrow x = y$ (séparation),
3. $\forall x, y, z \in \mathrm{E}, d(x, z) \leq d(x + y) + d(y + z)$ (inégalité triangulaire).

À partir de la définition d'une distance, vue comme une application satisfaisant à certains axiomes, d'autres notions de distance peuvent être définies, comme par exemple la distance entre deux parties, ou la distance d'un point à une partie, sans que ces dernières

répondent à la définition première d'une distance. En l'occurrence, on s'intéresse à la notion de distance dans un espace vectoriel normé.

Dans un espace vectoriel normé $(\mathrm{E}, \|\ \|)$, on peut toujours définir de manière canonique une distance d à partir de la norme. En effet, il suffit de poser :

$$\forall (x, y) \in \mathrm{E} \times \mathrm{E}, d(x, y) = \|y - x\|.$$

Le **produit scalaire** est une opération algébrique s'ajoutant aux lois s'appliquant aux vecteurs. À deux vecteurs elle associe leur produit scalaire, qui est un nombre (ou scalaire). Elle permet d'exploiter les notions de la géométrie euclidienne traditionnelle : longueurs, angles, orthogonalité en dimension deux et trois, mais aussi de les étendre à des espaces vectoriels réels de toute dimension, et aux espaces vectoriels complexes. Plus formellement, soit E une espace vectoriel sur K, on appelle produit scalaire sur E une application :

$$f : \mathrm{E} \times \mathrm{E} \to \mathbb{C}$$

vérifiant les propriétés suivantes :

1. $\forall u, v \in \mathrm{E}, f(u, v) = \overline{f(v, u)}$,
2. $\forall u, v, w \in \mathrm{E}, f(u + v, w) = f(u, w) + f(v, w)$,
3. $\forall a \in \mathbb{C}, \forall u, v \in \mathrm{E}, f(u, av) = af(u, v)$,
4. $\forall u \in \mathrm{E}, f(u, u) \neq 0$, avec l'égalité si et seulement si $u = 0$.

Autrement dit, un produit scalaire est une forme bilinéaire définie positive.

Espace vectoriel euclidien, hermitien, préhilbertien :

Un espace vectoriel E sur K muni d'un produit scalaire est dit pré-hilbertien. En particulier, si $K = \mathbb{R}$ ($K = \mathbb{C}$) et E est de dimension finie, E est dit également euclidien (hermitien).

Espace métrique/normé :

Un espace métrique/normé est une structure mathématique qui développe des propriétés géométriques de distance compatible avec les opérations de l'algèbre (linéaire).

De manière plus formelle : soit K un corps muni d'une **valeur absolue**, et non discret (par exemple le corps des réels ou des complexes). Un K-espace vectoriel E est dit métrique/normé lorsqu'il est muni d'une **distance/norme**.

Espace complet :

Un espace normé N est dit complet si toute suite de Cauchy de N a une limite dans N (c'est-à-dire qu'elle converge dans N). La propriété de complétude dépend de la norme. Il

est donc important de toujours préciser la norme que l'on prend quand on parle d'espace complet.

Sans rentrer dans les détails formels de la définition, il suffit de comprendre qu'intuitivement, un espace est complet s'il « n'a pas de trou », s'il « n'a aucun point manquant ».

Par exemple, les nombres rationnels ne forment pas un espace complet, puisque $\sqrt{2}$ n'y figure pas alors qu'il existe une suite de Cauchy de nombres rationnels ayant cette limite. Il est toujours possible de « remplir les trous » amenant ainsi à la complétion d'un espace donné.

Espace de Banach :

On appelle espace de Banach un **espace vectoriel normé complet**.

Espace de Hilbert :

Un espace de Hilbert est un **espace de Banach** dont la **norme** $\| \ \|$ découle d'un **produit scalaire** ou **hermitien** $\langle \ , \ \rangle$ par la formule $\| \ x\| = \sqrt{\langle x, x\rangle}$. C'est la généralisation en dimension quelconque d'un **espace euclidien** ou **hermitien**.

De façon plus « pratique » (théorème de M. Fréchet, J. von Neumann et P. Jordan), un espace de Banach (respectivement espace vectoriel normé) est un espace de Hilbert (respectivement espace préhilbertien) si et seulement si sa norme vérifie l'égalité :

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y\|^2).$$

Cette égalité signifie que la somme des carrés des côtés d'un parallélogramme est égale à la somme des carrés des diagonales (règle du parallélogramme).

Annexe B

Un peu de géométrie projective

A l'origine...

La géométrie projective est le domaine des mathématiques qui modélise les notions intuitives de perspective et d'horizon. Elle étudie les propriétés des figures inchangées par projection. La géométrie projective, par rapport à la géométrie euclidienne ordinaire, est la « science des figures qui se tracent avec la règle seule », alors que la géométrie euclidienne est, en quelque sorte, « la science des figures qui se tracent à la règle et au compas ». La première ignore les droites parallèles, les droites perpendiculaires, les isométries, les cercles, les triangles rectangles, isocèles, etc. Ainsi dans sa définition comporte-t-elle moins d'axiomes que la géométrie euclidienne et en cela est-elle plus générale, « plus souple ».

On va donner une petite idée de ce qu'est la géométrie projective sur un corps (cf. section B.1), cas le plus simple et le plus concret afin d'appréhender ce qu'est cette géométrie si particulière. Ensuite, et c'est ce qui est déterminant pour les chapitres 4 et 5, on s'intéressera à une vision de la géométrie projective à la fois, plus générique, puisqu'elle s'appliquera aux anneaux (finis), et plus particulière, puisqu'on ne parlera que de droites, plans, et espaces projectifs (cf. section B.2). Seront introduites également d'autres entités de la géométrie projectives (cf. section B.3).

B.1 Sur les corps

B.1.1 Définition algébrique

Soit E_{n+1} un espace vectoriel de dimension $n+1$ sur un corps K (où K est $\mathbb{R}$ ou $\mathbb{C}$), soit une relation d'équivalence $\mathcal{R}$ sur $E_{n+1}\backslash\{0\}$ telle que :

$$x\mathcal{R}y \text{ signifie } \exists\lambda \in K\backslash\{0\} \text{ tel que } y = \lambda x \tag{B.1}$$

Les classes d'équivalence sont donc les directions (ou les droites vectorielles) de E_{n+1}. L'ensemble des classes d'équivalence est appelé **espace projectif de dimension n**,

construit à partir de E_{n+1}, il sera noté $P[E_{n+1}]$.

Remarque :

Une **relation d'équivalence** R sur un ensemble E vérifie trois propriétés :

1. R est réflexive : $\forall x \in E$, xRx.
2. R est symétrique : $\forall x, y \in E$, $xRy \Longrightarrow yRx$.
3. R est transitive : $\forall x, y, z \in E$, xRy et $yRz \Longrightarrow xRz$.

Soit $n \geq 1$, soit H un hyperplan (cf. section B.2.2) de E_{n+1} ne passant pas par l'origine, alors on obtient une représentation partielle de l'espace projectif en prenant les intersections des droites vectorielles de l'espace E_{n+1} avec H. Ceci donne une « carte » de $P[E_{n+1}]$, à ceci près que les points de l'espace projectif correspondant aux directions parallèles à H ne sont pas représentés sur cette carte. Ainsi l'espace projectif $P[E_{n+1}]$ apparaît-il comme l'espace affine H auquel se rajoutent les points correspondant aux directions parallèles à H, appelés points à l'infini de H.

NB : la notion de point à l'infini est affine, dans l'espace projectif lui-même tous les points ont le même statut. Il n'y a de notion de point à l'infini que par rapport à une carte et ces points se dessinent alors à distance finie sur une autre carte.

Quelques correspondances :

- Si $n = 0$ (c'est-à-dire E_{n+1} est une droite vectorielle) alors l'espace projectif correspondant est un point.

- Si $n = 1$ alors l'espace projectif correspondant est une droite projective qui se décompose en une droite affine à laquelle on rajoute un point à l'infini.

- Si $n = 2$ alors l'espace projectif correspondant est un plan projectif qui se décompose en un plan affine auquel on ajoute une droite projective à l'infini.

Système de coordonnées projectives :

Soit $\{e_1, e_2, ..., e_{n+1}\}$ une base de E_{n+1}, soit $x = (x_1, x_2, ..., x_{n+1})$ un vecteur non nul de E_{n+1}. Le point correspondant M de l'espace projectif est la classe des points dont les coordonnées sont de la forme $(\lambda x_1, \lambda x_2, ..., \lambda x_{n+1})$, où $\lambda \in K\backslash\{0\}$. On peut donc, de la même façon que pour les vecteurs, définir une relation d'équivalence sur les n-uplets des coordonnées. On note $(x_1 : x_2 : ... : x_{n+1})$ la classe de $(x_1, x_2, ..., x_{n+1})$, elles sont dites **coordonnées homogènes/projectives** du point M.

Exemple : $(1:0:1) = (2:0:2)$ représentent le même point ; $(0:0:0)$ n'existe pas.

NB : si on utilise la base $(\lambda e_1, \lambda e_2, ..., \lambda e_{n+1})$, M est le même. En revanche, si on veut définir un repère projectif afin que les coordonnées des points projectifs ne dépendent plus d'une base de l'espace vectoriel et aboutir à une notion plus intrinsèque de la géométrie projective, il va falloir rajouter une information. En effet, il n'est pas suffisant de se donner $n+1$ points projectivement indépendants dans un espace projectif de dimension n pour avoir un repère projectif. Considérons par exemple le cas $n = 2$: soient 3 points projectivement indépendants, ces trois points sont 3 directions de E_3. Si on prend une base formée d'un vecteur non nul pour chaque direction : (e_1, e_2, e_3), on a, par rapport à cette base, pour tout point M, des coordonnées homogènes $(X : Y : Z)$. Si on prend, maintenant, la base $(2e_1, e_2, e_3)$, les vecteurs de cette base correspondent exactement aux mêmes points de l'espace projectif que les précédents, et pourtant, les coordonnées projectives de ce même point M ne sont plus proportionnelles aux précédentes. Pour pallier à ceci, on rajoute donc une information, par exemple la position du point $(1 : 1 : \ldots : 1)$, nommé point unité.

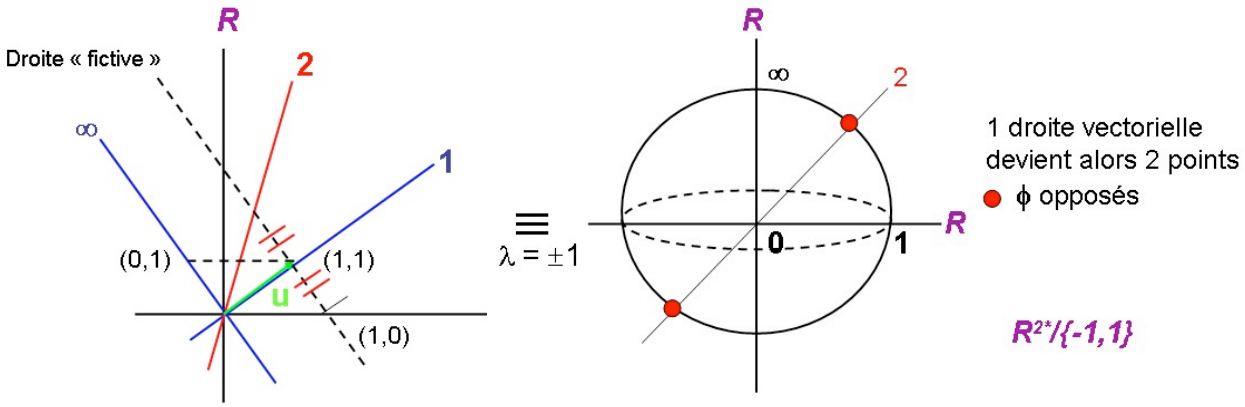
Exemple : un repère projectif de la droite projective est donné par 3 points : $\infty = (1:0)$ (point à l'infini), $0 = (0:1)$ et $1 = (1:1)$.

Droite projective sur $\mathbb{R}$:

Le cas le plus concret et le plus simple est celui pour lequel $n = 1$, cas que l'on étudie sur le corps, lui aussi le plus simple car le plus intuitif, celui des réels : $\mathbb{R}$. Il va s'agir de la droite projective sur $\mathbb{R}$, notée $P^1_{\mathbb{R}} = \frac{\mathbb{R}^2 \backslash \{(0,0)\}}{\sim}$.

L'ensemble des classes d'équivalence est donc équivalent à l'ensemble de droites vectorielles (celles « passant toutes » par 0), c'est pourquoi on considère $\mathbb{R}^2 \backslash \{(0,0)\}$ afin d'avoir une partition. Un point projectif correspond à une droite vectorielle et on peut représenter un point projectif $\frac{b}{a}$ par un point « classique » (a, b).

Pour représenter la droite projective sur $\mathbb{R}$, on définit un repère projectif $(0, 1, \infty)$ et on passe de la représentation $\frac{b}{a}$ à celle suivant (a, b), *via* un vecteur $\mathbf{u}$ de référence situé sur le point projectif 1.



Remarque : la droite projective est différente de la droite réelle achevée car, dans le dernier cas, on distingue $+\infty$ de $-\infty$.

B.1.2 Quelques intérêts de la géométrie projective

1. « Plus de problèmes » avec ∞ défini concrètement :

Historiquement, une des causes de l'apparition de la géométrie projective, du point de vue de l'analyse, est la discontinuité dont « souffre » la fonction tangente.

2. Homogénéisation des théorèmes :

Sur les droites au sein d'un plan projectif :

- avant : distinction entre les cas droites parallèles/droites sécantes,
- après : toutes les droites sont sécantes, les droites parallèles se coupant à l'infini.

Sur les plans :

- avant : 4 cas, à savoir 2 plans parallèles, le 1^{er} parallèle et le 2^{nd}, ...
- après : on considère juste le plan projectif : 1 seul cas !

3. Unification de l'étude des coniques :

Si on change de carte (c'est-à-dire un changement de repère projectif), une ellipse devient une hyperbole, ou une parabole, et ainsi de suite.

4. Principe de dualité :

Énoncé :

Soit $P[E_{n+1}]$, soit E^*_{n+1} le dual de E_{n+1}, ce dernier est aussi un espace vectoriel de dimension $n+1$. Ainsi l'espace projectif $P[E^*_{n+1}]$ a-t-il la même dimension que $P[E_{n+1}]$. Par suite, on peut considérer une forme linéaire comme un point de E^*_{n+1}, c'est-à-dire comme un représentant d'un point de $P[E^*_{n+1}]$, mais également comme un objet géométrique plus complexe dans $P[E_{n+1}]$. Si on associe à chaque forme linéaire non nulle x^* son noyau (qui

est un hyperplan vectoriel), puisque ce dernier caractérise, non pas seulement x^*, mais aussi l'ensemble des formes linéaires λx^*, alors $P[E^*_{n+1}]$ est exactement l'espace des hyperplans vectoriels de E_{n+1} ou, ce qui revient au même, l'espace des hyperplans de $P[E_{n+1}]$.

Preuve pour $n = 2$:

Le but est de relier des propriétés de points de $P[E^*_{n+1}]$ avec des comportements géométriques des hyperplans correspondants de $P[E_{n+1}]$. Pour simplifier et pour être plus concret, la démonstration concerne le cas $n = 2$.

Soient E un espace vectoriel de dimension 3, $P[E]$ le plan projectif associé, $\{e_1, e_2, e_3\}$ une base de E, la base duale associée est alors : $\{e^*_1, e^*_2, e^*_3\}$, c'est une base de E^* et définie telle que : $e^*_i(e_j) = \delta_{ij} = 1$ si $i = j$, 0 sinon.

Soit $P^* = P[E^*]$, soit m un point de P^*, soit H_m la droite de P associée, alors on a : $H_m = \{(X : Y : Z)/m(X, Y, Z) = 0\}$. Si les coordonnées homogènes de m sont $(u : v : w)$ alors l'équation de la droite est $H_m : uX + vY + wZ = 0$.

Si m_1 et m_2 sont deux points distincts de P^*, ils définissent respectivement les deux équations suivantes : $m_1(X, Y, Z) = 0$ et $m_2(X, Y, Z) = 0$, celles-ci déterminent deux droites dans P. Les points m de la droite de P^* qui passe par m_1 et m_2 sont de la forme $\lambda m_1 + \mu m_2$ et sont donc associés aux équations $\lambda m_1(X, Y, Z) + \mu m_2(X, Y, Z) = 0$. Ce sont aussi des équations de droites de P. Toutes ces droites passent par le point d'intersection des deux droites de P, correspondant à m_1 et m_2.

À partir de là :

- Un point m de P^* est caractérisé par une droite H_m de P.
- Trois points distincts m_1, m_2 et m_3 du plan P^* sont alignés si et seulement si les droites H_{m_1}, H_{m_2} et H_{m_3} sont trois droites distinctes, concourantes, du plan P.
- Une droite d de P^* correspond à la famille des droites de P passant par un même point, que l'on peut donc caractériser dans P, par un point noté M_d. Une telle famille est appelée faisceau de droites de point de base M_d.
- La figure formée dans P^* par une droite d, passant par deux points m_1 et m_2, correspond aux deux droites H_{m_1} et H_{m_2} se coupant au point M_d.

5. « Quantiquement parlant » :

Un qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ pourrait correspondre à un point projectif $(\frac{\beta}{\alpha})$.

B.1.3 Définition géométrique (en terme d'axiomes)

1. Chaque ligne contient au moins 3 points.

Si on considère la définition algébrique précédente, on constate que deux points effectuent le même office sur la ligne que celui qu'ils accompliraient pour une droite euclidienne, le troisième jouant le rôle de direction de la droite (à l'infini ou non).

2. Deux points distincts A et B sont sur une ligne unique (AB).

3. Axiome de Veblen Young :

Soit A, B, C, et D (cf. figure B.1) quatre points tels que (AB) et (CD) aient un point commun, alors (AC) coupe également (BD) (en supposant D différent de B et C).

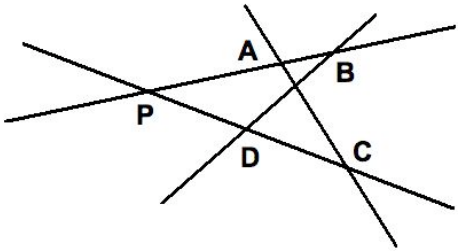


Fig. B.1 – Axiome 3

Il existe une autre formulation de l'axiome de Veblen Young plus concise : si une droite (ici (BD)) coupe deux côtés (ici AP et CD) d'un triangle (ici APC), alors la droite coupe le troisième côté (nommé AC).

Cet axiome est donc un moyen ingénieux de dire que deux droites d'un plan ont une intersection (même si on n'a pas encore défini ce qu'était un plan, cf. Remarque 2). Il exclue donc l'existence même de droites parallèles en matière de géométrie projective !

Remarque 1 : si, de plus, il y a au moins deux droites, l'espace projectif (définition en section B.2.4) est dit non dégénéré.

Remarque 2 : par définition, un plan projectif (définition en section B.2.2) est un espace projectif dans lequel l'axiome 3 est remplacé par l'axiome $3'$ suivant : soit deux droites alors elles ont au moins un point commun.

Remarque 3 : le principe de dualité se résume alors au fait que l'on peut intervertir le rôle des points et des lignes.

4. Il y a au moins deux lignes.

B.1.4 Propriétés importantes de la géométrie projective sur les corps finis

Si on se place sur le corps fini à q éléments $\mathbb{F}_q$ (cf. section A.3.2 de l'annexe A), alors le nombre de points et de lignes des espaces projectifs est connu.

Soient un espace projectif fini P de dimension d et d'ordre q, U un sous espace de dimension t de P, alors :

- Le nombre de points de U est : $S(t) = q^t + ... + q + 1 = \frac{q^{t+1}-1}{q-1}$.
- Le nombre de points de P est : $S(d) = \frac{q^{d+1}-1}{q-1}$.
- Le nombre de lignes de U, passant par un point fixé de U, vaut : $S(t)$.
- Le nombre total de lignes de U vaut : $\frac{S(t)S(t)}{q+1}$.
- Le nombre d'hyperplans de P est : $S(d)$.
- Le nombre d'hyperplans de P, passant par un point fixé de P, est : $S(d-1)$.

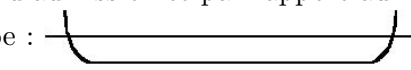
Pour en finir avec la géométrie projective sur les corps, il existe des configurations très particulières, telles que celle de **Pappus** ou celle de **Desargues** (cf. section B.2.3) pour ne citer qu'elles, du nom des mathématiciens qui ont été des pionniers dans ce domaine si particulier qu'est la géométrie projective. Elles ont donné lieu à deux théorèmes fondateurs sur la perspective (au sens des peintres), deux théorèmes concrets montrant un pan de l'intérêt que l'on peut porter à la géométrie projective, également appelée géométrie de **Laguerre** en hommage à son inventeur. On a donné une petite idée de ce qu'est la géométrie projective sur un corps, cas le plus simple et le plus concret. Dans la suite de cet exposé, il va s'agir d'une vision à la fois, plus générique puisqu'elle s'applique aux anneaux, mais également plus particulière puisqu'on ne parlera que de droites, plans, et espaces projectifs. Dans les chapitres suivants, on verra que la géométrie projective sur les anneaux sera déterminante.

B.2 Sur les anneaux finis

B.2.1 Droite projective sur un anneau fini $\mathcal{A}$

La définition d'une droite projective sur un corps a été donnée précédemment (cf. équation B.1 pour $n = 1$). Dans le cas des corps, tous les points d'une droite projective sont dits *admissibles* car tous les éléments (sauf l'élément neutre pour la multiplication)

d'un corps sont inversibles. Ce n'est pas le cas pour les anneaux non intègres pour lesquels $\mathcal{R}$ (cf. équation B.1) n'est plus une relation d'équivalence.

On introduit donc un test d'admissibilité par rapport aux points. De façon imagée, si on a une configuration de type :  , alors 1 des 2 points n'est pas admissible.

Plus rigoureusement : soit un anneau associatif et unifère $\mathcal{A}$, soit $\mathbb{GL}(2,\mathcal{A})$ le groupe des matrices inversibles 2×2 sur $\mathcal{A}$, une paire (α, β) est dite **admissible** sur $\mathcal{A}$ si :

$$\exists(\gamma,\delta) \in \mathcal{A}^2 \text{ tel que } \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathbb{GL}(2,\mathcal{A}) \tag{B.2}$$

La **droite projective sur $\mathcal{A}$** est alors définie [Hav04] comme l'ensemble des classes d'équivalence des paires ordonnées (ordre « au sens de » q) $(q\alpha, q\beta)$, où q sont les unités de $\mathcal{A}$, telles que (α, β) soit admissible (dans un anneau fini, il n'y a que deux types d'éléments : les **unités**, qui sont les éléments inversibles, et les autres, qui sont des **diviseurs de 0**).

On peut ensuite définir sur une telle droite projective (qui n'est pour l'instant qu'un ensemble de points) une structure de graphe, de la façon suivante [Hav04] : deux points distincts $X = (q\alpha, q\beta)$ et $Y = (q\gamma, q\delta)$ sont dits **voisins** (et seront reliés) si $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \notin \mathbb{GL}(2,\mathcal{A})$; sinon, ils sont dits **distants**.

Une classification explicite car menée par construction des droites projectives sur les premiers (par ordre croissant) anneaux finis a été réalisée [SPKP07, SPK06]. Ce n'est que lors de l'apparition de diviseurs de 0 que la structure de graphe définie ci-dessus a un quelconque intérêt. On en trouve un exemple dans la section 5.1.4 du chapitre 5.

B.2.2 Plan projectif sur un anneau fini $\mathcal{A}$

Définition d'un hyperplan projectif :

Un **hyperplan** H d'une géométrie finie est un ensemble de points tel que chaque ligne de la géométrie contienne exactement un point de H, ou soit incluse dans H.

Remarque 3 : la définition **hyperplan** est plus restrictive que celle de **sous espace** : un ensemble de points d'un espace projectif constitue un **sous espace** si et seulement si pour chaque ligne, l'ensemble contient 0 point, 1 point, ou tous les points de la ligne.

Définition d'un plan projectif :

Un plan projectif est un espace 2D tel que tous ses hyperplans (sous espaces de dimension 2) sont des droites projectives.

Le plan de Fano :

On aura besoin de la définition du plan projectif de Fano en terme d'axiomes, c'est-à-dire en terme de points et de lignes (cf. section B.1.3). La définition que l'on a donnée de la droite projective sur un anneau était de nature analytique (cf. section B.1.1). Considérer la géométrie projective en terme d'axiomes sera souvent plus simple à utiliser.

Le **plan de Fano** est défini comme suit :

- il possède 7 points et 7 lignes,
- chaque ligne possède 3 points,
- chaque point est sur 3 lignes.

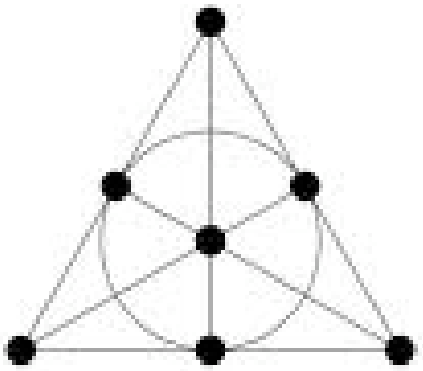


FIG. B.2 – Le plan de Fano

Ordre d'un plan :

Plus généralement, dans un **plan projectif**, chaque point/ligne (dualité, cf. section B.1.2) est incident avec le même nombre $k+1$ de lignes/points, où k constitue **l'ordre du plan**. De plus, le plan projectif possède k^2+k+1 points/lignes.

On constate ainsi que le plan de Fano est le plus petit plan projectif ($k=2$).

B.2.3 Les configurations projectives

Le plan de Fano appartient également à la famille des configurations projectives. Une **configuration projective** est un ensemble fini de points et de lignes tel que chaque point est relié à un même nombre de lignes, et chaque ligne est reliée à un même nombre de points. Une telle configuration peut être notée (v_a, e_b), où v et e sont respectivement le nombre de points et de lignes, a et b les nombres de lignes et de points incidents. Si cette configuration contient le même nombre de points et de lignes, on la note (v_a) (bien qu'en général, une telle configuration ne sera pas unique). Le plan de Fano est la configuration (7_3). Il existe

également deux configurations intéressantes : la **configuration de Pappus** (9_3), et la **configuration de Desargues** (10_3). N'importe quelle configuration peut également être vue comme un graphe en considérant ses points comme des sommets et ses lignes comme des arêtes.

B.2.4 Les espaces projectifs

Définition :

Un **espace projectif** est un espace 3D tel que tous ses hyperplans sont des plans projectifs.

Les espaces linéaires :

Par définition, un **espace linéaire** est un espace tel que toute ligne a au moins 2 points, et 2 points sont *exactement* sur une ligne.

Remarque 4 : Le plan de Fano est un espace linéaire.

Remarque 5 : si on remplace « exactement » par « au maximum », on a affaire à un **espace presque linéaire**.

Il y a, depuis un moment déjà, la conjecture suivante : un plan projectif d'ordre k existe si et seulement si k est la puissance d'un nombre premier. Par la suite, cette conjecture fut reliée à l'existence d'ensembles complets de MUBs pour N qudits [SPR04].

B.2.5 L'espace polaire

Définition :

Un **espace polaire** $S = \{P, L\}$ est un espace presque linéaire tel que pour tout point P n'appartenant pas à la ligne L, le nombre de points de L, reliés à P grâce à une ligne, égale soit 1 (comme pour le quadrangle généralisé, cf. section B.3.1), soit le nombre de points de la ligne.

Ordre :

Un **espace polaire d'ordre** N ($N \geq 2$) peut être vu comme un ensemble $\{P\}$ de points dont certains sous ensembles, appelés sous espaces, doivent vérifier :

1. Chaque sous espace, ainsi que ses propres sous espaces, est isomorphe à l'espace projectif $PG(d, q)$ (la notation signifie : d'ordre d et défini sur le corps de Galois à q éléments, F_q), tel que d soit au maximum égal à $N - 1$.
2. L'intersection de deux sous espaces est un sous espace.

3. Pour chaque point P n'appartenant pas à un sous espace E de dimension $N-1$, il existe un unique sous espace S, de dimension $N-1$, tel que $E \cap S$ soit de dimension $N-2$.
4. Il existe au moins deux sous espaces disjoints de dimension $N-1$.

Remarque 7 : un espace polaire de rang 2 est un quadrangle généralisé (cf. section B.3.1).

Espace polaire symplectique :

Un **espace polaire symplectique** est un espace vectoriel $V(d,q)$ de dimension d sur le corps de Galois F_q, muni d'une forme bilinéaire alternée non dégénérée. Une **forme** est une application d'un espace vectoriel dans son corps de nombre (le corps de nombre désigne l'ensemble des nombres définissant la multiplication externe des vecteurs, en général ce sont les nombres réels ou complexes). Cette forme est dite, **bilinéaire** si elle s'applique à deux vecteurs, **alternée** si et seulement si la propriété suivante s'applique :

$$\forall x \in V(d,q), < x \mid x >= 0,$$

et enfin **non dégénérée** si :

$$\forall x \in V(d,q) \backslash \{0\}, \exists y \in V(d,q) \mid < x \mid y > \neq 0.$$

B.3 Autres « figures » de la géométrie projective

B.3.1 Le quadrangle

Définition :

Un **quadrangle généralisé** [PT84] est un espace presque linéaire tel que pour une ligne donnée L, et un point P n'appartenant pas à cette ligne, il y a exactement une ligne K passant par P qui coupe L en un point Q.

Ordre :

Un **quadrangle généralisé fini** est dit d'ordre (s,t) si chaque ligne contient $s+1$ points, et si chaque point est sur exactement $t+1$ lignes.

Remarque 6 : si $s=t$ alors on a un quadrangle d'ordre s.

Exemple important : le plus simple quadrangle généralisé, dans le cas où $s>1$ et $t>1$, est celui d'ordre 2, noté $W(2)$. C'est un objet dual (on peut intervertir le rôle des points et des lignes), possédant 15 points/lignes.

Hyperplans d'un quadrangle d'ordre (s,t) :

La grille :

Le premier hyperplan d'un quadrangle d'ordre (s,t) est un sous quadrangle d'ordre (s,t') tel que $t' < t$.

Pour certains quadrangles, dont ceux qui nous intéresserons en l'occurrence, un tel hyperplan se nomme **grille** et est alors un quadrangle généralisé fini d'ordre $(s, 1)$ ou $(1, t)$.

L'ovoïde :

Un **ovoïde** d'un quadrangle généralisé est un ensemble de points O tel que chaque ligne du quadrangle contient exactement un point de O, chaque ovoïde contient $st + 1$ points.

L'ensemble perpendiculaire :

Deux points x et y d'un quadrangle généralisé sont dits **colinéaires** si une ligne du quadrangle les rejoignent et on les note $x \sim y$ Soient x et y respectivement un point donné et des points du quadrangle, on définit l'**ensemble perpendiculaire** de x, noté $x^{\perp}$, comme suit :

$$x^{\perp} = \{y \mid y \sim x\}$$

Le quadrangle d'ordre 2 et ses hyperplans sont illustrés par des figures dans la section 5.1.3, les hyperplans du quadrangle généralisé d'ordre 3 le sont dans la section 5.3.3.

Annexe C

Un peu de théorie des graphes

C.1 Quelques définitions

C.1.1 Le graphe

Un **graphe** G est constitué de deux ensembles : un ensemble non vide de **sommets** $V(G)$ et un ensemble $E(G)$ formé de couples d'éléments de $E(G)$, nommés **arêtes**. Graphiquement, ces dernières relient deux points qui sont deux sommets de G. Les sommets sont appelés également **points**, et les arêtes, **lignes**.

C.1.2 L'adjacence

Deux sommets distincts sont dits **adjacents** si ils sont reliés par une arête ; de même, deux arêtes le sont si elles ont un sommet en commun. Si un sommet appartient à une arête, les deux sont aussi dits adjacents.

La **matrice d'adjacence** $A = [a_{ij}]$ d'un graphe G possédant v sommets $\left(\mid V(G) \mid^2 = v\right)$ est une matrice $v \times v$, pour laquelle $a_{ij} = 1$ si les sommets v_i et v_j (distincts) sont adjacents, $a_{ij} = 0$ sinon.

C.1.3 Le degré et le caractère régulier

Le **degré** D du sommet d'un graphe G est le nombre d'arêtes adjacentes à celui-ci. Un **graphe régulier** est un graphe pour lequel chacun de ses sommets possède le même degré.

Un **graphe fortement régulier** est un graphe régulier pour lequel chacun de deux sommets adjacents a le même nombre l de sommets adjacents, et pour lequel chacun de deux sommets non-adjacents a le même nombre n de sommets adjacents. La plupart du temps n est différent de l.

C.1.4 Le spectre

Le **spectre** d'un graphe G, noté $spec(G)$, est l'ensemble des valeurs propres dotées de leur **multiplicités** respectives (c'est-à-dire le nombre de fois où elles « apparaissent ») de sa matrice d'adjacence. Pour un graphe régulier, la valeur propre la plus grande correspond au degré du graphe et la valeur absolue des autres valeurs propres est toujours inférieure à D.

C.1.5 Isomorphisme

Deux graphes G et H sont dits **isomorphes** (notés $G \cong H$) si il existe une relation sommet à sommet qui préserve l'adjacence.

C.1.6 Les invariants

Un **invariant** d'un graphe G est un nombre associé à ce dernier qui conserve la même valeur pour chacun des graphes isomorphes à G. Un ensemble complet d'invariants caractériserait ainsi complètement un graphe, à un isomorphisme près ; mais, à ce jour, on n'en connaît pour aucun graphe.

Les plus importants invariants d'un graphe G sont les suivants : le nombre de ses sommets v ($\mid V(G) \mid = v$), celui de ses arêtes e ($\mid E(G) \mid = e$), le degré de chacun de ses sommets, sa **circonférence**, notée $g(G)$ (*girth*) : il s'agit de la longueur du **cycle** (séquence de sommets reliés en boucle) le plus court de G si il y en a, son **diamètre** : la plus grande distance séparant deux sommets. La **distance** entre deux sommets d'un graphe est la longueur (en terme de nombre d'arêtes) du chemin le plus court les reliant, s'il existe. Un autre invariant important de G s'appelle **nombre chromatique**, noté $\kappa(G)$. Le **coloriage d'un graphe** (problème NP–complet) consiste à affecter une couleur à un sommet de telle façon à ce que tous les sommets non adjacents entre eux soient de la même couleur ; si on note c le nombre minimum nécessaire de couleurs à utiliser, on a alors $\kappa(G) = c$.

La notion d'invariants est fondamentale dans toutes les sciences, et c'est souvent en les recherchant que les scientifiques « touchent du doigt » quelque chose d'important.

C.2 Graphes remarquables et opérations

C.2.1 Les sous graphes remarquables

Un **sous graphe** de G est un graphe dont l'ensemble des sommets et arêtes est contenu dans G.

Pour un ensemble S de sommets de G donné, on définit le **sous graphe induit** $\langle S \rangle$ de G comme étant le sous graphe maximal de G ayant comme ensemble de sommets S.

Un sommet et une arête se **recouvrent** mutuellement si ils sont adjacents. Un ensemble de sommets recouvrant toutes les arêtes d'un graphe G est appelé un **recouvrement de**

sommets de G ; celui qui possède le plus petit nombre d'éléments est nommé le **recouvrement minimum de sommets** de G. Ce dernier induit un sous graphe naturel de G, G', composé des sommets du recouvrement minimum et des arêtes les rejoignant originellement dans G.

Un **ensemble indépendant** (ou coclique) I d'un graphe G est un sous ensemble de sommets tel qu'aucune paire de sommets ne représente une arête dans G.

Si on considère le recouvrement minimum de G et le sous graphe induit G', un ensemble indépendant maximum I est constitué de tous les sommets n'appartenant pas à G'. Les graphes G' et I constituent ensemble une partition du graphe G.

C.2.2 Quelques graphes remarquables

Le **graphe complet** $\mathcal{K}_n$, d'ordre n, est l'unique graphe à isomorphisme près possédant n sommets tous reliés deux à deux par une arête.

L'ensemble des sommets d'un **graphe bipartite** se décompose en deux ensembles disjoints tels que deux sommets du graphe appartenant au même sous ensemble sont adjacents.

L'ensemble des sommets d'un **graphe tripartite** se décompose en trois ensembles disjoints tels que deux sommets du graphe appartenant au même sous ensemble sont adjacents.

Le graphe de Petersen :

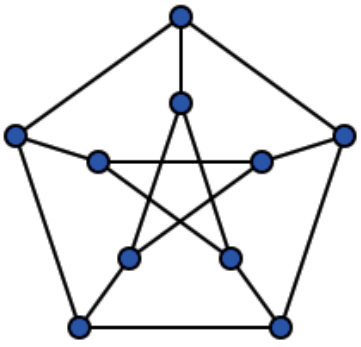


Fig. C.1 – Partition (PF) – (C)

Le graphe de Petersen est, en théorie des graphes, un graphe particulier possédant 10 sommets et 15 arêtes. Il s'agit d'un petit graphe qui sert d'exemple et de contre-exemple pour plusieurs problèmes de la théorie des graphes. Il porte le nom du mathématicien Julius Petersen qui l'introduisit en 1898.

C.2.3 Quelques opérations sur les graphes

Très souvent il est possible de décrire la structure d'un graphe de façon plus compacte en utilisant des graphes plus petits et des opérations s'appliquant sur ces derniers. On a, par exemple, la possibilité d'utiliser les opérations usuelles de la théorie des ensembles : **union**, **intersection**, **produit**, **complément** (pour le dernier, pratiquement, on inverse les 0 et les 1 de la matrice d'adjacence, etc.). Une autre opération, qui sera mentionnée à plusieurs reprises dans le chapitre 5, est ce qu'on appelle le **graphe d'incidence** (*line graph* en anglais), notée $L(G)$, de G : le nouveau graphe aura un sommet associé à chacune des arêtes de G, et possèdera une arête si et seulement si les deux arêtes de G partagent un sommet.

Table des figures

Liste des tableaux

Bibliographie

[ABG06] E Aïmeur, G. Brassard, and S. Gambs, *Machine learning in a quantum world*, Lecture Notes in Computer Science **4013** (2006), 431 – 442.

[ABG07] E. Aïmeur, G. Brassard, and S. Gambs, *Quantum clustering algorithms*, ICML '07 Proceedings of the 24th international conference on Machine learning (2007).

[ADR82] A. Aspect, J. Dalibard, and G. Roger, *Experimental test of Bell's inequalities using time-varying analyzers*, Phys. Rev. Lett. **49, Issue 25** (1982), 1804–1807.

[AE88] M. Born et H. Born A. Einstein, *Correspondance 1916-1955 (traduit de l'allemand par P. Leccia)*, Éditions Seuil (1972, 1988).

[AGR82] A. Aspect, P. Grangier, and G. Roger, *Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment : A new violation of Bell's inequalities*, Phys. Rev. Lett. **49, Issue 2** (1982), 91–94.

[Alb06] O. Albouy, *Bases maximalement décorrélées et théorie de l'information quantique*, ENS de Lyon, Sciences de la matière - Rapport de stage Master 2, 2006.

[Alt05] S. L. Altmann, *Rotations Quaternions and Double Groups*, Oxford, 2005.

[aMS07] M. Planat. and. M. Saniga, *Pauli graph and finite projective lines/geometries*, quant-ph/0703154v1 (2007).

[Art98] E. Artin, *Galois theory*, Dover Publications, Inc., 1998.

[Asp07] A. Aspect, *To be or not to be non local*, Nature **446** (2007), 866–967.

[Bat97] L. M. Batten, *Combinatorics of finite geometries - Second Edition*, Cambridge University Press, 1997.

[BB84] C. H. Bennett and G. Brassard, *Quantum cryptography : Public key distribution and coin tossing*, IEEE (1984), 175–179.

[BBRV02] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vartan, *A new proof for the existence of MUBs*, Algorithmica **34** (2002), 512.

[Bel66] J. S. Bell, *On the problem of hidden variables in quantum mechanics*, Rev. Mod. Phys. **38** (1966).

[Bel05] M. Le Bellac, *Introduction à l'informatique quantique*, Belin, 2005.

[BF02] R. Bonner and R. Freivalds, *A survey of quantum learning*, Third International Workshop, QCL (2002).

[Cab97] A. Cabello, *A proof with 18 vectors of the Bell-Kochen-Specker theorem*, M. Ferrero and A. van der Merwe (eds.), New Developments on Fundamental Problems in Quantum Physics, Kluwer Academic, Dordrecht, Holland (1997), 59–62.

[CEA97] A. Cabello, J. M. Estebaranz, and G. G. Alcaine, *Bell-Kochen-Specker theorem : A proof with 18 vectors*, quant-ph/9706009v1 (1997).

[Cla06] S. Clark, *Valence bond solid formalism for d-level one-way quantum computation*, J. Phys. A : Math. Gen. **39** (2006), 2701–2721.

[Cle02] F. De Clerck, *(alpha,beta)-geometries from polar spaces*, Summer School "Giuseppe Tallini", Brescia (2002).

[CLN05] A. Childs, D. Leung, and M. Nielsen, *Unified derivations of measurement-based schemes for quantum computation*, Phys. Rev. A **71** (2005), 032318.

[CN00] I. Chuang and M. Nielsen, *Quantum computation and quantum information*, Cambridge, 2000.

[Col06] G. P. Collins, *Computing with quantum knots*, Scientific American (2006).

[Con] A. Connes, *La pensée d'évariste Galois et le formalisme moderne*, ftp ://ftp.alainconnes.org/galoistext.pdf.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete*, Phys. Rev. **47 (15)** (1935), 777–780.

[Gle05] I. Glendinning, *The Bloch sphere*, QIA Meeting (2005).

[GPK+07] S. Gröblacher, T. Paterek, R. Kaltenbaek, C. Brukner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger, *An experimental test of non-local realism*, arXiv : 0704.2529 (2007).

[Gra06] M. Grassl, *Quantum designs : MUBs, SICPOVMs, and (a little bit) more*, Third Central European Quantum Information Processing Workshop (2006).

[Hav04] H. Havlicek, *Divisible Designs, Laguerre Geometry, and Beyond*, Summer School on Combinatorial Geometry and Optimisation, Italy (2004).

[Hav07] H Havlicek, *A Mathematician's insight into the Saniga-Planat theorem*, Keynote Lecture : Finite Projective Geometry in Quantum Theory, Tatranska Lomnica, Slovakia (2007).

[HDE+05] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. Briegel, *Entanglement in graph states and its applications*, in the Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos" (2005).

[HS07] H. Havlicek and M. Saniga, *Projective ring line of a specific qudit*, J. Phys. A : Math. Theor. (2007).

[Joz05] R. Jozsa, *An introduction to measurement-based quantum computation*, quant-ph/0508124v2 (2005).

[JP03] P. Jorrand and S. Perdrix, *Non-probabilistic termination of measurement-based quantum computation*, quant-ph/ 0311122v2 (2003).

[JP04] P Jorrand and S Perdrix, *Unifying quantum computation with projective measurements only and one-way quantum computation*, quant-ph/ 0404125v1 (2004).

[KABW10] M. R. Kibler, M. Atakishiyev, N. Bernardo, and K. Wolf, *SU(2) and SU(1,1) approaches to phase operators and temporally stable phase states : Applications to mutually unbiased bases and discrete Fourier transforms*, Symmetry **2** (2010), 1461.

[Kem03] J. Kempe, *Quantum random walks - an introductory overview*, Contemporary Physics **44** (2003), 307–327.

[Ker94] M. Kernaghan, *Bell-Kochen-Specker theorem for 20 vectors*, J. Phys. A **27** (1994), 829.

[Kib08] M. R. Kibler, *Variations on a theme of Heisenberg, Pauli and Weyl*, J. Phys. A : Math. Theor. **41** (2008), 375302.

[Kib09] M R. Kibler, *An angular momentum approach to quadratic Fourier transform, Hadamard matrices, Gauss sums, mutually unbiased bases, unitary group and Pauli group*, J. Phys. A : Math. Theor. **42** (2009), 353001.

[Kib10] M. R Kibler., *Quadratic discrete Fourier transform and mutually unbiased bases*, Fourier Transforms, Theory and Applications, G. Nikolic (Ed.) (2010).

[KP95] M. Kernaghan and A. Peres, *Kochen-Specker theorem for eight-dimensional space*, Phys. Lett. A **198** (1995), 1–5.

[KS67] S. Kochen and E.P. Specker, *The problem of hidden variables in quantum mechanics*, Journal of Mathematics and Mechanics **17** (1967), 59–87.

[KSSdG05] A. Klimov, L. Sanchez-Soto, and H. de Guise, *Multicomplementary operators via finite Fourier transform*, J. Phys. A **38** (2005), 2747–2760.

[Lal06] M. Lalire, *Développement d'une notation algorithmique pour le calcul quantique*, Ph.D. thesis, Laboratoire Leibniz de Grenoble, 2006.

[Law04] J. Lawrence, *Mutually unbiaised bases and trinary operators sets for N qutrits*, Phys. Rev. A. **70** (2004), 012302.

[LBZ02] J. Lawrence, C. Brukner, and A. Zeilinger, *Mutually unbiaised binary observable sets on N-qubits*, Phys. Rev. A **65** (2002), 0322320.

[Leg03] A. J. Leggett, *Non local hidden-variable theories and quantum mechanics : An incompatibility theorem*, Foundations of Physics **33** (2003), 1469–1493.

[Leu02] D. Leung, *Two-qubit projective measurements are universal for quantum computation*, quant-ph/ 0111122v2 (2002).

[Leu04] D Leung, *Quantum computation by measurements*, International Journal of Quantum Computation **2 :33** (2004).

[LN97] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[Mer90a] N. D. Mermin, *Simple unified form for the major no-hidden-variables theorems*, Phys. Rev. Lett. **65** (1990), 3373.

[Mer90b] N D Mermin, *What's wrong with these elements of reality ?*, Physics Today **43, Issue 6** (1990), 9–11.

[Mer93] N. D. Mermin, *Hidden variables and two theorems of John Bell*, Rev. Mod. Phys. **65 (3)** (1993), 803–815.

[NC97] M. Nielsen and I. Chuang, *Programmable quantum gates array*, Phys. Rev. Lett. **79** (1997), 321–324.

[Nie03] M. Nielsen, *Universal quantum computation using projective measurements, quantum memory and preparation of the 0 state*, Phys. Rev. A **308** (2003), 96–100.

[oP00] Stanford Encyclopedia of Philosophy, *The Kochen-Specker theorem*.

[PB07] M. Planat and A-C Baboin, *Qudits of composite dimension, mutually unbiaised bases and projective ring geometry*, J. Phys. A 40, F1005 **40** (2007).

[PBS07] M. Planat, A-C Baboin, and M. Saniga, *Multi-line geometry of qubit-qutrit and higher-order Pauli operators*, Int. J ; Theor. Phys. **70** (2007).

[Pen92] R. Penrose, *L'esprit, l'ordinateur et les lois de la physique*, InterEditions, 1992.

[Per91] A. Peres, *Two simple proofs of the Kochen-Specker theorem*, J. Phys. A : Math. Gen **24** (1991), 175–178.

[Per05] S. Perdrix, *State transfer instead of teleportation in measurement-based quantum computation*, International Journal of Quantum Computation **3 (1)** (2005), 219–223.

[Per06] S Perdrix, *Modèles formels du calcul quantique : ressources, machines abstraites et calcul par mesure*, Ph.D. thesis, Laboratoire Leibniz de Grenoble, 2006.

[PJ08] M. Planat and P. Jorrand, *On group theory for quantum gates and quantum coherence*, Journal of Physics A Mathematical and Theoretical **41** (2008).

[PK10] M. Planat and M. Kibler, *Unitary reflection groups for quantum fault tolerance*, Journal of Computational and Theoretical Nanoscience **7** (2010), 1759–1770.

[Pla09] M. Planat, *Clifford group dipoles and the enactment of Weyl/Coxeter group W(E8) by entangling gates*, hal-00378095-version 4 (2009).

[Pla10a] M Planat, *Clifford quantum computer and the Mathieu groups*, Invertis Journal of Science and Technology **3,2** (2010), 1–4.

[Pla10b] M. Planat, *Three-qubit entangled embeddings of CPT and Dirac groups within E8 Weyl group*, International Journal of Theoretical Physics **24** (2010), 1044–1054.

[Pla11] M. Planat, *Pauli graphs when the Hilbert space dimension contains a square : why the Dedekind psi function ?*, J. Phys. A : Math. Theor. **44** (2011).

[PR05] M. Planat and H. Rosu, *Mutually-unbiaised phase states, phase uncertainties and Gauss sums*, Eur. Phys. J **D 36** (2005), 133–139.

[PS08] M. Planat and M. Saniga, *On the Pauli graphs of N-qudit*, Quantum Information and Computation **1-2** (2008), 127–146.

[PS09] M. Planat and P. Solé, *Clifford groups of quantum gates, BN-pairs and smooth cubic surfaces*, Journal of Physics A Mathematical and Theoretical **42** (2009).

[PSK06] M. Planat, M. Saniga, and M. Kibler, *Quantum entanglement and projective ring geometry*, SIGMA **2 : paper 66** (2006).

[PT84] S. E. Payne and J. A. Thas, *Finite generalized quadrangles. Research Notes in Mathematics*, Boston, MA, 1984.

[Rau03] R. Raussendorf, *Measurement-based quantum computation with cluster states*, Ph.D. thesis, 2003.

[SG04] R. A. Servedio and S. J. Gortler, *Equivalences and separations between quantum and classical learnability*, SIAM J. Comput. **33** (2004), 1067 – 1092.

[Sin99] S. Singh, *Histoire des codes secrets*, Poche, 1999.

[SP07a] M Saniga and M Planat, *Multiple qubits as symplectic polar spaces of order two*, Advanced Studies in Theoretical Physics **1** (2007), 1 – 4.

[SP07b] M. Saniga and M. Planat, *The projective line over the finite quotient ring $Z_2[x]/ < x^3 - x >$ and quantum entanglement : Theoretical background*, Theoretical and Mathematical Physics **151** (2007), 475–482.

[SPK06] M. Saniga, M. Planat, and M. Kibler, *A classification of the projective lines over small rings - 2. non commutative case*, math. AG/0606500 (2006).

[SPKP07] M. Saniga, M. Planat, M. Kibler, and P. Pracna, *A classification of the projective lines over small rings*, Chaos, Solitons and Fractals **33** (2007), 1095–1102.

[SPP08] M. Saniga, M. Planat, and P. Pracna, *Projective ring line encompassing two qubits*, Theoretical and Mathematical Physics **155** (2008), 905–913.

[SPR04] M. Saniga, M. Planat, and H. Rosu, *Mutually unbiaised bases and finite projective planes*, J. Opt. B : Quantum Semiclass Opt. **6** (2004), 19–20.

[Str08] N. Straumann, *A simple proof of the Kochen-Specker theorem on the problem of hidden variables*, arXiv :0801.4931v1 (2008).

[Sua07] A. Suarez, *Time and non-local realism : consequences of the before-before experiment*, arXiv : 0708.1997 (2007).

[SZGS02] A. Stefanov, H. Zbinden, N. Gisin, and A. Suarez, *Quantum correlations with spacelike separated beam splitters in motion : Experimental test of multisimultaneity*, Phys. rev. Lett. **88** (2002).

[Tha71] J. Thas, *The m-dimensional projective space Sm(Mn(GF(q))) over the total matrix algebra Mn(GF(q)) of the $n \times n$ matrices with elements in the Galois Field GF(q)*, Rend Mat Roma **4** (1971), 459–532.

[Tha07] K. Thas, *Pauli operators of N-qubit Hilbert spaces and the Saniga-Planat conjecture*, Chaos, Solitons and Fractals (2007).

[Tur36] A. Turing, *On computable numbers with an application to the Entscheidungsproblem*, Proc. London Math. Soc, Ser. 2, Vol. 43,. No. 2198 (1936).

[VC04] F. Verstraete and J. Cirac, *Valence-bond state for quantum computation*, Phys. Rev. A **70** (2004), 060302(R).

[Vou07] A. Vourdas, *Quantum systems in finite Hilbert space : Galois fields in quantum mechanics*, J. Phys. A : Math. Theor. **40** (2007), 285–331.

[Wol91] P. Wolper, *Introduction à la calculabilité*, Dunod, 1991.

Résumé

Cette thèse a pour première vocation d'être un état de l'art sur le calcul quantique, sinon exhaustif, simple d'accès (chapitres 1, 2 et 3). La partie originale de cet essai consiste en deux approches mathématiques du calcul quantique concernant quelques systèmes quantiques : la première est de nature algébrique et fait intervenir des structures particulières : les corps et les anneaux de Galois (chapitre 4), la deuxième fait appel à la géométrie dite projective (chapitre 5). Cette étude a été motivée par le théorème de Kochen et Specker et par les travaux de Peres et Mermin qui en ont découlé.

Abstract

The first vocation of this thesis would be a state of the art on the field of quantum computation, if not exhaustive, simple access (chapters 1, 2 and 3). The original (interesting) part of this treatise consists of two mathematical approaches of quantum computation concerning some quantum systems : the first one is an algebraic nature and utilizes some particular structures : Galois fields and rings (chapter 4), the second one calls to a peculiar geometry, known as projective one (chapter 5). These two approaches were motivated by the theorem of Kochen and Specker and by work of Peres and Mermin which rose from it.