Thèse de doctorat
Université Bordeaux 1

Spécialité :
Mathématiques Pures

École doctorale :
Mathématiques et Informatique

Présentée par
Nicolas Delfosse

Constructions et performances de codes LDPC quantiques

Dirigée par Gilles Zémor

Soutenue le 12 décembre 2012 devant le jury composé de :

Christine Bachoc	Professeure - IMB - Université Bordeaux 1	examinatrice
Cyril Gavoille	Professeur - LaBRI - Université Bordeaux 1	président
Renato Renner	Professeur - ETH Zürich	rapporteur
Jean-Pierre Tillich	Chargé de Recherche - INRIA Rocquencourt	rapporteur
Rüdiger Urbanke	Professeur - EPFL Lausanne	examinateur
Gilles Zémor	Professeur - IMB - Université Bordeaux 1	directeur

Institut de Mathématiques de Bordeaux
351, cours de la Libération
F 33405 TALENCE cedex

Table des matières

Table des figures

Remerciements

En premier lieu, j'aimerais remercier Gilles Zémor de m'avoir permis de découvrir ce domaine de recherche passionnant. C'est d'abord le sujet de mémoire de master 2 qu'il a proposé qui a attiré mon attention. Le fan de science-fiction que je suis ne pouvait pas rester insensible à une première phrase comme : «Si l'ordinateur quantique doit voir le jour, ce ne se fera que grâce à l'aide des correcteurs quantiques». Ce mémoire a ensuite débouché sur une thèse que Gilles a encadré avec une grande pédagogie. J'ai régulièrement été impressionné par la facilité avec laquelle, après quelques instants de réflexion, il rendait tout à fait intuitif un raisonnement que je ne parvenais pas à cerner depuis plusieurs jours. Travailler avec Gilles a été une expérience extrêmement enrichissante.

Je remercie la DGA qui a financé cette thèse et le CNRS pour sa gestion administrative. Merci à l'Université Bordeaux 1 et à l'Institut de Mathématiques de Bordeaux de m'avoir fourni un cadre de travail idéal.

Je suis très honoré que Renato Renner et Jean-Pierre Tillich aient accepté de rapporter cette thèse. Je remercie Renato Renner pour l'attention qu'il a prêté à ce manuscrit. Je remercie également Jean-Pierre Tillich pour son soutien et ses conseils, ainsi que pour l'intérêt qu'il a porté à mes travaux. Je tiens également à remercier Christine Bachoc, Cyril Gavoille et Rüdiger Urbanke d'avoir accepté de faire partie du jury.

Les premiers mois de ma thèse furent consacrés à l'étude de la théorie de l'information quantique et à la compréhension des différentes définitions du canal à effacement quantique. Je remercie Damian Markham pour son soutien et ses éclairages à ce sujet.

Mes remerciements s'adressent ensuite à Alain Couvreur qui nous a rejoint à Bordeaux lors de ma seconde année de thèse et avec qui nous avons travaillé sur des constructions de codes basées sur des graphes de Cayley. Ses intuitions géométriques, souvent illustrées par des diagrammes, me font regretter de ne pas maîtriser les outils de la géométrie algébrique aussi bien que lui. Mais à vrai dire je crois que je préfère dessiner des graphes. Je le remercie aussi pour son soutien et pour ses conseils fréquents. Alain a aussi participé à l'extension de la communauté du codage quantique en réussissant à convaincre Benjamin Audoux d'utiliser ses connaissances sur l'homologie de Khovanov dans le cadre des codes LDPC quantiques. J'en profite donc pour remercier Benjamin d'avoir accepté de passer une semaine à Bordeaux pour nous présenter les jolis objets sur les lesquels il travaille.

Différents objets combinatoires apparaissent dans mon domaine de recherche, la

proximité du LaBRI m'a permis d'assister occasionnellement à des exposés sur ces thèmes. Je remercie Jean-François Marckert pour son aide au sujet de l'utilisation de séries génératrices. Je remercie Jérôme Javelle, Simon Perdrix et Mehdi Mhalla de m'avoir accueilli quelques jours à Grenoble et pour leurs explications concernant les états graphes et les partages de secrets.

A la fin de ma thèse, je me suis intéressé à la notion de systole qui est apparu dans le domaine des codes correcteurs quantiques avec les travaux de Freedman, Meyer et Luo. Ceci m'a poussé à aller déranger des géomètres de l'IMB. Je remercie Christophe Bavard et Louis Merlin de m'avoir écouté et de m'avoir fait profiter de leurs connaissances sur le sujet.

Je remercie David Poulin et toute son équipe de m'avoir accueilli chaleureusement pendant quelques jours à Sherbrooke. Je remercie également Sergey Bravyi de m'avoir proposé de lui rendre visite au superbe laboratoire d'IBM à Yorktown Heights.

Je tiens à remercier le Laboratoire d'Informatique de l'École Polytechnique qui m'accueille pour l'année 2012-2013. Merci tout particulièrement à l'équipe Crypto, très conviviale, Daniel Augot, François Morain, Françoise Levy-dit-Vehel, Ben Smith, Alain Couvreur, Guillaume Quintin dont la porte est toujours ouverte, Cécile Gonçalves, Julia Pieltant, Johan Nielsen et Claire Lucas. Merci à Alexander Zeh de m'avoir fait découvrir Chez Gladines. Je remercie aussi Eric Fusy, Ekaterina Vassilieva et l'ensemble de l'équipe Combinatoire du LIX.

Un grand merci à Nicola et Aurélien pour ces quelques années de vie à trois au bureau 376. Merci de m'avoir dit que je faisais de jolis dessins au tableau sans vous sentir obligés de demander ce qu'ils signifiaient (moi non plus je ne sais pas trop). Félicitation Nicola, tu hérites officiellement du business des paris sportifs. Aurélien, à nous deux, nous cumulons 18 années passées à Bordeaux 1 (c'est une équation diophantienne), merci pour ton humour toujours de mauvais goût. J'ai eu l'occasion de participer aux nombreuses activités organisées par l'association des doctorants de l'IMB. Je remercie donc nos chers organisateurs Fred et Claire, puis Arthur et Louis, notamment pour l'organisation du groupe de travail Parcelle. Merci à Pierre qui est toujours disponible pour discuter devant un café et à Pierre qui est toujours disponible pour discuter devant un coca. Merci à Giovanni de nous apprendre des expressions italiennes charmantes, à Jean-Matthieu pour ses conseils en informatique, à Sophie d'être toujours de bonne humeur et toujours en voyage, à Vincent, notre spécialiste du café, parti se perfectionner au Brésil, à Fabien qui n'aime pas prêter son trône et à Cédric et Guillaume dont la subtilité des jeux de mots nous manque. Merci à Diomba puisqu'il faut bien un perdant pour les paris. Je pense aussi à Dimitri qui n'est plus bordelais. Je le remercie de m'avoir fait découvrir la Poutine et surtout les écureuils mangeurs de Poutine. Merci à Guihlem pour ses explications cryptographiques et ses conseils. Un grand merci à Bertrand pour ses nombreux conseils lors de mon arrivée à Paris. Pour terminer ce paragraphe dédié aux bordelais, je souhaite remercier l'ensemble de mes collègues de l'institut de mathématique et les enseignants de ce laboratoire qui m'ont marqué. Je pense notamment à Alain Hénaut que je remercie pour ses cours de géométrie

avec les mains, à Philippe Cassou-Noguès dont les cours d'algèbre sont un exemple de pédagogie, et à Jean Fresnel qui a toujours été disponible.

Je pense également aux codeurs et cryptographes que je rencontre régulièrement en conférence, qu'ils soient quantiques : Mamdouh Abbara, Denise Maurice, Anne Marin, ou classiques : Morgan Barbier, Matthieu Legeay, Vincent Herbert, Julien Schrek et Slim Bettaieb, Luca De Feo.

Je pense à mes amis Coutrions ou Beychacais-et-Caillalais : Ben, petit, Pyoul, qui était contre, Remy, exilé fiscal, Vincent et toutes ses motos, qui m'accompagnent depuis de nombreuses années. Enfin, je remercie ma famille, mes grand-parents, mes parents et mon frère Guillaume. Merci à mes grand-parents pour le paté de lièvre, toujours délicieux, qu'ils ont préparé pour le pot. Un grand merci à mes parents qui m'ont toujours soutenu durant ces trois dernières années ainsi que les précédentes. Ils ont eu la lourde tache de jouer le rôle du correcteur d'orthographe et il ne leur a fallu qu'un week-end pour lire l'ensemble de cette thèse. Ce fut un bel anniversaire pour ma mère. Merci à Guillaume d'avoir accépté de subir ma dernière répétition. Je remercie finalement ma petite Chloé pour ses nombreuses relectures, ses conseils et dont la présence à mes côtés m'est indispensable.

Introduction

Contexte

L'intérêt pour la théorie de l'information quantique n'a cessé de croître depuis près de vingt-cinq ans. Ces recherches ont d'abord été justifiées par l'impossibilité de simuler un système quantique avec un calculateur classique remarquée par Feynman en 1982 [44]. Deux ans plus tard, Bennett et Brassard ont proposé un protocole de partage de clé dont la sécurité, inconditionnelle, repose sur les lois de la mécanique quantique [9]. Enfin, des algorithmes quantiques plus efficaces que leurs versions classiques ont été proposés, le plus emblématique étant l'algorithme de factorisation de Shor qui permet de factoriser les entiers en temps polynomial [86].

Nous nous intéressons à ce modèle d'information quantique. Les états quantiques sont des superpositions d'états classiques. L'efficacité des algorithmes quantiques est basée sur l'utilisation de ces superpositions. L'interaction d'un système quantique avec son environnement projette ces états quantiques sur leurs composantes classiques, d'où la nécessité de protéger ces fragiles superpositions quantiques. Dans cette optique, Shor a proposé le premier code correcteur quantique en 1995 [87]. Cet exemple a été suivi par l'introduction de la famille des codes CSS par Calderbank, Shor et Steane [28, 90], généralisée par Gottesman sous la forme des codes stabilisateurs [51]. Ces différentes constructions offrent une grande variété de codes quantiques. Les codes quantiques construits par ces procédés sont définis à partir de codes classiques. Ils permettent de transférer certaines stratégies de la théorie des codes classiques vers le codage quantique. Nous chercherons à comprendre comment protéger l'information quantique grâce aux méthodes issues du codage classique moderne et des codes LDPC (Low Density Parity–Check) de Gallager [49].

Les codes LDPC sont très utilisés aujourd'hui car ils permettent de transmettre de l'information avec un rendement élevé, tout en disposant d'un algorithme de décodage efficace et performant. La connaissance d'un tel algorithme est essentielle sinon les messages reçus s'accumulent sans pouvoir être décodés. Il a été démontré que cette famille de codes atteint la capacité du canal à effacement et récemment qu'elle atteint la capacité du canal binaire symétrique. Le but de cette thèse est d'étudier leur analogue quantique.

Le premier chapitre est consacré aux prérequis de théorie de l'information quantique. Nous présentons les bases de mécanique quantique nécessaires, ou plutôt le modèle mathématique décrivant les systèmes quantiques et leur évolution. Nous expliquons ensuite ce qui joue le rôle de l'information et nous définissons les codes correcteurs quantiques et les canaux quantiques. Enfin, nous détaillons le formalisme des codes stabilisateurs. Cette famille de codes quantiques fait le lien entre

codes quantiques et classiques. La sous-famille des codes CSS permet notamment de construire un code quantique à partir de deux codes classiques orthogonaux.

Deux grandes familles des codes LDPC quantiques

La première question qui se pose concernant les codes LDPC quantiques est de savoir s'il est possible de construire d'en construire de bons, c'est-à-dire des codes possédant un bon rendement et pour lesquels un décodage efficace et performant est possible. Les constructions de codes LDPC quantiques peuvent être regroupées en deux grandes familles.

La première famille est composée des codes quantiques issus directement de la théorie classique. Ces codes peuvent être décodés avec un algorithme classique. Les méthodes aléatoires fournissent de bons codes LDPC classiques. Malheureusement, les conditions d'orthogonalité sur les matrices de parité rendent difficile la mise en place de telles constructions. Les codes LDPC quantiques issus de constructions classiques sont basés sur des familles de codes LDPC classiques qui satisfont les conditions d'orthogonalité. De tels codes quantiques ont été construits à partir des familles classiques de codes LDPC basés, par exemple, sur des géométries finies, des carrés latins, des objets combinatoires ou des codes quasi-cycliques [1,2,29,57,73,84]. L'inconvénient majeur de ces constructions est leur distance minimale qui est souvent constante ou bornée. On ne peut donc pas espérer un décodage performant pour de grandes longueurs. De plus, le décodage itératif utilisé pour ces familles ne tient pas compte du caractère quantique ce qui laisse une grande marge d'amélioration.

Pour ces raisons, nous nous sommes concentrés sur les codes LDPC quantiques dits topologiques. Cette seconde grande famille de codes LDPC quantiques est issue de l'idée de Kitaev, qui a proposé de construire une famille de codes quantiques à partir d'un pavage carré du tore, en 1997 [66]. Cette méthode permet plus généralement d'associer un code LDPC quantique à un pavage de surface. On parle de codes de surface [18]. De nombreuses variantes de ces codes topologiques ont été proposées. On peut citer, par exemple, les codes couleur basés sur des pavages coloriés [17], des codes basés sur des pavages tridimensionnels [19, 22, 56] ou sur des surfaces à bords [21] ou encore les codes topologiques de sous-système utiles en calcul quantique [4, 14]. Ces codes ne sont pas seulement utiles du point de vue de la théorie de l'information, ils sont aussi à la base du calcul topologique quantique. Ces codes présentent l'avantage de bien faire apparaître l'aspect quantique du décodage. Ceci a permis de mettre en place des algorithmes surpassant le décodage itératif. C'est ce qui nous pousse à nous intéresser principalement à cette famille. L'inconvénient majeur de la plupart des codes topologiques étudiés est leur faible dimension. En effet, la majorité des travaux effectués concernent le code torique ou des codes similaires qui sont de dimension constante. Pour obtenir des codes de rendement élevé, on peut considérer des surfaces de genre élevé.

Les codes topologiques

Le chapitre 2 commence avec les rappels nécessaires sur les codes de surface. Nous expliquons comment définir un code quantique à partir d'un pavage de surface, mais aussi comment ses paramètres s'interprètent géométriquement. Le genre de la

surface nous donne la dimension et la longueur d'un plus court cycle d'homologie non triviale est la distance minimale. Nous rappelons ensuite la construction des codes de surface hyperboliques de Zémor [100]. Ces codes forment l'une des rares familles de codes de surface de rendement constant et de distance croissante [47, 65, 100].

Les codes couleur sont, avec les codes de surface, les codes topologiques les plus étudiés [17]. Ils présentent des avantages en calcul topologique. Pour construire de tels codes, il suffit de se donner un pavage de surface trivalent dont les faces sont 3-coloriables. Dans ce chapitre nous démontrons qu'un tel pavage hyperbolique existe en définissant un revêtement adapté de pavages hyperboliques trivalents. Nous obtenons ainsi une généralisation des codes de surface hyperboliques aux codes couleur. Ces codes couleur hyperboliques forment une nouvelle famille de codes topologiques de rendement constant et de distance croissante.

Ces deux familles de codes hyperboliques surpassent tous les codes définis par des générateurs locaux sur un pavage carré. En effet, Bravyi Poulin et Terhal ont démontré que les paramètres de ces codes sont limités par une équation de la forme $kd^2 \leq cn$ pour une constante c qui ne dépend que de la localité des générateurs [23]. L'utilisation des pavages hyperboliques nous permet de nous soustraire à cette borne. Il est donc naturel de chercher une généralisation de la borne de Bravyi Poulin et Terhal qui s'adapte à tous type de pavage. Grâce à des résultats de Gromov sur la géométrie systolique [54], nous démontrons que les codes de surface et les codes couleur, définis sur des pavages dont les longueurs des faces et les degrés des sommets sont bornés par une constante m, sont sujets à une borne de la forme :

$$kd^2 \leq c(\log k)^2 n,$$

pour une constante c. Cette nouvelle borne s'applique notamment aux codes hyperboliques de Zémor et à notre nouvelle famille de codes couleur hyperboliques. On démontre ainsi que les paramètres de ces deux familles de codes sont optimaux à une constante près.

Une construction exotique de codes LDPC quantiques

Le chapitre 3 est consacré à l'étude d'une nouvelle construction de codes LDPC quantiques. Ce travail a été réalisé avec Alain Couvreur et Gilles Zémor et présenté lors de la conférence ISIT 2012 [32,33]. Nous nous penchons sur une famille proposée par MacKay, Mitchison et Shokrollahi dans un article nommé « More Sparse Graph Codes for Quantum Error-Correction » en 2007. Cette construction est basée sur le graphe de Cayley de $\mathbb{F}_2^n$ engendré par les colonnes d'une matrice de parité d'un code classique. Leurs résultats numériques semblaient prometteurs mais rien n'était connu des paramètres de ces codes. Nous proposons dans ce chapitre une borne inférieure générale sur la distance minimale du code quantique en $O(dn^2)$ où d est la distance minimale du code classique.

Lorsque le code classique est le code de répétition de paramètres $[n, 1, n]$, nous obtenons exactement les paramètres du code quantique associé. La dimension et la distance minimale sont toutes les deux en $O(\sqrt{N})$ où N est la longueur du code quantique. Il s'agissait d'une question laissée ouverte par Shokrollahi.

Étude des performances des LDPC quantiques

Afin de pouvoir étudier les performances des codes LDPC quantiques nous devons introduire la capacité d'un canal quantique. C'est l'objet du chapitre 4. Nous détaillons deux exemples qui illustrent bien les particularités quantiques. Le premier est le canal de dépolarisation. C'est l'analogue du canal binaire symétrique et c'est l'un des canaux les plus utilisés. Le problème est que nous ne disposons pas de formule simple pour sa capacité. La détermination de cette valeur est l'un des problèmes centraux de la théorie de l'information quantique.

Nous présentons ensuite le canal à effacement quantique. Il s'agit d'un canal quantique dont la capacité est connue. Cette valeur a été calculée grâce au théorème de non-clonage, en 1997, par Bennet, DiVicenzo et Smolin [10]. Lorsque nous nous intéressons aux performances d'une famille de codes, cette borne de non-clonage, qui ne dépend pas des codes utilisés, semble difficile à préciser. Nous proposons dans ce chapitre une preuve purement combinatoire du calcul de la capacité du canal à effacement quantique, pour les codes stabilisateurs. Á notre connaissance cette approche de la capacité quantique est originale et offre de nouveaux outils pour étudier les codes stabilisateurs d'une part et la capacité du canal de dépolarisation d'autre part.

Le chapitre 5 est consacré à l'étude des performances des codes LDPC quantiques. En suivant l'évolution de la théorie des codes classiques, nous étudions les performances des codes LDPC quantiques sur le canal à effacement, plutôt que sur le modèle d'erreur le plus répandu : le canal de dépolarisation. Ceci est motivé par plusieurs raisons. Le modèle des effacements présente l'avantage d'être plus simple que le canal de dépolarisation, pour lequel même la capacité est inconnue. De plus, la ressemblance entre ces deux canaux est forte, on peut donc raisonnablement espérer que de bons codes pour le canal à effacement se comporteront bien pour le canal de dépolarisation.

Nous établissons dans ce chapitre une borne supérieure sur le rendement des codes stabilisateurs dont les générateurs sont de poids borné. Nous précisons ensuite cette borne pour les codes CSS de type (ℓ, m) qui sont définis par des matrices dont les lignes sont de poids m et dont les colonnes sont de poids ℓ.

Cette borne supérieure sur les performances des codes LDPC quantiques réguliers prouve qu'ils n'atteignent pas la capacité du canal à effacement. Nous en déduirons certaines caractéristiques nécessaires pour approcher la capacité du canal. Par exemple, nous démontrons que pour atteindre la capacité de ce canal, certaines lignes de la matrice stabilisatrice du code quantique doivent avoir un poids non borné. Ce résultat est similaire au cas classique. Ce chapitre est le fruit d'un travail en commun avec Gilles Zémor et a donné lieu à un article soumis [37]. Ces résultats ont été présentés lors de la conférence « Quantum Error Correction 2011 » à Los Angeles.

Le chapitre 6 est une application de la théorie de l'information quantique en combinatoire. Il concerne le phénomène de percolation. Dans une première partie nous

expliquons la ressemblance entre effacements quantiques et théorie de la percolation. Ensuite, nous nous intéressons au cas des codes hyperboliques. On utilise une famille de codes construits à partir de pavages hyperboliques auto-duaux finis et on considère le seuil de percolation de leur revêtement hyperbolique infini. Nous parvenons à démontrer que, lorsque la probabilité d'effacement est sous le seuil de percolation du revêtement infini de ce graphe, la probabilité d'erreur par qubit tend vers 0. En utilisant ceci, nous bornons le seuil de percolation en fonction de la borne supérieure sur la capacité du canal à effacement. Enfin, notre borne sur les performances des codes LDPC quantiques s'applique ici pour améliorer cette borne sur le seuil de percolation des graphes hyperboliques auto-duaux. Ce résultat a été obtenu avec Gilles Zémor et fait l'objet de l'article [37]. Une version préliminaire a été publié à l'occasion de la conférence ITW 2010 [36].

Décodage des codes topologiques

Le dernier chapitre de cette thèse s'adresse au problème du décodage des codes topologiques. Plusieurs idées ont été développées pour décoder ces codes LDPC quantiques. On peut essayer d'adapter le décodage itératif classique à la famille des codes LDPC quantiques [29,78]. Duclos-Cianci et Poulin ont proposé un algorithme par groupe de renormalisation basé sur des idées de la physique statistique [40]. Nous nous intéressons plus particulièrement au décodage par couplage parfait de Wang, Fowler, Stephens, et Hollenberg [95]. Nous commençons par rappeler le fonctionnement de ce décodage des codes de surface.

Dans un second temps, nous nous concentrons sur le décodage des codes couleur. Nous proposons un nouvel algorithme de décodage de ces codes par couplage parfait. C'est le résultat principal de ce chapitre. Cet algorithme est basé sur la projection d'une erreur agissant sur le code couleur sur une erreur agissant sur un code de surface. Les performances de notre implémentation de ce décodage dépassent celles de Raussendorf et Sarvepalli pour une famille de codes couleur définis sur un pavage hexagonal du tore [85]. Ce procédé de décodage a aussi des conséquences théoriques. Il nous permet de transférer des résultats des codes de surface vers les codes couleur. Nous obtenons ainsi une borne sur le seuil d'erreur tolérable d'une famille de codes couleur en fonction des seuils d'erreur tolérables des codes de surface.

Chapitre 1

Prérequis de théorie de l'information quantique

1.1 Les axiomes de la mécanique quantique

1.1.1 L'état d'un système quantique

Dans cette partie nous rappelons les axiomes de la mécanique quantique tels que nous les utilisons dans le contexte de la théorie de l'information quantique.

Axiome 1.1 : *état d'un système.* *A tout système quantique isolé est associé un espace de Hilbert. Le système est entièrement décrit par un vecteur unitaire de cet espace de Hilbert.*

Ce vecteur est appelé *l'état du système*. Il est noté $|\psi\rangle$ en suivant les notations de Dirac. La notation $|\psi\rangle$ désigne un vecteur d'un espace de Hilbert $\mathcal{H}$. Son vecteur dual est noté $\langle\psi|$. C'est un vecteur de l'espace $\mathcal{H}^\star$ des formes linéaires sur $\mathcal{H}$ à valeurs complexes. En appliquant cette forme linéaire à un vecteur $|\phi\rangle$ de $\mathcal{H}$, on obtient $\langle\psi|.|\phi\rangle = \langle\psi|\phi\rangle$ ce qui justifie cette notation. Le projecteur orthogonal sur le vecteur unitaire $|\psi\rangle$ est donc noté $|\psi\rangle\langle\psi|$ de sorte que $|\psi\rangle\langle\psi|.|\phi\rangle = \langle\psi|\phi\rangle|\psi\rangle$.

Considérons le cas de l'espace de Hilbert $\mathbb{C}^2$. On note $|0\rangle$ et $|1\rangle$ deux vecteurs de $\mathcal{H}$ formant une base orthonormale. Par exemple, posons :

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

Tout état $|\psi\rangle$ de cet espace est de la forme :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \text{ avec } |\alpha|^2 + |\beta|^2 = 1.$$

On parle d'un bit quantique ou *qubit*. On peut le voir comme une superposition des bits classiques 0 et 1. Le vecteur $\langle 0|$ est dans ce cas la forme linéaire qui envoie le $|0\rangle$ sur $\langle 0|0\rangle = 1$ et qui envoie $|1\rangle$ sur $\langle 0|1\rangle = 0$. En appliquant cette forme linéaire au vecteur $|\psi\rangle$ on arrive à $\langle 0|\psi\rangle = \alpha$.

1.1.2 Évolution d'un système quantique

Dans cette partie, nous décrivons les deux types d'évolution possibles d'un système quantique.

Axiome 1.2 : *évolution.* *L'évolution du système est unitaire. Si $|\psi\rangle$ est l'état du système au temps t et $|\psi'\rangle$ est l'état du système au temps t' alors il existe un opérateur unitaire U tel que :*

$$|\psi'\rangle = U|\psi\rangle.$$

Revenons à l'exemple du système quantique de dimension 2. L'état du système est $\alpha|0\rangle+\beta|1\rangle$ avec α et β des nombres complexes tels que $|\alpha|^2+|\beta|^2 = 1$. Supposons que l'évolution du système corresponde à l'opérateur unitaire de matrice :

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

L'état du système après cette évolution est $\beta|0\rangle + \alpha|1\rangle$. On parle d'inversion de qubit. Les rôles de $|0\rangle$ et $|1\rangle$ sont échangés. Une telle évolution est réversible, dans l'exemple précédent l'évolution X est son propre inverse.

La seconde évolution d'un système quantique que nous allons envisager correspond à la *mesure* d'un système quantique. Lorsque l'on souhaite connaître l'état d'un système quantique, on le mesure. La particularité de cette mesure quantique est double, son résultat est probabiliste et cette mesure modifie l'état du système. Avant de présenter l'axiome qui définit les mesures quantiques, nous introduisons une notation. L'adjoint d'un opérateur ou d'une matrice A est noté A^*. Lorsque $A \in \mathcal{M}_n(\mathbb{C})$, c'est la transposée de la matrice conjuguée de A : $A^* = \bar{A}^t$. On notera la matrice transposée A^t ou ${}^tA$ suivant les cas pour limiter les risques de confusion. Étant donné deux vecteurs $|\psi\rangle$ et $|\phi\rangle$ d'un espace de Hilbert $\mathcal{H}$ et A un opérateur sur $\mathcal{H}$, le produit scalaire hermitien de $|\psi\rangle$ et $A|\phi\rangle$ est noté :

$$\langle\psi|A|\phi\rangle.$$

Par définition de l'adjoint, c'est aussi le produit scalaire entre $A^*|\psi\rangle$ et $|\phi\rangle$. Le produit scalaire entre $A|\psi\rangle$ et $B|\phi\rangle$ est noté :

$$\langle\psi|A^*B|\phi\rangle$$

La norme vectorielle utilisée est la norme associée au produit scalaire hermitien. La norme du vecteur $|\psi\rangle$ est $|||\psi\rangle|| = \sqrt{\langle\psi|\psi\rangle}$.

Axiome 1.3 : *mesure.* *Soit $\mathcal{H}$ un espace de Hilbert décrivant le système quantique et $|\psi\rangle$ l'état du système. Une famille $(M_m)_m$ d'opérateurs de $\mathcal{H}$ définit une mesure du système quantique si elle vérifie :*

$$\sum_m M_m^\star M_m = I,$$

où I est l'identité sur $\mathcal{H}$.

Dans ce cas, le résultat de la mesure du système est m avec probabilité $||M_m|\psi\rangle||^2$. Après mesure, le système est dans l'état :

$$\frac{M_m|\psi\rangle}{||M_m|\psi\rangle||}.$$

Le résultat d'une mesure quantique est donc un indice d'un opérateur. Ce n'est pas un vecteur d'un espace de Hilbert. Comme nous l'avons signalé précédemment, ce résultat est probabiliste et mesurer modifie l'état du système. On remarque aussi que mesurer deux fois consécutivement le même système quantique donne deux fois le même résultat.

Regardons l'effet d'un mesure sur le système quantique de dimension deux dont l'état est $|\psi\rangle = \alpha|0\rangle + |1\rangle$. Les projecteurs $M_0 = |0\rangle\langle 0|$ et $M_1 = |1\rangle\langle 1|$ définissent une mesure quantique dont la sortie est un élément de $\{0, 1\}$. Le résultat de cette mesure est 0 avec probabilité $|\alpha|^2$ et 1 avec probabilité $|\beta|^2$. Supposons que ce résultat est 1, alors l'état est projeté sur le vecteur $|1\rangle$. Comme prévu une seconde mesure du système, désormais dans l'état $|1\rangle$, renvoie à nouveau le résultat 1 avec probabilité 1.

On peut généraliser cette construction de mesure à partir d'une décomposition orthogonale de l'espace de Hilbert. Dans le cas où $\mathcal{H}$ s'écrit :

$$\mathcal{H} = \bigoplus_m^{\perp} \mathcal{H}_m,$$

les projecteurs orthogonaux P_m, associés aux espaces $\mathcal{H}_m$, définissent une mesure. Le résultat de la mesure du système dont l'état est décrit par le vecteur unitaire : $|\psi\rangle = \sum_u |\psi_u\rangle$ est l'indice u avec probabilité : $|||\psi_u\rangle||^2$. Après mesure l'état du système est envoyé sur le vecteur $|\psi_u\rangle$ normalisé.

Enfin, nous pouvons remarquer que multiplier le vecteur $|\psi\rangle$ par un nombre complexe de module 1 n'influence pas les mesures. Nous aurions donc pu définir l'état du système comme un vecteur du quotient $\mathcal{H}/\mathbb{C}^\star$. On dit que la *phase* globale ne joue aucun rôle.

1.1.3 État d'un système quantique composé

Axiome 1.4 : *système composé.* *Un système composé de deux systèmes quantiques dans des états $|\psi_1\rangle \in \mathcal{H}_1$ et $|\psi_2\rangle \in \mathcal{H}_2$ est décrit par le produit tensoriel :*

$$|\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2.$$

Le produit tensoriel $|\psi\rangle \otimes |\phi\rangle$ de $|\psi\rangle \in \mathcal{H}$ et $|\phi\rangle \in \mathcal{H}'$ est parfois abrégé : $|\psi\rangle|\phi\rangle$ ou $|\psi\phi\rangle$. Lorsque l'on travaille avec l'espace de Hilbert $\mathcal{H} = \mathbb{C}^2$, on utilise une base orthonormale $(|0\rangle, |1\rangle)$ de $\mathcal{H}$ indexée par les éléments de $\mathbb{F}_2$. On en déduit une base orthonormale de $\mathcal{H}^{\otimes n}$ indexée par les vecteurs de $\mathbb{F}_2^n$, composée des produits tensoriels :

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle = |x_1 x_2 \dots x_n\rangle,$$

avec $x_i \in \mathbb{F}_2$ pour tout $i = 1, 2, \dots, n$. On note $(|x\rangle)_{x\in\mathbb{F}_2^n}$ cette base orthonormale. On appelle qubit un vecteur de $\mathcal{H}$, nous avons pu remarquer que c'est une superposition

des bits classiques 0 et 1. Les vecteurs de $\mathcal{H}^{\otimes n}$ sont des suites de n qubits, ce sont des superpositions des suites de n bits. Ils joueront le rôle des messages de longueur n en théorie de l'information quantique.

Cet axiome décrit un système quantique en fonction des sous-systèmes qui le composent. Réciproquement, comment décrire un sous-système en fonction de l'état d'un système quantique ? Lorsque l'état du système composé est de la forme $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$, les sous-systèmes correspondant aux espaces $\mathcal{H}_1$ et $\mathcal{H}_2$ sont définis par les vecteurs $|\psi_1\rangle$ et $|\psi_2\rangle$. Mais un état de $\mathcal{H}_1 \otimes \mathcal{H}_2$ ne s'écrit pas toujours sous cette forme. Par exemple, dans l'espace $\mathbb{C}^2 \otimes \mathbb{C}^2$, où $\mathbb{C}^2$ est muni de la base orthonormale $(|x\rangle)_{x\in\mathbb{F}_2}$, le vecteur suivant n'est pas un produit tensoriel de deux vecteurs de $\mathbb{C}^2$:

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle).$$

On parle d'*état non-local* ou bien d'*état enchevêtré*. Il reste à comprendre comment décrire les sous-systèmes d'un système quantique. Pour répondre à cette question nous avons besoin du formalisme des matrices de densité.

1.2 Le formalisme des opérateurs de densité

Nous disposons d'un ensemble d'axiomes nous permettant de décrire un système quantique isolé, nous avons vu que son évolution est unitaire. Néanmoins, nous nous intéresserons à des sous-systèmes de systèmes quantiques isolés. Dans ce cas, contrairement à ce que prévoient les axiomes de la mécanique quantique pour un système isolé, l'état n'est pas un vecteur unitaire et l'évolution n'est pas unitaire.

1.2.1 États probabilistes et opérateurs de densité

Nous allons à présent introduire les opérateurs de densité. Ce formalisme permet notamment de travailler avec des états définis de manière probabiliste. C'est le cas, par exemple, lorsque l'on souhaite envisager tous les résultats possibles d'une mesure. Supposons que l'on souhaite mesurer un système dans un état $|\psi\rangle$ avec la mesure définie par la famille d'opérateurs $(M_m)_m$. Le résultat de cette mesure est un état qui est $|\psi_m\rangle$ avec probabilité $p(m) = |||\psi_m\rangle||^2$. On dira que c'est un état mixte, c'est la mixture $\{|\psi_m\rangle, p(m)\}$. Un état qui est connu avec probabilité 1 est dit pur.

Définition 1.5. *Soient $|\psi_i\rangle$ une famille de vecteurs d'un espace de Hilbert $\mathcal{H}$ et soient p_i des nombres réels de l'intervalle $[0,1]$ tels que $\sum_i p_i = 1$. L'*état mixte *$\{|\psi_i\rangle, p_i\}$ de $\mathcal{H}$ est l'état $|\psi_i\rangle$ avec probabilité p_i. Il est représenté par l'opérateur sur $\mathcal{H}$ défini par la somme de projecteurs :*

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

*C'est l'*opérateur de densité *de l'état $\{|\psi_i\rangle, p_i\}$.*

On note $\Delta(\mathcal{H})$ l'ensemble des opérateurs de densité sur l'espace de Hilbert $\mathcal{H}$. C'est le sous-ensemble de l'espace des opérateurs sur $\mathcal{H}$ composé des opérateurs hermitiens positifs de trace 1.

Par exemple, le résultat de la mesure de l'état $\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle$ dans la base orthonormale $(|0\rangle, |1\rangle)$ de $\mathbb{C}^2$ est l'état mixte $\{(|0\rangle, \frac{1}{2}), (|1\rangle, \frac{1}{2})\}$ qui vaut $|0\rangle$ ou $|1\rangle$ avec probabilité $\frac{1}{2}$. À cet état est associé l'opérateur de densité $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$.

Nous allons maintenant reformuler les axiomes en décrivant les systèmes quantiques par des opérateurs de densité.

Axiome 1.6 : *état d'un système.* *A tout système quantique isolé est associé un espace de Hilbert $\mathcal{H}$. Le système est entièrement décrit par un opérateur de densité $\rho \in \Delta(\mathcal{H})$.*

On peut remarquer immédiatement que lorsque le système quantique est décrit par l'opérateur de densité ρ_i avec probabilité p_i alors l'opérateur de densité du système est $\sum p_i \rho_i$.

A chaque système quantique décrit par un vecteur unitaire ou une famille de vecteurs apparaîssant avec une certaine probabilité, on peut associer un opérateur de densité. Néanmoins, la réciproque est fausse. On ne peut peut pas retrouver la famille de vecteurs utilisée pour définir le système à partir de la matrice de densité. Considérons par exemple l'état défini de manière probabiliste qui vaut $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ avec probabilité $\frac{1}{2}$ et qui vaut $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ avec probabilité $\frac{1}{2}$. A cet état est associé l'opérateur de densité :

$$\begin{aligned}\rho &= \frac{1}{4}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) + \frac{1}{4}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \\ &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|.\end{aligned}$$

On retrouve le même opérateur que dans le cas de l'état $\{(|0\rangle, \frac{1}{2}), (|1\rangle, \frac{1}{2})\}$. Nous verrons dans la prochaine partie que ces collisions dans la représentation des systèmes quantiques ne posent pas problème car la mesure de deux systèmes quantiques décris par la même matrice de densité donne toujours le même résultat. Ces systèmes ne sont pas distinguables.

Lorsqu'un système quantique dans un état $|\psi\rangle$ évolue suivant l'opération unitaire U, l'opérateur $\rho = |\psi\rangle\langle\psi|$ est envoyé sur l'opérateur de densité associé au vecteur $U|\psi\rangle$. C'est l'axiome de l'évolution :

Axiome 1.7 : *évolution.* *L'évolution du système est unitaire. Si ρ est l'état du système au temps t et ρ' est l'état du système au temps t' alors il existe un opérateur unitaire U tel que :*

$$\rho' = U\rho U^*.$$

1.2.2 Non distinguabilité par la mesure

Cette description des systèmes quantiques et l'observation que plusieurs familles de vecteurs peuvent donner lieu au même opérateur de densité laissent à penser que l'on perd de l'information sur le système quantique en utilisant ce formalisme. Nous allons voir qu'il n'en est rien, il est en fait impossible de distinguer deux systèmes quantiques de même matrice de densité par une mesure quantique.

Revenons à notre exemple de système quantique dont l'état est $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ou $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ avec probabilité $\frac{1}{2}$. Supposons que l'on veuille mesurer ce système suivant la base orthonormale $(|0\rangle, |1\rangle)$. Le résultat de la mesure est 0, correspondant au projecteur $P_0 = |0\rangle\langle 0|$, avec probabilité :

$$\left\| P_0 \left(\frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \right) \right\|^2 = \left(\frac{\langle 0| \pm \langle 1|}{\sqrt{2}} \right) |0\rangle\langle 0| \left(\frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \right) = \frac{1}{2}.$$

On trouve le même résultat pour la probabilité d'obtenir 1. Cette mesure donne donc le même résultat lorsqu'elle est appliquée à l'état que nous venons de considérer ou à l'état $\{(|0\rangle, \frac{1}{2}), (|0\rangle, \frac{1}{2})\}$ qui possède le même opérateur de densité.

Il s'agit en fait d'une propriété plus générale, nous allons voir en reformulant l'axiome de la mesure à l'aide des opérateurs de densité que le résultat d'une mesure quantique ne dépend que de l'opérateur de densité du système.

Axiome 1.8 : *mesure.* *Soit $\mathcal{H}$ un espace de Hilbert décrivant le système quantique et $\rho \in \Delta(\mathcal{H})$ l'état du système. Une famille $(M_m)_m$ d'opérateurs de $\mathcal{H}$ définit une mesure du système quantique si elle vérifie :*

$$\sum M_m^\star M_m = I,$$

où I est l'identité sur $\mathcal{H}$.
Dans ce cas, le résultat de la mesure du système est m avec probabilité $\mathrm{Tr}(M_m^* M_m \rho)$. *Après mesure, le système est dans l'état :*

$$\frac{M_m \rho M_m^*}{\mathrm{Tr}(M_m^* M_m \rho)}.$$

Pour établir les formules précédentes, il suffit d'observer que :

$$\langle\psi| M_m^* M_m |\psi\rangle = \mathrm{Tr}(M_m^* M_m |\psi\rangle\langle\psi|).$$

Le résultat de la mesure est $\rho_m = \frac{M_m \rho M_m^*}{\mathrm{Tr}(M_m^* M_m \rho)}$ avec probabilité $p(m) = \mathrm{Tr}(M_m^* M_m \rho)$. L'état final peut donc être représenté par l'opérateur :

$$\sum_m p(m)\rho_m = \sum_m M_m \rho M_m^*,$$

lorsque l'on souhaite prendre en compte tous les résultats possibles de cette mesure.

1.2.3 Description d'un sous-système par la trace partielle

La transcription de l'axiome décrivant un système quantique composé est claire. Nous allons voir que le formalisme des matrices de densité permet de décrire un sous-système d'un système quantique en fonction de l'opérateur de densité du système tout entier. Nous n'étions pas en mesure d'obtenir cette propriété en utilisant les vecteurs d'état.

Axiome 1.9 : *système composé.* *Un système composé de deux systèmes quantiques d'opérateurs de densité ρ_1 agissant sur $\mathcal{H}_1$ et ρ_2 agissant sur $\mathcal{H}_2$ est décrit par le produit tensoriel :*

$$\rho_1 \otimes \rho_2.$$

Pour passer d'un opérateur de densité sur un produit tensoriel à un opérateur sur l'une de ses composantes, on utilise *la trace partielle*. La trace partielle de l'opérateur $|\psi_1\rangle\langle\psi_2| \otimes |\phi_1\rangle\langle\phi_2|$ de l'espace $\mathcal{H}_1 \otimes \mathcal{H}_2$ est :

$$\mathrm{Tr}_{\mathcal{H}_2}(|\psi_1\rangle\langle\psi_2| \otimes |\phi_1\rangle\langle\phi_2|) = |\psi_1\rangle\langle\psi_2| \,\mathrm{Tr}(|\phi_1\rangle\langle\phi_2|).$$

Supposons que l'on veuille mesurer uniquement la première composante d'un système d'opérateur de densité $\rho \in \Delta(\mathcal{H}_A \otimes \mathcal{H}_B)$, grâce à une mesure $(M_m)_m$ sur l'espace $\mathcal{H}_A$. Appliquer cette mesure revient à appliquer la mesure $(M_m \otimes I)$ à l'espace $\mathcal{H}_A \otimes \mathcal{H}_B$ car la composante B ne subit aucune évolution. Nous allons voir que l'on peut décrire le résultat de cette mesure en utilisant l'opérateur $\mathrm{Tr}_B(\rho)$. Le résultat de la mesure de ρ avec la famille $(M_m \otimes I)_m$ est identique au résultat de la mesure de $\mathrm{Tr}_B(\rho)$ avec la famille $(M_m)_m$. Nous utiliserons donc la trace partielle pour décrire les sous-systèmes.

Proposition 1.10. *Soit $\rho \in \Delta(\mathcal{H}_A \otimes \mathcal{H}_B)$ un opérateur de densité décrivant un système composé. L'opérateur $\rho_A = \mathrm{Tr}_B(\rho) \in \Delta(\mathcal{H}_A)$ défini par la trace partielle par rapport à $\mathcal{H}_B$ est l'opérateur de densité du sous-système A sur l'espace $\mathcal{H}_A$.*

Nous allons démontrer que l'opérateur $\rho_A = \mathrm{Tr}_B(\rho) \in \Delta(\mathcal{H}_A)$ permet de prédire le résultat de toute mesure sur la première composante de ρ. De plus, la mesure commute avec la trace partielle, ce qui signifie que prendre la trace partielle avant ou après la mesure mène au même opérateur de densité. L'opérateur qui décrit le sous-système après mesure est bien défini.

Démonstration. Considérons une mesure $(M_m)_m$ sur l'espace du système A. Cette famille permet de définir une mesure $(M_m \otimes I)_m$ sur l'espace du système composé $\mathcal{H}_A \otimes \mathcal{H}_B$. Le résultat de la mesure de ρ sur le système composé est l'indice m avec probabilité :

$$\begin{aligned}\mathrm{Tr}((M_m \otimes I)^*(M_m \otimes I)\rho) &= \mathrm{Tr}((M_m^* M_m \otimes I)\rho) \\ &= \mathrm{Tr}_A(\mathrm{Tr}_B((M_m^* M_m \otimes I)\rho)) \\ &= \mathrm{Tr}_A(M_m^* M_m \,\mathrm{Tr}_B(\rho))\end{aligned}$$

C'est aussi la probabilité d'obtenir m en mesurant l'opérateur de densité $\rho_A = \mathrm{Tr}_B(\rho)$ avec la famille $(M_m)_m$.

Enfin l'état du système composé après ce résultat m par la mesure $(M_m \otimes I)_m$ est :

$$\frac{(M_m \otimes I)\ \rho\ (M_m \otimes I)^*}{\mathrm{Tr}((M_m \otimes I)^*(M_m \otimes I)\rho)}$$

En prenant sa trace partielle par rapport à B on obtient :

$$\frac{M_m \operatorname{Tr}_B(\rho) M_m^*}{\operatorname{Tr}(M_m^* M_m \operatorname{Tr}_B(\rho))}.$$

On retrouve l'opérateur résultant de la mesure de ρ_A avec la famille $(M_m)_m$. Ceci prouve que la trace partielle et la mesure commutent. □

1.3 Les canaux quantiques

1.3.1 Définition d'un canal quantique

Nous allons définir un canal quantique en considérant l'évolution d'un système quantique non nécessairement isolé. Ce système quantique Q interagit donc avec un autre système quantique E, que l'on peut voir comme son environnement, suivant une opération unitaire sur le produit tensoriel des deux espaces de Hilbert correspondants $\mathcal{H}_Q \otimes \mathcal{H}_E$. L'évolution observée sur le sous-système Q est décrite par la trace partielle suivant E, d'où la définition d'un canal quantique :

Définition 1.11. *Un* canal quantique *sur l'espace de Hilbert $\mathcal{H}_Q$ est une application sur l'ensemble des opérateurs de densité de $\mathcal{H}_Q$ de la forme :*

$$\begin{aligned} \mathcal{N} : \Delta(\mathcal{H}_Q) &\longmapsto \Delta(\mathcal{H}_Q) \\ \rho &\longrightarrow \operatorname{Tr}_E(U_{QE}(\rho \otimes |0\rangle\langle 0|_E)U_{QE}^*) \end{aligned}$$

où E est un système quantique d'espace de Hilbert $\mathcal{H}_E$ et U_{QE} est un opérateur unitaire sur l'espace $\mathcal{H}_Q \otimes \mathcal{H}_E$.

On parle de la *représentation unitaire* d'un canal quantique. Contrairement au cas d'une évolution unitaire, cette évolution n'est pas réversible, ce qui a longtemps laissé penser qu'une information stockée au niveau quantique n'était pas stable et subissait une détérioration irrémédiable au fil du temps. On parle de décohérence. Nous verrons qu'il est tout de même possible de protéger un sous-ensemble d'états d'un espace Hilbert en adaptant des techniques issues de la théorie des codes correcteurs.

Dans la proposition suivante nous donnons une seconde définition des canaux quantiques. Celle-ci permet de considérer un canal quantique sans faire intervenir un environnement.

Proposition 1.12. *Une application $\mathcal{N}$ sur $\Delta(\mathcal{H})$ est un canal quantique si et seulement s'il admet une* représentation de Krauss *:*

$$\mathcal{N}(\rho) = \sum_i A_i \rho A_i^*,$$

avec A_i des opérateurs sur $\mathcal{H}$ tels que $\sum_i A_i^* A_i = I_{\mathcal{H}}$.

Démonstration. Montrons que tout canal quantique admet une représentation de Krauss. SOit $\mathcal{N}$ un canal quantique de la forme $\mathcal{N}(\rho) = \mathrm{Tr}_E(U_{QE}(\rho \otimes |0\rangle\langle 0|_E)U_{QE}^*)$. Nous utilisons les notations de Dirac pour exprimer la trace partielle d'un opérateur sur $\mathcal{H}_Q \otimes \mathcal{H}_E$. Si $|u\rangle$ et $|v\rangle$ sont des vecteurs de $\mathcal{H}_E$ et si $M \otimes M'$ est un opérateur de $\mathcal{H}_Q \otimes \mathcal{H}_E$ alors on note $\langle u|M \otimes M'|v\rangle$ l'opérateur $(\langle u|M'|v\rangle)M$ où $(\langle u|M'|v\rangle)$ est un scalaire. En utilisant une base orthonormale $(e_k)_k$ de l'espace $\mathcal{H}_E$, le nombre complexe $(\langle e_k|M'|e_l\rangle)$ est le coefficient d'indice (k,l) de la matrice de l'opérateur M dans la base $(e_k)_e$. On étend cette notation à tout opérateur sur $\mathcal{H}_Q \otimes \mathcal{H}_E$ par linéarité. L'opérateur image de $\rho \in \Delta(\mathcal{H})$ s'écrit alors :

$$\begin{aligned}\mathcal{N}(\rho) = \mathcal{N}(\rho) &= \mathrm{Tr}_E(U_{QE}(\rho \otimes |0\rangle\langle 0|_E)U_{QE}^*) \\ &= \sum_k \langle e_k|U_{QE}(\rho \otimes |0\rangle\langle 0|)U_{QE}^*|e_k\rangle \\ &= \sum_k A_k \rho A_k^*\end{aligned}$$

avec A_k les opérateurs sur $\mathcal{H}_Q$ définis par $A_k = \langle e_k|U_{QE}|0\rangle_E$.
Comme l'image par $\mathcal{N}$ d'un opérateur de densité de $\Delta(\mathcal{H}_Q)$ est un opérateur de densité, il est aussi de trace 1, de sorte que $\mathrm{Tr}(\mathcal{N}(\rho)) = \mathrm{Tr}(\sum_k A_k^* A_k \rho) = \mathrm{Tr}(\rho)$, pour tout $\rho \in \Delta(\mathcal{H})$. La trace Tr définit un produit scalaire sur l'espace des opérateurs linéaires sur $\mathcal{H}_Q$ et d'après l'égalité précédente, l'opérateur $(\sum_k A_k^* A_k) - I$ est orthogonal à l'espace des applications linéaires sur $\mathcal{H}_Q$. Cet opérateur est donc nul, ce qui prouve l'égalité $(\sum_k A_k^* A_k) - I$ qui apparaît dans la caractérisation des canaux quantiques.

Réciproquement, partons d'un canal sous la forme $\mathcal{N}(\rho) = \sum_k A_k \rho A_k^*$ et montrons qu'il admet une représentation unitaire. On considère un espace de Hilbert $\mathcal{H}_E$ dont une base orthonormale $(e_k)_k$ est en bijection avec la famille dénombrable des opérateurs A_k. En s'inspirant de l'écriture de $\mathcal{N}(\rho)$ en fonction des notations de Dirac, on pose $U(|\psi\rangle \otimes |0\rangle_E) = \sum_k (E_k|\psi\rangle)|e_k\rangle$, pour $|\psi\rangle \in \mathcal{H}_Q$. On retrouve ainsi l'écriture de $\mathcal{N}$ comme la trace partielle de l'évolution unitaire U. Le fait que U est unitaire, ou plutôt s'étend en un opérateur unitaire, vient du fait que U conserve le produit scalaire entre les vecteurs de la forme $|\psi\rangle \otimes |0\rangle_E$:

$$\langle \psi|\langle 0|_E U^* U|\phi\rangle|0\rangle_E = \sum_k \langle \psi|A_k^* A_k|\phi\rangle = \langle \psi|\phi\rangle.$$

Cette propriété est vérifiée pour tous les états $|\psi\rangle$ et $|\phi\rangle$ de $\mathcal{H}_Q$. La dernière égalité est tirée de la relation $\sum_k A_k^* A_k = I$. □

Il existe une troisième caractérisation des canaux quantiques que nous ne démontrerons pas. On peut définir un canal quantique comme une application linéaire $\mathcal{N}$ sur l'ensemble des opérateurs de $\mathcal{H}$ qui préserve la trace et qui est complètement positive, *i.e.* toute extension de $\mathcal{N}$ de la forme $\mathcal{N} \otimes I_E$ agissant les opérateurs sur $\mathcal{H}_Q \otimes \mathcal{H}_E$ transforme un opérateur positif en un opérateur positif. On parle d'*application CPTP* pour Completely Positive Trace Preserving map. Une preuve est disponible par exemple dans [75].

1.3.2 Le canal de dépolarisation

Le but de cette section est d'introduire le modèle d'erreur le plus commun. Il est représenté par le canal de dépolarisation. C'est l'analogue quantique du canal binaire symétrique. A travers le canal de dépolarisation, chaque qubit est laissé inchangé avec probabilité $(1-q)$ ou bien remplacé par un qubit totalement aléatoire d'opérateur de densité $I/2$ avec probabilité q. L'opérateur de densité $I/2$ définit bien, dans un sens, un qubit aléatoire car étant donné une base orthonormale quelconque de $\mathbb{C}^2$, la mesure suivant cette base projette l'état $I/2$ sur chacun des vecteurs de la base avec probabilité $1/2$. Ce canal transforme l'état ρ en une mixture entre ρ et $I/2$. Autrement dit, il s'écrit : $\mathcal{N}(\rho) = (1-q)\rho + q\frac{I}{2}$.

Nous allons maintenant nous pencher sur la représentation de Krauss de cette évolution. Nous utilisons la base orthonormale suivante, attribuée à Pauli, de l'espace des matrices 2×2 :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

Ces matrices permettent d'écrire $\frac{I}{2}$ sous la forme : $\frac{I}{2} = \frac{1}{4}(\rho + X\rho X + Y\rho Y + Z\rho Z)$. On en déduit la représentation de Krauss du canal de dépolarisation qui mène à la définition suivante :

Définition 1.13. *Le* canal de dépolarisation *sur $\mathcal{H} = C^2$ de probabilité $p \in [0,1]$ est le canal quantique $\mathcal{N}$ agissant sur $\Delta(\mathcal{H})$ par :*

$$\mathcal{N}(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z),$$

Les nombres p et q de ces deux définitions du canal de dépolarisation sont reliés par l'égalité avec $p = \frac{3}{4}q$.

Pour obtenir une représentation unitaire de ce canal, nous introduisons un espace environnement de dimension quatre engendré par la base orthonormale formée des vecteurs $|0\rangle_E, |1\rangle_E, |2\rangle_E$ et $|3\rangle_E$. L'opérateur unitaire U_{QE} qui définit le canal agit sur le produit cartésien $\mathcal{H} \otimes \mathcal{H}_E$ en envoyant le vecteur $|\psi\rangle|0\rangle_E$ sur le vecteur :

$$\sqrt{1-p}|\psi\rangle|0\rangle_E + \sqrt{\frac{p}{3}}(X|\psi\rangle)|1\rangle_E + \sqrt{\frac{p}{3}}(Y|\psi\rangle)|2\rangle_E + \sqrt{\frac{p}{3}}(Z|\psi\rangle)|3\rangle_E.$$

On considère que les erreurs surviennent sur une suite de n qubits de manière indépendante, autrement dit, c'est un canal sans mémoire. Son extension de $\mathcal{H}$ à $\mathcal{H}^{\otimes n}$ définit l'évolution :

$$\begin{aligned} \mathcal{N}^{\otimes n} : \Delta(\mathcal{H}^{\otimes n}) &\longrightarrow \Delta(\mathcal{H}^{\otimes n}) \\ \rho &\longmapsto \sum_{E \in \mathcal{P}_n} \left(\frac{p}{3}\right)^{|E|} (1-p)^{n-|E|} E\rho E^*. \end{aligned}$$

où $\mathcal{P}_n$ est l'ensemble des produits tensoriels de n matrices de $\{I, X, Y, Z\}$. Ces opérateurs agissent sur l'espace $\mathcal{H}^{\otimes n}$ et $|E|$ désigne le poids d'un éléments de $\mathcal{P}_n$, c'est le nombre de ses composantes qui diffèrent de I.

Remarque 1.14. *Cette définition continue du canal de dépolarisation par des matrices de densité admet une version discrète. Par le canal de dépolarisation, un qubit est inchangé avec probabilité* $1-p$ *ou subit une erreur de Pauli* X*,* Y *ou* Z *avec probabilité* $p/3$*.*

1.3.3 Destruction des superpositions d'erreurs par la mesure

Avant de détailler le fonctionnement des codes correcteurs quantiques, nous étudions un exemple de bruit pour observer l'action de la mesure sur un ensemble d'erreurs *a priori* continu. Nous allons ainsi observer un phénomène qui est la base de la discrétisation des erreurs quantiques : les erreurs, qui sont des opérateurs linéaires, sont projetées sur un ensemble fini d'erreurs possibles. Supposons que l'on veuille transmettre un état de la forme $\alpha|000\rangle + \beta|111\rangle$ de l'espace $\mathcal{H}^{\otimes 3}$ et qu'il est sujet à une évolution qui transforme cet état $\rho = |\psi\rangle\langle\psi|$ en l'état $\sum_k A_k \rho A_k^*$, où les opérateurs A_k sont tous de la forme $(a_k I + b_k X) \otimes I \otimes I$. Pour simplifier, nous considérons que ces opérateurs A_k n'agissent non trivialement que sur le premier qubit de ρ et nous nous restreignons à des opérateurs A_k engendrés par I et X. Le cas général sera traité dans la partie suivante à l'aide des codes stabilisateurs.

Un tel opérateur $A_k = a_k I + b_k X$ envoie le vecteur $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ sur le vecteur :

$$a_k|\psi\rangle + b_k X|\psi\rangle = a_k(\alpha|000\rangle + \beta|111\rangle) + b_k(\alpha|100\rangle + \beta|011\rangle).$$

Pour distinguer les composantes de $|\psi\rangle$ de celles de $X|\psi\rangle$, on utilise la parité de la somme $x_1 + x_2$ associée à un vecteur $|x_1x_2x_3\rangle$. On introduit donc la mesure définie par la décomposition orthogonale :

$$\mathcal{H}^{\otimes 3} = \Big((\mathbb{C}|00\rangle \oplus \mathbb{C}|11\rangle) \otimes \mathbb{C}\Big) \overset{\perp}{\bigoplus} \Big((\mathbb{C}|01\rangle \oplus \mathbb{C}|10\rangle) \otimes \mathbb{C}\Big).$$

La première composante est l'espace engendré par les vecteurs tels que $x_1 + x_2$ est pair et la seconde est engendrée par les vecteurs tels que $x_1 + x_2$ est impair. Après mesure, les opérateurs $A_k \rho A_k^*$ sont soit tous projetés sur le vecteur $|\psi\rangle$, soit tous projetés sur le vecteur $X|\psi\rangle$. L'état final du système quantique est donc soit $|\psi\rangle$, soit $X|\psi\rangle$.

Cette mesure a permis de rompre la superposition des erreurs. Nous généralisons cette stratégie dans la prochaine section en utilisant des codes stabilisateurs et en mesurant le syndrome d'une erreur.

1.4 Les codes stabilisateurs

La majorité des constructions de codes quantiques est issue de cette famille. Ils présentent l'avantage de se rapprocher des codes correcteurs classiques. Un code stabilisateur de paramètres $[[n, k]]$ est un sous-espace vectoriel de dimension 2^k de $\mathcal{H}^{\otimes n} = (\mathbb{C}^2)^{\otimes n}$. Il est défini comme l'ensemble des points fixes d'un groupe abélien d'opérateurs de Pauli. Dans cette partie, nous rappelons les définitions et propriétés

basiques des codes stabilisateurs. Nous renvoyons le lecteur vers le livre de Nielsen et Chuang [75] pour une description plus complète de la théorie de l'information quantique et des codes correcteurs quantiques avec un point de vue binaire. L'article de Calderbank, Rains, Shor et Sloane [27] propose un point de vue quaternaire.

1.4.1 Codes correcteurs classiques

Avant d'introduire les codes stabilisateurs qui se rapprochent des codes classiques, rappelons les notations et concepts classiques.

Les codes correcteurs sont utilisés pour transmettre de l'information à travers un canal bruité qui introduit des erreurs. Pour lutter contre ces apparitions d'erreurs, on introduit de la redondance. On cherchera donc à protéger, non pas toutes les suites de n bits, mais un sous-ensemble de ces 2^n suites. Ce sous-ensemble est le code correcteur. Nous travaillerons ici avec des codes qui possèdent une structure d'espace vectoriel :

Définition 1.15. *Un* code linéaire binaire *de paramètres* $[n, k]$ *est un sous-espace vectoriel de dimension* k *de* $\mathbb{F}_2^n$*. L'entier* n *est la* longueur *du code.*

Dans la suite, les codes classiques utilisés seront des codes linéaires binaires. On parlera souvent de code linéaire, de code, ou de code classique. Les vecteurs du code sont appelés les mots du code.

Un code linéaire présente l'avantage d'avoir une description compacte, on peut le voir comme le noyau d'une matrice. Une telle matrice est appelée une *matrice de parité* du code. La proposition suivante exprime les paramètres d'un code en fonction de sa matrice de parité.

Proposition 1.16. *Soit* C *un code classique et* $H \in \mathcal{M}_{r,n}(\mathbb{F}_2)$ *une matrice de parité de* C*. La longueur du code* C *est* n *le nombre de colonnes de* H *et la dimension de ce code est* $k = n - \operatorname{rg} H$*.*

La preuve est immédiate. Nous insistons sur ce résultat pour mettre en valeur le parallèle avec les codes stabilisateurs qui viennent ensuite.

La distance minimale est une mesure de la capacité de correction d'un code linéaire. C'est la plus petite distance de Hamming entre deux mots du code. Rappelons que la distance de Hamming entre deux vecteurs x et y de $\mathbb{F}_2^n$ est le nombres de composantes i telles que $x_i \neq y_i$. On note $w(x)$ le poids d'un vecteur $x \in \mathbb{F}_2^n$, *i.e.* le nombre de composantes non nulles de x. Par linéarité, on peut définir la distance minimale par :

Définition 1.17. *La* distance minimale d *d'un code linéaire binaire* C *est le poids minimum d'un vecteur de* C *:*

$$d = \inf\{w(x) \mid x \in C\}.$$

On inclut la distance d dans les paramètres $[n, k, d]$ d'un code de longueur n et de dimension k.

La transmission d'information grâce à un code C de paramètres $[n, k]$ se décompose en 3 étapes. L'encodage introduit de la redondance en transformant un message de k bits en un mot $x \in C$ du code, qui est donc composé de n bits. Le canal introduit une erreur, il transforme x en un vecteur $x' = x + e$ perturbé par une erreur $e \in \mathbb{F}_2^n$. À la réception de x', on corrige en cherchant le mot $\tilde{x}$ du code C qui est le plus proche de x'. Lorsque l'erreur est suffisamment petite et si les mots du code sont assez éloignés les uns des autres, on a bien corrigé l'erreur : $\tilde{x} = x$.

Pour finir nous introduisons la fonction syndrome associé à une matrice de parité H d'un code binaire. Le syndrome d'un vecteur x' est une information sur l'erreur qu'il a subi. C'est cette information que nous utiliserons pour estimer l'erreur.

Définition 1.18. *Soit $H \in \mathcal{M}_{r,n}(\mathbb{F}_2)$ une matrice de parité d'un code binaire. La* fonction syndrome *associée à la matrice H est la fonction :*

$$\begin{aligned} s : \mathbb{F}_2^n &\longrightarrow \mathbb{F}_2^r \\ x &\longmapsto Hx^t. \end{aligned}$$

Le syndrome est une application linéaire dont le noyau est le code C. Supposons qu'un mot x du code C est transmis. S'il subit une erreur $e \in \mathbb{F}_2^n$, le vecteur reçu est $x' = x + e$. Le syndrome de ce vecteur est $s(x + e) = s(x) + s(e) = s(e)$ ce qui prouve que le syndrome ne dépend que de l'erreur subie.

A chaque syndrome $s \in \mathbb{F}_2^r$, on associe un vecteur $e \in \mathbb{F}_2^n$ de poids minimum tel que $s(e) = s$. Pour décoder le mot de code x' de syndrome s on ajoute alors cette erreur minimale $e' = e'(s)$ à x'. Le résultat est un mot de code $x'' = x' + e'$ tel que $s(x'') = 0$. C'est le mot du code C le plus proche du vecteur x reçu. Cette procédure de décodage est appelé *décodage à distance minimale* et elle fonctionne pour toute erreur e jusqu'à un certain poids :

Proposition 1.19. *Le décodage à distance minimale permet de corriger toute erreur de poids inférieur à $\lfloor \frac{d-1}{2} \rfloor$.*

Démonstration. Supposons que le mot reçu est $x' = x + e$ avec $x \in C$ le mot envoyé et $e \in \mathbb{F}_2^n$ une erreur de poids $w(e) \leq \lfloor \frac{d-1}{2} \rfloor$. Après décodage à distance minimale, on obtient le mot $x'' = x' + e'$ tel que $s(e') = s(x') = s(e)$. Le vecteur x est donc translaté par un vecteur $e' + e$ de syndrome 0, c'est un vecteur de C. Nous allons voir que ce mot $e + e'$ est le mot de code nul. Par construction, le vecteur e' est de poids minimum parmi les erreurs de syndrome $s(e)$. En particulier, le poids de e' est au plus $w(e') \leq w(e)$. L'hypothèse sur le poids de e nous assure donc que $e' + e$ est un mot de code de poids strictement inférieur à d, c'est donc le mot 0. Ceci prouve que l'erreur e à été corrigée. On retrouve le vecteur $x'' = x$. □

Cette proposition confirme l'intuition que la distance influence les performances du décodage. Nous avons considéré ici un décodage à distance minimale qui est dans un certain sens optimal. En pratique, il est impossible d'implémenter cet algorithme de manière rapide et performante. L'usage des codes LDPC, qui sont des codes linéaires de matrice de parité creuse, permet d'approximer cette recherche du mot

de code le plus proche par un algorithme quasi-linéaire. Tanner a popularisé le graphe qui porte son nom pour analyser le décodage itératif des codes LDPC [91].

Définition 1.20. *Le* graphe de Tanner *associé au code de matrice de parité H est le graphe biparti dont les sommets correspondent aux lignes et aux colonnes de H. Il y a une arête entre la ligne i et la colonne j si et seulement si $H_{i,j} = 1$.*

Les sommets du graphe de Tanner sont partitionnés en deux sous-ensembles, l'un correspond aux colonnes de la matrice de parité H, c'est-à-dire aux variables et l'autre correspond aux lignes de H donc aux équations définissant le code. Notons V_1 les sommets variables et V_2 les sommets équations de ce graphe biparti. Si le code est de longueur n, un vecteur $x \in \mathbb{F}_2^n$ correspond à un ensemble de sommets du graphe inclus dans V_1. Ce vecteur x est un mot du code $\operatorname{Ker} H$ si et seulement si l'ensemble des sommets correspondants contient un nombre pair de sommets parmi les voisins de chaque sommet de V_2.

Pour conclure ces rappels sur les codes linéaires, nous rappelons la définition des codes auto-orthogonaux.

Définition 1.21. *Un code linaire C de longueur n est dit* auto-orthogonal *s'il est inclus dans son orthogonal $C^\perp$. Lorsque l'on a égalité $C = C^\perp$, on parle d'un code* auto-dual.

En regardant les dimensions de l'espace C et de son dual $C^\perp$, on voit que la dimension d'un code auto-orthogonal de longueur n ne peut pas dépasser $n/2$. Un code auto-dual est un code auto-orthogonal de dimension exactement $n/2$. Ces codes font le lien avec les codes quantiques. En effet, nous allons voir que tout code auto-orthogonal définit un code quantique par la construction CSS de la partie 1.4.5. La suite de ce chapitre concerne les codes stabilisateurs que l'on peut voir comme une version quantique des codes linéaires.

1.4.2 Groupes de Pauli et codes stabilisateurs

Le groupe de Pauli

Rappelons la définition des *matrices de Pauli* qui forment une base orthonormale de l'espace des matrices 2×2 :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$$

Ces matrices satisfont les relations suivantes :

$$\begin{cases} X^2 = Y^2 = Z^2 = I, \\ XY = -YX = iZ, \\ YZ = -ZY = -iX, \\ ZX = -XZ = iY. \end{cases}$$

Le groupe de Pauli sur un qubit $\tilde{\mathcal{P}}_1$ est le groupe engendré par ces matrices.

$$\tilde{\mathcal{P}}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$$

Notez le fait que deux éléments de ce groupe commutent ou anticommutent. De plus, deux opérateurs $i^\alpha E$ et $i^\beta E'$ de $\mathcal{P}_1$ anticommutent si et seulement si E et E' sont deux matrices différentes de l'ensemble $\{X, Y, Z\}$.

Définition 1.22. *Le* groupe de Pauli *sur n qubits $\tilde{\mathcal{P}}_n$ est le groupe multiplicatif des produits tensoriels de n éléments de $\tilde{\mathcal{P}}_1$:*

$$\tilde{\mathcal{P}}_n = \{i^a E_1 \otimes E_2 \otimes \cdots \otimes E_n \mid a = 0, 1, 2 \text{ ou } 3 \text{ et } E_i = I, X, Y \text{ ou } Z\}$$

Le nombre complexe i^a est la *phase* de l'opérateur de Pauli. Une importante conséquence de cette construction est le fait que deux opérateurs de Pauli commutent ou anticommutent. Plus précisément, étant donné deux erreurs E et E' de $\tilde{\mathcal{P}}_n$, on a :

$$EE' = (-1)^{f(E,E')} E'E,$$

où $f(E, E')$ est le nombre de composantes i telles que E_i et E'_i sont deux matrices de Pauli différentes et non-triviales. Par exemple les opérateurs $I \otimes X \otimes Z$ et $X \otimes Y \otimes Z$ de $\tilde{\mathcal{P}}_3$ anticommutent puisqu'ils anticommutent uniquement sur la seconde composante. Cette propriété sera à l'origine de la mesure du syndrome.

Les codes stabilisateurs

Définition 1.23. *Un* groupe stabilisateur *est un sous-groupe commutatif S de $\tilde{\mathcal{P}}_n$ qui ne contient pas $-I$. Le* code stabilisateur $C(S)$ *associé au groupe stabilisateur S est l'ensemble des points fixes de S dans $\mathcal{H}^{\otimes n}$:*

$$C(S) = \{\ |\psi\rangle \in \mathcal{H}^{\otimes n} \mid s|\psi\rangle = |\psi\rangle, \forall s \in S\ \}.$$

L'entier n est la longueur *du code quantique.*

Ce sous-espace $C(S)$ de $\mathcal{H}^{\otimes n}$ n'est pas trivial par définition des codes stabilisateurs. La condition $-I \notin S$ est en fait suffisante dans ce cas, elle implique la commutativité du groupe S car c'est un groupe d'exposant 2. Nous conservons la condition S est commutatif en raison de son importance. La condition $-I \in S$, plus forte que la commutativité, sera utile dans la proposition 1.25.

Un groupe stabilisateur S est engendré par une famille d'opérateurs de Pauli $S =< S_1, S_2, \ldots, S_r >$ que l'on peut supposer de phase 1. La condition $-I$ est alors automatiquement vérifiée.

Supposons que $S = \langle S_1, S_2, \ldots, S_r \rangle$ est engendré par r générateurs $S_i \in \tilde{\mathcal{P}}_n$. On appelle *matrice stabilisatrice* de $C(S)$ la matrice $\mathbf{H} \in \mathcal{M}_{r,n}(\{I, X, Y, Z\})$ dont la i-ème ligne représente le générateur S_i. Le coefficient $\mathbf{H}_{i,j}$ de cette matrice est la j-ème composante de S_i. Par exemple, le code quantique associé au groupe engendré par les 3 générateurs $S_1 = (I \otimes X \otimes Z \otimes Y \otimes Z), S_2 = (Z \otimes Z \otimes X \otimes I \otimes Z)$, et

$S_3 = (I \otimes Y \otimes Y \otimes Y \otimes Z)$ est décrit par la matrice stabilisatrice :

$$\mathbf{H} = \begin{pmatrix} X & Z & I & I & Z \\ Z & X & X & Y & I \\ Y & Y & X & Y & Z \end{pmatrix}. \tag{1.1}$$

Un code stabilisateur est entièrement défini par sa matrice stabilisatrice, bien que plusieurs matrices différentes puissent définir le même groupe stabilisateur et le même code. On peut voir cette matrice comme l'analogue quantique de la matrice de parité d'un code classique.

1.4.3 Paramètres des codes stabilisateurs

Syndrome d'une erreur

Étant donné un groupe stabilisateur $S =< S_1, S_2, \ldots, S_r >$ de $\tilde{\mathcal{P}}_n$, supposons que l'état $|\psi\rangle \in C(S)$ subit une erreur de Pauli $E \in \tilde{\mathcal{P}}_n$. Le vecteur $|\psi\rangle$ est transformé en $E|\psi\rangle$. Pour retrouver l'état quantique original, on mesure le syndrome pour obtenir une information sur l'erreur.

Définition 1.24. *Le* syndrome *de $E \in \tilde{\mathcal{P}}_n$ est le vecteur $\sigma(E) = (\sigma_1, \sigma_2, \ldots, \sigma_r)$ de $\mathbb{F}_2^r$ défini par :*

$$\sigma_i = \begin{cases} 0 \text{ if } E \text{ et } S_i \text{ commutent} \\ 1 \text{ if } E \text{ et } S_i \text{ anticommutent} \end{cases}$$

La proposition suivante nous assure que l'on peut mesurer le syndrome de l'erreur E, à partir de l'état corrompu $E|\psi\rangle$.

Proposition 1.25. *Soit $S =< S_1, S_2, \ldots, S_r >$ un groupe stabilisateur, on note $C(u) = \{|\psi\rangle \in \mathcal{H}^{\otimes n} | S_i|\psi\rangle = (-1)^{u_i}|\psi\rangle\}$. Si les r générateurs S_i sont indépendants, alors on a la décomposition en somme directe orthogonale :*

$$\mathcal{H}^{\otimes n} = \overset{\perp}{\bigoplus_{u \in \mathbb{F}_2^r}} C(u)$$

Démonstration. On sait que $S_i^2 = I$ donc les valeurs propres de S_i sont ± 1. Comme les opérateurs S_i commutent, ils sont codiagonalisables. En notant $E_\lambda(S_i)$ le sous-espace propre de S_i associé à la valeur propre λ, on obtient la décomposition de $\mathcal{H}^{\otimes n}$ suivante :

$$\begin{aligned} \mathcal{H}^{\otimes n} &= \bigoplus_{u \in \mathbb{F}_2^r} E_{u_1}(S_1) \cap E_{u_2}(S_2) \cap \cdots \cap E_{u_r}(S_r) \\ &= \bigoplus_{u \in \mathbb{F}_2^r} \mathrm{Fix}((-1)^{u_1} S_1, (-1)^{u_2} S_2, \ldots, (-1)^{u_r} S_r) \\ &= \bigoplus_{u \in \mathbb{F}_2^r} C(u) \end{aligned}$$

Il reste à voir que cette somme directe est orthogonale. Si $|\psi\rangle \in C(u)$ et $\phi \in C(v)$ avec $u \neq v$ alors il existe i tel que $u_i \neq v_i$. Ces vecteurs sont donc situés dans des espaces propres distincts de l'opérateur unitaire S_i. L'orthogonalité découle donc de l'orthogonalité entre les sous-espaces propres d'un opérateur unitaire.

□

Le syndrome vérifie $\sigma(EE') = \sigma(E) + \sigma(E')$. Le syndrome d'une erreur $s \in S$ qui n'a aucun effet sur le code quantique est $\sigma(s) = 0$.

Distance minimale des codes stabilisateurs

La phase i^a d'un opérateur de Pauli $E \in \tilde{\mathcal{P}}_n$ ne joue aucun rôle puisqu'elle n'a aucune influence sur la valeur de l'opérateur de densité $E|\psi\rangle\langle\psi|E^*$. Nous considérons donc les erreurs $E \in \mathcal{P}_n$ définies modulo la phase. Dans la suite, sauf mention contraire, le groupe de Pauli sera le groupe quotient abélien :

$$\mathcal{P}_n = \tilde{\mathcal{P}}_n / \{\pm 1, \pm i\}.$$

Nous dirons que deux erreurs du groupe abélien $\mathcal{P}_n$, commutent si elles commutent dans le groupe original $\tilde{\mathcal{P}}_n$. Cet abus de langage n'est pas problématique puisque la commutativité ne dépend en aucun cas de la phase.

Imaginons que nous recevons un état corrompu $E|\psi\rangle$, où $|\psi\rangle$ est un vecteur du code quantique $C(S)$. Nous commençons par mesurer son syndrome $\sigma(E)$. Nous appliquons alors à $E|\psi\rangle$ une erreur $\tilde{E}$ telle que $\sigma(\tilde{E}) = \sigma(E)$. Après ce processus, l'état quantique est $\tilde{E}E|\psi\rangle$. Il est perturbé par une erreur $\tilde{E}E$ de syndrome 0, puisque $\sigma(\tilde{E}E) = \sigma(\tilde{E}) + \sigma(E) = 0$. Il y a deux types d'erreurs de syndrome zéro. Soit $\tilde{E}E$ appartient au groupe S et fixe alors le code quantique. Nous avons dans ce cas retrouvé l'état quantique original. Soit $\tilde{E}E \notin S$ et dans ce cas l'état quantique est probablement perdu. Les erreurs de syndrome nul qui ne sont pas dans le groupe S sont dites *non détectables* ou *problématiques*.

Proposition 1.26. *Une erreur de Pauli $E \in Pauli_n$ problématique pour un code stabilisateur $C(S)$ est une erreur de syndrome nul qui n'appartient pas à S. Les erreurs problématiques ne sont pas corrigibles.*

Cette observation nous amène à la définition de la distance minimale d'un code stabilisateur.

Définition 1.27. *La* distance minimale *d d'un code stabilisateur $C(S)$ est le poids minimum d'une erreur problématique :*

$$d = \min\{|E| \mid E \in \mathcal{P}_n \backslash S, \sigma(E) = 0\}.$$

où $|E|$ est le poids de E, c'est le nombre de composantes de E qui diffèrent de l'identité.

L'ensemble des erreurs de $\mathcal{P}_n$ de syndrome 0 est fréquemment noté $N(S)$ car c'est le normalisateur du sous-groupe S de $\tilde{\mathcal{P}}_n$. La distance minimale est donc aussi le poids minimum d'une erreur de $N(S)\backslash S$.

Dégénérescence

La *dégénérescence* est une caractéristique essentielle du codage quantique qui le distingue du codage classique. Elle permet d'utiliser la même procédure de décodage pour un grand nombre d'erreurs différentes. Plus précisément, toutes les erreurs d'une classe $E.S$ peuvent être corrigées par la même erreur E. En effet, supposons qu'un état $|\psi\rangle$ du code quantique est sujet à une erreur Es, avec $s \in S$. Alors, après application de E, nous retrouvons l'état quantique original puisqu'il est fixé par le groupe S. Nous avons $EEs|\psi\rangle = |\psi\rangle$. Pour corriger une erreur $E \in \mathcal{P}_n$, il suffit donc de déterminer sa classe $E.S$ modulo le groupe stabilisateur S.

Dimension d'un code stabilisateur

L'objectif de cette partie est de déterminer la dimension du code quantique $C(S)$. Pour cela nous allons voir que les sous-espaces $C(u)$ apparaîssant dans la décomposition orthogonale de la proposition 1.25 sont tous isomorphes au code quantique $C(S) = C(0)$.

Proposition 1.28. *La dimension du code quantique $C(S)$ est 2^k avec $k = n - \operatorname{rg} S$.*

L'entier k est le nombre de qubits encodés. Le quantité $\operatorname{rg} S$ est le rang du groupe abélien S, *i.e.* le taille d'une famille génératrice minimale. Étant donné une matrice stabilisatrice $\mathbf{H}$, on note aussi $\operatorname{rg}\mathbf{H}$ le rang du groupe S, de sorte que l'on retrouve la formule classique $k = n - \operatorname{rg}\mathbf{H}$. Par exemple le rang de la matrice $\mathbf{H}$ définie en 1.1 est 2 car la troisième ligne est le produit des deux premières lignes. Le code stabilisateur associé est donc de dimension $2^{5-2} = 2^3$, il encode 2 qubits en 5 qubits. Le rendement du code quantique est $R = k/n$.

Démonstration. Cette preuve utilise la structure vectorielle du groupe $\mathcal{P}_n$ qui sera détaillée dans la partie 1.4.4. Supposons que $S = \langle S_1, S_2, \ldots, S_r\rangle$ est engendré par r générateurs indépendants, *i.e.* $\operatorname{rg} S = r$. Cette hypothèse n'est pas restrictive car on peut toujours extraire une telle famille d'une famille génératrice. La preuve se résume à démontrer que pour tout vecteur $u \in \mathbb{F}_2^r$, il existe une erreur E_u de syndrome u. Pour cela, on cherche à quelle condition deux erreurs de $\mathcal{P}_n$ commutent. Chaque erreur $E \in \mathcal{P}_n$ correspond à un couple de vecteurs $(E_X, E_Z) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ par l'isomorphisme d'espaces vectoriels $\theta : \mathcal{P}_n \simeq \mathbb{F}_2^{2n}$ de la section 1.4.4. Dans le groupe $\tilde{\mathcal{P}}_n$, on a $EE' = (-1)^{f(E,E')}E'E$, où $f(E, E') = (E_X, E'_Z) + (E'_X, E'_Z)$ avec $(.,.)$ le produit scalaire canonique de l'espace $\mathbb{F}_2^n$. Cette application f est une forme bilinéaire symétrique non dégénérée et définit donc une notion d'orthogonalité. Le syndrome est un morphisme de groupes de $\mathcal{P}_n$ vers $\mathbb{F}_2^r$, il suffit de montrer que chaque vecteur e_i de la base canonique de $\mathbb{F}_2^r$ est atteint pour voir qu'il est surjectif. Pour obtenir un vecteur de syndrome e_1, on choisit :

$$E \in < (S_i)_{i=2}^r >^{\perp} \setminus < (S_i)_{i=1}^r >^{\perp}$$

Un tel vecteur existe car $< (S_i)_{i=1}^r >^{\perp} \subset < (S_i)_{i=2}^r >^{\perp}$ et on peut voir que l'inclusion est stricte en regardant les dimensions de ces deux espaces. Nous avons ainsi construit une erreur $E \in \mathcal{P}_n$ qui est orthogonale à tous les S_i sauf à S_1 pour le produit scalaire

f. Par définition de f, ceci prouve que E commute avec toutes les erreurs S_i sauf avec S_1, son syndrome est donc $\sigma(E) = e_1$. Cette méthode fournit des erreurs de n'importe quel syndrome.

Pour conclure, on utilise la décomposition orthogonale $\mathcal{H}^{\otimes n} = \overset{\perp}{\oplus} C(u)$ obtenue dans le proposition 1.25. On remarque que toute erreur E_u de syndrome u réalise un isomorphisme entre $C(S) = C(0)$ et $C(u)$. Ces espaces ont donc tous la même dimension, la formule $k = n - r$ suit. □

Au cours de cette preuve nous avons aussi démontré que les sous-espaces $C(u)$ sont tous isomorphes à $C(S) = C(0)$.

Nous avons définit trois paramètres des codes stabilisateurs, la longueur n, le nombre de qubits encodés k, et la distance minimale d. Nous noterons $[[n, k, d]]$ ces paramètres par analogie avec le cas des codes classiques.

1.4.4 La structure de $\mathbb{F}_2$-espace vectoriel de $\mathcal{P}_n$

Le groupe de Pauli $\mathcal{P}_n$ peut être vu comme un $\mathbb{F}_2$-espace vectoriel de dimension $2n$ à travers l'isomorphisme :

$$\begin{aligned} \theta : \mathcal{P}_n &\longrightarrow \mathbb{F}_2^n \times \mathbb{F}_2^n = \mathbb{F}_2^{2n} \\ X_i &\longmapsto (e_i|0) \\ Z_i &\longmapsto (0|e_i) \end{aligned}$$

où X_i est l'opérateur dont la i-ème composante est X et qui vaut l'identité sur les autres composantes. Les erreurs Y_i et Z_i sont définies de manière analogue. L'image de $Y_i = X_i Z_i$ par cet isomorphisme est $\theta(X_i Y_i) = (e_i|e_i)$. Par exemple, l'opérateur $I \otimes X \otimes Y \otimes Z$ correspond au vecteur $(0110|0011)$. Pour cette structure de $\mathbb{F}_2$-espace vectoriel, l'addition des vecteurs de $\mathbb{F}_2^{2n}$ correspond à la multiplication composante par composante des opérateurs de Pauli.

Par l'isomorphisme θ, les sous-groupes de $\mathcal{P}_n$ sont envoyés sur des sous-espaces $\mathbb{F}_2$-linéaires de $\mathbb{F}_2^{2n}$. Le *rang* d'un sous-groupe de $\mathcal{P}_n$ est donc la dimension du sous-espace correspondant. Si $\mathbf{H}$ est une matrice stabilisatrice, nous noterons $\operatorname{rg} \mathbf{H}$ le rang de l'espace des lignes de la matrice qui est aussi du sous-groupe de $\mathcal{P}_n$ engendré par les lignes de la matrice. Les r lignes de la matrice $\mathbf{H}$ ne sont pas nécessairement indépendantes et le rang de $\mathbf{H}$ n'est pas toujours r.

Cette structure vectorielle fait du syndrome une application $\mathbb{F}_2$-linéaire :

$$\begin{aligned} \sigma : \mathcal{P}_n &\longmapsto \mathbb{F}_2^r \\ E &\longrightarrow \sigma(E). \end{aligned}$$

En écrivant l'erreur E comme un couple de deux vecteurs binaires $(E_X, E_Z) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ et en écrivant la matrice $\mathbf{H}$ comme une paire de matrices $(\mathbf{H}_1|\mathbf{H}_2) \in \mathcal{M}_{r,2n}(\mathbb{F}_2)$, on peut écrire le syndrome comme :

$$\sigma(E_X, E_Z) = \mathbf{H}_1 E_X^t + \mathbf{H}_2 E_Z^t.$$

On note ces deux matrices $\mathbf{H}_1$ et $\mathbf{H}_2$ et non pas $\mathbf{H}_X$ et $\mathbf{H}_Z$ pour éviter les confusions avec la famille des codes CSS que nous allons présenter dans la prochaine section.

1.4.5 Les codes CSS

L'une des familles de codes quantiques les plus répandues est la construction CSS due à Calderbank, Shor et Steane. [28, 90]. Un code CSS est un code stabilisateur construit à partir d'un groupe stabilisateur S dont les générateurs sont partitionnés en deux ensembles :

$$S =< S_1, S_2, \ldots, S_{r_X}, S_{r_X+1}, \ldots, S_{r_X+r_Z} >$$

avec $S_1, S_2, \ldots, S_{r_X}$ des opérateurs de $\{I, X\}^{\otimes n}$ et $S_{r_X+1}, S_{r_X+2}, \ldots, S_{r_X+r_Z}$ appartiennent à $\{I, Z\}^{\otimes n}$. Cette condition permet de simplifier les relations de commutation puisque deux erreurs de $\{I, X\}^{\otimes n}$ commutent automatiquement. C'est aussi le cas avec deux opérateurs de $\{I, Z\}^{\otimes n}$. On décompose donc la matrice stabilisatrice $\mathbf{H}$ en deux matrices stabilisatrices $\mathbf{H}_X$ et $\mathbf{H}_Z$. La matrice $\mathbf{H}_X$ est formée de r_X lignes représentant les générateurs à coefficient dans $\{I, X\}$ et la matrice $\mathbf{H}_Z$ est composée de r_Z lignes qui définissent les stabilisateurs à coefficients dans $\{I, Z\}$.

On peut utiliser l'isomorphisme entre le groupe $\{I, X\}$ et le groupe $\mathbb{F}_2$ pour écrire la matrice $\mathbf{H}_X$ comme une matrice binaire. La même remarque est valable pour $\mathbf{H}_Z$. Par cet isomorphisme, les lignes de ces matrices peuvent être vues comme des vecteurs binaires de longueur n et la relation de commutation entre une ligne de $\mathbf{H}_X$ et une ligne de $\mathbf{H}_Z$ correspond à la relation d'orthogonalité entre ces vecteurs binaires dans $\mathbb{F}_2^n$. Finalement, un code CSS peut être défini en fonction de deux matrices binaires.

Définition 1.29. *Un* code CSS *est un code stabilisateur défini par deux matrices binaires* $\mathbf{H}_X \in \mathcal{M}_{r_X,n}(\mathbb{F}_2)$ *et* $\mathbf{H}_Z \in \mathcal{M}_{r_Z,n}(\mathbb{F}_2)$ *tel que les lignes de* $\mathbf{H}_X$ *sont orthogonales aux lignes de* $\mathbf{H}_Z$ *dans* $\mathbb{F}_2^n$.

La propriété suivante exprime les paramètres du code quantique obtenu en fonction de ces matrices binaires. On note C_X le code binaire de matrice de parité $\mathbf{H}_X$ et C_Z le code binaire de parité $\mathbf{H}_Z$.

Proposition 1.30. *Le code CSS défini par les matrices* $\mathbf{H}_X \in \mathcal{M}_{r_X,n}(\mathbb{F}_2)$ *et* $\mathbf{H}_Z \in \mathcal{M}_{r_Z,n}(\mathbb{F}_2)$ *est un code quantique de longueur* n *de dimension* 2^k *avec* $k = n - \operatorname{rg}\mathbf{H}_X - \operatorname{rg}\mathbf{H}_Z$ *et de distance minimale :*

$$d = \inf\{w(x) \mid x \in C_X \backslash C_Z^{\perp} \cup C_Z \backslash C_X^{\perp}\},$$

où $w(x)$ *est le poids de Hamming du vecteur binaire* x.

Démonstration. Pour déterminer la dimension du code quantique, on s'intéresse au rang de la matrice stabilisatrice. Comme deux opérateurs en X et en Z sont automatiquement indépendants, ce rang est la somme des rangs des deux matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$. Le rang de ces matrices vues comme des matrices à coefficients dans le groupe de Pauli ou comme des matrices binaires est inchangé.

D'après la définition 1.27, la distance minimale de ce code stabilisateur est le poids minimum d'une erreur du normalisateur $N(S)$ qui n'est pas dans S. D'après l'isomorphisme de la section 1.4.4, toute erreur $E \in \mathcal{P}_n$ se décompose en deux

vecteurs binaires E_X et E_Z de $\mathbb{F}_2^n$. Une erreur E est dans $N(S)$, *i.e.* commute avec les générateurs S_i, si et seulement si le vecteur E_X est orthogonal aux lignes de H_Z et le vecteur E_Z est orthogonal aux lignes de H_X. Autrement dit, E est dans $N(S)$ si et seulement si $E_X \in C_Z$ et $E_Z \in C_X$. De la même manière, on peut caractériser les erreurs de groupe S, ce sont les opérateurs E dont la décomposition binaire (E_X, E_Z) est telle que $E_X \in C_X^\perp$ et $E_Z \in C_Z^\perp$.

En combinant ces deux équivalences, on voit que l'on peut construire des vecteurs binaires (E_X, E_Z) de $\mathbb{F}_2^n$ tels que $E_X \in C_Z \backslash C_X^\perp$ ou $E_Z \in C_X \backslash C_Z^\perp$ en partant d'une erreur problématique E. L'un des ces deux vecteurs est donc un vecteur $x \in C_Z \backslash C_X^\perp \cup C_X \backslash C_Z^\perp$ et son poids est au maximum $w(x) \leq |E|$ par définition de θ. On en déduit que la distance est majorée comme on le souhaite.

Montrons maintenant l'inégalité $d \leq \inf\{w(x) \mid x \in C_X \backslash C_Z^\perp \cup C_Z \backslash C_X^\perp\}$. Supposons que $x \in \mathbb{F}_2^n$ est un vecteur de $C_X \backslash C_Z^\perp$. Il définit une erreur $E \in I, Z^{\otimes n}$ de $N(S) \backslash S$ par l'isomorphisme $\mathbb{F}_2 \simeq \{I, Z\}$. La distance minimale du code est donc majorée par le poids $|E| = w(x)$ de cette erreur problématique. Le même argument est valable à partir de l'ensemble $C_Z \backslash C_X^\perp$, donnant ainsi la majoration de d. □

De cette démonstration, nous retiendrons la caractérisation des erreurs de syndrome nul et des erreurs problématiques :

Proposition 1.31. *Une erreur de Pauli agissant sur un code CSS de matrices* $\mathbf{H}_X \in \mathcal{M}_{r_X,n}(\mathbb{F}_2)$ *et* $\mathbf{H}_Z \in \mathcal{M}_{r_Z,n}(\mathbb{F}_2)$ *admet une décomposition binaire* $(E_X, E_Z) \in (\mathbb{F}_2^n)^2$. *Son syndrome est le vecteur* $(\mathbf{H}_X E_Z^t, \mathbf{H}_Z E_X^t) \in \mathbb{F}_2^{r_X + r_Z}$. *Cette erreur est de syndrome nul si et seulement si* $E_X \in C_Z$ *et* $E_Z \in C_X$. *Les erreurs problématiques sont celles qui vérifient, en plus de la condition précédente,* $E_X \notin C_X^\perp$ *ou* $E_Z \notin C_Z^\perp$.

Chapitre 2

Codes topologiques battant la borne de Bravyi-Poulin-Terhal

Après avoir rappelé les propriétés nécessaires des codes de surface et des codes couleur [17, 18, 66], nous nous intéressons à la borne de Bravyi Poulin et Terhal [23]. Les auteurs considèrent les codes stabilisateurs définis par des générateurs agissant sur les sommets d'un pavage carré. Ils ont démontré que si les générateurs d'un tel code sont inclus dans des boules de rayon fixé m du pavage carré, alors les paramètres $[[n, k, d]]$ du code quantique vérifient $kd^2 \leq cn$ où c est une constante qui ne dépend que de m.

Pour contourner cette limitation, des codes de surface définis sur des graphes hyperboliques ont étés proposés [47, 65, 100]. Nous rappelons la construction des codes de surface hyperboliques de Zémor [100]. Ces codes dépassent la borne de Bravyi, Poulin et Terhal puisqu'ils fournissent une famille de codes de surface de rendement k/n constant et de distance minimale logarithmique en n.

À notre connaissance, de tels paramètres n'ont pas été atteints avec des codes couleur. Nous proposons une famille de codes couleur de rendement constant et de distance croissante. Cette famille de codes couleur hyperboliques est basée sur un revêtement des pavages hyperboliques de Zémor.

Pour conclure ce chapitre nous démontrons une nouvelle borne sur les paramètres des codes topologiques. Tout code de surface et tout code couleur construit à partir d'un pavage de surface dont les longueurs des faces et les degrés des sommets sont bornés par une constante m, est sujet à une borne :

$$kd^2 \leq c(\log k)^2 n$$

pour une constante c qui ne dépend que de m. La preuve de ce résultat est basée sur des inégalités systoliques de Gromov [54]. Cette borne s'applique à tout type de pavage de surface. Elle prouve que la distance minimale des codes de surface hyperboliques et des codes couleur hyperboliques est optimale à une constante près.

2.1 Définition des codes de surface

2.1.1 Les codes des cycles

Nous commençons par introduire une famille de codes classiques dont la matrice de parité est creuse : les codes des cycles. Nous souhaitons construire un code dont la matrice de parité a exactement deux symboles 1 sur chaque colonne. Une autre manière de le voir est de considérer cette matrice comme la matrice d'incidence d'un graphe.
Un *graphe* est un couple $G = (V, E)$ tel que V est un ensemble et E est un ensemble de parties de V à deux éléments. Les éléments de V sont les *sommets* du graphes et E est l'ensemble des *arêtes* du graphe. Comme l'ensemble E ne contient que des paires d'éléments de V, le graphe ne contient pas de boucle. Il n'y a pas non plus d'arête multiple puisque E est un ensemble. Sans perte de généralité, on peut supposer que $V = \{1, 2, \ldots, |V|\}$ et que les arêtes sont ordonnées : $E = \{e_1, e_2, \ldots, e_{|E|}\}$. On peut aussi définir un graphe par un ensemble de sommet V, un ensemble d'arêtes E et une relation d'incidence entre les sommets et les arêtes telle que chaque arête est incidente à exactement deux sommets.

Nous nous intéressons aux cycles du graphe G. La définition d'un cycle peut varier en fonction du contexte. La notion utilisée dans ce document est la suivante.

Définition 2.1. *Un* cycle *c d'un graphe $G = (V, E)$ est un ensemble $c \subset E$ d'arêtes de G tel que tout sommet du graphe est contenu dans un nombre pair d'arêtes de c.*

L'ensemble des cycles du graphe est un code linéaire. Pour le voir, nous pouvons introduire la matrice d'incidence du graphe. C'est la matrice $I(G)$ à coefficients binaires, de taille $|V| \times |E|$, dont les colonnes sont les vecteurs caractéristiques des arêtes. Plus précisément, la i-ème ligne de $I(G)$ contient un coefficient $I_{i,j} = 1$ si et seulement si le sommet i est incident à la j-ème arête. Un cycle c est une partie de E, on peut regarder cette partie comme un vecteur binaire de $\mathbb{F}_2^{|E|}$: son vecteur caractéristique dont la j-ème composante est 1 si et seulement si l'arête e_j est contenue dans le cycle c. Avec ce point de vue vectoriel, l'ensemble des cycles d'un graphe G est le noyau de la matrice d'incidence du graphe : $\operatorname{Ker} I(G)$. Cette propriété est immédiate lorsque l'on observe que la i-ème ligne de la matrice d'incidence est le vecteur caractéristique de l'ensemble des arêtes incidentes au sommet i. On en déduit sa structure vectorielle. La propriété suivante exprime graphiquement les paramètres de ce code linéaire.

Proposition 2.2. *Soit $G = (V, E)$ un graphe fini composé de $\kappa(G)$ composantes connexes. Le code des cycles du graphe G est un code linéaire binaire de longueur $|E|$, de dimension $|E| - |V| + \kappa(G)$. Sa distance minimale est la maille du graphe G.*

Avant de passer à la preuve de cette proposition, rappelons que la *maille* d'un graphe est la longueur du plus court cycle de ce graphe. Par longueur, nous entendons le nombre d'arêtes du cycle.

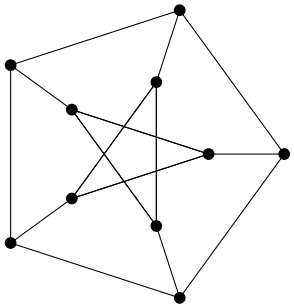


Figure 2.1 – Le graphe de Petersen

Démonstration. La structure vectorielle a été observée précédemment. L'expression de la distance minimale est immédiate. La seule chose à démontrer est la formule annoncée pour la dimension. Nous présentons ici une preuve élégante que l'on peut trouver par exemple dans le livre de Berge [12]. Soit T un sous-arbre maximal de G. Un tel arbre existe car le graphe est fini. Il contient tous les sommets de G et $|V|-\kappa$ arêtes. Il suffit de raisonner sur une composante connexe pour s'en convaincre. Pour chaque arête e_i qui n'est pas dans T, il existe un unique cycle c_i contenu dans $T \cup \{e_i\}$. Montrons que la famille $(c_i)_i$ composée de $|E| - |V| + \kappa$ cycles forme une base du code des cycles. Soit x un cycle de C. On note $\varepsilon_i = 1$ si x contient l'arête e_i et $\varepsilon_i = 0$ sinon. Alors $x + \sum \varepsilon_i c_i$ est un cycle du sous-graphe T. En effet, c'est clairement un cycle et chaque arête $e_i \notin T$ qui apparaît dans x est aussi présente dans la somme $\sum_i \varepsilon_i c_i$. Il est inclus dans l'arbre T. Un tel cycle est forcément nul. On en déduit que $x = \sum \varepsilon_i c_i$ et la famille $(c_i)_i$ est génératrice. Si $\sum \lambda_i c_i = 0$ alors chaque e_i apparaît un nombre pair de fois dans cette somme. Mais le seul des cycles c_j qui contient e_i est c_i, donc $\lambda_i = 0$. On a bien construit une base de cardinal $|E| - |V| + \kappa$. □

Le graphe de Petersen dessiné figure 2.1 est un graphe composé de 10 sommets et de 15 arêtes, son code des cycles est un code de paramètres $[15, 6, 5]$.

2.1.2 Les codes de surface

Définition combinatoire des surfaces

Dans cette partie nous détaillons la construction des codes de surface. On peut voir ces codes comme une généralisation quantique des codes des cycles. Ces codes ont été introduits par Kitaev qui a proposé d'associer un code stabilisateur à un pavage carré du tore, en 1997 [66]. Bombin et Martin-Delgado ont ensuite proposé de baser cette construction sur un pavage de surface quelconque en 2007 [19].

Commençons par définir le terme surface. La définition combinatoire suivante est la plus adaptée au domaine des codes topologiques. Nous verrons une surface comme un recollement de polygones. Nous parlerons de surface ou de pavage de surface.

Un cycle est dit *élémentaire* s'il ne s'écrit pas comme la réunion de deux cycles non nuls.

Définition 2.3. *Un* pavage de surface*, ou tout simplement une* surface*, est un triplet $G = (V, E, F)$ tel que $G = (V, E)$ est un graphe et F est un ensemble de cycles élémentaires appelés faces, avec les propriétés suivantes :*

- *Deux faces se rencontrent en au plus une arête et chaque arête appartient à exactement deux faces.*
- *Pour tout sommet v, si F_v est l'ensemble des faces incidentes à v, alors toute arête appartenant à deux faces de F_v est une arête contenant v. Soit γ_v le graphe dont les sommets sont les éléments de F_v, tel que deux sommets sont déclarés adjacents si les faces correspondantes ont une arête commune dans G. Alors γ_v est un cycle élémentaire.*

Cette définition nous permet de construire le *pavage dual* ou la *surface duale* G^* de $G = (V, E, F)$. Les sommets de la surface duale sont les éléments de $V^* = F$. Deux sommets sont voisins si les faces correspondantes partagent une arête. Autrement dit, chaque arête de G est transformée en une arête de son dual. A chaque sommet $v \in V$ du graphe G, on associe une face du graphe G^*. C'est le cycle élémentaire γ_v construit dans la définition 2.3. Finalement, on peut voir la surface duale de la surface $G = (V, E, F)$ comme la surface $G^* = (F, E, V)$. Pour simplifier, on parlera parfois du graphe G et de son *graphe dual* G^* plutôt que la surface G et de sa surface duale G^*, sans oublier que ce graphe dual dépend du graphe G mais aussi de ses faces.

Homologie et codes de surface

Pour associer un code quantique à un tel pavage de surface, nous utilisons la construction CSS. Notre but est de construire deux matrices binaires $\mathbf{H}_X$ et $\mathbf{H}_Z$ qui respectent les relations d'orthogonalité de la définition 1.29. On a besoin de l'orthogonalité entre toute ligne de $\mathbf{H}_X$ et toute ligne de $\mathbf{H}_Z$. Pour obtenir ces relations géométriquement, on utilise les groupes d'homologie d'une surface [50, 58]. Cette partie regroupe les notions d'homologie utilisées.

Soit $G = (V, E, F)$ une surface. On note $C_0(G)$ l'espace des sommes formelles de sommets à coefficients binaires. En notant v_i les sommets de G on a :

$$C_0(G) = \left\{ \sum_{i=1}^{|V|} \lambda_i v_i \mid \lambda_i \in \mathbb{F}_2 \right\}.$$

On définit de manière similaire les groupes basés sur les arêtes et sur les faces du graphe :

$$C_1(G) = \left\{ \sum_{i=1}^{|E|} \lambda_i e_i \mid \lambda_i \in \mathbb{F}_2 \right\},$$

et

$$C_2(G) = \left\{ \sum_{i=1}^{|F|} \lambda_i f_i \mid \lambda_i \in \mathbb{F}_2 \right\}.$$

On dispose d'une application bord notée ∂_2 de $C_2(G)$ vers $C_1(G)$. C'est l'application $\mathbb{F}_2$-linéaire ∂_2 qui envoie une face $f \in C_2(G)$ sur la somme de ses arêtes $\partial(f) =$

$\sum_{e\in f} e \in C_1(G)$. L'application bord ∂_1 de $C_1(G)$ vers $C_0(G)$ est l'application $\mathbb{F}_2$-linéaire qui transforme une arête $e \in C_1(G)$ en la somme de ses deux extrémités $\partial_1(e) = \sum_{v\in e} v \in C_0(G)$. En résumé :

Définition 2.4. *Le* complexe de chaîne *associé au pavage de surface $G = (V, E, F)$ est le triplet de $\mathbb{F}_2$-espaces vectoriels :*

$$C_2(G) = \bigoplus_{f\in F} \mathbb{F}_2 f, \qquad C_1(G) = \bigoplus_{e\in E} \mathbb{F}_2 e, \qquad C_0(G) = \bigoplus_{v\in V} \mathbb{F}_2 v$$

muni des applications bord ∂_2 *et* ∂_1 *qui sont les applications linéaires :*

$$C_2(G) \xrightarrow{\partial_2} C_1(G) \xrightarrow{\partial_2} C_0(G)$$

telles que $\partial_2(f) = \sum_{e\in f} e$ et $\partial_1(e) = \sum_{v\in e} v$.

On notera l'espace des *i-chaînes* par $C_i = C_i(G)$ lorsqu'aucune confusion n'est possible. On notera aussi C_i^* l'espace des i-chaînes du graphe dual G^*.

Les vecteurs de C_0, C_1 ou C_2 sont des vecteurs indicateurs d'ensemble de sommets, d'arêtes ou de faces respectivement. On les considérera comme des vecteurs ou comme des parties suivant les cas. Les sous-espaces $\operatorname{Ker}\partial_1$ et $\operatorname{Im}\partial_2$ admettent ainsi une description géométrique :

Lemme 2.5. *Soit $C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_2} C_0$ le complexe de chaîne associé à G.*
- *le sous-espace* $\operatorname{Ker}\partial_1$ *est le code des cycles du graphe G,*
- *le sous-espace* $\operatorname{Im}\partial_2$ *est l'espace des sommes de faces du graphe G.*

Proposition 2.6. *La composée de ces deux applications bord du complexe de chaîne associé à $G = (V, E, F)$ est nulle : $\partial_1 \circ \partial_2 = 0$.*

Démonstration. Il suffit de le vérifier sur les faces qui forment une base de C_2. Soit $f \in F$ une face de G. Le bord de cette face est $\partial_2(f) = \sum_{e\in f} e$. Par linéarité de ∂_1, on a :

$$\partial_1(\partial_2(f)) = \sum_{e\in f} \partial_1(e) = \sum_{e=\{u,v\}\in f} (u + v).$$

Comme les faces sont des cycles, chaque sommet $v \in V$ du graphe G est contenu dans un nombre pair d'arêtes de f. On en déduit que l'image de f par la composée des deux applications bord est nulle. □

De cette relation, on tire l'inclusion $\operatorname{Im}\partial_2 \subset \operatorname{Ker}\partial_1$. Le quotient $\operatorname{Ker}\partial_2/\operatorname{Im}\partial_1$ est le *premier groupe d'homologie* du pavage de surface G. Il est noté $H_1(G, \mathbb{F}_2)$ C'est le quotient de l'espace des cycles du graphe par le sous-espace engendré par les faces du pavage. Deux cycles du graphe qui différent d'une somme de faces sont dans la même classe dans le groupe quotient $H_1(G, \mathbb{F}_2)$, ils sont dits *homologues*. Un cycle *homologue à zéro* est un cycle qui est somme de faces, c'est un cycle de la classe de zéro dans le groupe d'homologie.

La proposition 2.6 nous donne les relations d'orthogonalité nécessaires à la définition d'un code CSS. On note $V = \{v_1, v_2, \ldots, v_{|V|}\}$ l'ensemble des sommets du

graphe, $E = \{e_1, e_2, \ldots, e_{|E|}\}$ est l'ensemble de ses arêtes et $F = \{f_1, f_2, \ldots, f_{|F|}$ est l'ensemble de ses faces. Soit $\mathbf{H}_X$ la matrice de l'application linéaire ∂_1 en fonction de la base $(e_i)_{i=1}^{|E|}$ de C_1 et de la base $(v_i)_{i=1}^{|V|}$ de C_0 et soit $\mathbf{H}_Z$ la transposée de la matrice de l'application linéaire ∂_2 en fonction de la base $(f_i)_{i=1}^{|F|}$ de C_2 et de la base $(e_i)_{i=1}^{|E|}$ de C_1. De l'égalité $\partial_1 \circ \partial_2 = 0$, on tire $\mathbf{H}_X \mathbf{H}_Z^t = 0$, d'où l'orthogonalité entre les lignes des matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$. On en déduit la définition suivante des codes de surface.

Définition 2.7. *Le* code de surface *associé à une surface $G = (V, E, F)$ est le code CSS de matrices :*

- $\mathbf{H}_X \in \mathcal{M}_{|V|,|E|}(\mathbb{F}_2)$ *la matrice d'incidence du graphe G.*
- $\mathbf{H}_Z \in \mathcal{M}_{|F|,|E|}(\mathbb{F}_2)$ *la matrice dont les lignes sont les vecteurs caractéristiques des faces du graphe G.*

D'après la proposition 1.30, les paramètres du code quantique défini par ces matrices s'expriment en fonction de deux codes classiques, les codes binaires $C_X = \operatorname{Ker} \mathbf{H}_X$ et $C_Z = \operatorname{Ker} \mathbf{H}_Z$, et de leurs duaux $C_X^\perp$ et $C_Z^\perp$.

Lemme 2.8. *Soit $C_X = \operatorname{Ker} \mathbf{H}_X$ et $C_Z = \operatorname{Ker} \mathbf{H}_Z$ les codes classiques associés à un code de surface G. Le code C_X est le code des cycles du graphe G et le code $C_Z^\perp$ est le sous-espace des sommes de faces du graphe G. Le code C_Z est le code des cycles du graphe G^* et le code $C_X^\perp$ est le sous-espace des sommes de faces du graphe G^*.*

Démonstration. Par définition, le code C_X est le code $\operatorname{Ker} \partial_1$. C'est le code des cycles du graphe G. Le code $C_Z^\perp$ est engendré par les lignes de la matrice $\mathbf{H}_Z$. C'est le code $\operatorname{Im} \partial_2$ des sommes de faces du graphe G.

Afin d'obtenir une description analogue des codes C_Z et $C_Z^\perp$, regardons le complexe de chaîne associé au graphe dual $G^* = (F, E, V)$:

$$C_2^* \xrightarrow{\partial_2^*} C_1^* \xrightarrow{\partial_2^*} C_0^*.$$

Par définition du graphe dual, on a $C_2^* = C_0, C_1^* = C_1$ et $C_0^* = C_2$. Ainsi la matrice $\mathbf{H}_X$ est aussi la transposée de la matrice de l'application linéaire ∂_2^* et la matrice $\mathbf{H}_Z$ est la matrice de l'application ∂_1^*. On en déduit l'expression souhaitée des codes $C_Z = \operatorname{Ker} \partial_1^*$ et $C_X^\perp = \operatorname{Im} \partial_2^*$. □

Le lemme précédent nous amène à une formulation géométrique des paramètres des codes de surface.

Théorème 2.9. *Le code de surface associé à la surface $G = (V, E, F)$ est un code CSS de longueur $n = |E|$ et de dimension $k = 2\kappa(G) - \chi(G)$. Sa distance minimale est la plus petite longueur d'un cycle du graphe G ou de son graphe dual G^* qui n'est pas somme de faces.*

Rappelons que $\kappa(G)$ est le nombre de composantes connexes du graphe G et donc aussi de son dual G^*. La quantité $\chi(G)$ est la caractéristique d'Euler du graphe G : $\chi(G) = |V| - |E| + |F|$. Lorsque l'on part d'une surface connexe orientable G [50],

ce nombre satisfait l'équation $\chi(G) = 2 - 2g$. Le nombre de qubits encodés est donc le double du genre de la surface. Avec une surface non orientable, on a $\chi(G) = 2 - g$ et le nombre de qubits encodés est égal au genre de la surface.

Démonstration. Le fait que la longueur est $n = |E|$ est clair. Déterminons la valeur de k. D'après la proposition 1.30, la dimension de ce code quantique est $k = n - \operatorname{rg} \mathbf{H}_X - \operatorname{rg} \mathbf{H}_Z$. Il reste à exprimer ces rangs en fonction de V, E et F. Les noyaux de ces matrices sont les codes des cycles du graphe G et de son dual G^*. On peut appliquer la proposition 2.2. On en déduit les rangs de ces matrices : $\operatorname{rg} \mathbf{H}_X = |V| - \kappa(G)$ et $\operatorname{rg} \mathbf{H}_Z = |F| - \kappa(G)$. La formule annoncée suit.

Regardons la formulation géométrique de la distance minimale. La proposition 1.30 donne l'expression de la distance minimale du code en fonction des codes classiques C_X et C_Z :

$$d = \inf\{\ w(x) \mid x \in C_X \backslash C_Z^\perp \text{ ou } x \in C_Z \backslash C_X^\perp\ \}.$$

Le lemme précédent permet de conclure. □

Notre but dans ce chapitre est d'étudier les paramètres des codes topologiques. La formulation géométrique que nous venons d'obtenir sera un outil essentiel.

La proposition suivante exprime le syndrome géométriquement. Elle sera utile lors de l'étude du décodage des codes de surface au chapitre 7.

Proposition 2.10. *Une erreur de Pauli agissant sur un code de surface $G = (V, E, F)$ admet une décomposition binaire (E_X, E_Z) où $E_X \in C_0^*$ et $E_Z \in C_0$. Son syndrome est le vecteur $(s_Z, s_X) \in C_0 \times C_0^*$ avec $s_Z = \partial_1(E_Z)$ et $s_Z = \partial_1^*(E_X)$.*

Démonstration. Par la proposition 1.31, nous disposons d'une expression du syndrome d'une erreur agissant sur un code CSS. En remarquant que $\mathbf{H}_X$ est la matrice de l'application ∂_1 et que $\mathbf{H}_Z$ est la matrice de l'application ∂_1^*, on obtient la proposition. □

Le code torique de Kitaev

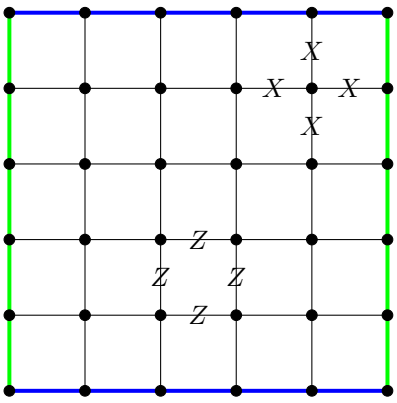


Figure 2.2 – Un pavage carré du tore et les générateurs du code de Kitaev

Le code torique de Kitaev [66] est défini sur un pavage carré du tore représenté figure 2.2. Les bords opposés de même couleur sont identifiés. Deux générateurs du groupe stabilisateur sont représentés. Les générateurs en X, qui correspondent aux lignes de $\mathbf{H}_X$, sont composés des quatre arêtes contenant un sommet et les générateurs en Z, sont définis par les faces du pavage.

On peut aussi définir ce pavage de surface comme le graphe de Cayley de $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ muni de la partie génératrice $\{\pm(1,0),\pm(0,1)\}$. D'après le théorème 2.9, le code quantique obtenu ainsi est un code quantique de paramètres $[[2m^2,2,m]]$. Les calculs de la longueur et de la dimension sont immédiats alors que l'évaluation de la distance minimale nécessite l'étude de la longueur des cycles d'homologie non-triviale dans le graphe et dans son dual. Ce graphe présente l'avantage d'être auto-dual, il n'est donc pas nécessaire de considérer son dual. On s'aperçoit rapidement que les cycles qui ne sont pas somme de faces sont ceux qui s'enroulent autour du tore et, parmi ceux-là, les plus courts sont ceux qui forment une ligne horizontale ou verticale comme dans la figure 2.3.

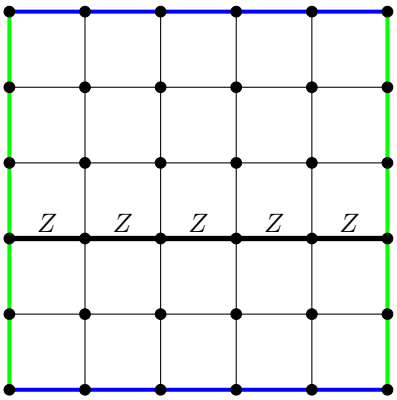


FIGURE 2.3 – Un cycle du tore, non homologue à zéro, de longueur minimale

Ces cycles, de longueur m, sont clairement non homologues à zéro. La distance minimale du code quantique est donc inférieure à m. Pour montrer que la distance est exactement m, nous allons utiliser un argument qui reviendra fréquemment dans l'étude de la distance des codes topologiques. Considérons un cycle c du graphe de longueur inférieure à $d-1$. Ce cycle est inclus dans une boule de rayon $\frac{d-1}{2}$ du graphe. Or cette boule est planaire par construction. Comme un cycle d'un graphe planaire est toujours somme de faces, le cycle c n'apparaît pas dans le calcul de la distance minimale qui est donc bien m.

2.2 Définition des codes couleur

2.2.1 Les codes couleur

Dans cette partie nous présentons une seconde famille de codes topologiques : les codes couleur. Comme les codes de surface, ils sont définis à partir d'un pavage de surface, mais dans cette construction, les qubits sont placés sur les sommets du graphe et non sur les arêtes. Ces codes sont issus des travaux de Bombin et Martin-

Delgado [17]. Nous présentons dans cette partie une nouvelle description des codes classiques associés à ces codes quantiques.

Définition 2.11. *Une surfaces $G = (V, E, F)$ est dite* trivalente *si tous les sommets du graphe $G = (V, E)$ sont de degré 3.*

Nous allons considérer des surfaces dont les faces sont coloriées en rouge, vert ou bleu. On notera R, V et B ces trois couleurs. Le choix de ces couleurs est arbitraire, seul le nombre de couleurs aura une importance.

Définition 2.12. *On dit que les faces d'une surface $G = (V, E, F)$ sont* 3-coloriables *s'il est possible d'associer une couleur $\mathbf{c} \in \{R, V, B\}$ à chaque face de la surface G de telle sorte que deux faces qui partagent une arête ne portent pas le même couleur.*

Ces deux propriétés des surfaces suffisent à définir un code couleur :

Définition 2.13. *Soit $G = (V, E, F)$ une surface trivalente dont les faces sont 3-coloriables. Le* code couleur *associé à la surface G est le code CSS de matrices :*
- $\mathbf{H}_X \in \mathcal{M}_{|F|,|V|}(\mathbb{F}_2)$ *la matrice dont les lignes sont les vecteurs caractéristiques des faces du graphe G vu comme des ensembles de sommets.*
- $\mathbf{H}_Z = \mathbf{H}_X$.

Pour justifier cette définition nous devons démontrer l'orthogonalité entre les lignes de $\mathbf{H}_X$. Comme le graphe est trivalent, deux faces différentes de ce pavage partagent forcément $2t$ sommets, où t est le nombre d'arêtes communes à ces deux faces. Les lignes de $\mathbf{H}_X$ définis par ces deux faces sont donc orthogonales. Pour voir qu'une ligne de $\mathbf{H}_X$ est orthogonale à elle même, on remarque que les faces de ce pavage sont toutes de longueur paire :

Lemme 2.14. *Toutes les faces d'un pavage trivalent, dont les faces sont 3-coloriées, sont de longueur paire.*

Démonstration. Les faces voisines d'une face rouge f sont nécessairement vertes ou bleues. Comme le graphe est trivalent, cette face rouge est entourée d'une suite alternée de faces vertes et bleu. Cette alternance implique que la longueur de f est paire. □

Ces matrices définissent bien un code CSS. On peut remarquer que la coloriabilité des faces est une condition suffisante pour définir un code quantique mais elle n'est pas nécessaire. Néanmoins, cette coloration s'avère très utile pour décrire le normalisateur du groupe stabilisateur et les erreurs problématiques. De plus, les applications de ces codes en calcul topologique reposent sur cette coloration [14,15,17]. Nous ne considérerons pas les codes construits à partir de pavages dont les faces ne sont pas 3-coloriables.

La définition des matrices d'un code couleur implique la propriété suivante :

Proposition 2.15. *La matrice $\mathbf{H}_X = \mathbf{H}_Z$ définissant le code couleur associé au*

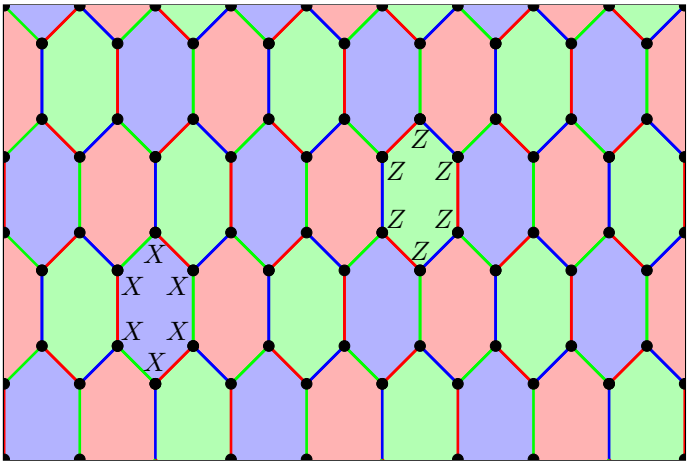


FIGURE 2.4 – Un pavage 3-colorié du tore et la coloration induite sur ses arêtes. Le groupe stabilisateur associé est engendré par les opérateurs X_f qui valent X autour d'une face f et les opérateurs $Z_{f'}$ qui valent Z sur les sommets autour d'une face f'.

pavage $G = (V, E, F)$ est la matrice de l'application linéaire de C_0 dans C_2 qui associe à un sommet $v \in V$, la somme des faces le contenant $s(v) = \sum_{v \in f} f$.

Cette application linéaire définit donc le syndrome d'une erreur de Pauli agissant sur un code couleur.

Proposition 2.16. *Une erreur de Pauli agissant sur le code couleur défini sur le pavage G admet une décomposition binaire de la forme (E_X, E_Z) où E_X et E_Z sont des vecteurs de C_0. Le syndrome de cette erreur est le vecteur $(s(E_Z), s(E_X)) \in C_2^2$.*

Cette proposition est un application immédiate de la proposition 1.31. Dans la suite, nous regardons le code $C = \operatorname{Ker} \mathbf{H}_X = \operatorname{Ker} \mathbf{H}_Z$ comme le noyau de l'application linéaire s. Les erreurs peuvent donc être considérées comme des couples de vecteurs de l'espace C_0, c'est-à-dire comme des parties de l'ensemble V des sommets du graphe. Une telle partie est un mot du code C si et seulement si son intersection avec toute face du graphe G est de cardinal pair.

2.2.2 Les graphes rétrécis

La détermination des paramètres du code quantique est plus délicate que dans le cas des codes de surface. Nous allons introduire les graphes rétrécis pour obtenir une expression géométrique du code. L'utilisation des graphes rétrécis est une idée de Bombin et Martin-Delgado [17]. Nous utilisons ici ces outils pour obtenir une description exacte du code $C = \operatorname{Ker} \mathbf{H}_X = \operatorname{Ker} \mathbf{H}_Z$. On en déduira une nouvelle expression géométrique des paramètres des codes couleur.

Pour définir les graphes rétrécis nous avons besoin d'une coloration des arêtes du graphes. C'est la 3-coloration induite par la 3-coloration des faces du pavage :

Définition 2.17. *Soit $G = (V, E, F)$ une surface trivalente et dont les faces sont 3-*

coloriées. La 3-coloration des faces de G induit une 3-coloration des arêtes du graphe G. Une arête porte la couleur qui n'apparaît pas sur les deux faces qui la contiennent.

Le graphe rétréci de couleur $\mathbf{c}$ est le graphe induit par les arêtes de couleur C du graphe G :

Définition 2.18. *Soit $G = (V, E, F)$ une surface trivalente et dont les faces sont 3-coloriées. Le* graphe rétréci *de couleur $\mathbf{c}$ associé à la surface G est le graphe $G_{\mathbf{c}} = (F_{\mathbf{c}}, E_{\mathbf{c}})$ dont les sommets sont les faces de couleur $\mathbf{c}$ de G et dont les arêtes sont les arêtes de couleur $\mathbf{c}$ de G. Un sommet et une arête sont incidents dans $G_{\mathbf{c}}$ si la face et l'arête correspondantes dans le graphe G partagent un sommet.*

On peut voir les arêtes du graphe $G_{\mathbf{c}}$ comme des versions prolongées des arêtes de couleur $\mathbf{c}$ de G. Ce graphe possède une structure naturelle de pavage de surface. Ses faces se déduisent de celles du pavage d'origine G :

Lemme 2.19. *Soit $G = (V, E, F)$ une surface trivalente et dont les faces sont 3-coloriées par les couleurs $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$. Si $f \in F$ est une face de couleur $\mathbf{c}_1$ alors f est une face de longueur paire $2m$, formée de m arêtes de couleur $\mathbf{c}_2$ et de m arêtes de couleur $\mathbf{c}_3$ alternées.*

Démonstration. La preuve de ce lemme est analogue à la preuve du lemme 2.14 □

Proposition 2.20. *Soit $G = (V, E, F)$ une surface trivalente et dont les faces sont 3-coloriées et soit $G_{\mathbf{c}}$ un graphe rétréci associé à G. Soit f une face de G de couleur $\mathbf{c}' \neq \mathbf{c}$. La restriction de cette face aux arêtes de couleur $\mathbf{c}$ est un cycle élémentaire du graphe $G_{\mathbf{c}}$ que l'on note $f_{\mathbf{c}}$. Le graphe $G_{\mathbf{c}}$ muni des faces $F(G_{\mathbf{c}}) = \{f_{\mathbf{c}} \mid f \in F \backslash F_{\mathbf{c}}\}$ est un pavage de surface.*

Un dessin suffit pour se convaincre que ces faces équipent bien les graphes rétrécis d'une structure de pavage de surface. La structure de surface du pavage G est transférée à ces graphes rétrécis $G_{\mathbf{c}}$. Par exemple, une face verte de longueur $2m$ est bordée par m arêtes rouges et m arêtes bleues. Les m arêtes bleues forment une face du graphe rétréci bleu G_B. Le graphe G_B issu d'un pavage hexagonal 3-colorié du tore est tracé figure 2.5.

2.2.3 Description graphique du normalisateur

Le code classique associé à un code couleur de graphe G est le code $C = \operatorname{Ker} \mathbf{H}_X = \operatorname{Ker} \mathbf{H}_Z$. Ce code correspond au normalisateur du code stabilisateur. C'est un code auto-orthogonal. Nous allons maintenant nous intéresser à ce code classique et à son dual $C^{\perp}$. Un vecteur de ce code est un vecteur de $C_0(G)$, c'est-à-dire un ensemble de sommets du graphe, qui a une intersection de cardinal pair avec toutes les faces du graphe. Nous allons relier ce code C aux codes des cycles des pavages rétrécis $G_{\mathbf{c}}$ grâce aux vecteurs de cycle :

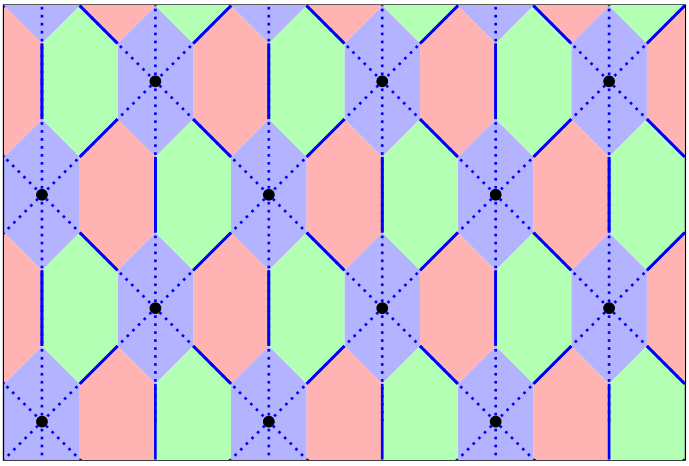


FIGURE 2.5 – Un pavage rétréci bleu construit à partir d'un pavage hexagonal du tore. Ses arêtes sont les arêtes bleues prolongées en pointillés. Ses faces correspondent aux faces rouges et vertes du pavage hexagonal

Définition 2.21. *Soit $\gamma_{\mathbf{c}}$ un élément du code des cycles du graphe rétréci $G_{\mathbf{c}}$. Le* vecteur de cycle $X(\gamma_{\mathbf{c}})$ *est le vecteur de $C_0(G)$:*

$$X(\gamma_{\mathbf{c}}) = \sum_{\substack{\{u,v\}\in E(G)\\ \{u,v\}\in\gamma_{\mathbf{c}}}} (u+v) = \sum_{e\in\gamma_{\mathbf{c}}} \partial_1^G(e).$$

Les arêtes du graphe $G_{\mathbf{c}}$ sont, par définition, des arêtes de G. Le vecteur de cycle $X(\gamma_{\mathbf{c}})$ est composé des sommets du graphe G contenus dans des arêtes du cycle $\gamma_{\mathbf{c}}$ de $G_{\mathbf{c}}$. Ces vecteurs de cycle engendrent le code C :

Proposition 2.22. *Soit G un pavage de surface trivalent dont les faces sont 3-coloriables. Le code classique $C = \operatorname{Ker}\mathbf{H}_X = \operatorname{Ker}\mathbf{H}_Z$ associé au code couleur de graphe G est le code :*

$$C = \langle\ X(\gamma_R), X(\gamma_V)\rangle$$

où γ_R parcourt les cycles du graphe G_R et γ_V parcourt les cycles du graphe G_V.

Démonstration. Démontrons que ces vecteurs de cycle sont dans le code C. Sans perte de généralité, on peut considérer un vecteur $X(\gamma_R)$ associé à un cycle γ_R du pavage rétréci rouge. On regarde le vecteur $X(\gamma_R)$ comme un ensemble de sommets de G. Il suffit de démontrer que le vecteur $X(\gamma_R)$ contient un nombre pair de sommets autour de chaque face du graphe G.
Soit $f \in F$ une face rouge du graphe G. On sait que γ_R est un cycle du graphe G_R. Il contient donc un nombre pair d'arêtes autour de chaque sommet du graphe G_R. Les sommets du graphe G_R sont les faces rouges du graphe G. On en déduit que $X(\gamma_R)$ contient un nombre pair de sommets autour de chaque face rouge de G.
Montrons que c'est encore le cas avec les faces vertes et bleues. Considérons une face verte f de longueur $2m$. Elle est bordée par m arêtes rouges d'après le lemme 2.19 et ces arêtes sont disjointes. Chacune d'entre elles contribue donc soit à zéro soit à

deux sommets de $X(\gamma_R)$, autour de la face f. Le même raisonnement reste valable avec les faces bleues.
Les vecteurs de cycle sont bien des vecteurs du code C.

Regardons maintenant l'inclusion réciproque. Soit $x \in C_0(G)$ un vecteur du code C. Ce vecteur correspond à un ensemble de sommet du graphe G dont l'intersection avec chaque face du graphe est de cardinal pair. Nous allons construire deux cycles γ_R et γ_V tels que $x = X(\gamma_R) + X(\gamma_V)$.
On considère la restriction x_f de x à une face bleue f. Cette face est composée de $2m$ sommets :

$$\{v_1, v_2, \ldots, v_{2m-1}, v_{2m}\},$$

où v_i et v_{i+1} sont des sommets voisins.
À partir de l'ensemble x_f, nous construisons un ensemble $\gamma_R(x_f)$ d'arêtes rouges de G et un ensemble $\gamma_V(x_f)$ d'arêtes vertes du graphe G. Une représentation graphique de cette transformation est proposée figure 2.6. Elle est composée des trois étapes suivantes :

- Le vecteur x_f contient un nombre pair de ces sommets. On note

  $$\{u_1, u_2, \ldots, \ldots, u_{2r-1}, u_{2r}\}$$

  la sous-suite des sommets de f contenus dans x_f. L'ordre des sommets u_i est celui induit par l'ordre des v_i.
- En respectant l'orientation de la face définie par l'ordre des sommets v_i, on sélectionne alors les chemins γ_j joignant les sommets u_j et u_{j+1} lorsque j est impair.
- Comme la face bleue f est composée de m arêtes rouges et d'autant d'arêtes vertes, la réunion des chemins γ_j est partitionnée en un ensemble d'arêtes rouges que l'on note $\gamma_R(x_f)$ et un ensemble d'arêtes vertes que l'on note $\gamma_V(x_f)$.

Après avoir procédé ainsi pour toutes les faces bleues, nous définissons γ_R comme la réunion des $\gamma_R(x_f)$ pour toute les faces bleues f. L'ensemble γ_V est défini de manière analogue.
Pour conclure, nous devons démontrer que ces ensembles d'arêtes sont des cycles des graphes rétrécis G_R et G_V et qu'ils vérifient :

$$X(\gamma_R) + X(\gamma_V) = x.$$

Pour montrer que γ_R est un cycle du graphe G_R, nous allons voir qu'il est dans le noyau de l'application bord $\partial_1^{G_R}$. Le bord de cet ensemble d'arêtes est par linéarité :

$$\partial_1^{G_R}(\gamma_R) = \sum_{f \in F_B} \partial_1^{G_R}(\gamma_R(x_f)).$$

D'après le lemme 2.23, démontré ensuite, cette somme peut être reformulée :

$$\partial_1^{G_R}(\gamma_R) = \sum_{f \in F_B} s(x_f)_{|F_R} = s(x)_{|F_R}.$$

La dernière égalité est obtenue en remarquant que x est la somme des x_f lorsque f parcourt l'ensemble des faces bleues du graphe G. Ceci provient du fait que ces faces forment une partition des sommets de G. Comme x est un mot du code C, son syndrome est nul. L'ensemble γ_R est bien un cycle du graphe G_R. Ce raisonnement permet aussi de voir que γ_V est bien un cycle du graphe G_V.
Pour démontrer que l'on a $X(\gamma_R) + X(\gamma_V) = x$, on écrit $X(\gamma_R)$ sous la forme $X(\gamma_R) = \sum_{f \in F_B} \partial_1^G(\gamma_R(x_f))$, on fait de même pour le cycle vert, puis on applique le lemme 2.24 dont la preuve suit. Nous avons ainsi démontré l'inclusion réciproque. □

Lemme 2.23. *Soit $s(x_f) \in C_2(G)$ le syndrome du vecteur $x_f \in C_0(G)$.*
- *La restriction de $s(x_f)$ à l'ensemble F_R des faces rouges de G est le vecteur :*

$$s(x_f)_{|F_R} = \partial_1^{G_R}(\gamma_R(x_f)).$$

- *La restriction de $s(x_f)$ à l'ensemble F_V des faces vertes de G est le vecteur :*

$$s(x_f)_{|F_V} = \partial_1^{G_V}(\gamma_V(x_f)).$$

Démonstration. D'après la proposition 2.16, le syndrome $s(x_f)_{|F_R}$ est l'ensemble des faces rouges du graphe G qui contiennent un nombre impair de sommets de x_f. Il suffit de considérer les faces voisines de la face bleue f. Soit f' une face rouge voisine de f. Ces deux faces partagent une arête verte $\{v_i, v_{i+1}\}$. Il y a huit cas à considérer pour vérifier que $s(x_f)$ et $\partial_1^{G_R}(\gamma_R(x_f))$ coïncident sur cette face f' : l'indice i est pair ou impair, le sommet v_i est contenant dans x_f ou non et le sommet v_{i+1} appartient à x_f ou non. L'examen de ces huit configurations permet de démontrer le lemme. Le cas des faces vertes se traite de manière identique. □

Lemme 2.24. *On note $X(\gamma_{\mathbf{c}}(x_f))$ l'image de $\gamma_{\mathbf{c}}(x_f) \in C_1(G)$ par l'application ∂_1. On a $X(\gamma_R(x_f)) + X(\gamma_V(x_f)) = x_f$.*

Démonstration. Soit v_i un sommet de f. Supposons que ce sommet est inclus dans x_f. Alors, par construction, l'ensemble des chemins γ_j contient soit l'arête $\{v_{i-1}, v_i\}$, soit l'arête $\{v_i, v_{i+1}\}$ mais pas ces deux arêtes (lorsque $i = 1$ ou $2m$ on considère les indices modulo $2m$). On en déduit que le sommet v est contenu dans une arête de $\gamma_R(x_f)$ ou bien dans une arête de $\gamma_V(x_f)$. Le lemme est donc vérifié pour ce sommet. Le cas d'un sommet v_i qui n'est pas dans x_f est analogue. □

Nous pouvons en fait démontrer un résultat plus précis en utilisant la transformation précédente. Nous obtenons une description exacte du normalisateur en fonction du code des cycles du graphe G_R, noté Γ_R et du code des cycles du graphe G_V, noté Γ_V.

Proposition 2.25. *Soit G un pavage de surface trivalent dont les faces sont 3-coloriables. On note Γ_R le code des cycles du graphe G_R et Γ_V le code des cycles du graphe G_V. Le code classique $C = \operatorname{Ker} \mathbf{H}_X = \operatorname{Ker} \mathbf{H}_Z$, associé au code couleur de graphe G est un $\mathbb{F}_2$-espace vectoriel isomorphe au quotient suivant :*

$$C \simeq \Gamma_R \times \Gamma_V / \langle\ (\gamma_R(f), \gamma_G(f)) | f \in F_B \rangle$$

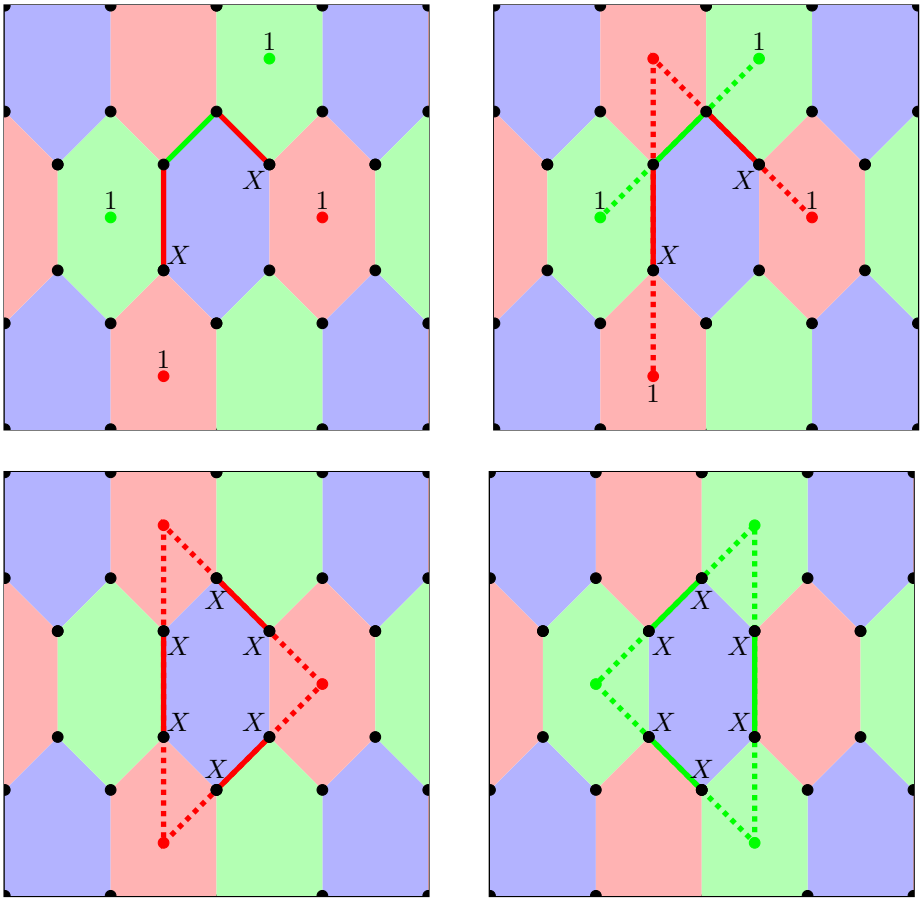


Figure 2.6 – Les deux premières figures illustrent la preuve de la proposition 2.22. Nous construisons des chemins γ_R et γ_V autour d'une face bleue. En bas deux cycles l'un vert et l'autre rouge représentant le même vecteur $X(f)$ associé à une face bleue.

où $\gamma_R(f)$ est le cycle du graphe G_R défini par la face bleue f et $\gamma_V(f)$ est le cycle du graphe G_V défini par la face f.

Démonstration. Dans la preuve de la proposition 2.22, nous avons introduit une application qui associe une paire de cycles (γ_R, γ_V) de l'espace $\Gamma_R \times \Gamma_V$ à un vecteur du code C. Pour démontrer ce théorème, il suffit de remarquer que cette application est un morphisme d'espace vectoriel et que son noyau est l'espace : $\langle(\gamma_R(f), \gamma_G(f))|f \in F_B\rangle$. □

Nous disposons d'une description exacte du code classique $C = \operatorname{Ker}\mathbf{H}_X = \operatorname{Ker}\mathbf{H}_Z$. La distance minimale du code quantique est le poids minimum d'un vecteur de $C\backslash C^\perp$. Comment voir l'orthogonal du code C dans la description géométrique précédente de C ? Le prochain corollaire nous permet d'utiliser les propriétés homologiques des pavages rétrécis pour étudier la distance minimale.

Corollaire 2.26. *L'orthogonal du code classique C associé au code couleur est :*

$$C^\perp = \text{vect}\{\ X(\gamma_R), X(\gamma_V)\ \},$$

où γ_R parcourt les cycles de G_R qui sont des sommes de faces et γ_V parcourt les sommes de faces de G_V.

Démonstration. Ce code $C^\perp$ est engendré par les lignes de la matrice $\mathbf{H}_X$. Il suffit alors de remarquer que les lignes correspondent aux faces du graphe et de regarder l'image de ces faces par l'isomorphisme de la proposition 2.25. □

Nous sommes maintenant en mesure de calculer les paramètres d'un code couleur en fonction du pavage de surface G, en utilisant les pavages rétrécis G_R et G_V et la proposition 2.25.

Théorème 2.27. *Soit G un pavage de surface dont les faces sont 3-coloriables. On note Γ_R le code des cycles du graphe G_R et Γ_V le code des cycles du graphe G_V. Le code couleur associé au pavage G est un code quantique de longueur $n = |V|$, qui encode $k = 4 - 2\chi(G)$ qubits et de distance minimale d telle que :*

$$d = \inf\{\ w(x) \mid x = X(\gamma_R) + X(\gamma_V) \text{ avec } \gamma_R \text{ ou } \gamma_V \text{ non somme de faces }\}.$$

Démonstration. La longueur du code est égale au nombre de sommets par définition. La dimension du code quantique est $n - 2\operatorname{rg}\mathbf{H}$ avec $\mathbf{H} = \mathbf{H}_X = \mathbf{H}_Z$. Pour calculer le rang de $\mathbf{H}$ nous utilisons l'isomorphisme de la proposition 2.25. Commençons par calculer la dimension des codes des cycles Γ_R et Γ_V des graphes rétrécis G_R et G_V. La proposition 2.2 permet d'exprimer la dimension d'un code des cycles en fonction de son nombre d'arêtes, son nombre de sommets et son nombre de composantes connexes κ. On obtient $\dim\Gamma_R = |E_R| - |F_R| + \kappa(G_R)$ et $\dim\Gamma_V = |E_V| - |F_V| + \kappa(G_V)$. On peut remarquer que les vecteurs de la forme $(\gamma_R(f), \gamma_G(f))$ sont indépendants lorsque f parcourt les faces bleues du graphe G. Ces vecteurs engendrent donc un sous-espace de $\Gamma_R \times \Gamma_V$ de dimension $|F_B|$. La dimension du code $C = \operatorname{Ker}\mathbf{H}$ suit :

$$\begin{aligned}\dim C &= \dim\Gamma_R + \dim\Gamma_V - \dim\{\operatorname{vect}(\gamma_R(f), \gamma_G(f)) | f \in F_B\} \\ &= 2\kappa - |F| + |E| - |E_B|.\end{aligned}$$

On en déduit le rang de la matrice $\mathbf{H}$ et la dimension du code quantique. Pour arriver à la quantité $4\kappa - 2\chi(G)$, on utilise l'égalité $|V| = 2|E_B|$.

D'après la proposition 2.22, les vecteurs de C sont décrit par des couples de cycles de Γ_R et Γ_V. Le corollaire 2.26 prouve que lorsque ces cycles sont homologues à 0, il définissent un vecteur de $C^\perp$. L'expression voulue de la distance minimale suit. □

En partant du pavage 3-colorié du tore dessiné figure 2.7, on obtient un code quantique de longueur $n = 48$ qui encode $k = 4$ qubits et de distance minimale $d = 4$. Dans cette figure, on représente une erreur problématique et les cycles rouges et verts correspondants dans la proposition 2.25. La distance minimale est atteinte par exemple en considérant un cycle vertical composé de deux arêtes qui s'enroule autour du tore.

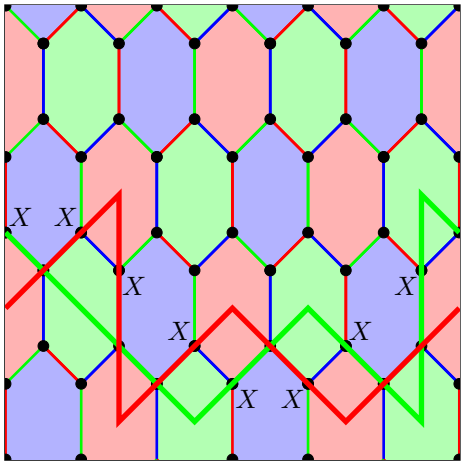


Figure 2.7 – Une erreur problématique pour le code couleur hexagonal.

2.3 Une famille de pavages hyperboliques finis

Cette section est consacrée à la construction de pavages hyperboliques finis. Ces graphes permettent de définir des surfaces de genre élevé et donc des codes quantiques de grande dimension.

2.3.1 Les groupes triangulaires de Širáň

Les pavages hyperboliques que nous utiliserons sont basés sur une famille de groupes de finis étudiée par Širáň [93]. Nous présentons ces groupes dans cette partie.

Rappelons qu'un groupe est *triangulaire* s'il admet la présentation suivante :

$$T =< y, z \mid y^l = z^m = (yz)^2 = 1 > . \tag{2.1}$$

Cela signifie que T est engendré par deux éléments y et z et que les seules relations entre les générateurs sont celles issues des 3 relations annoncées.

Le cadre naturel de ce graphe est la géométrie hyperbolique. Dans le disque de Poincaré, on peut construire un polygone régulier à l cotés centré en 0 et d'angles $2\pi/m$ lorsque $\frac{1}{l} + \frac{1}{m} < \frac{1}{2}$. On note y la rotation hyperbolique de centre 0 et d'angle $2\pi/m$, et z la rotation hyperbolique centrée en un sommet du polygone et d'angle $2\pi/m$. En appliquant le groupe d'isométries hyperboliques engendré par y et z au polygone, nous obtenons un pavage hyperbolique dont les faces sont de longueur l et les sommets sont de degré m. De plus, le groupe engendré par y et z est un groupe triangulaire qui admet la présentation (2.1) et c'est le groupe des automorphismes du pavage qui préserve l'orientation.

La stratégie de Širáň est de partir de deux matrices qui engendrent un groupe triangulaire infini et de réduire leurs coefficients modulo un nombre premier pour en déduire un groupe fini. De plus, en choisissant un nombre premier p assez grand, on peut s'assurer qu'il n'y a pas de relations courtes entre générateurs autre que celles issues du groupe d'origine. Cette idée a d'abord été utilisée par Margulis pour construire des codes LDPC à partir de graphe de Cayley de grande maille [74, 100].

On note $P_k(X) = 2\cos(k \arccos(X/2))$ le k-ème polynôme de Chebychev normalisé et $\xi = 2\cos(\pi/lm)$. Soit X et Z les matrices de $SL_3(\mathbb{Z}[\xi])$ définies par :

$$Y = \begin{pmatrix} P_l(\xi)^2 - 1 & 0 & P_l(\xi) \\ P_m(\xi) & 1 & 0 \\ -P_l(\xi) & 0 & -1 \end{pmatrix} \quad \text{et} \quad Z = \begin{pmatrix} -1 & -P_m(\xi) & 0 \\ P_m(\xi) & P_m(\xi)^2 - 1 & 0 \\ P_l(\xi) & P_l(\xi)P_m(\xi) & 1 \end{pmatrix}.$$

Ces deux matrices engendrent un groupe triangulaire $T(l, m)$ [93]. Pour obtenir les relations annoncées en (2.1) poser $y = Y$ et $z = Z$. Pour voir que ces matrices sont bien à coefficients dans $\mathbb{Z}[\xi]$, on peut remarquer que les polynômes de Chebychev normalisés T_k vérifient la relation de récurrence $P_{k+2}(X) = XP_{k+1}(X) - P_k(X)$ avec $P_0(X) = 1$ et $P_1(X) = X$. Cette relation permet aussi de calculer rapidement ces polynômes.

Pour obtenir un groupe fini, on peut réduire les coefficients de ces matrices modulo un nombre premier p. Ces coefficients sont situés dans l'anneau $\mathbb{Z}[\xi]$, qui est isomorphe au quotient $\mathbb{Z}[X]/h(X)$ avec h le polynôme minimal de l'entier algébrique ξ. La réduction des coefficients modulo p, définit un morphisme de groupe de $SL_3(\mathbb{Z}[\xi])$ vers $SL_3(\mathbb{F}_p[X]/(h(X))$. On s'intéresse à l'image du groupe $T(l, m)$ que l'on note $\bar{T}(l, m)$. En suivant Širáň, on introduit le rayon d'injectivité du groupe $\bar{T}(l, m)$. Širáň définit cette quantité graphiquement, nous utilisons ici une définition plus générale qui ne dépend pas du choix de la partie génératrice car nous allons construire plusieurs familles de graphes à partir de ces groupes triangulaires. Soit S un ensemble de générateurs de $T(l, m)$ stable par passage à l'inverse. On note P_r l'ensemble des produits de, au plus, r éléments de S.

Définition 2.28. *Soit p un nombre premier. Le* rayon d'injectivité *du groupe $\bar{T}(l, m)$ muni de la partie génératrice S est le plus grand entier r tel que la restriction à P_r de la surjection de $T(l, m)$ vers $\bar{T}(l, m)$ est injective.*

Le théorème suivant, dû à Širáň [93], prouve que l'on peut choisir un groupe triangulaire réduit dont le rayon d'injectivité est aussi grand que l'on souhaite et dont la taille ne grandit pas trop vite.

Théorème 2.29. *Pour tout entier r, il existe un nombre premier p et un groupe $\bar{T}(l, m)$, de rayon d'injectivité supérieur à r et de cardinal $|\bar{T}(l, m)| \leq C^r$ pour une constante C. Ce groupe est noté T_r ou $T_r(l, m)$.*

Attention au fait que la constante C, comme la définition du rayon d'injectivité, dépend de la partie génératrice S.

L'argument de Širáň est le suivant. Si jamais un produit de matrices Y et Z, qui diffère de l'identité dans le groupe $T(l, m)$ se réduit sur l'identité, alors au moins l'un de ces coefficient dépasse p après réduction modulo $h(X)$. Or les coefficients d'un produit de au plus r matrices Y et Z ne grandissent pas trop vite. On en déduit que pour obtenir un tel produit de générateurs, il faut un grand nombre de matrices lorsque p est grand. Pour rendre cet argument rigoureux, nous allons introduire des outils pour mesurer la taille des coefficients. C'est le rôle des trois lemmes suivants qui ne nécessitent pas de démonstration.

Les coefficients des matrices du groupe $T(l,m)$ sont des classes de polynômes à coefficients entiers. Nous mesurons la taille d'un polynôme $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, en fonction de sa norme : $||f|| = \max_{0\leq i\leq n}\{|a_i|\}$ et de sa largeur : $w(f) = \#\{i|a_i \neq 0\}$.

Lemme 2.30. *La norme de la somme et du produit de deux polynômes f et g de $\mathbb{Z}[X]$ sont majorés par :*
- $||f+g|| \leq ||f|| + ||g||$,
- $||fg|| \leq \min\{w(f), w(g)\}||f||||g||$.

Cette notion de norme et de largeur est transmise aux polynômes de l'anneau quotient $\mathbb{Z}[\xi]$ en utilisant le reste de la division euclidienne par h le polynôme minimal de ξ. Si $f(\xi)$ est un polynôme de $\mathbb{Z}[\xi]$ et si r est le reste de la division euclidienne de f par h, alors la norme de $f(\xi)$ est $||f(\xi)|| = ||r||$ et sa largeur est $w(f(\xi)) = w(r)$.

Lemme 2.31. *La norme d'un produit de deux polynômes $f(\xi)$ et $g(\xi)$ de l'anneau quotient $\mathbb{Z}[\xi]$ est majorée par :*

$$||f(\xi)g(\xi)|| \leq ws^{d-1}||f(\xi)||||g(\xi)||$$

avec $w := \min\{w(f), w(g)\}, s = (1 + ||h||), d = \deg h$.

Des deux lemmes précédents, on tire une majoration de la taille d'un produit de matrices à coefficients dans $\mathbb{Z}[xi]$. Nous appelons norme de $A = (A_{i,j}) \in SL_3(\mathbb{Z}[\xi])$ la quantité $||A|| = \max_{1\leq i,j\leq 3} ||A_{i,j}(\xi)||$ et largeur de A est $w(A) = \max_{1\leq i,j\leq 3} w(A_{i,j}(\xi))$.

Lemme 2.32. *La norme d'un produit de r matrices $A_1, A_2, \ldots, A_r \in SL_3(\mathbb{Z}[\xi])$ est majorée par :*

$$||A_1 A_2 \ldots A_r|| \leq \left(3ws^{d-1}\right)^{r-1} ||A_1||||A_2|| \ldots ||A_r||$$

avec $w := \max\{w(A_1), w(A_2), \ldots, w(A_r)\}, s = (1 + ||h||), d = \deg h$.

Nous sommes désormais en mesure de démontrer le théorème 2.29. On s'assure que le rayon d'injectivité dépasse r par le choix d'un nombre premier p qui dépasse la norme de tous les produits de au plus r matrices génératrices. Pour ne pas obtenir un groupe trop grand, on fait appel au postulat de Bertrand.

Démonstration du théorème 2.29. D'après le lemme 2.32, tout produit, $x \in P_r$, de longueur inférieure à r, est majoré en norme par :

$$||\pi(x)|| \leq (3ws^{d-1})^{r-1} N^r = C(r)$$

où $s = 1 + ||h||, d = \deg h$ et N est un majorant des normes des éléments de S.

On a donc une matrice x qui n'est pas l'identité et dont tous les coefficients sont majorés. Pour être sûr que sa réduction $\pi(x)$ n'est pas l'identité, il suffit de choisir un nombre premier p au delà que la borne $C(r)$. Soit p premier tel que $p > C(r)$ et

G le groupe correspondant. Un élément du groupe est une matrice composée de 9 coefficients qui sont des classes de $\mathbb{F}_p[X]/(\overline{h(X)})$. On peut donc majorer brutalement la taille du groupe $\bar{T}(l,m)$ par p^{9d}.

Pour obtenir une majoration indépendante de p, on fait intervenir le postulat de Bertrand. Il nous assure de l'existence d'un nombre premier p tel que :

$$(3ws^{d-1})^{r-1}N^r < p < (3ws^{d-1})^{r-1}N^r(3ws^{d-1}) = C^r$$

avec $C = (3ws^{d-1}N)$, d'où la majoration du cardinal du groupe. □

2.3.2 Les pavages hyperboliques trivalents de Zémor

Nous allons construire une surface à partir de son graphe de Cayley. Ces graphes ont été proposés par Zémor [100] qui a utilisé les groupes de Širáň pour construire des codes de surface. Nous présenterons une seconde famille de pavages hyperboliques, dû a Širáň, dans le chapitre 6. Dans cette partie, nous utiliserons les générateurs a et b du groupe triangulaire $T(l,m)$ qui satisfont les relations $a^2 = b^l = (ab)^m = 1$. Cette définition est compatible avec la définition du groupe triangulaire par l'équation (2.1) en considérant les générateurs $y = ab$ et $z = b^{-1}$. Soit $\tau(l,m)$ le graphe de Cayley du groupe $T(l,m)$ muni de la partie génératrice $S = \{a, b, b^{-1}\}$. Les faces sont définies par les suites de sommets voisins :

$$\{x, xb, xb^2, \ldots, xb^{l-1}, xb^l = x\} \tag{2.2}$$

et

$$\{x, xa, x(ab), \ldots, x(ab)^{m-1}a, x(ab)^m = x\} \tag{2.3}$$

pour tout sommet x de τ.
On note que le sommet x est aussi bordé par la face :

$$\{x, xb^{-1}, x(b^{-1}a), \ldots, x(b^{-1}a)^m = x\}.$$

On retrouve cette face comme une face du second type associée au sommet x en lisant les sommets dans le sens inverse. Nous avons ainsi défini une surface $\tau(l,m) = (G, V, F)$. La figure 2.8 représente ce graphe autour du sommet correspondant à l'élément 1 du groupe $T(l,m)$.

En partant du pavage carré du plan, on peut facilement identifier des arêtes pour obtenir un pavage carré fini qui peut être utilisé pour construire un code topologique. Le cas hyperbolique est plus délicat. La stratégie est de construire un groupe fini dans lequel les relations courtes entre générateurs sont les mêmes que dans le groupe triangulaire. Le graphe de Cayley aura alors la même structure locale tout en étant fini, ce qui permet de définir un code quantique. C'est ici qu'interviennent les groupes de Širáň présentés dans la partie précédente. Ce groupe nous permet de définir une surface finie $\bar{\tau}$ en définissant les faces de manière analogue aux faces du graphe de Cayley triangulaire.

Définition 2.33. *Le pavage de surface $\tau_r(l,m)$ est le graphe de Cayley de $T_r(l,m)$ muni de la partie génératrice $S = \{\bar{a}, \bar{b}, \bar{b}^{-1}\}$ dont les faces sont les images des faces de $\tau(l,m)$.*

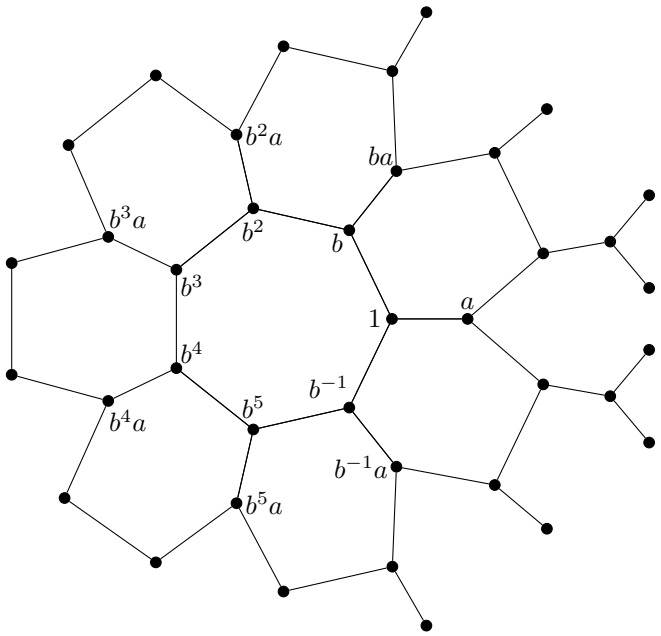


Figure 2.8 – Structure locale d'un pavage hyperbolique $\tau(3,7)$

Autrement dit, les faces du pavage hyperbolique fini τ_r sont définies par les équations (2.2) et (2.3) dans lesquelles on remplace les éléments du groupe T par ceux du groupe quotient T_r. Le morphisme de groupe surjectif de $T(l,m)$ vers $T_r(l,m)$ induit un morphisme de graphe surjectif π du graphe infini $\tau(l,m)$ vers le graphe fini $\tau_r(l,m)$.

Nous allons voir maintenant voir que ce graphe τ_r ressemble localement au pavage hyperbolique infini τ. Pour démontrer cet isomorphisme local, on fait appel au rayon d'injectivité. Cette propriété justifie la terminologie rayon d'injectivité de la définition 2.28.

Proposition 2.34. *Toute boule de rayon $\frac{r-1}{2}$ du graphe $\tau_r(l,m)$ est isomorphe à une boule de même rayon dans le graphe planaire $\tau(l,m)$.*

Démonstration. Supposons que deux sommets u et v de $\tau(l,m)$, situés dans une même boule de rayon $(r_1)/2$ du graphe, ont même image par π. La matrice uv^{-1} du groupe $T(l,m)$ se réduit sur l'identité de $T_r(l,m)$. Ces sommets u et v sont à distance au plus $r-1$ l'un de l'autre dans le graphe de Cayley $\tau(l,m)$ du groupe $T(l,m)$. On en déduit que la matrice uv^{-1} s'écrit comme un produit de moins de $r-1$ générateurs, contredisant la définition du rayon d'injectivité. □

Le lemme suivant énumère les arêtes et les faces du pavage en fonction du nombre de sommets.

Lemme 2.35. *Soit $\chi = |V| - |E| + |F|$, la caractéristique du graphe τ_r. On a :*
- $|E| = \frac{3}{2}|V|$,
- $|F| = \left(\frac{1}{l} + \frac{1}{m}\right)|V|$,
- $\chi = \left(\frac{1}{l} + \frac{1}{m} - \frac{1}{2}\right)|V|$,

Démonstration. Il s'agit d'une application directe du principe des bergers. Chaque sommet est bordé par 3 arêtes et chaque arête est composée de 2 sommets, donc $|V| = \frac{2}{3}|E|$. Autour de chaque sommet, on trouve une face de longueur l et deux faces de longueur $2m$. Ainsi le nombre de faces est :

$$|F| = (\frac{1}{l} + \frac{2}{2m})|V|.$$

□

2.4 Deux familles de codes topologiques battant la borne de Bravyi, Poulin et Terhal

2.4.1 La borne de Bravyi, Poulin et Terhal

Le code torique et ses généralisations sont extrêmement étudiés, notamment du point de vue du calcul quantique. Sa capacité de correction est importante mais il ne permet de protéger que deux qubits d'information. Tant du point de vue de la théorie de l'information que du calcul quantique, il serait judicieux de s'attacher à construire des généralisations de ce code qui sont de rendement constant. La structure forte des codes topologiques limite les paramètres atteignables. Bravyi et Terhal ont démontré que l'on ne peut pas dépasser une distance minimale en $O(L^{D-1})$ avec des codes stabilisateurs définis sur un pavage cubique en dimension D et dont les générateurs sont locaux [24]. Par une approche différente, Fetaya a prouvé que la distance en $O(\sqrt{n})$ du code torique ne peut pas être dépassée en utilisant des codes homologiques [43]. En ce qui concerne la dimension des codes topologiques, Bravyi, Poulin et Terhal ont remarqué que les paramètres des codes construits sur un pavage carré du plan par des générateurs locaux sont sujets à la borne suivante [23] :

Théorème 2.36. *Soit $S = \langle S_1, S_2, \ldots, S_r \rangle$ un groupe stabilisateur dont les générateurs S_i sont à support inclus dans une boule de rayon ρ du pavage $m \times m$ du tore. Alors les paramètres $[[n, k, d]]$ du code stabilisateur $C(S)$ vérifient $kd^2 = cn$, où c est une constante qui ne dépend que de ρ.*

Les auteurs ont démontré dans le cas d'un pavage à bord mais s'étend facilement au cas d'un pavage du tore. Cette borne interdit la construction de codes quantiques de rendement constant asymptotiquement à partir d'un tel pavage. En effet, la distance minimale d'un tel code serait constante en la longueur, ce qui est problématique pour le décodage.

Pour échapper à cette contrainte, on peut considérer d'autre géométries. C'est la stratégie adoptée par Freedman, Meyer et Luo [47], Kim [65] ou Zémor [100] pour construire des codes de surface de rendement constant et de distance croissante en utilisant la géométrie hyperbolique. Dans la suite de cette partie nous commençons par rappeler brièvement la construction de Zémor [100] Cet exemple apporte aussi la preuve que le choix, fait très fréquemment, de disposer les qubits sur un pavage carré

est une forte restriction sur les performances. L'utilisation de pavages hyperboliques mène ici à des paramètres battant la borne de Bravyi-Poulin-Terhal.

Nous généraliserons ensuite cette construction en définissant des codes couleur hyperboliques. Cette construction fournit une nouvelle famille de codes topologiques de rendement constant et de distance croissante. L'avantage majeur de cette nouvelle construction est qu'elle se transforme immédiatement en une famille de codes de sous-système, facilitant ainsi la mesure du syndrome. Ce passage des codes couleur aux codes de sous-systèmes, ainsi que leurs avantages, est présenté dans [14, 15].

2.4.2 Les codes de surface hyperboliques de Zémor

Soit τ_r la surface de rayon d'injectivité au moins r introduit par la définition 2.33. Les codes de surface associés aux différents pavages τ_r sont des codes quantiques de longueur $n = |E|$. On les appelle *codes de surfaces hyperbolique*. Sa dimension est $2 - \chi$, où χ est la caractéristique d'Euler de la surface, calculée dans le lemme 2.35. La dimension du code quantique suit. Le rendement obtenu est :

$$R = \frac{k}{n} \geq \frac{2}{3}\left(\frac{1}{2} - \frac{1}{l} - \frac{1}{m}\right).$$

Nous choisissons l et m tels que $\frac{1}{2} + \frac{1}{l} + \frac{1}{m} < 1$. De sorte que le rendement soit asymptotiquement constant. Cette inégalité correspond au cas d'un groupe triangulaire hyperbolique.

Rappelons maintenant que la distance minimale croît au moins linéairement en le rayon d'injectivité r. En effet, d est la longueur d'un plus court cycle du graphe τ_r, ou de son graphe dual τ_r^*, qui n'est pas somme de faces. Tout cycle γ de τ_r, de longueur inférieure à $2r - 1$, est inclus dans une boule de rayon r du graphe τ_r. Par définition de τ_r, une telle boule est isomorphe à la boule de même rayon dans le graphe planaire $\tau(l, m)$. On peut donc regarder le cycle γ comme un cycle de son revêtement planaire. Or un cycle d'un graphe planaire est toujours somme de faces. Le cycle γ n'apparaît donc pas dans le calcul de la distance minimale. On peut répéter cet argument en partant d'un cycle du graphe dual, en utilisant le dual du revêtement. Comme le rayon d'injectivité du graphe dual est au moins $r/\max(l, 2m)$, la distance est au moins proportionnelle à r. Cette croissance est logarithmique en la longueur d'après le théorème 2.29.

La proposition suivante résume les propriétés des codes de surface hyperboliques.

Proposition 2.37. *Le code de surface associé au pavage τ_r est un code quantique de longueur $n = |E|$ qui encode $k = \frac{2}{3}\left(\frac{1}{2} - \frac{1}{l} - \frac{1}{m}\right) n + 2$ qubits et de distance minimale $d \geq r/\max(l, 2m) = O(\log(n))$.*

Pour conclure, remarquons que cette famille de codes de surface surpasse la borne de Bravyi $kd^2 = O(n)$ puisque l'on a $k = O(n)$ et $d = O(\log n)$. Cette borne a été prouvée pour des pavages carrés en dimension 2. Nous la dépassons avec l'aide de la géométrie hyperbolique en dimension 2.

2.4.3 Une famille de codes couleur hyperboliques

Nous nous intéressons maintenant à l'utilisation de ces pavages hyperboliques pour construire des codes couleur. Dans le cas où les faces du pavage hyperbolique ne sont pas 3-coloriables, nous allons construire un revêtement de ce graphe, qui possède les même propriétés locales et dont les faces peuvent être 3-coloriées.

Pour commencer nous allons caractériser les graphes τ_r qui possèdent des faces 3-coloriables. Pour cela, nous introduisons le sous-graphe H_r du graphe dual τ_r^*. C'est le graphe dont les sommets sont les faces de longueur $2m$ de τ_r de la forme :

$$\{x, xa, x(ab), \ldots, x(ab)^{m-1}a, x(ab)^m = x\}$$

et

$$\{x, xb^{-1}, x(b^{-1}a), \ldots, x(b^{-1}a)^m = x\}.$$

Deux sommets de H_r sont voisins si les faces correspondantes de τ_r partagent une arête. Ce graphe H_r est régulier de degré 3. Il permet la caractérisation suivante :

Lemme 2.38. *Les faces du graphe τ_r sont 3-coloriables si et seulement si le graphe H_r est biparti.*

Rappelons qu'un graphe est *biparti* si ses sommets se décomposent en deux sous-ensembles tels que aucune arête n'est incluse dans l'un de ces sous-ensembles.

Démonstration. Supposons que le graphe H_r est biparti. Alors ses sommets sont coloriables de deux couleurs différentes. On en déduit une coloration des faces correspondantes dans le graphe τ_r. Supposons que l'on a utilisé les couleurs rouge et verte. Il ne reste plus qu'à colorier les faces de longueur l définies par les puissances du générateur b. Nous savons qu'il n'y a qu'une seule face de cette forme autour de chaque sommet. Ainsi deux telles faces ne sont jamais voisines. Pour obtenir une 3-coloration des faces, il ne reste donc plus qu'à colorier les faces restantes en bleu.

Pour la réciproque, on considère un graphe τ_r dont les faces sont 3-coloriées. Le choix des couleurs de 3 faces autour d'un sommet fixe la coloration du graphe entier puisque le graphe est connexe et de degré 3. La structure locale du graphe implique que les faces engendrées par b portent toutes la même couleur. Les faces restantes sont bordées par une telle face et contiennent donc l'une des deux couleurs restantes. De la 3-coloration des faces de τ_r, on déduit ainsi une 2-coloration des sommets du graphe H_r. C'est un graphe biparti. □

Lorsque les faces du graphe τ_r ne sont pas 3-coloriables, il ne peut pas être utilisé pour définir un code couleur. Dans ce cas nous travaillerons sur le revêtement suivant du graphe τ_r.

Définition 2.39. *Soit $\tau_r = (V, E, F)$ un graphe hyperbolique. Le* graphe *$\tilde{\tau}_r$ est le graphe dont les sommets sont les éléments de $V \times \mathbb{F}_2$ et les arêtes sont de la forme $\{(x, i), (y, j)\}$ avec $\{x, y\}$ une arête de τ_r et $j = i + 1$. Chaque face $\{x_1, x_2, \ldots, x_{2s}\}$ du graphe τ_r définit deux faces du 2-revêtement $\tilde{\tau}_r$ de la forme :*

$$\{(x_1, , i_0), (x_2, i_0 + 1), \ldots, (x_{2s}, i_0 + 1)\},$$

avec $i_0 = 0$ ou 1.

Ce 2-revêtement présente l'avantage d'avoir des faces 3-coloriables lorsque les faces de τ_r ne le sont pas :

Proposition 2.40. *Si les faces du graphe $\tau_r = (V, E, F)$ ne sont pas 3-coloriables, alors le graphe $\tilde{\tau}_r = (\tilde{V}, \tilde{E}, \tilde{F})$ est un graphe dont les faces sont 3-coloriables tel que :*
- *toute boule de rayon r de $\tilde{\tau}_r$ est isomorphe aux boules de rayons r du graphe τ_r,*
- *$|\tilde{V}| = 2|V|, |\tilde{E}| = 2|E|$ et $|\tilde{F}| = 2|F|$.*

Démonstration. Étant donné un sommet $(x, k) \in \tilde{V}$, on considère l'application suivante :

$$\begin{aligned} \pi : \tilde{V} &\longrightarrow V \\ (u, i) &\longmapsto u \end{aligned}$$

Nous allons voir que la restriction de π à une boule de rayon r autour de x est un isomorphisme de graphe. Supposons que deux sommets différents de cette boule (u, i) et (v, j) sont envoyés sur la même image $u = v$. Nous avons alors $i \neq j$.

Il existe un chemin de (x, k) vers (u, i) dans la boule du revêtement. Il existe aussi un tel chemin entre (x, k) et (v, j). La concaténation de ces deux chemins est un chemin allant de (u, i) à (v, j) en passant par (x, k), dans le graphe $\tilde{\tau}_r$. La longueur de ce chemin est impaire car la parité de cette longueur est aussi la parité de $i + j$. L'image de ce chemin par π est un cycle inclus dans la boule $B(x, r)$ du graphe τ_r. Nous pouvons supposer que sa longueur est inchangée. En effet, si π induit une identification de deux sommets de sur ces chemins avant d'atteindre (u, i) et (v, j), on peut remplacer (x, i) et (y, j) par des sommets plus proches de (x, k). Nous obtenons finalement un cycle de longueur impaire, inclus dans la boule de rayon r du graphe τ_r. Par construction de τ_r, un tel cycle est une somme de faces de τ_r. Mais les faces contiennent toutes un nombre pair d'arêtes. Ce cycle devrait donc être de longueur paire. Cette contradiction démontre l'injectivité de π restreint à une boule de rayon r. Cette propriété ne dépend pas du sommet (x, k).

Nous avons démontré que le revêtement possède la même structure locale que le graphe τ_r. Il hérite donc du même rayon d'injectivité. De plus, nous allons voir qu'il est 3-coloriable. On ne peut pas appliquer immédiatement le lemme 2.38 puisqu'il est énoncé pour le graphe τ_r mais nous allons utiliser un argument similaire. On peut colorier en rouge les faces isolées correspondant au générateur b. Ensuite, il ne reste plus qu'à prouver que le graphe $\tilde{H}_r$ est biparti. Pour cela, nous allons transférer la structure biparti de $\tilde{\tau}_r$ au graphe $\tilde{H}_r$. Le graphe $\tilde{H}_r$ est construit de manière similaire au graphe H_r. Ses sommets sont les faces du graphe $\tilde{\tau}_r$ qui ne sont pas définies par les puissances de b. Une telle face s'écrit :

$$F(x, i) = \{(x, i), (xa, i + 1), (x(ab), i + 2), \ldots, (x(ab)^{m-1}a, 2m - 1)\}.$$

Nous allons utiliser l'indice $i \in \mathbb{F}_2$ pour partitionner les sommets de H_r en deux sous-ensembles. On note $V_i(H)$ l'ensemble des faces $F(x, i)$, avec $i \in \mathbb{F}_2$. Ces deux ensembles définissent un graphe biparti car deux faces de $F(x, i)$ et $F(x, j)$ ne sont jamais voisines. Pour voir ceci, il suffit de vérifier que si une arête sépare deux faces

de $V(\tilde{H}_r)$, c'est une arête de type $\{(x,0),(xa,1)\}$. Or une telle arête est bordée par les faces $F(x,0)$ et $F(xa,1)$. □

Nous sommes désormais en mesure de construire une famille de codes couleur de rendement constant et de distance croissante.

Théorème 2.41. *Soit m la longueur maximale d'une face du graphe τ_r.*

- *Si les faces du pavage $\tau_r = (V,E,F)$ sont 3-coloriables, alors il définit un code couleur de paramètres :*

$$n = |V|, \quad k = 2\left(\frac{1}{2} - \frac{1}{l} - \frac{1}{m}\right)|V| + 4, \quad d \geq \frac{8r}{m} = O(\log n).$$

- *Si les faces du pavage $\tau_r = (V,E,F)$ ne sont pas 3-coloriables, alors son revêtement $\tilde{\tau}_r = (\tilde{V},\tilde{E},\tilde{F})$ définit un code couleur de paramètres :*

$$n = 2|V|, \quad k = 2\left(\frac{1}{2} - \frac{1}{l} - \frac{1}{m}\right)(2|V|) + 4, \quad d \geq \frac{8r}{m} = O(\log n).$$

Les rendements de ces codes sont asymptotiquement constants. Ces rendements sont tous les deux équivalents à $2\left(\frac{1}{2} - \frac{1}{l} - \frac{1}{m}\right)$.

Démonstration. Nous traitons uniquement le cas du pavage $\tilde{\tau}_r$. Les paramètres du code couleur associé à τ_r s'obtiennent de manière similaire. Contrairement au cas des codes de surface, la longueur est égale au nombre de sommet. D'après le théorème 2.27, il suffit de déterminer la caractéristique d'Euler de la surface pour calculer la dimension du code quantique. D'après le lemme 2.35 et la proposition 2.40, la caractéristique d'Euler du revêtement $\tilde{\tau}_r$ est le double de celle de τ_r. On en déduit la dimension du code quantique :

$$k = 2\left(\frac{1}{2} - \frac{1}{l} - \frac{1}{m}\right)(2|V|) + 4.$$

Pour la distance minimale, nous utilisons le fait que chaque boule de rayon r du graphe $\tilde{\tau}_r$ est planaire. Soit C le code $\operatorname{Ker}\mathbf{H}_X$ et soit $x \in C$, un vecteur de poids $w(x) \leq r/\max(l,2m)$. On note $\tilde{G}_{\mathbf{c}}$ le pavage rétréci de couleur $\mathbf{c}$ associé au graphe $\tilde{\tau}_r$, pour $\mathbf{c}$ la couleur rouge ou verte. D'après le proposition 2.22, le vecteur x s'écrit $X(\gamma_R) + X(\gamma_V)$ avec $\gamma_{\mathbf{c}}$ un cycle du graphe rétréci $\tilde{G}_{\mathbf{c}}$. Quitte à travailler sur les composantes connexes, on peut supposer que ces cycles sont connexes. On supposera aussi que l'écriture de x sous la forme $X(\gamma_R) + X(\gamma_V)$ est minimale. On en déduit, en particulier que ces cycles contiennent au plus le moitié des arêtes d'une face bleu. La longueur de ces deux cycles $\gamma_{\mathbf{c}}$ est donc au plus $\ell(\gamma_{\mathbf{c}}) \leq \frac{w(x)}{2}\frac{m}{2}$ car à chaque paire de sommets de x on associe au plus $m/2$ arêtes, où m est la longueur maximale d'une face du graphe. Si cette longueur est strictement inférieure à $2r$ alors le cycle $\gamma_{\mathbf{c}}$ est inclus dans une boule de rayon r du graphe τ_r. Cette boule est planaire par construction de τ_r, ce qui fait du cycle $\gamma_{\mathbf{c}}$ une somme de faces.

Nous avons montré que si $w(x) \leq \frac{8r}{m}$, alors $x \in C^{\perp}$ et donc x n'apparaît pas dans le calcul de la distance minimale. La distance est donc au moins de l'ordre de r. □

2.5 Application de la borne de Gromov

Nous avons rappelé la construction d'une famille de codes de surface battant la borne de Bravyi, Poulin et Terhal. Cette borne a été établie en supposant que le code stabilisateur est défini sur un pavage carré et peut être dépassée, par exemple, en se plaçant dans un graphe hyperbolique. Avec des outils similaires, nous avons obtenu une famille de codes couleur battant elle aussi cette borne sur les paramètres des codes topologiques. Ces deux familles de codes possèdent un rendement constant et une distance minimale croissante, logarithmique en la longueur. Il est désormais naturel de chercher à savoir si ces paramètres sont optimaux et quel est le compromis entre distance minimale et dimension que l'on peut atteindre avec des codes définis sur un pavage quelconque. Nous obtenons dans cette partie une borne analogue à la borne de Bravyi, Poulin et Terhal qui s'applique à un code de surface ou à un code couleur défini sur un graphe fini quelconque.

Pour cela, nous utilisons la notion de systole et les bornes de Gromov. Commençons par rappeler le résultat de Gromov qui nous intéresse. Nous nous plaçons dans le premier groupe d'homologie singulière d'une 2-variété [58, 59]. La *systole* est par définition la longueur du plus court cycle non homologue à zéro [13]. Les liens entre systole et codes de surface ont été étudiés notamment par Freedman, Meyer et Luo [47]. Plus récemment, Fetaya a démontré que l'on ne peut pas construire de codes homologiques dont la distance croît plus rapidement qu'une racine carrée de la longueur. Il a obtenu ce résultat en partant de bornes supérieures sur la systole d'une variété de dimension n en fonction de son volume [43]. Nous allons utiliser le résultat plus précis suivant, dû à Gromov, qui borne la systole d'une surface en fonction du genre et du volume de la surface [54] :

Théorème 2.42. *La systole* $\operatorname{syst} H_1(\mathcal{V}, \mathbb{F}_2)$ *d'une 2-variété* $\mathcal{V}$ *fermée, connexe, de genre* $g \geq 2$*, équipée d'une métrique riemannienne vérifie :*

$$(\operatorname{syst} H_1(\mathcal{V}, \mathbb{F}_2))^2 \leq C \frac{(\log g)^2}{g} \operatorname{Aire}(\mathcal{V}). \tag{2.4}$$

où C *est une constante qui ne dépend ni de la métrique, ni de la surface* $\mathcal{V}$*.*

Notre objectif est de transférer cette inégalité dans le domaine des codes topologiques. Nous souhaitons démontrer que le volume de la surface correspond au nombre de faces et donc à la longueur n du code, le genre est proportionnel à la dimension k et la systole correspond à la distance du code quantique. On obtient alors une inégalité de la forme :

$$kd^2 \leq C'(\log k)^2 n.$$

Attachons-nous à rendre cette inégalité rigoureuse.

La notion discrète de systole qui apparaît dans l'étude des codes topologiques est la suivante.

Définition 2.43. *La* systole combinatoire $\operatorname{csyst} H_1(G, \mathbb{F}_2)$ *d'un pavage de surface* $G = (V, E, F)$ *est la longueur du plus court cycle du graphe* G *qui n'est pas somme de faces.*

Afin de nous ramener aux bornes de Gromov (2.4), nous allons regarder un pavage combinatoire de surface introduit dans la définition 2.3 comme une 2-variété riemannienne. Par définition, un tel pavage combinatoire définit une 2-variété topologique. On peut le munir d'une structure de 2-variété lisse. Nous équipons ensuite cette 2-variété d'une métrique riemannienne telle que la systole combinatoire est du même ordre de grandeur que la systole de la 2-variété. Pour cela, nous faisons appel à un lemme dû à Fetaya [43] :

Lemme 2.44. *Il existe deux constantes C_1 et C_2 telles que, pour tout pavage combinatoire de surface $T = (V, E, F)$ dont les faces sont triangulaires, il existe une métrique riemannienne sur la 2-variété T telle que :*

- *le volume de toute face f de T vérifie* $\mathrm{Aire}(f) \leq C_1$,
- $\mathrm{csyst}\, H_1(T, \mathbb{F}_2) \leq C_2\, \mathrm{syst}\, H_1(T, \mathbb{F}_2)$.

Fetaya a démontré ce lemme en considérant des triangulations. Pour passer d'un pavage de surface combinatoire quelconque à une triangulation, il suffit de découper chaque face de longueur m en m triangles. Le lemme précédent permet d'appliquer les inégalités de Gromov à tout code de surface et à tout code couleur.

Théorème 2.45. *Soit G un pavage de surface dont les faces sont de longueur inférieure à m et dont les sommets sont de degré inférieur à m. Les paramètres $[[n, k, d]]$ du code de surface et du code couleur (s'il existe) associés au graphe G vérifient :*

$$kd^2 \leq C(\log k)^2 n,$$

pour une constante C qui ne dépend que de m.

Démonstration. Soit $G = (V, E, F)$ un pavage de surface. La triangulation induite par G est le pavage de surface obtenu en ajoutant un sommet au centre de chaque face et en le reliant par une arête à chacun des sommets qui bordent cette face. Cette triangulation que l'on peut construire à partir de n'importe quel pavage de surface nous permet d'appliquer le lemme de Fetaya.

Soit γ un cycle de la triangulation T déduite du pavage de surface G. Nous pouvons transformer ce cycle en un cycle du graphe G. Pour cela, il suffit de remplacer tout chemin inclus dans γ, passant par le centre d'une face de G, par un chemin longeant le bord de cette face. Par cette transformation, on remplace certaines paires d'arêtes par des chemins de longueur au plus $m/2$. De plus, cette transformation conserve la classe d'homologie. On en déduit une majoration de la systole du pavage G :

$$\mathrm{csyst}\, H_1(G, \mathbb{F}_2) \leq \frac{m}{4}\, \mathrm{csyst}\, H_1(T, \mathbb{F}_2).$$

On peut maintenant appliquer le lemme 2.44 puis le théorème 2.42 à la 2-variété $\mathcal{V}$

définie par le pavage T :

$$(\operatorname{csyst} H_1(G,\mathbb{F}_2))^2 \leq (\frac{m}{4} C_2 \operatorname{syst} H_1(\mathcal{V},\mathbb{F}_2))^2$$
$$\leq C' m^2 \frac{(\log g)^2}{g} \operatorname{Aire}(\mathcal{V}).$$

pour une constante C.

Le genre de la surface est $2k$ si elle est orientable et k dans le cas contraire. D'après le lemme 2.44, l'aire de la surface, qui est la somme des aires des triangles, est majorée par $\operatorname{Aire}(\mathcal{V}) \leq C_1|F(T)|$ où $|F(T)|$ est le nombre de triangles de cette triangulation. Ce nombre est exactement le double du nombre d'arêtes $|E| = n$ du graphe G. En effet, chaque arête est la base de exactement deux triangles de T inclus dans les deux faces de G contenant cette arête. On arrive ainsi à l'inégalité :

$$(\operatorname{csyst} H_1(G,\mathbb{F}_2))^2 \leq C m^2 \frac{(\log k)^2}{k} n.$$

Ce résultat est aussi valable pour la systole du graphe dual G^* car on a supposé que les degrés des sommets de G sont bornés par m. On peut donc remplacer le membre de gauche par la distance minimale d du code de surface associé à G qui est la plus petite des systoles combinatoires de G et G^*.

Le cas des codes couleur est similaire. Dans ce cas la distance minimale d est majorée par la systole des graphes rétrécis G_R, G_V et G_B car chaque cycle de ces graphes non homologue à zéro définit une erreur problématique dont le poids est le double de la longueur du cycle. On doit donc majorer la systole de ces pavages rétrécis. Lorsque l'on part d'un pavage dont les faces sont de longueur inférieure à m, on obtient des graphes rétrécis dont la longueur des faces est au plus $m/2$. On peut alors procéder comme dans le cas des codes de surface. □

Cette nouvelle borne étend la borne de Bravyi, Poulin et Terhal. En l'appliquant aux codes de surface hyperboliques et aux codes couleur hyperboliques, on voit que la distance minimale de ces codes ne peut pas dépasser $O(\log(n))$ car ils ont un rendement constant. Jusqu'à présent seule la borne inférieure du même ordre était connue. Plus généralement, on ne peut pas espérer construire des codes quantiques de rendement constant dont la distance minimale croit en n^α, avec $\alpha > 0$, en utilisant des codes de surface ou des codes couleur.

Conclusion

– Au cours de ce chapitre nous avons utilisé les pavages hyperboliques introduits par Zémor pour construire une nouvelle famille de codes topologiques de rendement constant et de distance logarithmique en la longueur. Ces codes couleur hyperboliques sont clairement différents des codes topologiques de rendement constant et de distance croissante construits jusqu'à présent. À notre

connaissance, il s'agit de la première famille de codes couleur de rendement constant et de distance croissante.

- Les codes couleur hyperboliques présentent l'avantage d'être transformables en codes couleur hyperboliques de sous-système [14, 15, 77]. On obtient ainsi une famille de codes de sous-système topologiques de rendement constant et de distance logarithmique en la longueur. Ces codes quantiques permettent une mesure plus précise du syndrome. Contrairement au cas des codes correcteurs classiques, la mesure du syndrome quantique est délicate et c'est une importante source d'erreur. Avec ces codes de sous-système, les mesures sont décomposées en mesures sur 2 qubits, diminuant ainsi la probabilité d'erreur de mesure. Le code torique peut être transformé en code de sous-système [20] mais il n'existe pas, à notre connaissance, de telle procédure s'adaptant aux codes de surface hyperboliques.
- Il a été observé récemment que beaucoup de systèmes quantiques font apparaître une asymétrie entre les erreurs de phase Z et les erreurs de qubit X [62]. Les codes de surface hyperboliques semblent plus adaptés à un modèle d'erreur asymétrique que leur version code couleur. À partir de pavages non auto-duaux, comme dans le cas des codes hyperboliques de Zémor, on peut supposer que les performances du décodage sont meilleures pour l'une des composantes de l'erreur. Une telle asymétrie paraît difficile à prendre en compte avec des codes couleur.
- Nous avons construit des familles des codes de surface et de codes couleur de rendement constant dont la distance est logarithmique en la longueur. Nous avons ensuite démontré, en faisant appel aux bornes systoliques de Gromov, que cet ordre de grandeur $O(\log n)$ est optimal pour la distance d'une famille de codes de surface ou de codes couleur de rendement constant. Il reste à déterminer quelle est la meilleure constante atteignable.
- La construction de codes LDPC quantiques de Zémor et Tillich [92] qui ne partage que certaines caractéristiques des codes topologiques dépasse la borne du théorème 2.45. Ces codes possèdent un rendement constant et une distance en $O(\sqrt{n})$. Freedman, Meyer et Luo ont proposé une famille de codes homologiques de dimension $k = 1$ dont la distance croît en $O(n^{1/2} \log n)^{1/2})$ [47]. Ces paramètres sont au delà de notre borne. Cette dernière famille de codes LDPC quantiques est la seule qui dépasse une distance minimale en $O(\sqrt{n})$, à notre connaissance.

Chapitre 3

Codes LDPC quantiques basés sur des graphes de Cayley

Nous étudions ici une construction de codes LDPC quantiques proposée par Mackay, Mitchison et Shokrollahi dans l'article non publié [70]. Cette famille de codes quantiques est définie à partir du graphe de Cayley de $\mathbb{F}_2^n$ engendré par les colonnes d'une matrice de parité d'un code classique C. Les auteurs expliquent leur méthode pour obtenir ainsi des codes auto-orthogonaux, ils estiment ensuite numériquement les paramètres de certains de ces codes quantiques. Finalement Shokrollahi propose une conjecture sur la dimension du code quantique issue du code de répétition.

Dans ce chapitre, nous nous intéressons à la distance minimale de ces codes quantiques. Nous donnons une borne inférieure sur la distance minimale de tout code quantique construit par ce procédé en $\mathcal{O}(dn^2)$ où d est la distance minimale du code classique utilisé et n est sa longueur.

Lorsque le code classique est le code de répétition, nous démontrons la formule proposée par Shokrollahi pour la dimension du code quantique. De plus, la méthode utilisée lors de cette preuve nous guide vers une formule exacte pour la distance minimale du code quantique. Le code quantique obtenu a pour paramètres $[[2^{n-1}, 2^{\frac{n}{2}}, 2^{\frac{n}{2}-1}]]$ lorsque le code classique C est le code de répétition de paramètres $[n, 1, n]$. Les matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$ définissant le code quantique sont des matrices creuses dont les lignes sont de poids n ce qui confère un caractère LDPC au code quantique. L'exemple dérivé du code de répétition est présenté dans la seconde section de ce chapitre. Ces résultats sont le fruit d'une collaboration avec Alain Couvreur et Gilles Zémor [32, 33].

3.1 La construction de MacKay, Mitchison et Shokrollahi

3.1.1 Des graphes de Cayley aux codes quantiques

Nous avons rappelé, au cours du chapitre d'introduction, que l'on peut définir un code quantique à partir de deux matrices binaires $\mathbf{H}_X$ et $\mathbf{H}_Z$ telles que les lignes de $\mathbf{H}_X$ sont orthogonales aux lignes de $\mathbf{H}_Z$. Nous allons utiliser des codes auto-

orthogonaux.

Nous utilisons la définition 1.21 des codes auto-orthogonaux et des codes auto-duaux. Une matrice génératrice $\mathbf{H}$ d'un code auto-orthogonal de longueur N permet donc de définir un code CSS de matrice $\mathbf{H}_X = \mathbf{H}_Z = \mathbf{H}$. Ses paramètres sont $[[N, K, D]]$ avec $K = N - 2\,\mathrm{rg}(\mathbf{H})$, et D, la distance minimale, est :

$$D = \inf\{w(x) \mid x \in \operatorname{Ker}\mathbf{H} \backslash \operatorname{Ker}\mathbf{H}^{\perp}\}.$$

Étant donnée la présence d'un code classique et d'un code quantique dans cette partie, nous utiliserons des majuscules pour décrire les paramètres du code quantique. Dans ce qui suit, r et n sont des entiers et n est pair. Le i-ème vecteur de la base canonique de $\mathbb{F}_2^r$ est noté e_i. On considère H une matrice $r \times n$ de rang plein et peut être vue comme la matrice de parité d'un code classique C de longueur n et de dimension $k = n - r$. On note S l'ensemble des vecteurs colonnes de la matrice H. Le graphe de Cayley de $\mathbb{F}_2^r$ engendré par les éléments de S est noté $G(H)$. Par définition du graphe de Cayley, les sommets de ce graphe sont les éléments de $\mathbb{F}_2^r$ et ses arêtes sont les couples de sommets $\{x, x+s\}$ pour tout x de $\mathbb{F}_2^r$ et pour tout s de S. Ce graphe ne dépend que du code $C = \operatorname{Ker} H$. On parle du graphe des classes de C. Ces graphes, ainsi que leurs revêtements, ont été étudiés par Friedman et Tillich [48].

Soit $A(H)$ la matrice d'adjacence du graphe $G(H)$. Cette matrice sera noté A dans le cas où aucune confusion n'est possible.

Proposition 3.1. *Soit n un entier pair et $H \in \mathcal{M}_{r,n}(\mathbb{F}_2)$ une matrice de rang r. La matrice $A(H)$ définit un code CSS Q_H de longueur $N = 2^r$ de matrices $\mathbf{H}_X = \mathbf{H}_Z = A(H)$. Les lignes de la matrice $A(H)$ sont de poids n.*

Démonstration. Il suffit de démontrer que A satisfait les relations d'orthogonalités. Puisque n est pair, les lignes de A sont de poids pair et sont donc orthogonales à elles-mêmes. Soient x et y deux vecteurs distincts de $\mathbb{F}_2^r$. On note A_x la ligne de A indexée par x et $A_{x,y}$ est l'entrée indexée par (x, y).

L'égalité $\langle A_x, A_{x'}\rangle = 0$ signifie que l'ensemble suivant est de cardinal pair :

$$\{y \in \mathbb{F}_2^r \mid A_{x,y} = A_{x',y} = 1\} = (x + S) \cap (x' + S)$$

Le sous-groupe $\{0, x + x'\}$ agit par translation sur l'ensemble $(x + S) \cap (x' + S)$ et son action est libre. Ainsi, $(x + S) \cap (x' + S)$ est une réunion disjointe de classes de cardinal 2. La parité du cardinal de l'ensemble $(x + S) \cap (x' + S)$ en découle, ce qui termine la preuve. □

Cette proposition est apparue dans [70]. Dans cette construction, le code $C = \operatorname{Ker} A$, est l'espace des vecteurs $\mathbf{c} \in \mathbb{F}_2^{2^r}$ tels que $A\mathbf{c}^t = 0$. Un mot du code $\mathbf{c} \in \operatorname{Ker} A$ est aussi le vecteur caractéristique d'un ensemble de sommets du graphe $G(H)$. Dans la suite, il sera utile de regarder un tel vecteur $\mathbf{c}$ comme un ensemble de sommets, ou un sous-graphe de $G(H)$.

La présence des indices, qui sont des éléments de $\mathbb{F}_2^r$ et des mots de l'espace $\mathbb{F}_2^{2^r}$, est un risque de confusion. Nous veillerons donc à noter en gras les vecteurs $\mathbf{c}$ de $\mathbb{F}_2^{2^r}$ alors que les vecteurs de l'espace des indices seront notés x ou y.

3.1.2 Le revêtement par le cube de Hamming

Pour commencer, nous étudions le cas où la matrice H est l'identité I_n. Le code quantique Q_H est alors trivial, mais le code classique $C = \operatorname{Ker} A(I_n) \subset \mathbb{F}_2^{2^r}$ ne l'est pas et sera utile ensuite. Nous allons voir qu'il y a un morphisme du graphe de Cayley $G(I_n)$ vers le graphe $G(H)$, pour toute matrice H de taille $r \times n$. On en déduira un morphisme de $\operatorname{Ker} A(I_n)$ vers $\operatorname{Ker} A(H)$.

Proposition 3.2. *Si n est un entier pair, alors la matrice $A(I_n)$ est de rang 2^{n-1}.*

Démonstration. Puisque l'espace des lignes de A est un code auto-orthogonal, son rang est au plus 2^{n-1}. Pour prouver l'inégalité dans l'autre sens, nous ordonnons les éléments de l'espace des indices $\mathbb{F}_2^n$ dans l'ordre lexicographique. La matrice $A(I_n)$ s'écrit alors par blocs :

$$A_n = \begin{pmatrix} A_{n-1} & I_{2^{n-1}} \\ I_{2^{n-1}} & A_{n-1} \end{pmatrix}.$$

En effet, la première moitié des éléments de $\mathbb{F}_2^n$ est l'ensemble des éléments de la forme $(x|0)$ où $x \in \mathbb{F}_2^{n-1}$ et le symbole $|$ désigne la concaténation. La seconde moitié des indices est composée des éléments $(x|1)$ avec $x \in \mathbb{F}_2^{n-1}$. Deux sommets du graphe $(x|0)$ et $(x'|1)$ sont alors voisins dans $G(I_n)$ si et seulement si $x = x'$. Ceci explique le bloc identité en haut à droite de la matrice $A(I_n)$. Un tel mineur dans la matrice A_n implique un rang supérieur à 2^{n-1}. □

Cet exemple est utile car il nous fournit un revêtement de tout graphe de Cayley de la forme $G(H)$ pour une matrice H quelconque. La proposition suivante montre que les graphes $G(I_n)$ et $G(H)$ sont les mêmes dans une boule suffisamment petite.

Proposition 3.3. *Si le code classique C de matrice de parité H a pour distance minimale d, alors nous avons un isomorphisme de graphe entre les boules de rayon $\lfloor d/2 \rfloor - 1$ de $G(H)$ et de $G(I_n)$:*

$$\pi : \mathbb{B}_{I_n}(y, \lceil d/2 \rceil - 1) \xrightarrow{\sim} \mathbb{B}_H(x, \lceil d/2 \rceil - 1)$$

pour tout x de $\mathbb{F}_2^r$ et pour tout y de $\mathbb{F}_2^n$.

Démonstration. Par transitivité des graphes de Cayley, il suffit de démontrer que les boules centrées en 0 sont isomorphes. Considérons l'application naturelle de l'ensemble des sommets de $G(I_n)$ dans ceux de $G(H)$:

$$\begin{array}{rccc} \pi : & \mathbb{F}_2^n & \longrightarrow & \mathbb{F}_2^r \\ & x & \longmapsto & Hx^t \end{array}$$

Il s'agit de l'application syndrome associée au code classique C. Désormais, regardons la restriction de cette application à la boule de rayon $\lfloor d/2 \rfloor - 1$ centrée en 0. C'est un isomorphisme de graphe et c'est une application bijective par définition de la distance minimale. Ainsi, π induit un isomorphisme entre les boules. □

On dit que $\mathbf{c}$ est inclus dans une boule si l'ensemble de sommets du graphe qu'il indique l'est. On note $\mathbb{S}(x)$ la sphère de centre x et de rayon 1 dans le graphe de Cayley. Ces sous-graphes $\mathbb{S}(x)$ jouent un rôle important puisqu'ils correspondent aux lignes de la matrice A. En particulier, dire qu'un vecteur de $\mathbb{F}_2^n$ est une somme de sphères revient à dire qu'il appartient à l'espace engendré par les lignes de la matrice A. On s'autorisera à dire qu'un mot $\mathbf{c}$ de $\mathbb{F}_2^{2r}$ est orthogonal à un ensemble de sommets lorsqu'il contient un nombre pair de ses sommets.

Le lemme suivant est la traduction graphique des équations définissant le code de matrice de parité $A(H)$.

Lemme 3.4. *Un vecteur $\mathbf{c} \in \mathbb{F}_2^{2r}$ est un mot du code $\operatorname{Ker} A(H)$ si et seulement s'il est orthogonal aux sphères $\mathbb{S}(x)$ pour tout $x \in \mathbb{F}_2^r$.*

Lemme 3.5. *Soit $\mathbf{c}$ un mot du code $\operatorname{Ker} A(I_n)$ qui est inclus dans une boule $\mathbb{B}(0,t)$ de rayon $0 < t < n$. Si $\partial\mathbf{c} := \mathbf{c} \cap \mathbb{S}(0,t)$ est non vide, alors pour tout $i \in \{1,\dots,n\}$, il existe $x \in \partial\mathbf{c}$ tel que $x_i \neq 0$.*

Démonstration. Supposons que $\partial\mathbf{c}$ est non vide et qu'il existe un indice i tel que $x_i = 0$ pour tout x de $\partial\mathbf{c}$. Soit x un élément de $\partial\mathbf{c}$. On considère la sphère de centre e_i. On a :

$$\mathbb{S}(x + e_i) \cap \mathbf{c} = \{x + e_i + e_j, 1 \leq j \leq n\} \cap \partial\mathbf{c} = \{x\}.$$

La dernière égalité provenant de l'hypothèse $x_i = 0$ pour tout x de $\partial\mathbf{c}$. C'est impossible car $\mathbf{c}$ doit satisfaire le lemme 3.4. □

Proposition 3.6. *Soit $\mathbf{c}$ un mot du code $\operatorname{Ker} A(I_n)$ qui est inclus dans une boule de rayon $\lfloor d/2 \rfloor - 1$. Alors $\mathbf{c}$ est une somme de sphères de rayon 1 qui sont incluses dans cette boule.*

Démonstration. Par transitivité sur les sommets, on peut supposer que le mot $\mathbf{c}$ est inclus dans la boule centrée en 0. Démontrons la proposition par récurrence sur le rayon t de cette boule.

Si $t = 0$, c'est le lemme 3.4, $\mathbf{c}$ est le mot de code nul et donc c'est la somme vide de sphères.

Supposons la propriété vraie pour $t - 1 \geq 0$. Si l'ensemble $\partial\mathbf{c} := \mathbf{c} \cap \mathbb{S}(0,t)$ est vide, alors $\mathbf{c} \subset \mathbb{B}(0,t-1)$ et le résultat est vrai d'après l'hypothèse de récurrence. On suppose maintenant que $\partial\mathbf{c} \neq \emptyset$. Posons :

$$T = \mathbb{S}(0,t) \cap \{x \in \mathbb{F}_2^r \mid x_r = 1\}.$$

D'après le lemme 3.5, nous avons $T \cap \partial\mathbf{c} \neq \emptyset$. Soit $u_1 + e_r, \dots, u_s + e_r$ les éléments de $T \cap \partial\mathbf{c}$, où u_i est dans $\mathbb{S}(0,t-1)$ et donc $\mathbb{S}(u_i) \subset \mathbb{B}(0,t)$. De plus, le seul voisin de u_i parmi les éléments de T est $u_i + e_r$. Ainsi, lorsque nous ajoutons la sphère $\mathbb{S}(u_i)$ à $\mathbf{c}$ les sommets $u_i + e_i$ sont supprimés de T sans autre modification de T. Ainsi le mot :

$$\mathbf{c}' := \mathbf{c} - \sum_{i=1}^{s} \mathbb{S}(u_i),$$

ne contient aucun élément de T. D'après le lemme 3.5, nous obtenons $\partial \mathbf{c}' = \emptyset$ et, en appliquant l'hypothèse de récurrence, $\mathbf{c}'$ est une somme de sphères contenues dans $\mathbb{B}(0, t-1)$. En conséquence, $\mathbf{c}$ est somme de sphères incluses dans $\mathbb{B}(0, t)$. □

3.1.3 Borne inférieure sur la distance minimale du code quantique

Pour borner la distance minimale du code quantique, nous nous intéressons aux poids des vecteurs de $\operatorname{Ker} A \setminus \operatorname{Ker} A^{\perp}$. D'après le lemme suivant, cet ensemble est $\operatorname{Ker} A \setminus \operatorname{Im} A$.

Lemme 3.7. $(\operatorname{Ker} A(H))^{\perp} = \operatorname{Im} A(H)$.

Démonstration. L'espace $\operatorname{Im} A$ est engendré par les colonnes de A. Par symétrie, c'est aussi l'espace des lignes. On a donc $\operatorname{Im} A^{\perp} = \operatorname{Ker} A$. Ceci prouve le lemme. □

Dans le lemme suivant nous nous penchons sur le poids des erreurs problématiques, c'est-à-dire des mots de $\operatorname{Ker} A(H) \setminus (\operatorname{Ker} A(H))^{\perp}$. En utilisant la structure locale du graphe, nous obtenons une première borne inférieure sur la distance minimale du code quantique Q_H associé à $A(H)$.

Lemme 3.8. *Supposons que la distance minimale du code binaire $C = \operatorname{Ker} A(H)$ est supérieure à 9. Soit $\mathbf{c}$ un mot de poids minimum de $C \setminus C^{\perp}$ et x un sommet de $\mathbf{c}$, alors on a :*

$$w(\mathbf{c} \cap \mathbb{B}(x, 4)) \geq Kn^2,$$

pour une constante $K > 0$.

Démonstration. Par transitivité, on peut supposer que $x = 0$ et d'après l'isomorphisme local de la proposition 3.3, on peut supposer que l'on travaille dans la boule de rayon 4, $\mathbb{B}(0, 4)$ du graphe $G(I_n)$.

Pour commencer montrons que $\mathbf{c}$ contient au moins $n/2$ sommets de la sphère de rayon 2. Le mot $\mathbf{c}$ contient le sommet 0 et est orthogonal aux sphères $\mathbb{S}(e_i)$. Il contient donc un autre sommet de chaque sphère $\mathbb{S}(e_i)$. Ces sommets sont de la forme $e_i + e_j$ avec $j \neq i$. Un tel sommet est inclus dans deux sphères : $\mathbb{S}(e_i)$ et $\mathbb{S}(e_j)$. Il satisfait les équations associées à au plus deux telles sphères. Pour que toutes ces équations soient satisfaites, il faut donc au moins $n/2$ sommets de $\mathbf{c}$ sur la couche de rayon 2.

Nous allons désormais voir, grâce à ces $O(n)$ sommets sur la couche 2, qu'il y a au moins $O(n^2)$ sommets sur la couche 4. Pour cela nous procédons en deux étapes. Nous partitionnons les sommets de $\mathbf{c}$ de la deuxième couche en deux sous-ensembles :

- Un ensemble maximal de sommets à supports disjoints. Quitte à réindexer les vecteurs de la base canonique de $\mathbb{F}_2^n$, ces sommets sont les $k/2$ sommets $e_1 + e_2, e_3 + e_4, \ldots, e_{k-1} + e_k$ avec $k \leq n$.
- Le complémentaire dans $\mathbf{c} \cap \mathbb{S}(0, 2)$ de cet ensemble de sommets.

La première étape est de montrer que s'il y a un grand nombre de paires disjointes $e_i + e_{i+1}$ dans $\mathbf{c}$ alors il y a un nombre quadratique en n de sommets de $\mathbf{c}$ dans la boule de rayon 4. Ensuite, on montre que c'est encore vrai dans le cas où cet ensemble est petit.

Étape 1. Supposons que $k \geq n/4$. Le mot $\mathbf{c}$ contient $k/2$ sommets de la forme $e_1 + e_2, \ldots, e_{k-1} + e_k$. Regardons les $(k/2)(n-2)$ sphères de centre $e_i + e_{i+1} + e_s$ avec $s \in \{1, \ldots, n\}$ autre que i et $i+1$.

La sphère $\mathbb{S}(e_i + e_{i+1} + e_s)$ contient le sommet $e_i + e_{i+1}$ et ne contient aucun autre sommet de la forme $e_{i'} + e_{i'+1}$. Cette sphère doit contenir au moins un autre sommet de $\mathbf{c}$. On traite les deux cas suivants séparément : soit ce sommet est dans la sphère de rayon 2, soit il est dans la sphère de rayon 4. Si le nouveau sommet est sur la deuxième couche, il est inclus dans au plus une autre sphère de centre $e_{i'} + e_{i'+1} + e_{s'}$. Autrement, ce sommet est sur la couche 4. Un sommet de cette couche est inclus dans au plus 4 sphères de centre $e_{i'} + e_{i'+1} + e_{k'}$, pour des raisons de degré. Ceci prouve l'existence d'un nombre quadratique de sommets de $\mathbf{c}$ dans la boule de rayon 4 :

$$w(c) \cap \mathbb{B}(0,4) \geq \frac{(k/2)(n-2)}{4}. \tag{3.1}$$

Étape 2. Supposons maintenant que $k < n/4$.

On sait que le mot $\mathbf{c}$ contient $k/2$ sommets de la forme $e_i + e_{i+1}$ pour $i = 1, 3, \ldots, k-1$. Aucun de ces sommets n'est inclus dans la sphère $\mathbb{S}(e_\ell)$ lorsque $\ell > k$. Comme cette sphère contient $0 \in \mathbf{c}$, elle doit contenir un autre sommet de $\mathbf{c}$, il est de la forme $e_{i_\ell} + e_\ell$. Par maximalité de k, on ne peut pas avoir $i_\ell > k$. Fixons un tel indice i_ℓ pour chaque $\ell > k$. Nous avons prouvé l'existence de $n-k$ sommets de $\mathbf{c}$ de la forme $e_{i_\ell} + e_\ell$ avec $\ell > k$ et $i_\ell \leq k$.

Fait 1. Pour tout $\ell > k$, il existe au moins $\frac{n}{2} - 1$ sommets $e_{i_\ell} + e_s$ avec $s \in \{1, 2, \ldots n\}$ tels que $e_{i_\ell} + e_s \notin \mathbf{c}$. En effet, s'il y avait strictement plus de $n/2$ sommets de $\mathbf{c}$ de la forme $e_{i_\ell} + e_s$, en ajouter la sphère $\mathbb{S}(e_{i_\ell})$ diminuerait le poids du mot $\mathbf{c}$:

$$w(\mathbf{c} + \mathbb{S}(e_{i_\ell})) < w(\mathbf{c}).$$

Cette inégalité contredit la minimalité du poids de $\mathbf{c}$.

Regardons alors les sphères centrées en les sommets $e_{i_\ell} + e_\ell + e_s$ avec $\ell, s > k$ tels que le sommet $e_{i_\ell} + e_s$ n'est pas un sommet de $\mathbf{c}$. Il y a $n-k$ possibilités pour ℓ, ensuite on choisit $s > k$ tel que $e_{i_\ell} + e_s \notin \mathbf{c}$, ce qui laisse $n/2-1-k$ valeurs possibles, d'après le *Fait 1.* Le nombres de telles sphères est donc $(n-k)(n/2-1-k)$. Le mot $\mathbf{c}$ est orthogonal à la sphère $\mathbb{S}(e_{i_\ell} + e_\ell + e_s)$ qui contient le sommet $e_{i_\ell} + e_\ell$ de $\mathbf{c}$. Il existe donc un autre sommet de $\mathbf{c}$ parmi les voisins de $e_{i_\ell} + e_\ell + e_s$. Les indices ℓ et s sont plus grands que k donc ce sommet n'est pas $e_\ell + e_s$ par maximalité de k. Il reste donc deux possibilités. Soit il s'agit d'un sommet de la couche 2 de la forme $e_{i_\ell} + e_s$ ou $e_\ell + e_s$, soit c'est un sommet de la quatrième couche de la forme $e_{i_j} + e_j + e_s + e_s$. Le premier cas est exclu car par le choix de s il n'y a pas de sommet $e_{i_\ell} + e_s$ dans

c. Dans le second cas un sommet de la couche 4 est atteint au plus 4 fois. Nous en déduisons donc $\frac{1}{4}(n-k)(n/2-1-k)$ nouveaux sommets de **c** :

$$w(c) \cap \mathbb{B}(0,4) \geq \frac{1}{4}(n-k)(n/2-1-k)\cdot \tag{3.2}$$

Pour conclure il ne reste plus qu'à combiner les deux inégalités (3.1) et (3.2). On en déduit une borne quadratique en n. □

De manière analogue au cas des codes de surface et des codes couleur, nous souhaiterions utiliser l'isomorphisme π de la proposition 3.3 pour dire qu'un mot **c** de $\operatorname{Ker} A(I_n)$, qui est inclus dans une boule suffisamment petite, n'apparaît pas dans le calcul de la distance minimale du code quantique. Pour cela, nous introduisons le graphe de parité qui contient les sommets de **c** et les centres des sphères voisines de **c**.

Définition 3.9. *Le* graphe de parité *de* $\mathbf{c} \in \operatorname{Ker} A(H)$*, est le graphe dont les sommets sont les éléments de* $\mathbf{c} \cup \mathbb{B}(\mathbf{c}, 1)$ *et les arêtes sont les arêtes de* $G(H)$ *qui joignent deux tels sommets.*

Nous disons que **c** est *connexe* si son graphe de parité l'est. On définit de manière analogue les *composantes connexes* d'un vecteur **c**. On peut voir qu'un mot de code **c** est connexe si et seulement si $\mathbf{c} = \mathbf{c}_1 + \mathbf{c}_2$ pour deux mots de codes à supports disjoints implique $\mathbf{c}_1 = 0$ or $\mathbf{c}_2 = 0$.

Proposition 3.10. *Soit* d *la distance minimale du code de matrice de parité* H*. Si* **c** *est un mot de code* $\operatorname{Ker} A(H)$ *tel que toute composante connexe de* **c** *est inclus dans une boule de rayon* $\lceil d/2 \rceil - 2$ *alors* c *est un mot de* $\operatorname{Im} A$*.*

Démonstration. Nous savons que $\operatorname{Im} A$ est l'espace engendré par les lignes de la matrice A. Dans le graphe de Cayley $G(A)$, c'est l'espace engendré par les sphères. Notre objectif est donc de démontrer que le mot **c** est une somme de sphères. Il suffit de prouver que chaque composante de **c** est somme de sphères. On peut donc supposer que **c** est connexe. Dans ce cas, **c** est inclus dans une boule de rayon $\lceil d/2 \rceil - 2$. De plus, les sphères qui ont une intersection non-triviale avec **c** sont toutes incluses dans la boule de rayon $\lceil d/2 \rceil - 1$. D'après la proposition 3.3, cette boule est isomorphe à une boule de même rayon dans le graphe $G(I_n)$. Dans ce revêtement, le mot **c** est encore un mot de code, c'est donc une somme de sphères, et ces sphères sont entièrement incluses dans la boule de rayon $\lceil d/2 \rceil - 2$. Cette décomposition en somme de sphères passe à l'isomorphisme, elle reste donc vraie dans le graphe $G(H)$. Ceci prouve que **c** est dans l'image de A. □

En remarquant qu'un mot **c** qui n'est pas somme de sphères quitte nécessairement une boule de rayon $\lceil d/2 \rceil - 1$, on arrive au théorème :

Théorème 3.11. *Supposons que la distance minimale du code classique de matrice de parité* H *est* $d \geq 9$*. Alors la distance minimale* D *du code quantique de matrice*

$A(H)$ est bornée inférieurement par :

$$D \geq adn^2,$$

pour une constante $a > 0$.

Démonstration. Soit $\mathbf{c}$ un mot de $\operatorname{Ker} A \setminus \operatorname{Im} A$. Nous sommes à la recherche d'une borne inférieure sur le poids de $\mathbf{c}$. Quitte à travailler sur les composantes connexes de $\mathbf{c}$, on peut supposer que $\mathbf{c}$ est connexe.

D'après la proposition 3.10, le mot $\mathbf{c}$ de $\operatorname{Ker} A \setminus \operatorname{Im} A$ définit un graphe de parité connexe qui n'est pas inclus dans une boule de rayon $\lceil d/2 \rceil - 2$. On peut donc couvrir partiellement $\mathbf{c}$ avec Md boules disjointes de rayon 4, pour une constante $M > 0$. L'utilisation du lemme 3.8 permet de conclure. □

3.2 Étude approfondie de l'exemple de Shokrollahi

Nous nous intéressons dans cette partie à une question ouverte proposée par Shokrollahi dans l'article [70]. Quels sont les paramètres du code quantique construit à partir du code de répétition ?

Dans ce qui suit, $n \geq 4$ est un entier pair et H_n est la matrice de parité $(n-1) \times n$ du code de répétition $[n, 1, n]$ dont les colonnes sont les n vecteurs $e_1, e_2, \ldots, e_{n-1}$ et $\sum_1^{n-1} e_i$ de $\mathbb{F}_2^{n-1}$.

$$H_n = \begin{pmatrix} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{pmatrix}.$$

On note A_n la matrice d'adjacence $A(H_n)$. C'est la matrice d'adjacence du graphe de Cayley de $\mathbb{F}_2^{n-1}$ engendré par les colonnes de H_n. Cette construction est détaillée dans la section précédente.

Le but de cette partie est de démontrer le théorème suivant :

Théorème 3.12. *Les paramètres du code quantique associé au code de répétition $[n, 1, n]$ sont :*

$$[[N = 2^{n-1}, K = 2^{\frac{n}{2}}, D = 2^{\frac{n}{2}-1}]].$$

On peut en fait améliorer les paramètres de cette famille de codes quantiques. Si nous ne conservons que les lignes de la matrice de parité indexées par des vecteurs de poids pair, nous obtenons le même rendement et la même distance mais pour une longueur divisée par 2. Les paramètres du code amélioré sont :

$$[[N = 2^{n-2}, K = 2^{\frac{n}{2}-1}, D = 2^{\frac{n}{2}-1}]].$$

Pour démontrer cette propriété, on regarde le graphe de Tanner de ce code dont la construction est rappelée par la définition 1.20. Il suffit de remarquer que ce graphe de Tanner se décompose en deux composantes connexes isomorphes. Dans

la première composante les sommets sont indexés par les vecteurs de poids pair et les équations sont indexées par les vecteurs de poids impair. Dans la seconde composante, c'est l'inverse.

3.2.1 Les matrices A_n

Les lignes de la matrice A_n et les sommets du graphe sont indexés par les éléments de $\mathbb{F}_2^{n-1}$. Nous veillerons à ne pas confondre les éléments de $\mathbb{F}_2^{n-1}$ avec les vecteurs de l'espace $\mathbb{F}_2^{2^{n-1}}$, comme par exemple les lignes de la matrice A_n.

En ordonnant les vecteurs de $\mathbb{F}_2^{n-1}$ dans l'ordre lexicographique, on obtient la matrice :

$$A_4 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Cette matrice est de rang 2 donc son noyau est un code classique de dimension 6 et le code quantique associé encode 4 qubits.

Pour passer de la matrice A_n à la matrice A_{n+1}, nous remarquons la formule suivante :

Lemme 3.13. *Pour tout entier $n \geq 4$, on a :*

$$A_{n+1} = \begin{pmatrix} A_n + J_n & I_n + J_n \\ I_n + J_n & A_n + J_n \end{pmatrix},$$

où J_n est la matrice binaire anti-diagonale de taille 2^{n-1}. Pour alléger les notations, I_n désigne la matrice identité de taille $2^{n-1} \times 2^{n-1}$

Démonstration. Lorsque l'on passe de A_n à A_{n+1}, l'ensemble des indices passe de $\mathbb{F}_2^{n-1}$ à $\mathbb{F}_2^n$. On sépare les colonnes et les lignes de A_{n+1} en deux ensembles. Celles dont les indices sont des vecteurs de F_2^n tels que $e_n = 0$ et celles telles que $e_n = 1$. Ceci nous donne une décomposition de la matrice en quatre blocs de la taille de A_n. Les générateurs du graphe de Cayley $\{e_1, e_2, \ldots, e_{n-1}\}$ ne modifient pas la dernière coordonnée des indices et induisent donc les blocs diagonaux $A_n + J_n$. Le terme J_n provient de la disparition du générateur $e_1 + e_2 + \cdots + e_{n-1}$. Ensuite, on ajoute des blocs identité I_n qui correspondent au générateur e_n. Enfin l'élément $\sum_1^n e_i$ induit des blocs J_n sur la diagonale montante. □

3.2.2 Calcul de la dimension du code quantique

Pour déterminer la dimension du code quantique, il suffit de calculer le rang de la matrice A_n. Nous nous intéressons donc à la dimension du noyau $\operatorname{Ker} A_n$.

Le lemme suivant ne nécessite pas de preuve. Nous l'énonçons pour souligner l'importance de l'involution de matrice J_n.

Lemme 3.14. $J_n^2 = I_n$.

En utilisant les symétries de la matrice A_n, nous obtenons le lemme suivant.

Lemme 3.15. *On a*
- $\mathbf{x} \in \operatorname{Ker} A_n \Leftrightarrow J_n\mathbf{x} \in \operatorname{Ker} A_n$,
- $\mathbf{x} \in \operatorname{Im} A_n \Leftrightarrow J_n\mathbf{x} \in \operatorname{Im} A_n$,
- $\operatorname{Im} A_n \subset \operatorname{Ker} A_n$.

Démonstration. Si $\mathbf{x} \in \operatorname{Im} A_n$ alors $\mathbf{x}$ est une combinaison linéaire de colonnes de A_n : $\mathbf{x} = \sum \lambda_i \mathbf{c}_i$. Donc $J_n\mathbf{x}$ est une combinaison linéaire des $J_n\mathbf{c}_i$. Appliquer J_n à un vecteur revient à lire ses coordonnées dans l'ordre inverse. En particulier, on peut voir que $J_n\mathbf{c}_i = \mathbf{c}_{N-i}$, où $N = 2^{n-1}$ est la taille de A_n. Pour se convaincre de cette égalité, on remarque que dans le graphe de Cayley, x et y sont voisins si et seulement si $x + \sum e_i$ et $y + \sum e_i$ le sont. Ceci prouve que $J_n\mathbf{x}$ est aussi dans l'image de la matrice A_n. Pour la réciproque, on utilise l'involutivité de J_n.

Soit $\mathbf{x}$ un élément de l'image de A_n. C'est une somme de colonnes de la matrice A_n. Comme cette matrice est symétrique, c'est aussi une somme de lignes. Comme les lignes sont deux à deux orthogonales, le vecteur $\mathbf{x}$ est un élément du code $\operatorname{Ker} A_n$. □

Lemme 3.16. *Soit* $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) \in \mathbb{F}_2^{2^{n+1}}$ *où* $\mathbf{x}_i$ *sont des vecteurs de* $\mathbb{F}_2^{2^{n-1}}$. *Alors, on a* $\mathbf{x} \in \operatorname{Ker} A_{n+2}$ *si et seulement si :*

$$\begin{cases} \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \text{ où } \mathbf{c}_1 \in \operatorname{Ker} A_n \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \text{ où } \mathbf{c}_2 \in \operatorname{Ker} A_n \\ A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1 \\ A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 \end{cases}.$$

Démonstration. De la formule de récurrence du lemme 3.13, on déduit :

$$A_{n+2} = \left(\begin{array}{cc|cc} A_n + J_n & I_n & I_n & J_n \\ I_n & A_n + J_n & J_n & I_n \\ \hline I_n & J_n & A_n + J_n & I_n \\ J_n & I_n & I_n & A_n + J_n \end{array}\right).$$

Nous pouvons donc caractériser les vecteurs du noyau de A_{n+2} en fonction de A_n. On obtient : $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) \in \operatorname{Ker} A_{n+2}$ si et seulement si :

$$\Leftrightarrow \begin{cases} A_n\mathbf{x}_1 = (\mathbf{x}_2 + \mathbf{x}_3) + J_n(\mathbf{x}_1 + \mathbf{x}_4) \\ A_n\mathbf{x}_2 = (\mathbf{x}_1 + \mathbf{x}_4) + J_n(\mathbf{x}_2 + \mathbf{x}_3) \\ A_n\mathbf{x}_3 = A_n\mathbf{x}_2 \\ A_n\mathbf{x}_4 = A_n\mathbf{x}_1 \end{cases}$$

$$\Leftrightarrow \begin{cases} \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \text{ où } \mathbf{c}_1 \in \operatorname{Ker} A_n \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \text{ où } \mathbf{c}_2 \in \operatorname{Ker} A_n \\ A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1 \\ A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 \end{cases}$$

□

Proposition 3.17. $\dim \operatorname{Ker} A_n = 2^{n-2} + 2^{\frac{n}{2}-1}$.

Démonstration. Le cas de A_4 est clair. Démontrons que la dimension du noyau de A_n vérifie $\dim \operatorname{Ker} A_{n+2} = 2 \dim \operatorname{Ker} A_n + 2^{n-1}$.

Si $\mathbf{x} \in \operatorname{Ker} A_{n+2}$ alors d'après la caractérisation du lemme 3.16, $\mathbf{c}_1 + J_n\mathbf{c}_2$ et $\mathbf{c}_2 + J_n\mathbf{c}_1$ sont dans l'image de la matrice A_n. Pour étudier ces couples $(\mathbf{c}_1, \mathbf{c}_2)$, nous introduisons l'application suivante :

$$\begin{array}{rcl} \varphi : \operatorname{Ker} A_n \times \operatorname{Ker} A_n & \longrightarrow & \operatorname{Ker} A_n / \operatorname{Im} A_n \\ (\mathbf{c}_1, \mathbf{c}_2) & \longmapsto & \mathbf{c}_1 + J_n\mathbf{c}_2 \end{array}$$

Le lemme 3.15 nous assure que $\mathbf{c}_1 + J_n\mathbf{c}_2$ et $\mathbf{c}_2 + J_n\mathbf{c}_1$ sont tous les deux dans l'espace $\operatorname{Im} A_n$ si et seulement si $(\mathbf{c}_1, \mathbf{c}_2)$ est dans le noyau de φ.

Étant donné un tel couple $(\mathbf{c}_1, \mathbf{c}_2)$, on peut construire un mot de code de $\operatorname{Ker} A_{n+2}$ en choisissant $\mathbf{x}_1$ et $\mathbf{x}_2$ des antécédents de $\mathbf{c}_1 + J_n\mathbf{c}_2$ et $\mathbf{c}_2 + J_n\mathbf{c}_1$ respectivement. Ceci va nous permettre de définir une bijection à valeur dans le code $\operatorname{Ker} A_{n+2}$. Soit L_n une application de $\operatorname{Im} A_n$ vers $\mathbb{F}_2^{2^{n-1}}$ telle que $L_n(\mathbf{y})$ est un antécédent de $\mathbf{y}$ par A_n, *i.e.* $A_n(L_n(\mathbf{y})) = \mathbf{y}$. On peut alors définir l'application Ψ :

$$\begin{array}{rcl} \operatorname{Ker}\varphi \times (\operatorname{Ker} A_n)^2 & \to & \operatorname{Ker} A_{n+2} \\ (\mathbf{c}_1, \mathbf{c}_2, \mathbf{s}_1, \mathbf{s}_2) & \mapsto & \left(\begin{array}{l} \mathbf{x}_1 = L_n(\mathbf{c}_2 + J_n\mathbf{c}_1) + \mathbf{s}_1 \\ \mathbf{x}_2 = L_n(\mathbf{c}_1 + J_n\mathbf{c}_2) + \mathbf{s}_2 \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \\ \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \end{array} \right) \end{array}$$

Cette application est injective car $\Psi(\mathbf{c}, \mathbf{s}) = \Psi(\mathbf{c}', \mathbf{s}')$ implique $\mathbf{x}_1 + \mathbf{x}_4 = \mathbf{x}'_1 + \mathbf{x}'_4$. C'est-à-dire $\mathbf{c}_1 = \mathbf{c}'_1$ et par le même procédé $\mathbf{c}_2 = \mathbf{c}'_2$. Par définition de L_n, nous obtenons $\mathbf{s} = \mathbf{s}'$. Pour voir que Ψ est surjective, nous utilisons la caractérisation des mots du code $\operatorname{Ker} A_{n+2}$, prouvée dans le lemme 3.16. On peut écrire ces vecteurs $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)$ avec :

$$\left\{ \begin{array}{l} \mathbf{x}_4 = \mathbf{x}_1 + \mathbf{c}_1 \\ \mathbf{x}_3 = \mathbf{x}_2 + \mathbf{c}_2 \\ A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1 \\ A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 \end{array} \right.$$

où $\mathbf{c}_1, \mathbf{c}_2 \in \operatorname{Ker} A_n$. Les vecteurs $\mathbf{c}_1$ et $\mathbf{c}_2$ apparaissent clairement et l'on peut voir que $A_n\mathbf{x}_1 = A_n(L_n(\mathbf{c}_2 + J_n\mathbf{c}_1))$ donc $\mathbf{x}_1$ et $L_n(\mathbf{c}_2 + J_n\mathbf{c}_1)$ sont égaux modulo un mot $\mathbf{s}_1$ du code $\operatorname{Ker} A_n$. Nous définissons $\mathbf{s}_2$ de manière similaire, ce qui nous donne un antécédent de $\mathbf{x}$. Nous avons ainsi démontré que l'application Ψ est bijective. Le cardinal de $\operatorname{Ker} A_{n+2}$ est donc $|\operatorname{Ker} A_n|^2.|\operatorname{Ker}\varphi|$. L'égalité : $\dim \operatorname{Ker} A_{n+2} = 2\dim \operatorname{Ker} A_n + \dim \operatorname{Ker}\varphi$ nous mène à la dimension du noyau de A_{n+2}. En effet, par le théorème du rang, nous obtenons : $\dim \operatorname{Ker}\varphi = 2^{n-1}$, puisque φ est surjective. Finalement, on trouve :

$$\dim \operatorname{Ker} A_{n+2} = 2\dim \operatorname{Ker} A_n + 2^{n-1}.$$

Le cas $n = 4$ permet de conclure. □

Nous savons que le nombre de qubits encodés est $N - 2\,\mathrm{rg}\,A_n$. De la proposition précédente, nous déduisons la dimension du code quantique.

Corollaire 3.18. *Les paramètres du code quantique Q_n associé à la matrice A_n sont :* $[[N = 2^{n-1}, K = 2^{\frac{n}{2}}]]$.

3.2.3 Calcul de la distance minimale du code quantique

Estimer la distance minimale d'un code quantique est, en général, un problème délicat. Il est parfois possible d'obtenir une borne inférieure de manière géométrique, comme dans le cas de codes topologiques, mais il est souvent difficile de tenir compte de la dégénérescence. Dans le cas de cette famille de codes de Shokrollahi, les outils développés lors de notre étude de la dimension peuvent être utilisés pour obtenir de manière exacte la distance minimale du code quantique. C'est l'objet de cette partie. Le but est donc d'examiner le poids des vecteurs de $\mathrm{Ker}\,A_n \setminus \mathrm{Ker}\,A_n^{\perp}$. D'après le lemme 3.7, cet ensemble est exactement l'ensemble $\mathrm{Ker}\,A_n \setminus \mathrm{Im}\,A_n$.

Lemme 3.19. *Tout mot de* $\mathrm{Ker}\,A_{n+2}/\,\mathrm{Im}\,A_{n+2}$ *admet un représentant de la forme* $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_2 + \mathbf{c}_2, \mathbf{x}_1 + \mathbf{c}_1)$ *avec* $\mathbf{c}_1, \mathbf{c}_2 \notin \mathrm{Im}\,A_n$ *ou bien de la forme* $(\mathbf{x}_1, 0, 0, \mathbf{x}_1)$ *avec* $\mathbf{x}_1 \in \mathrm{Ker}\,A_n$.

Démonstration. Les vecteurs de $\mathrm{Im}\,A_{n+2}$ sont de la forme :

$$\begin{pmatrix} A_n\mathbf{y}_1 + J_n(\mathbf{y}_1 + \mathbf{y}_4) + (\mathbf{y}_2 + \mathbf{y}_3) \\ A_n\mathbf{y}_2 + J_n(\mathbf{y}_2 + \mathbf{y}_3) + (\mathbf{y}_1 + \mathbf{y}_4) \\ A_n\mathbf{y}_3 + J_n(\mathbf{y}_2 + \mathbf{y}_3) + (\mathbf{y}_1 + \mathbf{y}_4) \\ A_n\mathbf{y}_4 + J_n(\mathbf{y}_1 + \mathbf{y}_4) + (\mathbf{y}_2 + \mathbf{y}_3) \end{pmatrix},$$

où $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3, \mathbf{y}_4 \in \mathbb{F}_2^{2^{n-1}}$. Soit $\mathbf{x}$ un vecteur de $\mathrm{Ker}\,A_{n+2}$. Le premier cas de l'énoncé est le lemme 3.16 lorsque $\mathbf{c}_1, \mathbf{c}_2 \notin \mathrm{Im}\,A_n$.

Supposons désormais que $\mathbf{c}_1 \in \mathrm{Im}\,A_n$. Alors $\mathbf{c}_2$ est aussi dans l'image de A_n puisque $A_n\mathbf{x}_1 = \mathbf{c}_2 + J_n\mathbf{c}_1$. Par symétrie, il s'agit du seul cas à étudier. Soit $\mathbf{b}_1$ et $\mathbf{b}_2$ des antécédents de $\mathbf{c}_1$ et $\mathbf{c}_2$ respectivement. Posons $\mathbf{y}_1 = \mathbf{y}_2 = 0$, $\mathbf{y}_3 = \mathbf{b}_2$ et $\mathbf{y}_4 = \mathbf{b}_1$, alors on a $(\mathbf{v}, J_n\mathbf{v}, J_n\mathbf{v} + \mathbf{c}_2, \mathbf{v} + \mathbf{c}_1) \in \mathrm{Im}\,A_{n+2}$ avec $\mathbf{v} := \mathbf{b}_2 + J_n\mathbf{b}_1$. Ainsi, modulo l'image, $\mathbf{x}$ peut s'écrire avec $\mathbf{c}_1 = \mathbf{c}_2 = 0$. Ceci donne $A_n\mathbf{x}_2 = \mathbf{c}_1 + J_n\mathbf{c}_2 = 0$. Ensuite, avec $\mathbf{y}_2 = J_n\mathbf{x}_2$ et $\mathbf{y}_1 = \mathbf{y}_3 = \mathbf{y}_4 = 0$, nous obtenons le vecteur de l'image $(J_n\mathbf{x}_2, \mathbf{x}_2, \mathbf{x}_2, J_n\mathbf{x}_2)$. On peut donc supposer que $\mathbf{x}_2 = \mathbf{x}_3 = 0$ et $\mathbf{x}_1 = \mathbf{x}_4$, ce qui mène à un représentant de la forme $\mathbf{x} = (\mathbf{x}_1, 0, 0, \mathbf{x}_1)$ avec $\mathbf{x}_1 \in \mathrm{Ker}\,A_n$. □

Proposition 3.20. *La distance minimale du code quantique Q_n est :*

$$D_n = 2^{\frac{n}{2}-1}.$$

Démonstration. Pour $n = 4$, en regardant la matrice A_4, on voit que la distance du code quantique est 2. En effet, tout mot de code non nul a un poids supérieur à 2 et, par exemple, le mot $e_2 + e_3 = (01100000)$ est dans le noyau de A_4 sans être une somme de lignes.

Nous allons démontrer que la distance minimale est au moins doublée lorsque n augmente de 2. Soit $\mathbf{x} \in \operatorname{Ker} A_{n+2}$. Supposons que nous sommes dans le premier cas du lemme 3.19. Le mot $\mathbf{x}$ admet un représentant de la forme $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_2+\mathbf{c}_2, \mathbf{x}_1+\mathbf{c}_1)$, où $\mathbf{c}_1$ et $\mathbf{c}_2$ sont dans $\operatorname{Ker} A_n$ mais ne sont pas sommes de lignes. Par définition de la distance minimale, le poids de ces vecteurs est minoré : $w(\mathbf{c}_i) \geq D_n$. Grâce à l'inégalité triangulaire pour la distance de Hamming, on trouve :

$$\begin{aligned} w(\mathbf{x}_1) + w(\mathbf{x}_1 + \mathbf{c}_1) &= d(0, \mathbf{x}_1) + d(\mathbf{x}_1, \mathbf{c}_1) \\ &\geq d(0, \mathbf{c}_1) \\ &\geq D_n. \end{aligned}$$

Ce raisonnement s'applique aussi à $\mathbf{c}_2$, donc le poids de $\mathbf{x}$ est un moins $2D_n$.

Supposons maintenant que nous sommes dans le second cas du lemme 3.19. Nous savons que $\mathbf{x}$ admet un représentant de la forme $\mathbf{x} = (\mathbf{x}_1, 0, 0, \mathbf{x}_1)$ avec $\mathbf{x}_1 \in \operatorname{Ker} A_n$. Supposons que $\mathbf{x}_1 \in \operatorname{Im} A_n$. Soit $\mathbf{w_1}$ un antécédent de $\mathbf{x}_1$. En prenant $\mathbf{y}_1 = \mathbf{y}_4 = \mathbf{w_1}$ et $\mathbf{y}_2 = \mathbf{y}_3 = 0$, nous obtenons un antécédent de $\mathbf{x}$. Ce vecteur est donc dans l'image de A_{n+2} et son poids n'apparaît pas dans le calcul de la distance minimale quantique. Si jamais $\mathbf{x}_1 \in \operatorname{Ker} A_n \setminus \operatorname{Im} A_n$, alors, par définition de la distance minimale de A_n, le poids de $\mathbf{x}$ est au moins $2D_n$.

Il reste à voir que cette borne inférieure sur D_{n+2} reste vraie lorsque l'on ajoute à $\mathbf{x}$ un vecteur de l'image de A_{n+2}. Un tel vecteur $\mathbf{y} \in \operatorname{Im} A_{n+2}$ s'écrit :

$$\mathbf{y} = \begin{pmatrix} A_n\mathbf{y}_1 + \mathbf{v} \\ A_n\mathbf{y}_2 + J_n\mathbf{v} \\ A_n\mathbf{y}_3 + J_n\mathbf{v} \\ A_n\mathbf{y}_4 + \mathbf{v} \end{pmatrix}$$

avec $\mathbf{v}$ un vecteur de $\mathbb{F}_2^{2^{n-1}}$ qui dépend de $\mathbf{y}$. Regardons le poids des deux premières composantes de $\mathbf{x} + \mathbf{y}$. L'inégalité triangulaire pour la distance de Hamming nous donne :

$$\begin{aligned} & w(\mathbf{x}_1 + A_n\mathbf{y}_1 + \mathbf{v}) + w(A_n\mathbf{y}_2 + J_n\mathbf{v}) \\ = \; & d(\mathbf{x}_1 + \mathbf{v}, A_n\mathbf{y}_1) + d(J_n\mathbf{v}, A_n\mathbf{y}_2) \\ \geq \; & d(\mathbf{x}_1 + \mathbf{v}, \operatorname{Im} A_n) + d(J_n\mathbf{v}, \operatorname{Im} A_n) \\ = \; & d(\mathbf{x}_1 + \mathbf{v}, \operatorname{Im} A_n) + d(\mathbf{v}, \operatorname{Im} A_n) \\ \geq \; & d(\mathbf{x}_1, \operatorname{Im} A_n) \\ \geq \; & D_n. \end{aligned}$$

L'égalité $d(J_n\mathbf{v}, \operatorname{Im} A_n) = d(\mathbf{v}, \operatorname{Im} A_n)$ provient du fait que J_n est une isométrie qui stabilise l'espace $\operatorname{Im} A_n$. Nous avons le même résultat pour les deux dernières composantes de $\mathbf{x} + \mathbf{y}$. Donc le poids de tout représentant de $\mathbf{x}$ est au moins $2D_n$.

Nous disposons d'un borne inférieure sur la distance minimale. Il s'agit en fait de la valeur exacte de la distance quantique. Pour le voir, regardons le vecteur $(0, 0, \mathbf{c}_2, \mathbf{c}_1)$. Il s'agit d'un vecteur du code $\operatorname{Ker} A_n$ et son poids est exactement $2D_n$ lorsque les $\mathbf{c}_i$ sont des mots de poids minimum dans l'ensemble $\operatorname{Ker} A_n \setminus \operatorname{Im} A_n$. Ce vecteur n'est pas dans l'image, sinon le vecteur $\mathbf{c}_1 = A_n(\mathbf{y}_1 + \mathbf{y}_4)$ serait dans l'image de A_n. □

Conclusion

- Nous avons obtenu une borne inférieure sur la distance minimale de tout code quantique associé à un code classique par la construction de MacKay *et al.*. Cette borne est en $O(dn^2)$ où n est la longueur du code classique et d est sa distance minimale. Ce résultat est basé sur l'énumération du nombre minimum de sommets d'un mot de $\operatorname{Ker} A \setminus \operatorname{Ker} A^{\perp}$ restreint à une boule de rayon 4. L'extension de ce résultat à des boules de plus grand rayon nous semble difficile. Nous conjecturons que la distance minimale du code quantique est en fait exponentielle en d.
- Cette famille de codes quantiques partage certaines caractéristiques des codes topologiques [17, 18, 66]. La distance minimale d'un code stabilisateur défini sur un pavage carré par des générateurs à support borné ne peut pas dépasser la borne de Bravyi et Terhal $D \leq \sqrt{N}$ [24]. La construction de MacKay *et al.* peut être vue comme une famille de codes topologiques sur un réseau de dimension croissante. Un tel code stabilisateur n'est pas *a priori* limité par la borne de Bravyi et Terhal.
- Certains codes LDPC quantiques sont à la base du calcul quantique tolérant aux fautes [80, 81], ce qui fournit une motivation supplémentaire pour leur étude. Le potentiel de cette famille de codes LDPC quantiques en calcul quantique mériterait d'être étudié. On pourrait par exemple chercher à comprendre quelles sont les opérations logiques qui peuvent être implémentées sur les donnés encodées sans décodage. Ces recherches pourraient être basées sur le lemme 3.19, grâce auquel on dispose de représentants des qubits encodés pour le code quantique associé au code de répétition.

Chapitre 4

Borne combinatoire sur la capacité du canal à effacement quantique

Ce chapitre prépare l'étude des performances des codes LDPC quantiques. Les codes LDPC classiques permettent d'approcher la capacité de différents canaux, tout en disposant d'un algorithme de décodage efficace. Nous nous intéressons à la version quantique de ce problème. Le modèle de bruit le plus commun est donné par le canal de dépolarisation. Une difficulté majeure dans le passage au cas quantique est la détermination de la capacité de ce canal. Nous nous intéressons donc à un modèle d'erreur plus simple et donc plus facile à étudier, le canal à effacement quantique. Cette stratégie s'inspire de la théorie des codes classiques. La construction de bons codes LDPC classiques sur le canal binaire symétrique est passée par l'étude du canal à effacement. Certaines idées développées pour approcher la capacité du canal à effacement ont ensuite pu être appliquées au canal binaire symétrique. La capacité du canal à effacement quantique est connue [10]. De plus la ressemblance avec le canal de dépolarisation, ainsi que l'expérience classique, nous permettent d'espérer que la construction de bons codes pour ce canal fournira aussi de bons codes pour le canal de dépolarisation. Enfin, ce modèle d'erreur n'est pas seulement un outil théorique, c'est un exemple réaliste de canal quantique [52].

Dans la première partie de ce chapitre, nous introduisons le canal à effacement quantique ainsi que sa capacité. Nous rappelons ensuite une preuve de la borne inférieure de hachage [10, 11, 79] et de la borne supérieure de non-clonage [10, 98] permettant de montrer que la capacité de ce canal est $1 - 2p$.

Le but de ce chapitre est ensuite de remplacer l'argument de non-clonage qui ne dépend pas des propriétés des codes stabilisateurs par un argument combinatoire. Nous obtenons une borne supérieure sur les rendements atteignables des codes stabilisateurs [37]. Cette nouvelle borne permet non-seulement de retrouver la borne supérieure de non-clonage, mais aussi d'étudier la distance à la capacité de familles de codes stabilisateurs. Nous appliquerons ce résultats aux codes LDPC quantique dans le chapitre suivant.

4.1 Capacité du canal à effacement quantique

4.1.1 Le canal à effacement quantique

Soit $\mathcal{H}_2$ l'espace de Hilbert $\mathbb{C}^3$ et soit $(|0\rangle, |1\rangle, |2\rangle)$ une base orthonormale de cet espace. L'espace $\mathcal{H}$ engendré par $|0\rangle$ et $|1\rangle$ est un sous-espace de $\mathcal{H}_2$. Le vecteur $|2\rangle$ est utilisé pour marquer les qubits effacés.

Définition 4.1. *Le* canal à effacement quantique *de probabilité p agit sur les opérateurs de densité de $\Delta(\mathcal{H}) \subset \Delta(\mathcal{H}_2)$ par :*

$$\mathcal{N}(\rho) = (1-p)\rho + p|2\rangle\langle 2|.$$

On peut voir ce canal comme la trace partielle par rapport à un système E de l'opération unitaire :

$$U_{QE}(|0\rangle|2\rangle_E) = \sqrt{1-p}|0\rangle|2\rangle_E + \sqrt{p}|2\rangle|0\rangle_E$$
$$U_{QE}(|1\rangle|2\rangle_E) = \sqrt{1-p}|1\rangle|2\rangle_E + \sqrt{p}|2\rangle|1\rangle_E$$

où l'espace environnement $\mathcal{H}_E$ est muni d'une base orthonormale $|0\rangle_E, |1\rangle_E, |2\rangle_E$. On choisit un environnement dont l'état de départ est fixé à $|2\rangle_E$, de sorte que l'opérateur unitaire échange les vecteurs $|0\rangle$ et $|1\rangle$ de $\mathcal{H}_Q$ et le vecteur $|2\rangle$ de l'environnement $\mathcal{H}_E$ avec probabilité p.

La décomposition orthogonale $\mathcal{H}_2 = \mathcal{H} \overset{\perp}{\oplus} \mathbb{C}|2\rangle$ définit une mesure quantique qui projette l'état du système sur l'état d'origine $|\psi\rangle$ avec probabilité $1-p$ ou sur l'état $|2\rangle$ avec probabilité p. Un qubit remplacé par $|2\rangle$ est dit effacé. Le résultat de la mesure de $|2\rangle$ nous permet de localiser les positions effacées, on remplace ensuite ces qubits par des qubits totalement aléatoires d'opérateur de densité $I/2$. Comme cet opérateur se décompose sous la forme $I/2 = \rho + X\rho X + Y\rho Y + Z\rho Z$, pour tout état $\rho = |\psi\rangle\langle\psi|$, on peut supposer qu'un qubit effacé subit une erreur de Pauli aléatoire I, X, Y ou Z avec probabilité $1/4$. On arrive ainsi à la définition discrète du canal à effacement quantique.

Définition 4.2. *Un* effacement quantique *sur n qubits est un couple $(\mathcal{E}, E)$ tel que $\mathcal{E} \in \mathbb{F}_2^n$ et $E \in \mathcal{P}_n$ est une erreur de Pauli telle que* $\mathrm{Supp}(E) \subset \mathrm{Supp}(\mathcal{E})$*. Lorsqu'un état de $\mathcal{H}^{\otimes n}$ est sujet à un effacement quantique $(\mathcal{E}, E)$, il subit l'erreur E et le vecteur d'effacement $\mathcal{E}$ est connu.*

Pour alléger les notations on écrira souvent $E \subset \mathcal{E}$ pour signifier que le support de l'erreur de Pauli E est inclus dans le support du vecteur $\mathcal{E}$, c'est-à-dire l'ensemble des composantes effacées.

Proposition 4.3. *Le canal à effacement quantique de probabilité p sur n qubits applique un effacement $(\mathcal{E}, E)$ à l'état du système tel que*

- *chaque composante du vecteur $\mathcal{E} \in \mathbb{F}_2^n$ vaut 1 avec probabilité p indépendamment des autres composantes,*

– *l'erreur E est uniformément distribuée parmi les erreurs dont le support est inclus dans le support de $\mathcal{E}$.*

Autrement dit, le canal à effacement quantique est donné par la probabilité qu'un effacement $(\mathcal{E}, E)$ perturbe l'état du système quantique : $\mathbb{P}((\mathcal{E}, E)) = \mathbb{P}(\mathcal{E})\mathbb{P}(E \mid \mathcal{E}) = p^{|\mathcal{E}|}(1-p)^{n-|\mathcal{E}|}2^{-2|\mathcal{E}|}$.

4.1.2 Capacité d'un canal quantique

Nous nous intéressons principalement aux codes stabilisateurs, nous utiliserons donc une définition discrète de la capacité du canal à effacement.

Définition 4.4. *Une* fonction de décodage *associée à un code stabilisateur C_r de groupe stabilisateur S_r de longueur n sur le canal à effacement quantique est une application $\mathcal{D}_r$ de la forme :*

$$\begin{aligned} \mathcal{D}_r : \mathbb{F}_2^n \times \mathcal{H}^{\otimes n} &\longrightarrow \mathcal{H}^{\otimes n} \\ (\mathcal{E}, E|\psi\rangle) &\longmapsto \tilde{E}E|\psi\rangle. \end{aligned}$$

L'erreur de Pauli $\tilde{E}$ est l'estimation de l'erreur subie E

La *probabilité d'erreur après décodage* est la probabilité que $\tilde{E}$ ne soit pas équivalente à E :

$$P_{err} = \mathbb{P}(\tilde{E} \notin E.S_r).$$

Définition 4.5. *Un rendement $R \in [0,1]$ est* atteignable *sur le canal à effacement quantique s'il existe une suite de codes quantiques C_r de rendements R_r convergeants vers R munis de fonctions de décodage $\mathcal{D}_r$ de probabilité d'erreur P_{err}^r tendant vers 0.*

Définition 4.6. *La* capacité *du canal à effacement quantique de probabilité p est le plus grand rendement atteignable sur ce canal.*

La capacité est traditionnellement définie en fonction de la proximité entre l'état reçu après décodage et l'état de départ. Pour cela on utilise la fidélité. La fidélité entre un état pur $|\psi\rangle$ et un opérateur de densité quelconque ρ est $F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle}$. Comme ρ est un opérateur positif de trace 1, cette quantité est un nombre réel de l'intervalle $[0,1]$. Plus la fidélité est proche de 1, plus l'état ρ_f est proche de l'état $|\psi\rangle$. Soit $|\psi\rangle$ un état d'un code quantique et soit ρ' l'opérateur de densité représentant l'état du système après le canal et le décodage. Lorsque la probabilité d'erreur tend vers 0, l'état du système après décodage est de la forme :

$$\rho_f = (1 - P_{err})|\psi\rangle\langle\psi| + P_{err}\rho'$$

où $|\psi\rangle\langle\psi|$ est l'opérateur de densité du système au départ qui correspond aux cas où la correction fonctionne et ρ'' est l'opérateur de densité des cas problématiques. La fidélité entre l'état du système au départ $|\psi\rangle$ et l'état final ρ_f est alors minorée par :

$$F(|\psi\rangle, \rho_f) \geq \sqrt{(1 - P_{err})},$$

car l'opérateur ρ' est positif donc le terme $\langle\psi|\rho'|\psi\rangle$ l'est aussi. On en conclut qu'une probabilité d'erreur qui tend vers 0 implique une fidélité qui tend vers 1. Cette définition discrète de la capacité est donc cohérente.

4.1.3 Borne inférieure de hachage

Nous présentons ici la borne inférieure de hachage sur la capacité du canal à effacement quantique [79].

Pour obtenir une borne inférieure sur la capacité du canal à effacement quantique, nous allons choisir une famille de codes stabilisateurs aléatoirement et nous verrons que les effacements typiques sont corrigibles. On en déduit que la probabilité d'erreur tend vers 0. Le rendement de cette famille de codes fournit alors une borne inférieure sur la capacité du canal. Pour prouver que la probabilité d'erreur tend vers 0, nous nous contenterons de démontrer que le syndrome d'une erreur E associée à un effacement $(\mathcal{E}, E)$ n'est en général pas atteint par une autre erreur $E' \subset \mathcal{E}$. C'est pourquoi on parle de borne de hachage.

Théorème 4.7. *La capacité du canal à effacement quantique de probabilité p est minorée par $1 - 2p$.*

Démonstration. Soit C un code stabilisateur choisi uniformément au hasard parmi les codes stabilisateurs de rendement R. Supposons qu'un état du code quantique subisse un effacement quantique $\mathcal{E} \in \mathbb{F}_2^n$. Le vecteur du code quantique est alors sujet à une erreur $E \in \mathcal{P}_n$ à support inclus dans $\mathcal{E}$. Dans ce cas, l'erreur E est corrigible si et seulement si il n'existe pas d'erreur $E' \subset \mathcal{E}$, en dehors de la classe $E.S$ de E, dont le syndrome est identique à celui de E. En particulier, si $\sigma(E')$ n'atteint jamais $\sigma(E)$ lorsque E' parcourt les erreurs incluses dans l'effacement $\mathcal{E}$, alors l'erreur survenue est corrigible.

On en déduit une borne supérieure sur la probabilité d'erreur après décodage :

$$P_{err}(C) \leq \sum_{(\mathcal{E},E)} \mathbb{P}(\mathcal{E}, E) X_{\mathcal{E},E}(C),$$

où $X_{\mathcal{E},E}(C)$ vaut 1 lorsqu'il existe une erreur E' à support dans $\mathcal{E}$ telle que $\sigma(E') = \sigma(E)$ et vaut 0 sinon.

L'espérance de la probabilité d'erreur sur l'ensemble des codes stabilisateurs de rendement R est donc majorée par :

$$\mathbb{E}(P_{err}(C)) \leq \sum_{(\mathcal{E},E)} \mathbb{P}(\mathcal{E}, E) \mathbb{E}(X_{\mathcal{E},E}(C)).$$

Soit $X_{E,E'}$ la variable aléatoire qui prend la valeur 1 lorsque $\sigma(E') = \sigma(E)$ et 0 sinon. En écrivant $X_{\mathcal{E},E}$ comme la somme des variables aléatoires $X_{E,E'}$ pour $E' \subset \mathcal{E}$, on obtient la borne supérieure $\mathbb{E}(X_{\mathcal{E},E}(C)) \leq 2^{2|\mathcal{E}|} 2^{-(1-R)n}$. En effet, il y a au plus $2^{2|\mathcal{E}|}$ erreurs $E' \subset \mathcal{E}$ et la probabilité de collision entre les syndromes de deux erreurs E et E' est $2^{-(1-R)n}$.

D'après la loi des grand nombres, il suffit de considérer les effacements typiques, c'est-à-dire de poids $np - \alpha \leq |\mathcal{E}| \leq np + \alpha$, pour une constante α aussi petite que l'on

souhaite. On en déduit une borne inférieure sur la probabilité d'erreur moyenne qui nous assure que $\mathbb{E}(P_{err})$ tend vers 0, lorsque $R < 1-2p$. Tout rendement $R < 1-2p$ est donc atteignable par des codes stabilisateurs. □

4.1.4 Borne supérieure de non-clonage

Nous démontrons maintenant que ces rendements atteignables obtenus par hachages sont optimaux. Pour cela nous rappelons la stratégie de la borne de non-clonage [10]. Il existe d'autres procédés pour déterminer la capacité de ce canal, comme les méthodes entropiques qui permettent de retrouver la borne supérieure de non-clonage [30]. Le théorème de non-clonage est dû à Wootters et Zurek en 1982 [98].

Théorème 4.8 : *non-clonage.* *Soit $\mathcal{H}$ un espace de Hilbert et $|0\rangle$ un état fixé de $\mathcal{H}$. Il n'existe pas d'opération unitaire U sur l'espace $\mathcal{H} \otimes \mathcal{H}$ telle que :*

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \text{et} \quad U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle,$$

lorsque $|\psi\rangle$ et $|\phi\rangle$ sont des états de $\mathcal{H}$ tels que $\langle\psi|\phi\rangle \notin \{0,1\}$.

Démonstration. Pour démontrer ce théorème, il suffit de remarquer que le produit scalaire entre $|\psi\rangle|0\rangle$ et $|\phi\rangle|0\rangle$ est $\langle\psi|\phi\rangle$ alors que, après application de U à ces deux états, le produit scalaire devient $\langle\psi|\phi\rangle^2$. L'opérateur unitaire U conserve le produit scalaire, ce qui implique $\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$. Les états $|\psi\rangle$ et $|\phi\rangle$ sont donc soit orthogonaux, soit égaux. □

Théorème 4.9. *La capacité du canal à effacement quantique de probabilité p est $1-2p$, lorsque $p < 1/2$ et 0 lorsque $p > 1/2$.*

Démonstration. Pour démontrer ce théorème, il reste à établir la borne supérieure. Nous nous contenterons de rappeler que la capacité du canal à effacement quantique de probabilité $1/2$ est nulle. Le théorème s'en déduit alors par interpolation entre un canal de capacité 1 et ce canal de capacité nulle [10, 11].

Regardons la représentation unitaire du canal à effacement de probabilité p sur un qubit. C'est l'opération unitaire U définie sur $\mathcal{H} \times \mathcal{H}$ par :

$$U_{QE}(|0\rangle|2\rangle_E) = \frac{1}{\sqrt{2}}|0\rangle|2\rangle_E + \frac{1}{\sqrt{2}}|2\rangle|0\rangle_E$$
$$U_{QE}(|1\rangle|2\rangle_E) = \frac{1}{\sqrt{2}}|1\rangle|2\rangle_E + \frac{1}{\sqrt{2}}|2\rangle|1\rangle_E$$

On remarque la symétrie entre les systèmes Q et E. C'est encore le cas sur n qubits. L'état du système quantique Q après la trace partielle par rapport à E est de la forme $\mathrm{Tr}_E(U|\psi\rangle\langle\psi| \otimes |2\rangle\langle 2|U^*)$. L'état de l'environnement après la trace partielle par rapport à Q est identique.

Les deux sous-systèmes sont identiques, nous allons maintenant voir que si l'on peut décoder dans Q, c'est aussi le cas dans E. On obtient ainsi une forme de

clonage de l'état de départ. Supposons que le système Q peut être décodé avec une fidélité qui tend vers 1 lorsque n tend vers l'infini. On peut alors appliquer la même évolution à l'environnent E. On en déduit un clonage approché de tout état du code quantique utilisé. Prenons $|\psi\rangle$un état du code quantique, et notons ρ_Q et ρ_E les états finaux après décodage dans Q et E. La fidélité du décodage $\langle\psi|\rho_Q|\psi\rangle$ tend vers 1. C'est aussi le cas avec ρ_E. Avec les même notations on peux aussi construire un clonage approché ρ'_Q, ρ'_E d'un autre état $|\psi'\rangle$ du code quantique. La quantité $\langle\psi|\rho_Q|\psi\rangle$ converge encore vers 1.

En considérant deux états $|\psi\rangle$ et $|\psi'\rangle$ tels que $\langle\psi|\psi'\rangle = \beta \neq 0, 1$, on obtient une contradiction similaire à celle de la preuve du théorème de non-clonage. Ceci prouve que la capacité du canal est nulle en ce point $p = 1/2$. □

4.1.5 Remarques sur le canal de dépolarisation

Dans le cas du canal de dépolarisation, on peut définir la capacité de manière analogue. La fonction de décodage ne prend en entrée que l'état perturbé $E|\psi\rangle$ et détermine une estimation $\tilde{E}$ de E. La probabilité d'erreur est la probabilité que $\tilde{E}$ n'ait pas le même effet que E sur le code quantique, c'est la probabilité que $\tilde{E}$ ne soit pas dans la classe $E.S$ de E modulo le groupe stabilisateur S.

On s'intéresse alors au maximum des rendements atteignables par des codes stabilisateurs que nous appellerons capacité du canal. Il s'agit d'un abus car nous devrions considérer l'ensemble de tous les codes quantiques. Cette restriction est raisonnable car tous les codes quantiques qui apparaitront sont issus de cette construction. Elle permet une discrétisation de ces notions de théorie de l'information quantique.

La capacité de ce canal est à ce jour inconnue. On peut se rendre compte de la difficulté de la détermination de cette valeur en adaptant les bornes de hachage et de non clonage au cas du canal de dépolarisation. Par exemple, la proposition suivante donne la borne de hachage [79] et la borne de non-clonage [25, 31] obtenues dans le cas du canal de dépolarisation. Ces deux bornes qui encadrent la capacité du canal de dépolarisation sont tracées figure 4.1.

Proposition 4.10. *La capacité du canal de dépolarisation de probabilité p est minorée par $1 - h(p) - p\log_2(3)$ et majorée par $1 - 4p$.*

Stratégie de la preuve. Nous nous intéressons plus particulièrement à l'aspect combinatoire de ces bornes. Nous résumons donc ici les arguments de la preuve de la borne inférieure de hachage.

Pour obtenir cette borne, on procède comme dans le cas du canal à effacement quantique. Notre objectif est de démontrer que la probabilité d'erreur moyenne tend vers 0. On introduit donc la variable aléatoire X_E qui vaut 1 lorsqu'il existe une erreur typique, *i.e.* de poids $np - \alpha \leq |E| \leq np + \alpha$, et qui vaut 0 sinon. Ainsi la probabilité d'erreur est :

$$P_{err} = \sum_E \mathbb{P}(E) X_E,$$

où $\mathbb{P}(E)$ est la probabilité d'apparition de E par le canal de dépolarisation.

Pour majorer l'espérance de X_E, on remarque qu'il y a environ $\binom{n}{np}3^{np}$ erreurs typiques différentes et que la probabilité de collision entre les syndromes de deux erreurs fixées est encore $2^{-(1-R)n}$. Les inégalités sur les coefficients binomiaux mènent à une borne supérieure avec un terme exponentiel de la forme $2^{n(h(p)+p\log_2(3)-1+R)}$.

On en déduit l'existence d'une famille de codes stabilisateurs de rendement R et de probabilité d'erreur tendant vers 0, pour tout rendement R tel que $R < 1 - h(p) - p\log_2(3)$. □

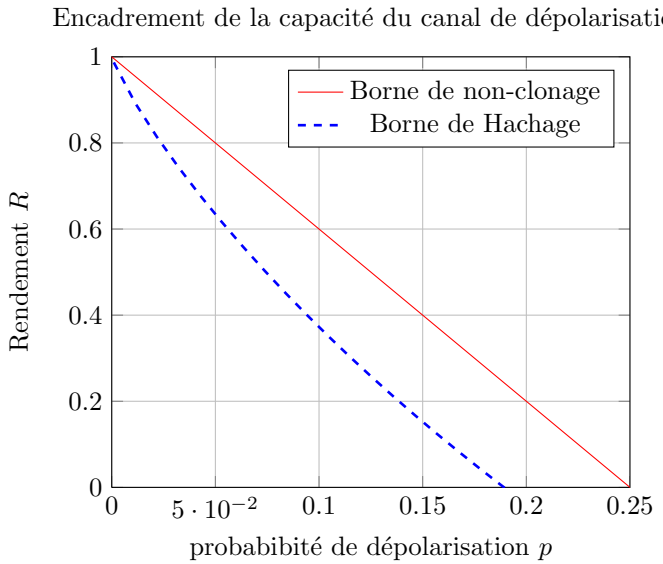


Figure 4.1 – La borne inférieure et la borne supérieure de la proposition 4.10 sur la capacité du canal de dépolarisation en fonction de la probabilité de dépolarisation p. En pointillés bleus, la borne inférieure de hachage et en rouge la borne supérieure de non-clonage.

Comme le montre la figure 4.1,Ces deux bornes qui coïncident lorsque l'on travaille avec le canal à effacement quantique ne sont plus identiques dans le cas du canal de dépolarisation. Pour obtenir une meilleure borne inférieure nous devons tenir compte de la dégénérescence. DiVincenzo, Shor et Smolin ont démontré que la borne de hachage pouvait être dépassée [39]. La borne supérieure la plus précise que nous connaissons est la borne de Smith et Smolin [88].

La suite de ce chapitre peut être vue comme l'analogue de ce problème dans le cas des effacements quantiques. Nous allons voir que l'on ne peut pas dépasser la borne de hachage en utilisant la dégénérescence, c'est-à-dire en corrigeant un grand nombre d'erreurs à partir d'un même syndrome. Nous retrouvons ainsi de manière combinatoire la borne supérieure de non-clonage dans le cas des codes stabilisateurs.

4.2 Une étude combinatoire de la capacité du canal à effacement

4.2.1 Un exemple d'effacement non-corrigible

Commençons par étudier un exemple d'effacement quantique problématique. On considère le code stabilisateur défini par la matrice :

$$\mathbf{H} = \begin{pmatrix} I & X & Z & Y & Z \\ Z & Z & X & I & Z \\ I & Y & Y & Y & Z \end{pmatrix}$$

Si l'effacement est $\mathcal{E} = (0, 1, 1, 0, 0)$, il y a $2^{2|\mathcal{E}|} = 2^4$ erreurs possibles :

$$\{E \in \mathcal{P}_n \mid E \subset \mathcal{E}\} = \{X_2^{a_2} Z_2^{b_2} X_3^{a_3} Z_3^{b_3} \mid a_i, b_i \in \mathbb{F}_2\},$$

où l'erreur X_i est l'erreur dont la i-ème coordonnée est X et qui est l'identité sur les autres composantes. L'opérateur Z_i est défini de manière similaire et Y_i est l'erreur $X_i Z_i$.
Concentrons nous sur la *sous-matrice effacée* :

$$\mathbf{H}_{\mathcal{E}} = \begin{pmatrix} X & Z \\ Z & X \\ Y & Y \end{pmatrix}$$

qui est la sous-matrice de $\mathbf{H}$ composée des colonnes de $\mathbf{H}$ indexées par les positions effacées. Il est naturel d'introduire cette matrice puisque le syndrome d'une erreur incluse dans l'effacement $\mathcal{E}$ ne dépend que de ces colonnes. Dans cet exemple, nous remarquons que la troisième ligne est le produit des deux premières lignes. Ainsi, le syndrome $u \in \mathbb{F}_2^3$ d'une erreur $E \subset \mathcal{E}$ vérifie $u_3 = u_1 + u_2$. Il ne dépend que des deux premières lignes de $\mathbf{H}_{\mathcal{E}}$. Il y a donc 2^2 syndromes différents d'erreur E contenues dans l'effacement.
Regardons maintenant les colonnes restantes. La *sous-matrice non-effacée* $\mathbf{H}_{\bar{\mathcal{E}}}$ est :

$$\mathbf{H}_{\bar{\mathcal{E}}} = \begin{pmatrix} I & Y & Z \\ Z & I & Z \\ I & Y & Z \end{pmatrix}.$$

Considérons deux erreurs E et E' agissant sur les qubits effacés, qui sont dans la même classe de dégénérescence. Cela signifie que ces erreurs diffèrent d'un élément du groupe stabilisateur $s \in S$ par multiplication. La restriction de l'erreur $s = EE'$ à $\bar{\mathcal{E}}$ est l'identité. Un tel opérateur s correspond donc à une relation entre les lignes de la matrice $\mathbf{H}_{\bar{\mathcal{E}}}$. Le rang de cette sous-matrice est $\operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}} = 2$ car la première et la troisième ligne de cette matrice sont identiques. Nous avons donc deux possibilités pour s : on a soit $s = I^{\otimes 5}$, soit $s = S_1 S_3 = I \otimes Z \otimes X \otimes I \otimes I$. Il y a donc deux erreurs dans chaque classe de dégénérescence et quatre syndromes possibles pour chaque classe. En conséquence, s'il n'y avait pas d'erreur problématique incluse dans $\mathcal{E}$, le nombre total d'erreurs sur les composantes effacées serait $2 \times 4 = 2^3$. Mais nous avons vu que le nombre total d'erreurs possibles est 2^4. L'effacement donné $\mathcal{E}$ couvre donc une erreur problématique. Il n'est pas corrigible.

4.2.2 Deux lemmes d'énumération

Nous allons généraliser cette approche. Notre stratégie est de déterminer le cardinal de deux ensembles d'erreurs de Pauli :

- $N(S)_\mathcal{E} = \{E \in N(S) \mid E \subset \mathcal{E}\}$,
  Rappelons que $N(S)$ désigne l'ensemble des erreurs de Pauli de syndrome nul.
- $S_\mathcal{E} = \{s \in S \mid s \subset \mathcal{E}\}$.

Nous allons utiliser les sous-matrices introduites dans l'exemple précédent.

La sous-matrice aléatoire $\mathbf{H}_\mathcal{E}$: Soit $\mathbf{H}$ la matrice d'un code stabilisateur. À tout effacement $\mathcal{E} \in \mathbb{F}_2^n$, nous associons la sous-matrice $\mathbf{H}_\mathcal{E}$ de la matrice stabilisatrice $\mathbf{H} \in \mathcal{M}_{r,n}(\mathcal{P}_1)$ composée des colonnes correspondant aux qubits effacés. C'est la sous-matrice des colonnes d'indice i tel que $\mathcal{E}_i = 1$. La matrice des qubits non-effacés $\mathbf{H}_\mathcal{E}$ est définie de manière similaire. Elle correspond au conjugué $\bar{\mathcal{E}}$ de $\mathcal{E}$ défini par : $\bar{\mathcal{E}}_i = \mathcal{E}_i + 1$.

Lemme 4.11. *Soit S un groupe stabilisateur de matrice $\mathbf{H} \in \mathcal{M}_{r,n}$. L'ensemble $N(S)_\mathcal{E}$ est un $\mathbb{F}_2$-espace vectoriel de dimension $2|\mathcal{E}| - \operatorname{rg} \mathbf{H}_\mathcal{E}$.*

Rappelons que le *rang* de la matrice quaternaire $\mathbf{H}_\mathcal{E}$ est la dimension du $\mathbb{F}_2$-espace vectoriel engendré par ses lignes. C'est aussi le rang du sous-groupe de $\mathcal{P}_n$ engendré par ses lignes.

Démonstration. La structure de $\mathbb{F}_2$-espace vectoriel a été détaillée dans le chapitre d'introduction dans la section 1.4.4. Le syndrome est une application $\mathbb{F}_2$-linéaire de $\mathcal{P}_n$ dans $\mathbb{F}_2^r$. Sa restriction $\sigma_\mathcal{E}$ à l'espace des erreurs de Pauli incluses dans $\mathcal{E}$ est aussi $\mathbb{F}_2$-linéaire. Comme le sous-espace $N(S)_\mathcal{E}$ est le noyau de $\sigma_\mathcal{E}$, sa dimension est $2|\mathcal{E}| - \dim \operatorname{Im} \sigma_\mathcal{E}$. Le syndrome restreint $\sigma_\mathcal{E}$ est une fonction qui ne dépend que de la matrice $\mathbf{H}_\mathcal{E}$. La dimension de son image est le rang de la matrice $\mathbf{H}_\mathcal{E}$. □

Lemme 4.12. *Soit S un groupe stabilisateur de matrice $\mathbf{H} \in \mathcal{M}_{r,n}$. L'ensemble $S_\mathcal{E}$ est un $\mathbb{F}_2$-espace vectoriel de dimension $\operatorname{rg} \mathbf{H} - \operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}}$.*

Démonstration. L'ensemble $S_\mathcal{E}$ est le noyau de l'application $\mathbb{F}_2$-linéaire :

$$\begin{aligned} S &\longrightarrow \{E \in \mathcal{P}_n \mid E \subset \mathcal{E}\} \\ s &\longmapsto s_{|\bar{\mathcal{E}}} \end{aligned}$$

Par définition du rang, l'image de cette application est un sous-espace de dimension $\operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}}$, et le groupe S est de dimension $\operatorname{rg} \mathbf{H}$. La dimension cherchée est donc, $\dim S_\mathcal{E} = \operatorname{rg} \mathbf{H} - \operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}}$. □

D'après ces deux lemmes, il y a $2^{\operatorname{rg} \mathbf{H}_\mathcal{E}}$ syndromes différents et dans chaque classe modulo S, il y a $2^{\operatorname{rg} \mathbf{H} - \operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}}}$ erreurs incluses dans $\mathcal{E}$. En conséquence, le nombre total d'erreurs corrigibles est $2^{\operatorname{rg} \mathbf{H} + \operatorname{rg} \mathbf{H}_\mathcal{E} - \operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}}}$, et comme il y a $2^{2|\mathcal{E}|}$ vecteurs erreurs couverts par $\mathcal{E}$, l'effacement $\mathcal{E}$ ne peut être corrigé que lorsque :

$$2|\mathcal{E}| \leq \operatorname{rg} \mathbf{H} + \operatorname{rg} \mathbf{H}_\mathcal{E} - \operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}}. \tag{4.1}$$

Le rang de $\mathbf{H}$ est $\operatorname{rg}\mathbf{H} = (1-R)n$ où R est le rendement du code quantique. Lorsque $p \leq 1/2$, il y a typiquement moins de composantes non-effacées que de composantes effacées et il est donc raisonnable de supposer que la matrice $\mathbf{H}_{\bar{\mathcal{E}}}$ aura un rang plus élevé que celui de la matrice $\mathbf{H}_{\mathcal{E}}$, de plus petite taille. En utilisant le fait que $2|\mathcal{E}| \leq \operatorname{rg}\mathbf{H}$ et en considérant un effacement de poids typique $|\mathcal{E}| = np$, l'équation (4.1) nous donne :

$$R \leq 1 - 2p.$$

On retrouve ainsi la borne supérieure provenant de la capacité du canal à effacement dans le cas des codes stabilisateurs. Nous rendrons cet argument rigoureux dans la prochaine section.

4.2.3 Une borne combinatoire sur la capacité

Nous allons maintenant donner une preuve rigoureuse en utilisant une formulation entropique de cette idée et en appliquant l'inégalité de Fano qui permet de borner inférieurement la probabilité d'erreur après décodage.

Rappelons qu'un rendement $R \in [0,1]$ est dit atteignable s'il existe une famille de codes de rendements R_t de limite R telle que la probabilité d'erreur après décodage tend vers 0. On note $\mathbb{E}$ l'espérance. Soit $(\mathbf{H}_t)$ une suite de matrice stabilisatrice et soit n_t la longueur du code défini par la matrice $\mathbf{H}_t$.

Définition 4.13. *La* fonction d'écart des rangs *D de la suite de matrices stabilisatrices $(\mathbf{H}_t)_t$ est la fonction : $D(p) = \limsup_t \Delta_t(p)$ où*

$$\Delta_t(p) = \frac{\mathbb{E}_p[\operatorname{rg}\mathbf{H}_{t,\bar{\mathcal{E}}} - \operatorname{rg}\mathbf{H}_{t,\mathcal{E}}]}{n_t}.$$

Théorème 4.14. *Les rendements atteignables R par une suite de codes stabilisateurs de matrices $(\mathbf{H}_t)_{t\in\mathbb{N}}$, sur le canal à effacement quantique de probabilité p, vérifient :*

$$R \leq 1 - 2p - D(p).$$

où D est la fonction d'écart des rangs de la suite de matrices stabilisatrices $(\mathbf{H}_t)_t$.

Démonstration. Nous voulons appliquer l'inégalité de Fano classique. Pour des rappels de théorie de l'information classique voir [34]. Rappelons cette inégalité qui permet d'obtenir une borne inférieure sur la probabilité d'erreur après décodage. Soient X, Y et $\hat{X}$ trois variables aléatoires telles que $\hat{X}$ ne dépend que de Y. Cette variable aléatoire $\hat{X}$ doit être comprise comme une estimation de X. Alors l'inégalité de Fano affirme que la probabilité d'erreur après décodage vérifie :

$$P_{err} := \mathbb{P}(\hat{X} \neq X) \geq \frac{H(X|Y) - 1}{\log(|\mathcal{X}|)}.$$

où X et $\hat{X}$ sont à valeur dans $\mathcal{X}$.

Avec le canal à effacement quantique, le vecteur effacement est une variable aléatoire $\mathcal{E}$ telle que $\mathbb{P}(\mathcal{E} = v) = p^{|v|}(1-p)^{n-|v|}$. La variable aléatoire erreur E est

alors uniformément distribuée parmi les erreurs dont le support est inclus dans $\mathcal{E}$. Nous appliquons la borne de Fano dans le cas ou X est l'information nécessaire pour retrouver l'état d'origine, c'est-à-dire la classe $E.S$ de l'erreur de Pauli E qui survient. La variable Y est le couple $(\mathcal{E}, \sigma(E))$ où $\mathcal{E}$ est le vecteur effacement aléatoire et $\sigma(E)$ est le syndrome de E. C'est l'information que l'on peut mesurer sur l'erreur subie. La variable $\hat{X}$ est la meilleure estimation possible de X à partir de la connaissance de Y. La probabilité d'erreur P_{err} est donc la probabilité que $\hat{X}$ soit différent de X.

Dans notre cas, l'entropie conditionnelle s'écrit :

$$H(X|\mathcal{E}, \Sigma) = \sum_{v,y} \mathbb{P}\Big((\mathcal{E}, \Sigma) = (v, y)\Big) H(X|\mathcal{E} = v, \Sigma = y).$$

Le membre de droite est calculé dans le lemme 4.15 :

$$H(X|\mathcal{E} = v, \Sigma = y) = 2|v| - \operatorname{rg} \mathbf{H} + \operatorname{rg} \mathbf{H}_{\bar{v}} - \operatorname{rg} \mathbf{H}_v$$

Nous pouvons remarquer que la quantité $H(X|\mathcal{E} = v, \Sigma = y)$ est indépendante de y, ainsi nous obtenons :

$$\begin{aligned} H(X|\mathcal{E}, \Sigma) &= \sum_v \mathbb{P}(\mathcal{E} = v)\Big(2|v| - \operatorname{rg} \mathbf{H} - \operatorname{rg} \mathbf{H}_v + \operatorname{rg} \mathbf{H}_{\bar{v}}\Big) \\ &= 2np - \operatorname{rg} \mathbf{H} + \mathbb{E}_p(\operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}} - \operatorname{rg} \mathbf{H}_{\mathcal{E}}). \end{aligned}$$

La variable aléatoire $X = E.S$ est à valeur dans le groupe quotient $\mathcal{X} = \mathcal{P}_n/S$. Ce groupe est composé de $|\mathcal{X}| = 2^{2n - \operatorname{rg} \mathbf{H}}$ classes. En majorant $2n - \operatorname{rg} \mathbf{H}$ par $2n$ dans l'inégalité de Fano, nous trouvons :

$$P_{err} \geq \frac{2np - \operatorname{rg} \mathbf{H} + \mathbb{E}_p(\operatorname{rg} \mathbf{H}_{\bar{\mathcal{E}}} - \operatorname{rg} \mathbf{H}_{\mathcal{E}}) - 1}{2n}$$

Le rendement du code quantique est $R = 1 - \operatorname{rg} \mathbf{H}/n$. Si la probabilité d'erreur tend vers zéro, alors la suite des rendements de la famille de codes satisfait l'inégalité :

$$\limsup R \leq 1 - 2p - D(p).$$

□

Lemme 4.15. *Soit S un groupe stabilisateur de matrice $\mathbf{H}$. L'entropie conditionnelle de $X = E.S$ étant donné $\mathcal{E} = v$ et $\Sigma = y$ est :*

$$H(X|\mathcal{E} = v, \Sigma = y) = 2|v| - \operatorname{rg} \mathbf{H} + \operatorname{rg} \mathbf{H}_{\bar{v}} - \operatorname{rg} \mathbf{H}_v,$$

lorsque la probabilité d'avoir $\mathcal{E} = v$ et $\Sigma = y$ est non nulle.

Démonstration. Rappelons que, étant donné un effacement $\mathcal{E}$, la distribution de E est uniforme parmi les erreurs à support dans $\mathcal{E}$. Donc la probabilité d'une classe $E.S$, connaissant l'effacement $\mathcal{E} = v$ et le syndrome $\Sigma = y$ est :

$$\mathbb{P}(X = E.S|\mathcal{E} = v, \Sigma = y) = \frac{|\{P \in E.S \mid P \subset v, \sigma(P) = y\}|}{|\{P \in \mathcal{P}_n \mid P \subset v, \sigma(P) = y\}|}.$$

Lorsque cette probabilité n'est pas nulle, on peut supposer, par linéarité, que le syndrome est $y = 0$. En effet, il suffit de multiplier par un opérateur de Pauli $T \subset v$ de syndrome y pour se ramener à ce cas. L'ensemble qui apparaît au dénominateur est alors le sous-groupe $N(S)_{\mathcal{E}}$, tandis que le numérateur est une classe du sous-groupe S_v. Des lemmes 4.11 et 4.12 on déduit :

$$\mathbb{P}(X = E.S|\mathcal{E} = v, \Sigma = y) = \frac{|S_v|}{|N(S)_v|} = 2^{-2|v|+\operatorname{rg}\mathbf{H}-\operatorname{rg}\mathbf{H}_{\bar{v}}+\operatorname{rg}\mathbf{H}_v},$$

d'où la formule annoncée pour l'entropie conditionnelle :

$$H(X|\mathcal{E} = v, \Sigma = y) = 2|v| - \operatorname{rg}\mathbf{H} + \operatorname{rg}\mathbf{H}_{\bar{v}} - \operatorname{rg}\mathbf{H}_v.$$

□

Le corollaire suivant prouve l'efficacité de notre méthode. Nous retrouvons la borne supérieure donnée par la capacité du canal à effacement quantique [10]. Cette borne s'obtient uniquement à partir d'arguments combinatoires sur les propriétés des codes stabilisateurs. Elle ne nécessite pas l'intervention du théorème de non-clonage.

Corollaire 4.16. *Les rendements atteignables R par une suite de codes stabilisateurs de matrices $(\mathbf{H}_t)_{t\in\mathbb{N}}$, sur le canal à effacement quantique de probabilité p, vérifient :*

$$R \leq 1 - 2p,$$

lorsque $p \leq 1/2$.

Démonstration. Pour démontrer ce corollaire, il suffit de remarquer que $\Delta_t(p)$ est positif lorsque $p \leq 1/2$. Observons que l'on peut écrire Δ_t comme :

$$\Delta_t(p) = \phi_t(1-p) - \phi_t(p),$$

où $\phi_t(p) = \mathbb{E}_p(\operatorname{rg}\mathbf{H}_{t,\mathcal{E}})/n_t$. Intuitivement, il est clair que ϕ_t est une fonction croissante de p. Ceci sera démontré dans la proposition 4.19. Le corollaire suit. □

4.3 Le rang d'une sous-matrice aléatoire

Le but de cette section est d'étudier la fonction $\phi(p) = \frac{1}{n}\mathbb{E}_p(\operatorname{rg}\mathbf{H}_{\mathcal{E}})$ qui apparaît dans la borne supérieure sur le rendement des codes stabilisateurs. Ces résultats permettront de conclure la preuve de la borne obtenue au corollaire 4.16. Nous allons aussi établir la concavité de cette fonction. Ce travail prépare le prochain chapitre qui précise cette borne sur le rendement des codes stabilisateurs dans le cas des codes LDPC quantiques.

La propriété clé de cette partie est la sous-modularité du rang :

Lemme 4.17. *Soit $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ une matrice de Pauli à n colonnes. La fonction rang :*

$$\begin{aligned}\mathcal{P}(\{1,2,\ldots,n\}) &\longrightarrow \mathbb{N}\\ A &\longmapsto \operatorname{rg}(A) = \operatorname{rg}(\mathbf{H}_A)\end{aligned}$$

est une fonction sous-modulaire. *C'est-à-dire, le rang satisfait l'inégalité suivante :*

$$\mathrm{rg}(A \cap B) + \mathrm{rg}(A \cup B) \leq \mathrm{rg}(A) + \mathrm{rg}(B).$$

Ce lemme recouvre aussi le cas d'une matrice binaire qui sera utile pour travailler sur les codes CSS. Ces propriétés du rang peuvent être obtenues dans le contexte, plus général, des matroïdes. Deux références classiques sur ce sujet sont [76] et [96]. Ces liens entre sous-modularité et convexité ont été étudiés par Lovász [68].

Démonstration. Nous allons prouver cette propriété pour une matrice binaire. Ensuite, nous expliquerons comment en déduire le cas quaternaire.

Soit A et B deux sous-ensembles de l'ensemble $\{1, 2, \ldots, n\}$. La formule de la dimension de la somme de deux sous-espaces vectoriels nous donne :

$$\begin{cases} \mathrm{rg}(A \cup B) = \mathrm{rg}(A) + \mathrm{rg}(B \backslash A) - \dim(\mathrm{Im}\, H_A) \cap (\mathrm{Im}\, H_{B\backslash A}) \\ \mathrm{rg}(A \cup B) = \mathrm{rg}(B) + \mathrm{rg}(A \backslash B) - \dim(\mathrm{Im}\, H_B) \cap (\mathrm{Im}\, H_{A\backslash B}) \\ \mathrm{rg}(A \cap B) = \mathrm{rg}(A) - \mathrm{rg}(A \backslash B) + \dim(\mathrm{Im}\, H_{A\cap B}) \cap (\mathrm{Im}\, H_{A\backslash B}) \\ \mathrm{rg}(A \cap B) = \mathrm{rg}(B) - \mathrm{rg}(B \backslash A) + \dim(\mathrm{Im}\, H_{A\cap B}) \cap (\mathrm{Im}\, H_{B\backslash A}) \end{cases}$$

Regardons les derniers termes de ces inégalités. L'inclusion $\mathrm{Im}\, H_{A\cap B} \subset \mathrm{Im}\, H_A$ est claire, l'espace $(\mathrm{Im}\, H_{A\cap B}) \cap (\mathrm{Im}\, H_{B\backslash A})$ est donc un sous-espace de $(\mathrm{Im}\, H_A) \cap (\mathrm{Im}\, H_{B\backslash A})$. Ce qui prouve l'inégalité suivante :

$$\dim(\mathrm{Im}\, H_{A\cap B}) \cap (\mathrm{Im}\, H_{B\backslash A}) \leq \dim(\mathrm{Im}\, H_A) \cap (\mathrm{Im}\, H_{B\backslash A}).$$

Ce résultat reste vrai en échangeant les rôles de A et B. En sommant les quatre inégalités et en appliquant l'inégalité précédente, nous obtenons le résultat souhaité :

$$\mathrm{rg}(A \cap B) + \mathrm{rg}(A \cup B) \leq \mathrm{rg}(A) + \mathrm{rg}(B).$$

Pour démontrer cette propriété dans le cas d'une matrice à coefficients dans $\mathcal{P}_1$, il suffit de démontrer que les outils d'algèbre linéaire nécessaires à la preuve sont encore disponibles avec une matrice quaternaire $\mathbf{H}$.

Comme nous l'avons rappelé dans le chapitre d'introduction, le groupe de Pauli $\mathcal{P}_n$ est muni d'une structure de $\mathbb{F}_2$-espace vectoriel. Il est isomorphe à $\mathbb{F}_2^{2n}$. On peut ainsi regarder la matrice $\mathbf{H} \in \mathcal{M}_{r,n}(\mathcal{P}_1)$, comme une matrice binaire $[H^X|H^Z] \in \mathcal{M}_{r,2n}(\mathbb{F}_2)$. Le rang de cette matrice est $\mathrm{rg}\,\mathbf{H} = \mathrm{rg}[H^X|H^Z]$ et le rang d'une sous-matrice de $\mathbf{H}$ s'écrit :

$$\mathrm{rg}\,\mathbf{H}_{\mathcal{E}} = \mathrm{rg}[H^X_{\mathcal{E}}|H^Z_{\mathcal{E}}].$$

Cette remarque permet d'adapter la preuve au cas des matrices quaternaires $\mathbf{H}$. □

Pour étudier les dérivées de ϕ, nous utilisons une fonction Φ, dépendant de n variables $x = (x_1, x_2, \ldots, x_n) \in [0, 1]^n$ définie par :

$$\Phi(x_1, x_2, \ldots, x_n) = \sum_{\mathcal{E}\in\mathbb{F}_2^n} \left[(\mathrm{rg}\,\mathbf{H}_{\mathcal{E}}) \left(\prod_{\mathcal{E}_i=1} x_i \right) \left(\prod_{\mathcal{E}_i=0} (1 - x_i) \right) \right].$$

Cette fonction peut être vue comme l'espérance du rang $\mathbb{E}_x(\mathrm{rg}\,\mathbf{H}_{\mathcal{E}})$ pour la loi de probabilité telle que la i-ème composante de e est 1 avec probabilité x_i et 0 avec probabilité $1-x_i$, indépendamment des autres composantes. Cette fonction polynomiale est indéfiniment dérivable et ses dérivées partielles satisfont :

Lemme 4.18. *Pour tout x de $[0,1]^n$, on a :*

$$\frac{\partial \Phi}{\partial x_i}(x) \geq 0, \qquad \forall i \in \{1, 2, \ldots, n\},$$

$$\frac{\partial^2 \Phi}{\partial x_i \partial x_j}(x) \leq 0, \qquad \forall i, j \in \{1, 2, \ldots, n\}.$$

Démonstration. Soit x un élément de $[0,1]^n$. On peut remarquer que Φ est affine en chacune de ses variables. Ses dérivées partielles vérifient donc :

$$\begin{aligned}
\frac{\partial \Phi}{\partial x_i}(x) &= \Phi(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) - \Phi(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \\
&= \mathbb{E}_x(\mathrm{rg}(\mathcal{E} \cup \{i\}) - \mathbb{E}_x(\mathrm{rg}(\mathcal{E} \backslash \{i\}) \\
&= \mathbb{E}_x\Big(\mathrm{rg}(\mathcal{E} \cup \{i\}) - \mathrm{rg}(\mathcal{E} \backslash \{i\} \Big) \\
&\geq 0.
\end{aligned}$$

Dans les expressions précédentes, le vecteur $\mathcal{E} \in \mathbb{F}_2^n$ est considéré comme un sous-ensemble de $\{1, 2, \ldots n\}$. Fixer $x_i = 1$ revient à remplacer le sous-ensemble $\mathcal{E}$ par $\mathcal{E} \cup \{i\}$ et fixer $x_i = 0$ est équivalent à considérer le sous-ensemble $\mathcal{E} \backslash \{i\}$.

Soit j un entier compris entre 1 et n tel que $j \neq i$. La dérivée partielle $\frac{\partial \mathcal{E}}{\partial x_i}(x)$ est aussi une fonction affine de la j-ème variable. On peut donc la dériver suivant le même procédé. On trouve :

$$\begin{aligned}
\frac{\partial^2 \Phi}{\partial x_j \partial x_i}(x) &= \frac{\partial}{\partial x_j} \frac{\partial \Phi}{\partial x_i}(x) \\
&= \mathbb{E}_x(\mathrm{rg}(\mathcal{E} \cup \{i, j\})) - \mathbb{E}_x(\mathrm{rg}(\mathcal{E} \cup \{i\} \backslash \{j\})) \\
&- \mathbb{E}_x(\mathrm{rg}(\mathcal{E} \cup \{j\} \backslash \{i\})) + \mathbb{E}_x(\mathrm{rg}(\mathcal{E} \backslash \{i, j\})) \\
&= \mathbb{E}_x\left[\mathrm{rg}(A_i \cup A_j) - \mathrm{rg}(A_i) - \mathrm{rg}(A_j) + \mathrm{rg}(A_i \cap A_j)\right] \\
&\leq 0
\end{aligned}$$

L'ensemble A_i est le sous-ensemble $\mathcal{E} \cup \{i\} \backslash \{j\}$ et A_j est le sous-ensemble $e \cup \{j\} \backslash \{i\}$. Cette quantité est négative par la sous-modularité prouvée lors du lemme 4.17 Lorsque $j = i$, la dérivée partielle seconde est nulle. □

Proposition 4.19. *Soit $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ une matrice de Pauli à n colonnes. La fonction $\phi(p) = \mathbb{E}_p(\mathrm{rg}\, \mathbf{H}_\mathcal{E})$ est une fonction croissante sur l'intervalle $[0,1]$.*

Démonstration. La fonction ϕ est la composée $\Phi \circ i$ de F et de l'injection i de $[0,1]$ dans $[0,1]^n$ qui envoie p sur le vecteur $(p, p \ldots, p)$. Les dérivées de ϕ s'expriment donc en fonction des dérivées partielles de Φ :

$$\phi'(p) = \sum_{i=1}^{n} p \frac{\partial \Phi}{\partial x_i}(i(p)).$$

D'après le lemme 4.18, cette quantité est toujours positive. □

Proposition 4.20. *Soit* $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ *une matrice de Pauli à* n *colonnes. La fonction* $\phi(p) = \mathbb{E}_p(\operatorname{rg} \mathbf{H}_{\mathcal{E}})$ *est une fonction concave sur l'intervalle* $[0, 1]$.

Démonstration. En conservant les mêmes notations que dans la preuve de la proposition 4.19, nous obtenons :

$$\phi''(p) = \sum_{i,j=1}^{n} p^2 \frac{\partial^2 \Phi}{\partial x_i \partial x_j}(i(p))$$

Le lemme 4.18 nous assure que cette quantité est toujours négative, d'où la concavité de ϕ. □

Proposition 4.21. *Soit* $\mathbf{H} \in M_{r,n}(\mathcal{P}_1)$ *une matrice de Pauli à* n *colonnes. Supposons que* $\phi(p) = \frac{1}{n}\mathbb{E}_p(\operatorname{rg} \mathbf{H})$ *est bornée supérieurement par* $M(p)$. *Alors, la fonction* $\Delta(p) = \phi(1-p) - \phi(p)$ *admet une borne inférieure :*

$$\Delta(p) \geq \left(\frac{1-2p}{1-p}\right)\left(\frac{\operatorname{rg} \mathbf{H}}{n} - M(p)\right).$$

Démonstration. Il suffit d'utiliser la concavité de ϕ. En effet, par concavité, le point $(1-p, \phi(1-p))$ est au dessus du segment joignant $(p, \phi(p))$ et $(1, \phi(1))$, de sorte que :

$$\phi(1-p) \geq \phi(p) + (1-2p)\left(\frac{\phi(1) - \phi(p)}{1-p}\right).$$

L'inégalité suit, en utilisant la valeur de $\phi(1) = \operatorname{rg} \mathbf{H}/n$ et la borne supérieure : $\phi(p) \leq M(p)$. □

Conclusion

- Nous avons obtenu une borne supérieure sur les rendements atteignables des codes stabilisateurs sur le canal à effacement quantique. Pour cela nous avons démontré que la borne de Hachage ne peut pas être dépassée en utilisant la dégénérescence des codes stabilisateurs. On retrouve ainsi la borne supérieure de non-clonage dans le cas des codes stabilisateurs de manière purement combinatoire.
- Notre borne supérieure sur les rendements atteignables des codes stabilisateurs sur le canal à effacement quantique est plus précise que la borne de non-clonage. La fonction d'écart des rangs que nous avons introduite à la définition 4.13 mesure la distance à la capacité du rendement d'une famille de codes stabilisateurs. Dans le chapitre 5, nous étudions la fonction d'écart des rangs de familles de codes LDPC quantiques. Nous démontrerons que ces codes n'atteignent pas la capacité du canal à effacement quantique.
- La détermination de la capacité du canal de dépolarisation est l'un des grands problèmes ouverts de la théorie de l'information quantique. Les outils combinatoires développés ici offrent une nouvelle approche de ce problème et de la

notion de dégénérescence. Le passage au canal de dépolarisation semble difficile car la probabilité d'apparition d'une erreur de Pauli dépend de son poids. Pour avancer dans cette direction, nous devons considérer les erreurs typiques.

Chapitre 5

Bornes supérieures sur les performances des codes LDPC quantiques

Les codes LDPC fournissent l'une des réponses les plus satisfisantes au problème de la transmission d'information sur un canal bruyant. Ils ont été introduits par Gallager dans sa thèse [49]. Il a démontré que ces codes permettent d'approcher la capacité du canal binaire symétrique en obtenant des bornes inférieures sur leurs performances. Il a aussi prouvé que ces codes n'atteignent pas la capacité de ce canal en établissant des bornes supérieures sur les performances des codes LDPC quantiques réguliers.

La généralisation quantique de ces bornes sur les codes LDPC n'a pas été étudiée jusqu'à présent. Dans la première partie de ce chapitre nous résumons la stratégie de Gallager ainsi que les travaux qui ont suivi. Nous démontrons dans la partie 5.2 que les codes stabilisateurs définis par une matrice stabilisatrice dont les lignes sont de poids borné par un entier m n'atteignent pas la capacité du canal à effacement quantique. Plus précisément, les rendements atteignables R de ces codes LDPC quantiques sont majorés par :

$$R \leq (1-2p)\frac{1-(1-p)^{m-1}}{1-(1-2p)(1-p)^{m-1}},$$

sur le canal à effacement quantique de probabilité p. Ce résultat s'applique aux codes de surface et aux codes couleur. Il nous donne une condition nécessaire pour atteindre la capacité du canal : certaines lignes de la matrice stabilisatrice doivent avoir un poids croissant. Les deux parties suivantes précisent cette borne dans le cas des codes CSS LDPC réguliers. Ces codes CSS sont définis par des matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$ de type (ℓ, m), c'est-à-dire dont les lignes sont de poids m et les colonnes sont de poids ℓ. Nous traitons en premier lieu le cas des codes CSS de type $(2, m)$, qui englobe la famille des codes de surface, dans la section 5.3. Cette partie est basée sur une interprétation graphique du rang d'une matrice. La généralisation aux codes CSS de type (ℓ, m) est présentée dans la partie 5.4. Les résultats de cette section sont obtenus en passant des graphes aux hypergraphes. Enfin, la dernière section est la transcription de ces bornes sur les rendements atteignables en bornes sur le

seuil d'effacement tolérable des codes LDPC quantiques réguliers. Ces bornes sont appliquées à l'étude du seuil de percolation des graphes hyperboliques au cours du chapitre 6.

Les résultats de ce chapitre ont donné lieu à l'article [37] en commun avec Gilles Zémor.

5.1 Borne supérieure de Gallager sur les codes LDPC classiques

Gallager a introduit les codes LDPC au début des années 60, lors de sa thèse [49]. Il proposait alors de construire des codes binaires dont la matrice de parité contient exactement ℓ coefficients 1 par colonne et m coefficients 1 par ligne. Ces codes sont dit *de type* (ℓ, m), ce sont des *codes LDPC réguliers*. Gallager a étudié les performances de ces codes en encadrant le seuil d'erreur tolérable sur le canal binaire symétrique. Ce seuil est la probabilité p du canal qui est maximale telle que la probabilité d'erreur après décodage tend vers 0. Ce résultat prouve que les performances des codes de Gallager sont proches de la capacité du canal mais ne l'atteignent pas. Leur rendement ne peut pas dépasser une fraction de la capacité du canal.

La borne supérieure de Gallager sur les performances des codes LDPC réguliers est basée sur la remarque suivante : le nombre de syndromes typiques de vecteurs reçus par le canal binaire symétrique est légèrement plus faible lorsque l'on travaille avec des codes LDPC. Plus précisément, supposons que l'on utilise une matrice de parité H dont les lignes sont de poids m. La i-ème composante s_i du syndrome $s = He^t$ du vecteur erreur e vaut 1 avec probabilité :

$$\mathbb{P}(s_i = 1) = \sum_{\substack{k=0 \\ kimpair}}^{m} \binom{m}{k} p^k (1-p)^{n-k}$$

où p est la probabilité du canal binaire symétrique. En effet, cette composante du syndrome est 1, si et seulement si le support du vecteur erreur e a une intersection impaire avec le support de la i-ème ligne de H. Comme cette ligne est de poids m, on obtient bien la probabilité annoncée.

Pour résumer, Gallager analyse l'entropie du syndrome d'une erreur aléatoire pour un code linéaire quelconque et il remarque que cette entropie est légèrement plus faible lorsque l'on se restreint aux codes LDPC. Il y a donc typiquement moins de syndromes différents et on peut donc corriger moins d'erreurs. Lorsque le nombre d'erreurs typiques dépasse le nombre de syndromes typiques, la probabilité d'erreur après décodage ne peut pas tendre vers 0.

Cette borne a ensuite été généralisée à d'autres canaux et a été précisée par Burshtein, Krivelevich, Litsyn, Miller et Barak, Burshtein, Feder [6, 26]. On ne peut donc pas atteindre la capacité du canal binaire symétrique en se restreignant à des lignes de poids borné. Pour se rapprocher de la capacité du canal, MacKay et Neal ont généralisé les codes de Gallager en conservant des matrices de parité creuses mais en assouplissant les conditions de régularité sur les lignes. Ils ont alors démontré que cette famille élargie de codes LDPC atteint la capacité du canal binaire

symétrique [71, 72]. Richardson, Shokrollahi et Urbanke [82] et Luby, Mitzenmacher et Shokrollahi [69] ont ensuite étudié les performances des codes LDPC en fonction de la distribution des poids des lignes et des colonnes. Ils décrivent les caractéristiques nécessaires sur la distribution des poids des lignes et des colonnes pour atteindre la capacité du canal à effacement. La ressemblance entre le canal à effacement et le canal binaire symétrique permet de transférer ces résultats au cas du canal binaire symétrique.

Nous nous intéressons dans ce chapitre à la généralisation de la borne supérieure de Gallager aux codes LDPC quantiques réguliers. En suivant l'évolution de la théorie classique, nous travaillons sur le canal à effacement quantique. Notre objectif est de démontrer que les codes LDPC quantiques réguliers n'atteignent pas la capacité du canal à effacement quantique. Nous commencerons par le cas des codes stabilisateurs LDPC, puis des codes CSS de type $(2, m)$ et nous généraliserons ces bornes aux cas des codes CSS de type (ℓ, m). Ces bornes s'appliquent notamment aux codes couleur et aux codes de surface. Nous en déduirons des conditions nécessaires pour atteindre la capacité du canal à effacement quantique avec des codes LDPC.

5.2 Le cas des codes stabilisateurs LDPC

Notre but est ici de préciser la borne obtenue lors du corollaire 4.16 en déterminant des bornes inférieures sur $\Delta(p)$ et $D(p)$. Ceci ne peut pas être fait pour l'ensemble des codes stabilisateurs car ils atteignent la capacité du canal à effacement. L'expérience classique nous permet d'imaginer que ce n'est plus le cas si l'on se restreint à des groupes stabilisateurs engendrés par des opérateurs de poids borné, c'est-à-dire des matrices stabilisatrices creuses. Le résultat principal de cette section est le théorème 5.1 qui borne les rendements atteignables des codes stabilisateurs LDPC en fonction du poids maximal des lignes des matrices stabilisatrices. Ces rendements sont bien séparés de la capacité du canal à effacement quantique.

Nous avons vu, à la fin du chapitre 3, que l'on peut déduire une borne inférieure sur Δ d'une borne supérieure sur ϕ par concavité. C'est la proposition 4.21. Pour obtenir une telle borne inférieure sur le rang moyen d'une sous-matrice aléatoire $\mathbf{H}_\mathcal{E}$ de $\mathbf{H}$, on regarde le nombre moyen de lignes nulles de cette sous-matrice.

Théorème 5.1. *Soit $(\mathbf{H}_t)_t$ une famille de matrices stabilisatrices dont les lignes sont de poids inférieur à m, définissant des codes stabilisateurs de rendement tendant vers R. Si la probabilité d'erreur après décodage sur le canal à effacement quantique de probabilité p tend vers 0, alors on a :*

$$R \leq (1-2p)\frac{1-(1-p)^{m-1}}{1-(1-2p)(1-p)^{m-1}}.$$

Démonstration. Nous cherchons une borne supérieure sur :

$$\phi_t(p) = \frac{\mathbb{E}_p(\operatorname{rg} \mathbf{H}_{t,\mathcal{E}})}{n}.$$

Dans la suite de cette preuve, nous omettons l'indice t dans $\mathbf{H} = \mathbf{H}_t$. Supposons que les lignes de la matrice $\mathbf{H}$ sont indépendantes. On s'intéresse au nombre $\mathbf{h}^0_\mathcal{E}$ de lignes

nulles dans la sous-matrice $\mathbf{H}_{\mathcal{E}}$. Chaque ligne de $\mathbf{H}_{\mathcal{E}}$ est nulle avec probabilité au moins $(1-p)^m$ car les lignes de $\mathbf{H}$ contiennent au plus m composantes non nulles. Par linéarité de l'espérance, le nombre moyen de lignes nulles vérifie :

$$\mathbb{E}(\mathbf{h}^0_{\mathcal{E}}) \leq (1-p)^m \operatorname{rg} \mathbf{H}.$$

On en déduit une borne supérieure sur le rang moyen de la sous-matrice $\mathbf{H}_{\mathcal{E}}$:

$$\begin{aligned}\phi_t(p) \leq & \frac{1}{n}\left[\operatorname{rg}\mathbf{H} - \mathbb{E}_p(\mathbf{h}^0_{\mathcal{E}})\right] \\ \leq & \frac{\operatorname{rg}\mathbf{H}}{n} - \frac{\operatorname{rg}\mathbf{H}}{n}(1-p)^m.\end{aligned}$$

En appliquant la borne de concavité de la proposition 4.21, nous obtenons :

$$\Delta(p) \geq \left(\frac{1-2p}{1-p}\right)\frac{\operatorname{rg}\mathbf{H}}{n}(1-p)^m \geq \frac{1-2p}{1-p}(1-R)(1-p)^m.$$

Le theoreme 4.14 s'applique alors et nous donne :

$$R \leq 1 - 2p - (1-R)(1-2p)(1-p)^{m-1}.$$

La preuve se termine en regroupant les termes convenablement. □

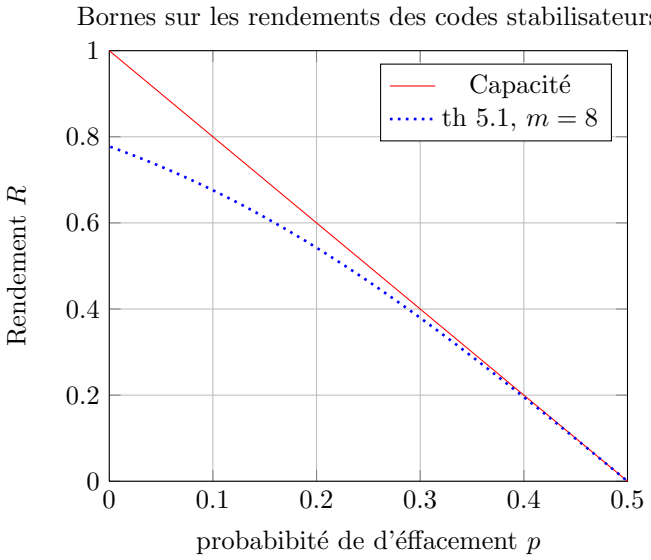


FIGURE 5.1 – En rouge, la capacité $1-2p$ du canal à effacement quantique de probabilité p. En bleu, la borne supérieure du théorème 5.1 sur les rendements atteignables des codes stabilisateurs définis par des matrices dont les lignes sont de poids $\leq m = 8$.

Par exemple, considérons la famille des codes couleur [17] dont la définition est rappelée dans la partie 2.2. Un code couleur est défini à partir d'un pavage de surface trivalent. Le poids des lignes de la matrice stabilisatrice est majoré par la longueur maximale d'une face du pavage. On peut donc appliquer le théorème 5.1 aux codes couleur définis à partir de surfaces dont les longueurs des faces sont bornées. La figure 5.1 représente la borne supérieure du théorème 5.1 appliquée à des codes stabilisateurs définis par des générateurs de poids inférieur à $m = 8$.

Nous allons maintenant améliorer le théorème 5.1.

5.3 Le cas des codes CSS de type $(2, m)$

Nous passons maintenant au cas des codes CSS. Un code CSS est dit *de type* $(2, m)$ s'il est défini par deux matrices binaires $\mathbf{H}_X$ et $\mathbf{H}_Z$ dont les colonnes sont de poids 2 et dont les lignes sont de poids m. C'est donc un code CSS défini par deux matrices de type $(2, m)$.

On peut voir ces codes comme une famille de codes de surface réguliers. En effet, les matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$ peuvent être regardées comme les matrices d'un pavage de surface. Les colonnes de ces matrices indexent les arêtes du graphe, les lignes de $\mathbf{H}_X$ définissent les sommets et les lignes de $\mathbf{H}_Z$ correspondent aux faces du complexe. Comme le poids des colonnes est 2, chaque arête contient exactement deux sommets et est à l'intersection de deux faces. Les conditions d'orthogonalité nous assurent que les faces sont des cycles du graphe. Le fait que les lignes sont de poids constant m fixe un degré m pour les sommets et une longueur m pour les faces.

L'existence d'un tel graphe n'est pas une propriété immédiate, et l'existence de familles de codes CSS de type $(2, m)$ de distance croissante l'est encore moins. En partant de la construction de pavages de surface réguliers, nous obtenons de tels codes quantiques dans la partie 6.3. Un exemple de surface de cette famille est dessiné figure 6.3 avec $m = 5$. Les matrices du code CSS associé à cette surface sont représentées figure 6.4.

5.3.1 Interprétation graphique du rang d'une sous-matrice

Rappelons que notre objectif est de déterminer une borne supérieure sur la fonction $\phi(p) = \mathbb{E}_p(\operatorname{rg} \mathbf{H}_\mathcal{E})/n$ pour une matrice stabilisatrice $\mathbf{H}$. Puisque nous travaillons maintenant avec des codes CSS, il est possible d'écrire cette fonction comme une somme :

$$\phi(p) = \phi_X(p) + \phi_Z(p),$$

où $\phi_X(p) = \mathbb{E}_p(\operatorname{rg} \mathbf{H}_{X,\mathcal{E}})/n$ et $\phi_Z(p) = \mathbb{E}_p(\operatorname{rg} \mathbf{H}_{Z,\mathcal{E}})/n$. Les deux matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$ sont des matrices $(2, m)$. Notre problème est donc de borner supérieurement le rang moyen d'une sous-matrice d'une matrice $(2, m)$ binaire.

Dans la suite de cette partie, nous notons $H \in \mathcal{M}_{r,n}$ une matrice binaire de type $(2, m)$. La sous-matrice aléatoire $H_\mathcal{E}$ est obtenue en prenant chaque colonne de H avec probabilité p, indépendamment des autres colonnes.

Le sous-graphe aléatoire $G_\mathcal{E}$: Comme ses colonnes sont de poids 2, nous pouvons regarder la matrice H comme la matrice d'incidence d'un graphe G. Ses sommets sont les éléments de $V = \{1, 2, \ldots, r\}$, i.e. les indices des lignes de la matrice H. Les arêtes du graphe sont définies par les colonnes de H. Chaque colonne de H contient exactement deux 1, les indices des lignes i et j de ces 1, définissent une arête $\{i, j\}$ dans le graphe G. Le poids constant m des lignes de H induit un graphe G qui est m-régulier, *i.e.* chaque sommet de G est de degré m.

Étant donné un vecteur aléatoire $\mathcal{E} \in \mathbb{F}_2^n$, nous notons $G_\mathcal{E}$ le sous-graphe de G de matrice d'incidence $H_\mathcal{E}$. Supposons que chaque composante de $\mathcal{E}$ est 1 avec probabilité p et 0 avec probabilité $1 - p$, indépendamment des autres composantes. Alors le graphe $G_\mathcal{E}$ est le sous-graphe de G de sommets $\{1, 2, \ldots, r\}$ et dont les arêtes

sont obtenues en prenant chaque arête de G avec probabilité p, indépendamment des autres arêtes. Autrement dit, choisir une sous-matrice aléatoire de H revient à choisir un sous-graphe aléatoire de G.

Le lemme suivant exprime le rang d'une sous-matrice en fonction du sous-graphe correspondant.

Lemme 5.2. *Si $H \in \mathcal{M}_{r,n}(\mathbb{F}_2)$ est une matrice $(2,m)$, alors $r - \operatorname{rg} H_{\mathcal{E}}$ est le nombre de composantes connexes $\kappa_{\mathcal{E}}$ du graphe $G_{\mathcal{E}}$, c'est-à-dire :*

$$\operatorname{rg} H_{\mathcal{E}} = r - \kappa_{\mathcal{E}}.$$

Ce résultat est une application de la proposition 2.2 qui calcule la dimension du code des cycles d'un graphe. En effet, la quantité $r - \operatorname{rg} H_{\mathcal{E}}$ est la dimension du code des cycles du graphe $G_{\mathcal{E}}$.

5.3.2 Nombre moyen de composantes connexes d'un graphe

D'après le lemme 5.2, le rang moyen de la sous-matrice $\mathbf{H}_{\mathcal{E}}$ s'exprime en fonction du nombre de composantes connexes du graphe $G_{\mathcal{E}}$:

$$\frac{\mathbb{E}_p(\operatorname{rg} H_{\mathcal{E}})}{n} = \frac{r}{n} - \frac{\mathbb{E}_p(\kappa_{\mathcal{E}})}{n} \tag{5.1}$$

Nous cherchons donc une borne inférieure sur la valeur moyenne de $\kappa_{\mathcal{E}}$. Si nous utilisons le fait que $\mathbb{E}_p(\kappa_{\mathcal{E}})$ est au moins le nombre de sommets isolés, nous retrouvons la borne du théorème 5.1 obtenue en comptant le nombre de lignes nulles de la sous-matrice. Nous allons obtenir une borne inférieure plus précise en énumérant des composantes connexes de plus grande taille.

Supposons que le graphe m-régulier G, construit à partir de la matrice H n'a pas de petit cycle. Il ressemble alors à l'arbre m-régulier G_m dans tout voisinage suffisamment petit d'un sommet. Nous introduisons donc le nombre a_k de sous-arbres de G_m, composés de k arêtes, qui contiennent un sommet fixé x de l'arbre G_m. Nous allons utiliser les méthodes issues de l'étude des séries génératrices. Deux références classiques sur ce sujet sont [45] et [97]. Le prochain paragraphe résume les propriétés de la série génératrice des a_k qui nous sont utiles ici.

La série génératrice des arbres enracinés : Soit G_m l'arbre m régulier et soit x un sommet fixé de G_m que nous appelons la racine de l'arbre. La série génératrice des sous-arbres enracinés de degré m est la fonction d'une variable réelle suivante :

$$T_m(z) = \sum_{k \geq 0} a_k z^k,$$

où a_k est le nombre de sous-arbres de G_m, composés de k arêtes et contenant la racine x.

Pour calculer cette série génératrice, nous utilisons une série génératrice auxiliaire :

$$T_m^1(z) = \sum_{k \geq 0} b_k z^k,$$

où b_k est le nombre de sous-arbres $\mathcal{T}$ de G_m possédant les propriétés suivantes :

– $\mathcal{T}$ est composé de k arêtes,
– la racine x est un sommet de $\mathcal{T}$,
– $\mathcal{T}$ contient une arête fixée $\{x, y\}$ parmi les arêtes incidentes à x, et aucune autre arête incidente à x n'est contenue dans $\mathcal{T}$.

Cette série génératrice ne dépend pas du choix de l'arête $\{x, y\}$ par régularité de l'arbre G_m. Cette fonction est parfois intitulée série génératrice des sous-arbres plantés, puisque x est un sommet de degré un dans ce sous-arbre.

Les coefficients b_k peuvent être calculés facilement grâce au théorème d'inversion de Lagrange car T_m^1 vérifie l'équation :

$$T_m^1(z) = z(1 + T_m^1(z))^{m-1}.$$

Cette formule provient du fait que chaque sommet de l'arbre, excepté la racine, possède $m - 1$ descendants. De sorte que le coefficient b_k est :

$$b_k = \frac{1}{k}\binom{k(m-1)}{k-1}.$$

Le calcul de la suite des a_k suit, grâce à l'expression de T_m en fonction de T_m^1.

$$T_m(z) = (1 + T_m^1(z))^m.$$

Pour démontrer cette formule, on remarque qu'un sous-graphe de G_m contenant la racine x se décompose en au plus m sous-arbres plantés de racine x. Cette méthode permet de calculer un grand nombre de coefficients a_k en utilisant un logiciel de calcul symbolique.

Nous pouvons désormais énoncer une borne supérieure sur le rang d'une sous-matrice $H_{\mathcal{E}}$ invoquant les nombres a_k. Rappelons que la maille d'un graphe est la longueur du plus petit cycle de ce graphe.

Proposition 5.3. *Soit H une matrice binaire de type $(2, m)$. Si la maille du graphe G de matrice d'incidence H est au moins $\delta + 2$, alors on a :*

$$\frac{\mathbb{E}_p(\operatorname{rg} H_{\mathcal{E}})}{n} \leq \frac{2}{m}\Big(1 - (1-p)^m S_\delta(p(1-p)^{m-2})\Big),$$

où $S_\delta(z) = \sum_{k=0}^{\delta} \frac{a_k}{k+1} z^k$ et les a_k sont les coefficients de la série génératrice T_m.

Démonstration. D'après l'équation (5.1) nous sommes à la recherche d'une borne inférieure sur le nombre de composantes connexes du graphe $G_{\mathcal{E}}$. Ce graphe est construit à partir de l'ensemble des arêtes de G en choisissant chaque arête, indépendamment, avec probabilité p. Déterminons, pour commencer, le nombre moyen de sommets isolés dans ce sous-graphe aléatoire, c'est-à-dire le nombre moyen de composantes de taille 0. Soit X_0 la variable aléatoire qui associe à un vecteur aléatoire $\mathcal{E}$, le nombre de sommets isolés dans le graphe $G_{\mathcal{E}}$. Cette variable aléatoire se décompose comme une somme $X_0(\mathcal{E}) = \sum_v X_v(\mathcal{E})$ avec $X_v(\mathcal{E}) = 1$ si le sommet v est isolé dans le graphe $G_{\mathcal{E}}$ et $X_v(\mathcal{E}) = 0$ sinon. Par linéarité de l'espérance, nous en déduisons que :

$$\mathbb{E}(X_0) = \sum_v \mathbb{E}(X_v) = \sum_v \mathbb{P}(X_v = 1) = |V|(1-p)^m.$$

En effet, chaque sommet est incident par m arêtes donc $\mathbb{P}(X_v = 1) = (1-p)^m$, quel que soit le sommet v.

Cette idée s'adapte au cas des composantes de taille $k \leq \delta$. Soit C un sous-graphe connexe de G composé de k arêtes et soit X_C la variable aléatoire qui vaut 1 lorsque C est une composante connexe du sous-graphe aléatoire $G_\mathcal{E}$ et qui vaut 0 sinon.

Le nombre moyen de composantes de taille k est

$$\mathbb{E}(X_k) = \sum_{\substack{C \text{ sous-graphe} \\ \text{connexe de taille } k}} \mathbb{E}(X_C) = \frac{|V|}{k+1} a_k (1-p)^m (p(1-p)^{m-2})^k.$$

Pour prouver cette égalité nous utilisons les deux lemmes suivants. D'après le lemme 5.4, l'espérance de X_C est $(1-p)^m(p(1-p)^{m-2})^k$, quel que soit ce sous-graphe à k arêtes. Ensuite le lemme 5.5 nous assure que le nombre de sous-graphes connexes C de taille k est $\frac{|V|}{k+1} a_k$. Le terme $|V|$ disparaît car $|V| = r$. Finalement, le quotient $\frac{r}{n}$ est exactement $\frac{2}{m}$ d'après le principe des bergers. Ceci termine la preuve de la proposition. □

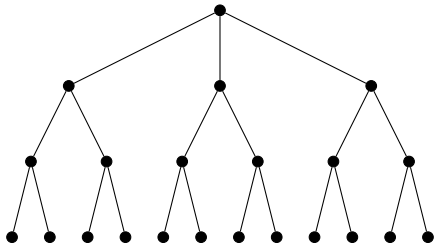


FIGURE 5.2 – Une boule de rayon 3 dans un graphe 3-régulier de maille au moins 7.

Lemme 5.4. *Soit G un graphe m-régulier de maille supérieure à $\delta + 2$. Si C est un sous-graphe connexe de G contenant k arêtes avec $k \leq \delta$, alors C est une composante connexe du graphe aléatoire $G_\mathcal{E}$ avec probabilité $(1-p)^m(p(1-p)^{m-2})^k$.*

Démonstration. Si $k = 0$, alors C est un sommet isolé. Cette composante apparaît dans le graphe aléatoire $G_\mathcal{E}$ avec probabilité $(1-p)^m$ car le graphe G est m-régulier. Supposons que la formule est satisfaite pour toute composante connexe de taille $k-1$ avec $k \leq \delta$. Un sous-graphe C de G de taille $k-1$ est inclus dans une boule de rayon $k-1$. Nous allons démontrer que la formule reste vraie lorsque l'on ajoute une arête à C. Soit x un sommet de C et soit $\{x, y\}$ une arête du graphe G qui n'est pas dans la composante C. On considère le sous-graphe $C' = C \cup \{x, y\}$. Il est composé de k arêtes. On note ∂C l'ensemble des arêtes de G ayant exactement une extrémité dans C. L'ensemble $\partial C'$ est défini de manière similaire. C'est le premier voisinage de C'. L'ensemble $\partial C'$ contient les arêtes de ∂C excepté l'arête $\{x, y\}$. De plus, il contient $m-1$ nouvelles arêtes : les arêtes $\{y, z\}$ avec $z \neq x$. Ces arêtes ne sont pas incluses dans l'ensemble ∂C. En effet, si $\{y, z\}$ appartient à ∂C, le graphe $C'' = C' \cup \{y, z\}$ contient $k+1$ arêtes et couvre un cycle. Pour voir qu'il couvre un cycle il suffit de remarquer qu'il reste connexe après la suppression de l'arête $\{y, z\}$. Ceci est impossible car la longueur du plus court cycle est au moins $\delta + 2$. La formule est donc satisfaite pour tout $k \leq \delta$. □

Lemme 5.5. *Soit G un graphe m-régulier de maille au moins $\delta + 2$. Le nombre de sous-graphes connexes de G composé de k arêtes, avec $k \leq \delta$, est au moins :*

$$\frac{|V|}{k+1} a_k.$$

où les nombres a_k sont les coefficients de la série génératrice T_m.

Démonstration. Étant donné un sommet y de G, le nombre de tels sous-graphes de G à k arêtes contenant le sommet y est aussi le nombre de sous-arbres de l'arbre m-régulier G_m possédant k arêtes et contenant la racine x de l'arbre. Ce nombre est a_k et ne dépend pas du sommet y. En faisant varier le sommet y, on compte ainsi tous les arbres et chaque sous-graphe est compté $k+1$ fois car il contient $k+1$ sommets. Le lemme s'en déduit. □

5.3.3 Rendements atteignables des codes CSS $(2, m)$

Soit $\mathbf{H} = \begin{pmatrix} \mathbf{H}_X \\ \mathbf{H}_Z \end{pmatrix}$ une matrice stabilisatrice d'un code CSS de type $(2, m)$. La maille du graphe associé à $\mathbf{H}_X$ est au plus m, puisque les lignes de $\mathbf{H}_Z$ définissent des cycles de longueur m du graphe. Le même raisonnement est valable dans le graphe dual, sa maille est donc aussi inférieure à m.

Nous transcrivons maintenant la borne supérieure de la proposition 5.3 en une borne inférieure sur la fonction d'écart des rangs $D(p)$ du théorème 4.14 pour une suite de codes CSS $(2, m)$.

Proposition 5.6. *La fonction d'écart des rangs d'une suite de codes CSS de type $(2, m)$ de maille $\delta + 2 \leq m$ vérifie :*

$$D(p) \geq \Big(\frac{1-2p}{1-p}\Big)\Big(\frac{4}{m} - \frac{4}{m}\Big(1 - (1-p)^m S_\delta(p(1-p)^{m-2})\Big)\Big),$$

où $S_\delta(z) = \sum_{k=0}^{\delta} \frac{a_k}{k+1} z^k$ et les nombres a_k sont les coefficients de la série génératrice T_m.

La condition $\delta + 2 \leq m$ est toujours satisfaite lorsque l'on considère des codes CSS de type $(2, m)$, car les vecteurs lignes de $\mathbf{H}_Z$, qui sont de poids m, définissent des cycles de longueur m du graphe de matrice d'incidence $\mathbf{H}_X$. Le même argument est valable dans le graphe de matrice d'incidence $\mathbf{H}_Z$ en utilisant les lignes de la matrice $\mathbf{H}_X$. La maille de ces deux graphes est donc bien majorée par m.

Démonstration. Pour obtenir ce résultat, il suffit d'appliquer la borne de concavité de la proposition 4.20. Pour cela nous avons besoin d'une borne supérieure sur $\phi(p) = \mathbb{E}(\mathrm{rg}(\mathbf{H}_\mathcal{E}))/n$. La proposition 5.3 nous fournit une telle borne en séparant les termes en X et les termes en Z : $\mathbb{E}(\mathrm{rg}(\mathbf{H}_{X,\mathcal{E}}))/n$ et $\mathbb{E}(\mathrm{rg}(\mathbf{H}_{Z,\mathcal{E}}))/n$. Le résultat suit. □

Finalement, la proposition 5.6 et le théorème 4.14 nous mènent au théorème suivant qui borne le rendement des codes CSS de type $(2, m)$.

Théorème 5.7. *Les rendements atteignables R par des codes CSS $(2, m)$ de maille $\delta + 2 \leq m$, sur le canal à effacement quantique de probabilité p, satisfont :*

$$R \leq (1-2p)\Big(\frac{4}{mp}\Big(1-(1-p)^m S_\delta(p(1-p)^{m-2})\Big)-1\Big).$$

où $S_\delta(z) = \sum_{k=0}^{\delta} \frac{a_k}{k+1} z^k$ et les nombres a_k sont les coefficients de la série génératrice T_m.

5.4 Le cas des codes CSS de type (ℓ, m)

Cette section est dévouée à la généralisation des résultats obtenus sur les codes CSS de type $(2, m)$ à des codes CSS définis par des matrices de poids quelconque ℓ. Nous avons choisi de détailler le cas $\ell = 2$ séparément pour plusieurs raisons. Tout d'abord, c'est un cas plus visuel, il rend donc les preuves plus lisibles, ensuite c'est le cas des codes de surface et il s'appliquera à la théorie de la percolation. Dans cette partie le rôle des graphes sera joué par des hypergraphes. Nous ne détaillerons pas les preuves qui sont des traductions immédiates du cas graphique de la section 5.3.

5.4.1 Interprétation hypergraphique du rang d'une sous-matrice

Dans le cas des codes LDPC de type (ℓ, m), nous utiliseront des hypergraphes ℓ-uniformes pour remplacer les graphes. Un tel hypergraphe G est défini par deux ensembles : $G = (V, E)$ avec V un ensemble fini de sommets et E un ensemble de parties de V. Les parties $e \in E$ de V sont les arêtes ou les hyperarêtes de l'hypergraphe G. Dans le cas où ces parties sont de cardinal 2, on retrouve la définition des graphes. Le terme ℓ-uniforme signifie que les arêtes de l'hypergraphe sont toutes composées de ℓ sommets. Un hypergraphe est m-régulier si chaque sommet est incident à exactement m arêtes. Nous allons commencer par adapter le lemme 5.2.

L'hypergraphe aléatoire $G_\mathcal{E}$: Un code LDPC de type (ℓ, m) est défini par une matrice de parité H dont les colonnes sont de poids ℓ et dont les lignes sont de poids m. Nous pouvons regarder cette matrice comme la matrice d'incidence d'un hypergraphe $G = (V, E)$. Les sommets de G sont les indices des lignes de la matrice H : $V = \{1, 2, \ldots, r\}$, et les arêtes correspondent aux colonnes de H. La j-ème colonne définit une arête composée des ℓ sommets i tels que $h_{i,j} = 1$. L'hypergraphe est m-régulier puisque les lignes sont de poids fixé m, et comme le poids des colonnes est ℓ, il est ℓ-uniforme. Tout comme dans le cas des graphes, choisir une sous-matrice aléatoire $H_\mathcal{E}$ est équivalent à choisir un hypergraphe aléatoire $G_\mathcal{E}$ de matrice d'incidence $H_\mathcal{E}$.

Lemme 5.8. *Soit $H \in \mathcal{M}_{r,n}(\mathbb{F}_2)$ et $\mathcal{E}$ un vecteur de $\mathbb{F}_2^n$. On note $C_\mathcal{E}^i = (V_\mathcal{E}^i, E_\mathcal{E}^i)$ les composantes connexes de l'hypergraphe G_e de matrice d'incidence H_e pour i variant de 1 à $\kappa_\mathcal{E}$. Le rang de $H_\mathcal{E}$ est majoré par :*

$$\operatorname{rg} H_\mathcal{E} \leq r - \sum_{|E_\mathcal{E}^i| < |V_\mathcal{E}^i|} (|V_\mathcal{E}^i| - |E_\mathcal{E}^i|).$$

Démonstration. La preuve graphique ne peut pas être généralisée ici. Nous considérons la décomposition en blocs de la matrice $H_{\mathcal{E}}$ correspondant à la décomposition en composantes connexes de $G_{\mathcal{E}}$.

Soit $C^i_{\mathcal{E}} = (V^i_{\mathcal{E}}, E^i_{\mathcal{E}})$ les composantes connexes de l'hypergraphe de matrice d'incidence $H_{\mathcal{E}}$. Une composante réduite à un sommet, c'est-à-dire un sommet isolé dans $G_{\mathcal{E}}$, correspond à une ligne nulle de la matrice $H_{\mathcal{E}}$. Lorsque la composante $C^i_{\mathcal{E}}$ n'est pas réduite à un sommet, nous lui associons le bloc $H^i_{\mathcal{E}}$ de $H_{\mathcal{E}}$, à l'intersection des lignes indexées par ses sommets et des colonnes qui définissent ses arêtes. Par construction, ces blocs n'ont, ni colonne, ni ligne en commun et $H_{\mathcal{E}}$ est nulle en dehors de ces blocs. Ainsi, le rang de $H_{\mathcal{E}}$ est la somme des rangs des blocs :

$$\operatorname{rg} H_{\mathcal{E}} = \sum_i \operatorname{rg} H^i_{\mathcal{E}}.$$

On a clairement : $\operatorname{rg} H^i_{\mathcal{E}} \leq \min\{|V^i_{\mathcal{E}}|, |E^i_{\mathcal{E}}|\}$, de sorte que :

$$\begin{aligned}\operatorname{rg} H_{\mathcal{E}} &\leq \sum_{|V^i_{\mathcal{E}}|<|E^i_{\mathcal{E}}|} |V^i_{\mathcal{E}}| + \sum_{|E^i_{\mathcal{E}}|<|V^i_{\mathcal{E}}|} \Big(|V^i_{\mathcal{E}}| - (|V^i_{\mathcal{E}}| - |E^i_{\mathcal{E}}|)\Big) \\ &= r - \sum_{|E^i_{\mathcal{E}}|<|V^i_{\mathcal{E}}|} (|V^i_{\mathcal{E}}| - |E^i_{\mathcal{E}}|).\end{aligned}$$

□

5.4.2 Nombre moyen de composantes connexes d'un hypergraphe

Cette section généralise l'énumération des petites composantes du graphe aléatoire décrite section 5.3.2.

Le graphe aléatoire devient un hypergraphe aléatoire $G_{\mathcal{E}}$. Dans la section 5.3.2, nous supposons que le graphe ne contient pas de petit cycle, de sorte que le graphe ressemble localement à un arbre. Pour obtenir un hypergraphe localement régulier, nous supposerons que son graphe de Tanner ne possède pas de petit cycle.

Le graphe de Tanner : Le graphe de Tanner associé à une matrice de parité H d'un code linéaire a été introduit dans la définition 1.20. Nous parlerons du graphe de Tanner associé à un hypergraphe G, c'est le graphe de Tanner de sa matrice d'incidence. Par définition, ce graphe de Tanner est le graphe biparti de sommets $V_1 \cup V_2$ où V_1 est l'ensemble des sommets de G et V_2 est l'ensemble des arêtes de G. Les sommets $x \in V_1$ et $y \in V_2$ sont liés par une arête dans le graphe de Tanner si et seulement si x et y sont incidents dans l'hypergraphe G. Un hypergraphe et son graphe de Tanner sont dessinés figure 5.3.

Un sous-graphe C de l'hypergraphe G est un sous-arbre s'il est connexe et si son graphe de Tanner ne contient pas de cycle. Si le graphe de Tanner de G ne contient pas de court cycle, alors l'hypergraphe est localement un cycle. Ceci nous permettra d'adapter la stratégie utilisée en travaillant avec des graphes. Nous considèrerons la maille du graphe de Tanner à la place de la maille du graphe.

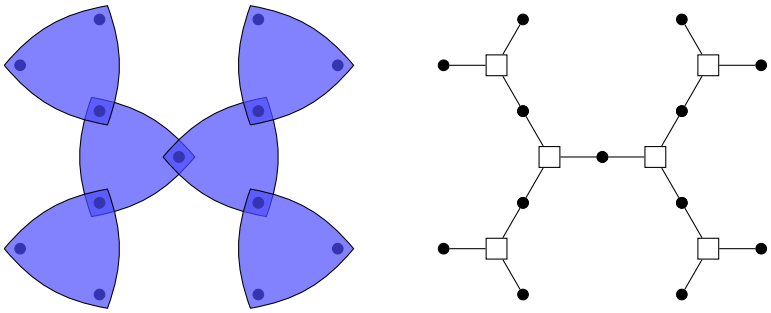


FIGURE 5.3 – A gauche : une boule de rayon 2 dans l'hyperarbre 2-régulier, 3-uniforme, dont le graphe de Tanner est de maille ≥ 10. A droite : son graphe de Tanner, les sommets carrés sont les sommets définis par les arêtes de l'hypergraphe.

Le second objet qui nous sera utile pour ce problème d'énumération est la généralisation de la série génératrice aux hypergraphes.

La série génératrice des hyperarbres enracinés : On note $G_{\ell,m}$ l'*hyperarbre* ℓ-uniforme de degré m. Dans cet hypergraphe, chaque arête est composée de ℓ sommets et chaque sommet est inclus dans m arêtes. On fixe un sommet privilégié x que l'on appellera la racine de $G_{\ell,m}$. Pour les hypergraphes, nous utiliserons la série génératrice $T_{\ell,m}$ des hyperarbres enracinés. C'est la fonction :

$$T_{\ell,m}(z) = \sum_{k\geq 0} a_k z^k,$$

avec a_k le nombre de sous-arbres de l'hyperarbre $G_{\ell,m}$, composés de k arêtes, et contenant la racine x.

Comme dans le cas graphique, cette fonction nous permettra de calculer un grand nombre des coefficients a_k qui apparaissent dans le théorème principal de cette partie. Rappelons brièvement les formules satisfaites par la fonction $T_{\ell,m}$. Il s'agit d'une traduction immédiate du cas graphique. La fonction $T_{\ell,m}$ s'exprime en fonction de la série génératrice $T^1_{\ell,m}$ comme :

$$T_m(z) = (1 + T^1_m(z))^m.$$

où la fonction $T^1_{\ell,m}$ est :

$$T^1_{\ell,m}(z) = \sum_{k\geq 0} \frac{1}{k} \binom{k(\ell-1)(m-1)}{k-1} z^k.$$

Cette méthode permet de calculer un grand nombre de coefficients a_k avec l'aide d'un logiciel de calcul symbolique. On peut noter que, lorsque $\ell = 2$, l'hypergraphe est un graphe et l'on retrouve la formule annoncée dans la section 5.3.2.

Proposition 5.9. *Si H est une matrice de parité (ℓ, m) d'un code dont le graphe de Tanner est un graphe de maille supérieure à $4\delta + 2$, alors on a :*

$$\frac{\mathbb{E}_p(\operatorname{rg} H_{\mathcal{E}})}{n} \leq \frac{\ell}{m}\Big(1 - (1-p)^m S_\delta(p(1-p)^{(\ell-1)(m-1)-1})\Big),$$

où $S_\delta(x) = \sum_{k=0}^{\delta} a_k \frac{(k(\ell-2)+1)}{k(\ell-1)+1} x^k$ *et les nombres* a_k *sont les coefficients de la série génératrice* $T_{\ell,m}$.

Démonstration. Dans le cas des codes $(2, m)$, il suffisait de calculer le nombre moyen de composantes connexes. Pour les hyperarbres, la tache est plus délicate car les sous-arbres auront une contribution différente au défaut de rang en fonction de leur taille. La présence d'un sous-arbre de taille k fera chuter le rang de $k(\ell-2)+1$. C'est la différence entre le nombre de ses sommets et le nombre de ses arêtes, d'après le lemme 5.12. Pour tout entier $k \leq \delta$, le nombre moyen de sous-arbres de taille k dans l'hypergraphe aléatoire $G_\mathcal{E}$ est :

$$\begin{aligned}\mathbb{E}(X_k) &= \sum_{\substack{C \text{ sous-graphe} \\ \text{connexe de taille } k}} \mathbb{E}(X_C) \\ &= a_k \frac{|V|}{k(\ell-1)+1}(1-p)^m (p(1-p)^{(\ell-1)(m-1)-1})^k.\end{aligned}$$

Ceci provient des lemmes 5.10 et 5.11, qui sont analogue aux lemmes cités dans le cas des graphes. Nous avons donc :

$$\frac{\mathbb{E}_p(\operatorname{rg} H_\mathcal{E})}{n} \leq 1 - \sum_{0}^{\delta} (k(\ell-2)+1) \frac{\mathbb{E}(X_k)}{|V|}.$$

□

Les lemmes suivants sont des transcriptions immédiates dans le contexte des hypergraphes des lemmes 5.4 et 5.5. Nous n'énoncerons pas les preuves puisque les variations sont mineures.

Lemme 5.10. *Soit* G *un hypergraphe* m*-régulier,* ℓ*-uniforme, dont le graphe de Tanner est de maille supérieure à* $4\delta + 2$. *Si* C *est un sous-graphe connexe de* G *composé de* $k \leq \delta$ *arêtes, alors* C *est une composante connexe de l'hypergraphe aléatoire* $G_\mathcal{E}$ *avec probabilité :* $(1-p)^m (p(1-p)^{(\ell-1)(m-1)-1})^k$.

Ce lemme coïncide avec le lemme 5.4 dans le cas où $\ell = 2$.

Lemme 5.11. *Soit* G *un hypergraphe* m*-régulier,* ℓ*-uniforme, dont le graphe de Tanner est de maille supérieure à* $4\delta + 2$. *Le nombre de sous-graphes connexes de* G *composés de* $k \leq \delta$ *arêtes est au minimum :*

$$\frac{|V|}{k(\ell-1)+1} a_k,$$

avec a_k *les coefficients de la série génératrice* $T_{\ell,m}$.

Lorsque $\ell = 2$, on retrouve le lemme 5.5.

Lemme 5.12. *Soit* C *un sous-graphe connexe, composé de* k *arêtes, inclus dans un hypergraphe* ℓ*-uniforme* G. *Si* C *est un arbre, alors on a :*

$$|V(C)| - |E(C)| = k(\ell-2) + 1.$$

Cette quantité vaut 1 lorsque $\ell = 2$. Ce lemme est particulier aux hypergraphes. Il prouve que différentes composantes peuvent avoir des contributions différentes au défaut de rang.

5.4.3 Rendements atteignables des codes CSS de type (ℓ, m)

Le théorème suivant englobe le cas des codes $(2, m)$ énoncé dans le théorème 5.7. La proposition 4.21 permet d'obtenir la borne suivante sur les rendements atteignables par des codes CSS LPDC réguliers.

Théorème 5.13. *Les rendements atteignables R des codes CSS de type (ℓ, m), de graphes de Tanner de mailles supérieures à $4\delta+2$, sur le canal à effacement quantique de probabilité p vérifient :*

$$R \leq (1-2p)\Big(\frac{2\ell}{mp}\Big(1-(1-p)^m S_\delta(p(1-p)^{(\ell-1)(m-1)-1})\Big)-1\Big)$$

avec $S_\delta(x) = \sum_{k=0}^{\delta} a_k \frac{(k(\ell-2)+1)}{k(\ell-1)+1} x^k$ et les nombres a_k sont les coefficients de la série génératrice $T_{\ell,m}$.

Dans l'énoncé de ce théorème, nous parlons des graphes de Tanner d'un code CSS. Ce sont les deux graphes de Tanner associés aux matrice $\mathbf{H}_X$ et $\mathbf{H}_Z$. La fonction S_δ n'est pas celle qui apparaît dans le théorème 5.7. C'est une généralisation qui dépend de ℓ.

5.5 Seuil d'effacement tolérable des codes LDPC quantiques

Dans cette partie, nous reformulons notre borne sur les rendements atteignables en une borne supérieure sur le seuil d'effacement tolérable par des codes LDPC quantiques réguliers.

La capacité du canal à effacement quantique est $1-2p$. Cela signifie que le rendement R d'une famille de codes quantiques, telle que la probabilité d'erreur après décodage tend vers 0 sur le canal à effacement quantique de probabilité p, vérifie $R \leq 1-2p$. On peut reformuler cette borne en fonction du *seuil d'effacement tolérable*. On se donne une famille de codes quantiques de rendement supérieur à R et on se demande quel est le taux d'effacement p maximum pour lequel la probabilité d'erreur après décodage tend vers 0. C'est le seuil d'effacement tolérable. Étant donné une famille de rendement supérieur à R, avec une probabilité d'erreur après décodage qui tend vers 0 sur le canal à effacement quantique de probabilité p, alors on a :

$$p \leq \frac{1-R}{2}.$$

On considère une famille de codes CSS de type $(2, m)$ définie par deux matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$ comptant chacune $2n/m$ lignes. Le nombre de qubits encodés est alors au moins $(1-4/m)n$. En utilisant la borne du théorème 5.7 et le fait que le rendement de ces codes est au moins $1-4/m$, on obtient :

Théorème 5.14. *Le seuil d'effacement tolérable d'une famille de codes CSS de type* $(2, m)$ *est majoré par la solution de l'équation :*

$$1 - \frac{4}{m} = (1-2p)\Big(\frac{4}{mp}\big(1-(1-p)^m S_{m-2}(p(1-p)^{(\ell-1)(m-1)-1})\big) - 1\Big)$$

où $p \in [0, 1/2]$.

Cette valeur est obtenue graphiquement à l'intersection de la représentation graphique de la borne supérieure sur le rendement du théorème 5.7 avec la droite d'équation $y = 1 - 4/m$ qui représente le rendement minimum de ces codes. Un exemple de ces courbes est tracé figure 5.4.

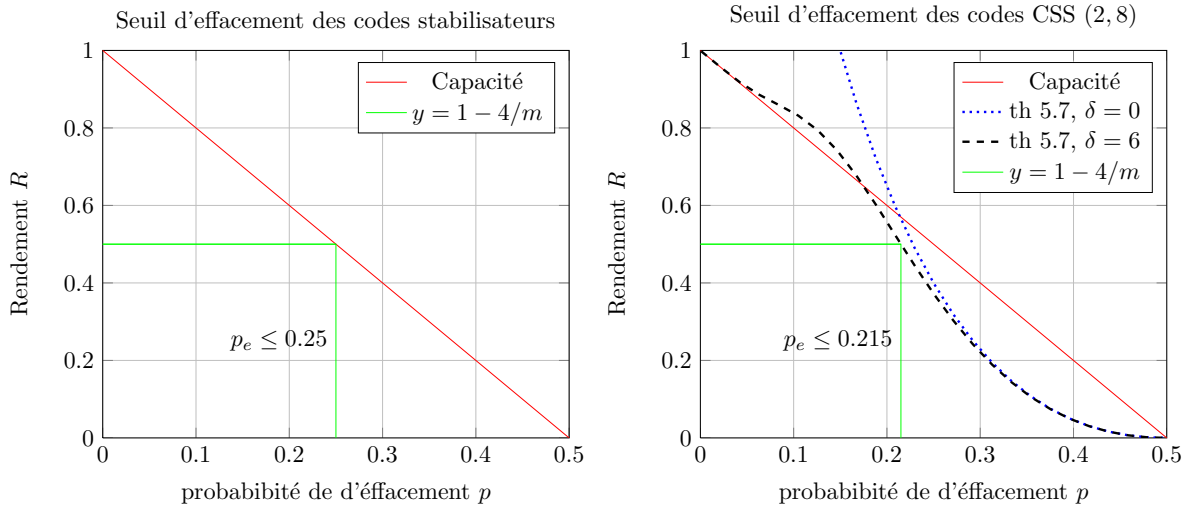


Figure 5.4 – (a) La borne $p_e \leq 0.25$ sur le seuil d'effacement tolérable des codes stabilisateurs de rendement $R \geq 1/2$, déduite de la capacité du canal à effacement tracée en rouge. (b) En vert, le rendement minimum $R = 1/2$ d'un code CSS de type $(2, 8)$. Son intersection avec la borne supérieure du théorème 5.14 pour $\delta = 6$ (en tirets noirs) mène à la borne $p_e \leq 0.215$ sur le seuil des codes CSS de type $(2, 8)$.

En utilisant un logiciel de calcul symbolique, nous obtenons différentes valeurs numériques de ces bornes sur le seuil d'effacement p_e. Quelques exemples sont proposés dans le tableau 5.1.

Table 5.1 – Bornes sur le seuil d'effacement tolérable de codes LDPC quantiques.

Type de codes :	Borne améliorée sur p_e :	Avec la capacité $p_e \leq 2/m$:
CSS(2,8) avec th. 5.1	0.228	0.25
CSS(2,8) avec th. 5.14	0.215	0.25
Stab(4,8) avec th. 5.1	0.228	0.25
CSS(2,5) avec th. 5.1	0.387	0.40
CSS(2,5) avec th. 5.14	0.381	0.40

Conclusion

- En utilisant la borne combinatoire sur le rendement des codes stabilisateurs obtenu au chapitre 4, nous avons obtenu une borne supérieure sur les rendements atteignables par les codes stabilisateurs définis par des matrices creuses. Une généralisation de cette approche au canal de dépolarisation serait particulièrement intéressante. La difficulté est le fait que la probabilité d'une erreur sur ce canal dépend de son poids. On doit donc considérer l'ensemble des erreurs typiques. Mais cet ensemble ne possède pas de structure algébrique forte alors que dans le cas du canal à effacement quantique, l'ensemble des erreurs possibles, pour un effacement fixé $\mathcal{E}$, est un espace vectoriel.
- Par des arguments graphiques, nous avons prouvé que les codes stabilisateurs et les codes CSS définis par des générateurs de poids borné n'atteignent pas la capacité du canal à effacement quantique. Ce résultat s'applique aux codes de surface et aux codes couleur ainsi qu'à des nombreuses constructions de codes LDPC quantiques issues des familles classiques. Ce résultat nous encourage à construire des familles de codes LDPC quantiques irréguliers et des familles basées sur des générateurs de poids croissant.
- À notre connaissance, cette méthode basée sur l'interprétation graphique du rang d'une matrice est originale. Elle permet aussi d'améliorer les bornes de Ridchadson et Urbanke sur les codes LDPC classiques de [83] théorème 3.93.

Chapitre 6

Codes topologiques et théorie de la percolation

Ce chapitre concerne les liens entre théorie de la percolation et la correction des effacements quantiques. Ces liens ne sont pas particuliers au cadre quantique. Par exemple, les performances des codes des cycles sur le canal à effacement sont reliées au seuil de percolation des arbres. Le seuil de percolation de l'arbre m-régulier est un seuil pour le taux d'effacement tolérable des codes des cycles de graphes m-réguliers [35, 99].

Stace, Barrett et Doherty ont démontré que le seuil de percolation du pavage carré est aussi un seuil pour le taux d'effacement tolérable par le code torique [89]. Le but de ce chapitre est d'étudier les similitudes entre seuil de percolation et seuil d'effacement tolérable dans le cas des graphes hyperboliques. Le calcul exact du seuil de percolation est en général difficile et le seuil de percolation des graphes hyperboliques est inconnu à ce jour [5, 7, 8, 55]. D'un autre côté, nous avons établi des bornes supérieures sur le seuil d'effacement tolérable des codes LDPC quantiques au cours du chapitre 5 et ces bornes s'appliquent aux codes construits sur des pavages hyperboliques.

L'objectif de ce chapitre est de transférer ces bornes sur les codes quantiques en théorie de la percolation. Le résultat principal de ce chapitre est une borne supérieure sur le seuil de percolation d'une famille de graphes hyperboliques auto-duaux. Cette borne supérieure fait intervenir la fonction de différence des rangs que nous avons introduite à la définition 4.13 pour mesurer la distance à la capacité d'une famille de codes stabilisateurs. Nous obtenons ainsi une borne en théorie de la percolation qui provient de la théorie de l'information quantique. Ce travail a été présenté lors de la conférence ISIT 2010 et a donné lieu à un article publié avec Gilles Zémor [36, 37].

6.1 Introduction

Soit G un graphe infini et E l'ensemble de ses arêtes. On note μ_p la mesure de probabilité sur $\{0, 1\}$ telle que $\mu_p(\{1\}) = p$. On considère l'espace mesurable Ω équipé de la mesure de probabilité produit $P_p = \mu_p^{\otimes E}$. Un évènement aléatoire peut être vu comme un sous-graphe aléatoire. Ce sous-graphe est obtenu en choisissant chaque arête avec probabilité p indépendamment des autres arêtes. Les arêtes de ce

sous-graphe sont dites *ouvertes*. L'objet de la théorie de la percolation est l'étude de la probabilité qu'une arête fixée e soit incluse dans une composante connexe ouverte infinie. Lorsque le graphe G est arête-transitif, cette propriété ne dépend pas de l'arête e. C'est le cas, par exemple du pavage carré infini dessiné sur la figure 6.1.

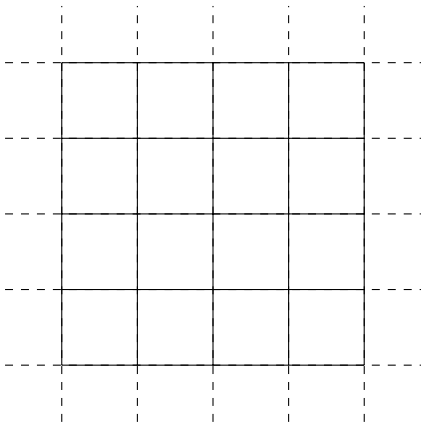


FIGURE 6.1 – Le pavage carré du plan

Le paramètre central en théorie de la percolation est le seuil de percolation :

Définition 6.1. *Soit G un graphe infini et arête-transitif. La* probabilité critique *ou le* seuil de percolation *de G est la quantité :*

$$p_c(G) = \inf\{p \in [0,1] \mid P_p(|\mathcal{E}(e)| = \infty) > 0\},$$

où $\mathcal{E}(e)$ est la composante connexe ouverte contenant e.

Le seuil de percolation du pavage carré est $p_c = 1/2$. Ce résultat a été démontré par Kesten [64], vingt ans après sa conjecture. Le calcul exact du seuil de percolation est, en général, très difficile. Nous nous intéressons ici au seuil de percolation d'une famille de graphes infinis qui généralisent le pavage carré.

Définition 6.2. *Soit $m \geq 4$ un entier. Le* graphe $G(m)$ *est le pavage du plan composé de faces de longueur m et dont les sommets sont de degré m.*

Lorsque $m = 4$, le graphe $G(4)$ est le pavage carré du plan. Le graphe $G(5)$ est le pavage pentagonal du plan tel que chaque sommet est bordé par 5 pentagones. La structure locale de ce graphe est présentée figure 6.2. Tout comme le pavage carré du plan, les graphes $G(m)$ sont auto-duaux.

Lorsque $m > 4$, ces graphes définissent des pavages réguliers du plan hyperbolique. Divers articles s'intéressent au phénomène de percolation dans les graphes hyperboliques [5, 7, 8, 55] et la détermination de leur probabilité critique est difficile. On peut obtenir une première borne inférieure qui revient à dire que le seuil de percolation $1/(m-1)$ de l'arbre m-régulier est inférieur à celui de du graphe $G(m)$:

Proposition 6.3. *Le seuil de percolation p_c du graphe $G(m)$ vérifie :*

$$\frac{1}{m-1} \leq p_c \leq 1 - \frac{1}{m-1}.$$

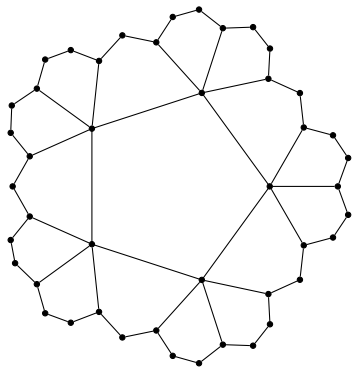


Figure 6.2 – Structure locale du graphe du pavage pentagonal $G(5)$

Démonstration. Nous adaptons la méthode de [53] page 14 dans le cas du pavage carré. Soit O un sommet fixé du graphe. Pour montrer cette inégalité, nous remarquons qu'il y a au plus $m(m-1)^{n-1}$ chemins de longueur n, partant de O, dans le graphe $G(m)$. La probabilité qu'un tel chemin soit ouvert est p^n. Dans le cas où $p < \frac{1}{m-1}$, la longueur moyenne d'un chemin ouvert partant de O est majorée par $\sum_{n=1}^{\infty} m(m-1)^{n-1}p^n < \infty$. On en déduit que cette valeur de p est située sous le seuil de percolation.

La même méthode mène à une borne supérieure $p_c \leq 1 - \frac{1}{m-1}$. La preuve peut être immédiatement adaptée du cas carré traité dans [53] page 14. □

6.2 Les graphes quotients

Afin de relier le seuil de percolation des pavages hyperboliques $G(m)$ et les performances d'une famille de codes topologiques, nous introduisons une famille de graphes hyperboliques finis qui sont localement isomorphes aux graphes $G(m)$. On peut voir les arbres réguliers comme des graphes de Cayley de groupes libres. Les graphes $G(m)$ admettent aussi une représentation algébrique [93] faisant appel à des groupes plus sophistiqués. De cette représentation algébrique, on déduira une version finie de ces graphes.

Au cours du chapitre 2, nous avons construit une famille de graphes hyperboliques. Ce sont les graphes de Cayley du groupe triangulaire engendré par les matrices :

$$y = \begin{pmatrix} P_m(\xi)^2 - 1 & 0 & P_m(\xi) \\ P_m(\xi) & 1 & 0 \\ -P_m(\xi) & 0 & -1 \end{pmatrix},$$

et

$$z = \begin{pmatrix} -1 & -P_m(\xi) & 0 \\ P_m(\xi) & P_m(\xi)^2 - 1 & 0 \\ P_m(\xi) & P_m(\xi)^2 & 1 \end{pmatrix},$$

où $P_k(X) = 2\cos(k \arccos(X/2))$ est le k-ème polynôme de Chebychev normalisé et $\xi = 2\cos(\pi/m^2)$.

Pour définir les graphes $G(m)$ de manière analogue, nous ne considérons pas le graphe de Cayley, qui est trivalent, mais le graphe des classes. Le groupe triangulaire

$T(m)$ engendré par les matrices y et z admet la présentation :

$$T(m) =< y, z \mid y^m = z^m = (yz)^2 = 1 > . \tag{6.1}$$

Définition 6.4. *Le* graphe des classes *associé au groupe triangulaire $T(m)$ est le graphe dont les sommets, les arêtes et les faces sont définis respectivement par les classes d'équivalences modulo les sous-groupes $\langle y\rangle, \langle yz\rangle$ et $\langle z\rangle$. Un sommet et une arête ou bien une arête et une face, sont incidents si les classes correspondantes ont une intersection non vide.*

Par exemple, le sommet $1\langle y\rangle$ est représenté par sa classe d'équivalence qui est l'ensemble $\{1, y, y^2, \ldots, y^{m-1}\}$. Ce sommet est incident aux m arêtes :

$$1\langle yz\rangle, y\langle yz\rangle, y^2\langle yz\rangle, \ldots, y^{m-1}\langle yz\rangle,$$

du graphe des classes du groupe $T(m)$. On peut raisonner de manière similaire avec les faces du graphe pour montrer que chaque face contient m arêtes. Ce graphe est autodual par symétrie entre les générateurs. C'est le graphe $G(m)$ de la définition 6.2.

Lors du chapitre 2, nous avons défini une version finie des graphes hyperboliques en considérant des quotients du groupe triangulaire $T(m)$ pour obtenir des groupes finis. Nous pouvons répéter ici cet argument. On utilise le groupe $T_r(m)$ du théorème 2.29. C'est un quotient fini du groupe triangulaire $T(m)$ dont le rayon d'injectivité est au moins r. Le graphe des classes associé à ce groupe est alors un graphe fini qui ressemble localement au graphe $G(m)$. En effet, Širáň a démontré que toute boule de rayon r de ce graphe est planaire [93]. On dit que le rayon d'injectivité du graphe est au moins r.

Définition 6.5. *Pour tout entier $r \geq 1$, le* graphe $G_r = G_r(m)$ *est le graphe des classes associé au groupe $T_r(m)$.*

Cette construction nous permet de définir la famille de graphe $G_r(m)_{r\geq 1}$ telle que chaque graphe $G_r(m)$ a un rayon d'injectivité minoré par r pour tout entier positif r.

6.3 Les codes de surface associés aux pavages $G_r(m)$

Chaque graphe $G_r(m)$ permet de définir un code de surface que nous noterons $Q_r(m)$. Rappelons que c'est un code CSS défini par deux matrices binaires, $\mathbf{H}_X$ la matrice d'incidence du graphe $G_r(m)$ et $\mathbf{H}_Z$ la matrice dont les lignes sont les vecteurs caractéristiques des faces. Deux codes classiques sont associés à ce code quantique. Le code $C_X = \operatorname{Ker} \mathbf{H}_X$, qui est le code des cycles du graphe $G_r(m)$ et $C_Z = \operatorname{Ker} \mathbf{H}_Z$, le code des cycles du graphe dual $G_r^*(m)$.

Du théorème 2.9, on tire la dimension de ces codes quantiques :

Proposition 6.6. *Le code quantique $Q_r(m)$ encode k qubits avec :*

$$k = \left(1 - \frac{4}{m}\right) n + 2.$$

Pour $m = 4$, le graphe $G_r(m)$ est un tore et le code associé est un code torique. Pour $m \geq 5$, les codes $Q_r(m)$ forment une famille de codes de rendement strictement positif et de distance minimale au moins $2r$ qui se comporte comme $\log(n)$ d'après le théorème 2.29 et la définition du graphe $G_r(m)$.

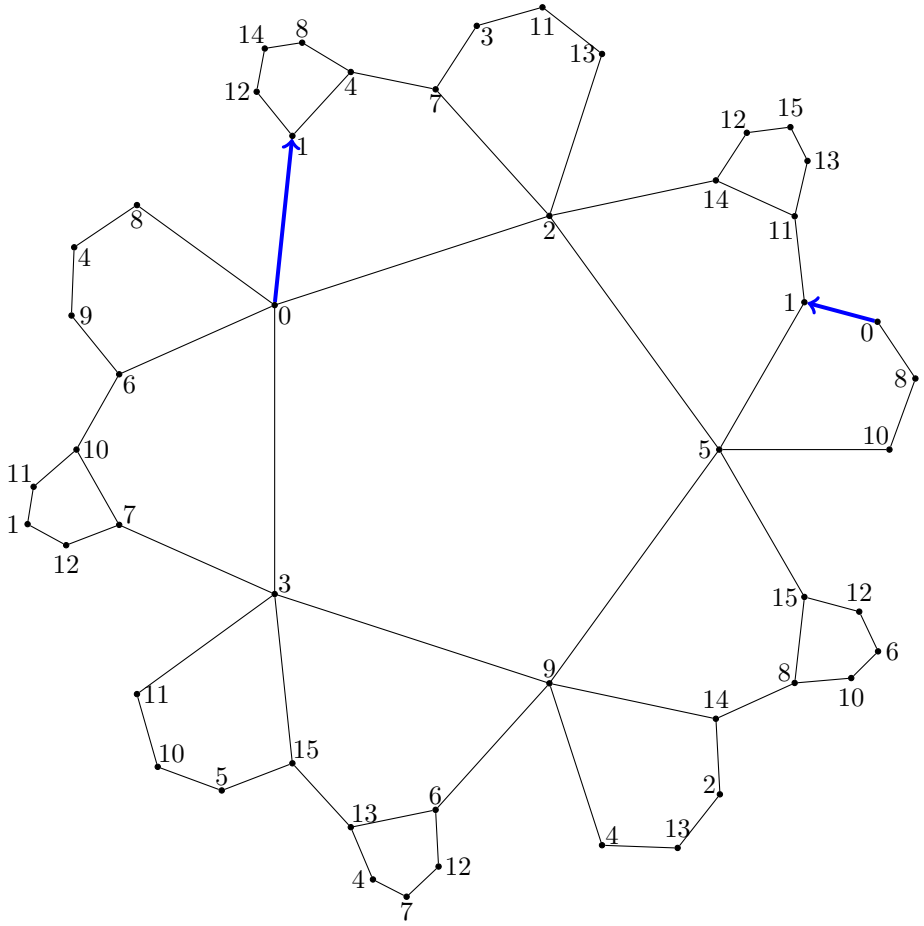


Figure 6.3 – Un exemple de pavage 5-régulier autodual d'un surface de genre 5 composé de 16 sommets, 40 arêtes et 16 faces. Chaque face est représentée une seule fois. Les sommets sont représentés plusieurs fois pour permettre une représentation planaire. Chaque arête du bord apparaît deux fois sur le bord. Pour construire la surface, on identifie les arêtes et les sommets présents en plusieurs exemplaires. En gras, l'identification des deux arêtes $\{0, 1\}$.

Un vecteur d'effacement peut être identifié à un ensemble d'arêtes de $G_r(m)$ ou de manière équivalente de son graphe dual $G_r^*(m)$. Cet ensemble d'arêtes est noté $\mathcal{E}$. Un effacement est non corrigible si et seulement si il couvre un erreur problématique. Dans la cas des codes de surface ceci revient à dire que $\mathcal{E}$ couvre un cycle de $G_r(m)$ qui n'est pas somme de faces, ou bien en regardant $\mathcal{E}$ comme un ensemble d'arêtes du graphe dual, il couvre un cycle de $G_r^*(m)$ qui n'est pas somme de faces.

Proposition 6.7. *Un effacement $\mathcal{E}$ sur le code de surface $G_r(m)$ est non-corrigible si et seulement s'il couvre un cycle du $G_r(m)$ ou de $G_r^*(m)$ qui n'est pas somme de faces.*

$$\mathbf{H}_X = \begin{pmatrix} 0 & 1 & 2 & 3 & 8 \\ 1 & 4 & 5 & 11 & 20 \\ 2 & 6 & 7 & 14 & 25 \\ 0 & 9 & 10 & 18 & 28 \\ 5 & 12 & 13 & 22 & 32 \\ 4 & 7 & 15 & 21 & 31 \\ 3 & 16 & 17 & 27 & 36 \\ 6 & 10 & 13 & 19 & 23 \\ 8 & 12 & 24 & 33 & 38 \\ 9 & 15 & 17 & 22 & 26 \\ 16 & 19 & 21 & 24 & 29 \\ 11 & 28 & 29 & 30 & 35 \\ 20 & 23 & 27 & 34 & 39 \\ 14 & 32 & 35 & 36 & 37 \\ 25 & 26 & 30 & 33 & 34 \\ 18 & 31 & 37 & 38 & 39 \end{pmatrix} \qquad \mathbf{H}_Z = \begin{pmatrix} 0 & 2 & 7 & 9 & 15 \\ 1 & 2 & 5 & 6 & 13 \\ 0 & 3 & 10 & 16 & 19 \\ 1 & 4 & 8 & 21 & 24 \\ 3 & 8 & 12 & 17 & 22 \\ 4 & 7 & 11 & 25 & 30 \\ 5 & 12 & 20 & 33 & 34 \\ 6 & 10 & 14 & 28 & 35 \\ 9 & 17 & 18 & 36 & 37 \\ 11 & 19 & 20 & 23 & 29 \\ 13 & 23 & 27 & 32 & 36 \\ 14 & 22 & 25 & 26 & 32 \\ 15 & 26 & 31 & 33 & 38 \\ 16 & 24 & 27 & 38 & 39 \\ 18 & 21 & 28 & 29 & 31 \\ 30 & 34 & 35 & 37 & 39 \end{pmatrix}$$

FIGURE 6.4 – Deux matrices de taille 16×40 définissant un code CSS de type $(2, 5)$ de paramètres $[[40, 10, 4]]$. Les colonnes sont indexées par les entiers $\{0, 2, \ldots, 39\}$ et les lignes sont décrites par leurs supports. Il s'agit du code de surface associé à la surface de la figure 6.3.

6.4 Percolation et probabilité d'erreur par qubit

Regardons maintenant le sous-graphe aléatoire $G_r(m)$ défini par la mesure produit $\mu_p^{\otimes E_r}$, où E_r est l'ensemble des arêtes du graphe $G_r(m)$. Autrement dit, c'est le sous-graphe ouvert de $G_r(m)$ obtenu en considérant chaque arête comme ouverte indépendamment avec probabilité p. Pour toute arête fixée e, on note $\mathcal{E}_r(e)$ la composante connexe du sous-graphe aléatoire $G_r(m)$ contenant l'arête e. Attention cette composante peut être vide. On note $f_r(p)$ la probabilité d'avoir $|\mathcal{E}_r(e)| > r$. On a alors :

Proposition 6.8. *Si $p < p_c(m)$ alors $f_r(p)$ tend vers 0 lorsque r tend vers l'infini.*

Démonstration. On observe que la probabilité $1 - f_r(p)$ que la composante ouverte de e soit de cardinal inférieur à r est la même dans le sous-graphe aléatoire du graphe fini $G_r(m)$ ou dans le sous-graphe aléatoire de son revêtement infini $G(m)$. Pour s'en convaincre, il suffit de remarquer que cet évènement ne dépend que de la boule de rayon r centrée en une extrémité de e. Or ces boules sont isomorphes dans le graphe $G_r(m)$ et dans le graphe $G(m)$.

On peut alors considérer que $f_r(p)$ est la probabilité de l'évènement $|\mathcal{E}(e)| > r$. Notons F_r cet évènement. La suite $(F_r(m))_r$ est une suite d'évènements décroissante et la probabilité $\mathbb{P}_p(\cap_{r\geq 1} F_r)$ est exactement la probabilité de percolation. Nous nous sommes placés sous le seuil de percolation : $p < p_c$. Par convergence monotone, on obtient donc $f_r(p) = \mathbb{P}_p(F_r) \to 0$. □

6.5 Borne sur le seuil de percolation de graphes hyperboliques

Considérons un élément quelconque de la famille de codes quantiques $Q_r(m)$ associée au graphe $G_r(m)$. Comme le graphe est auto-dual, les argument concernant le graphe $G_r(m)$ sont automatiquement valables dans son graphe dual $G_r^*(m)$. Nous nous concentrons donc sur la probabilité que l'effacement aléatoire $\mathcal{E}$ couvre un cycle qui n'est pas somme de faces dans le graphe $G_r(m)$.

Nous souhaitons obtenir une borne supérieure sur le seuil de percolation p_c en affirmant la propriété suivante : si $p < p_c$ alors la probabilité que l'ensemble d'arêtes aléatoire $\mathcal{E}$ couvre un cycle du graphe $G_r(m)$ qui n'est pas somme de faces tend vers 0 lorsque r tend vers l'infini. Si cette propriété est vraie alors le théorème 4.14 s'applique et le rendement limite R des codes quantiques $Q_r(m)$ est sujet à la borne $R < 1-2p-D(p)$ pour tout $p < p_c$. Ce rendement est calculé dans la proposition 6.6, $R = 1 - 4/m$, on en déduit une borne sur le seuil de percolation.

Malheureusement, nous ne sommes pas en mesure de démontrer que, lorsque p est strictement inférieur à p_c, le vecteur effacement $\mathcal{E}$ ne contient pas de cycle non somme de faces, avec une probabilité élevée. Ce que nous allons prouver est plus faible. Nous allons voir que si jamais $\mathcal{E}$ couvre un cycle qui n'est pas somme de faces, alors ce cycle admet un représentant de poids faible modulo l'espace des faces. Pour obtenir une famille de codes quantiques qui atteint une probabilité d'erreur tendant vers 0, on utilisera une version améliorée des codes $Q_r(m)$ que nous allons introduire maintenant.

Proposition 6.9. *Soit $Q_r(m)$ un code hyperbolique, n sa longueur et R son rendement. Supposons que $\rho \in]0, \frac{1}{2}[$ et $\alpha \in]0, 1[$ sont tels que :*

$$h(\rho) < \alpha < \frac{R}{2},$$

avec $h(\rho) = -\rho \log_2 \rho - (1-\rho)\log_2(1-\rho)$ la fonction d'entropie binaire. Alors on peut ajouter αn lignes à la matrice de parité $\mathbf{H}_X$ et αn lignes à la matrice de parité $\mathbf{H}_Z$ de $Q_r(m)$ pour obtenir un code CSS $Q'_r(m)$ de longueur n, de rendement $R-2\alpha$ et de distance minimale $d \geq \rho n$.

Démonstration. On note r_X et r_Z les dimensions des codes $C_X^\perp$ et $C_Z^\perp$ respectivement. On a $r_X = r_Z = \frac{2}{m}n - 1$.

Nous allons construire une matrice $\mathbf{H}'_X$ en ajoutant αn lignes à la matrice $\mathbf{H}_X$ telles que les lignes de $\mathbf{H}'_X$ sont orthogonales aux lignes de $\mathbf{H}_Z$ et le rang de $\mathbf{H}'_X$ est $r_X + \alpha n$. Soit C'_X le code de matrice de parité $\mathbf{H}'_X$.

Pour $\rho \in]0, 1/2[$, on définit X_ρ par

$$X_\rho(\mathbf{H}'_X) = |\{v \in C'_X \backslash C_Z^\perp | w(v) \leq \rho n\}|.$$

On peut écrire X_ρ comme une somme de variables aléatoires pour voir que :

$$\mathbb{E}(X_\rho) = \sum_{\substack{v \in C_X \backslash C_Z^\perp \\ v \in B(0,\rho n)}} \frac{|\{\mathbf{H}'_X | v \in C'_X\}|}{|\{\mathbf{H}'_X\}|}.$$

avec $B(0, \rho n)$ la boule de Hamming de rayon ρn. Soit $L_1, L_2, \dots L_{r_X}$ les r_X lignes de la matrice $\mathbf{H}_X$. Le nombre de matrices $\mathbf{H}'_X$ convenables est le nombre de familles $L'_1, L'_2, \dots L'_{\alpha n}$ de vecteurs de $\mathbb{F}_2^n$ telles que $L'_j \in C_Z$ pour tout j et les vecteurs $(L_1, L_2, \dots L_{r_X}, L'_1, L'_2 \dots, L'_{\alpha n})$ sont linéairement indépendants.

On peut construire une matrice convenable $\mathbf{H}'_X$ si et seulement si $r_X + \alpha n \leq \dim(C_Z)$, ceci nous donne la condition $\alpha < (1 - \frac{4}{m}) - \frac{2}{n}$. Dans ce cas le nombre de matrices est :

$$\prod_{i=r_X}^{r_X+\alpha n-1} (2^{n-r_Z} - 2^i).$$

Pour évaluer le cardinal de $|\{\mathbf{H}'_X | v \in C'_X\}|$ avec $v \in C_X \backslash C_Z^\perp$, il suffit d'ajouter la condition $L'_j \in \{v\}^\perp$ pour tout j. On obtient :

$$\prod_{i=r_X}^{r_X+\alpha n-1} (2^{n-r_Z-1} - 2^i).$$

Ainsi, on a :

$$\frac{|\{\mathbf{H}'_X | v \in C'_X\}|}{|\{\mathbf{H}'_X\}|} = \frac{2^{n-r_X-r_Z-\alpha n} - 1}{2^{n-r_X-r_Z} - 1} \leq 2^{-\alpha n}.$$

Cette borne ne dépend pas de v, de sorte que l'on a une borne supérieure sur l'espérance de la variable aléatoire X_ρ puisque le nombre de mots de la boule de rayon ρn n'est pas plus grand que $2^{nh(\rho)}$. On arrive à :

$$\mathbb{E}(X_\rho) \leq 2^{n(h(\rho)-\alpha)}.$$

Si $\alpha > h(\rho)$, l'espérance tend vers 0. Comme X_ρ est à valeurs entières, il existe une matrice $\mathbf{H}'_X$ telle que $X_\rho(\mathbf{H}_X) = 0$. On obtient un code CSS de matrice $\mathbf{H}'_X$ avec $r'_X = r_X + \alpha n$ et $\mathbf{H}_Z$ inchangées telles que le poids minimum d'un mot de $C'_X \backslash C_Z^\perp$ est au moins ρn.

Nous voulons répéter cet argument pour avoir le poids minimum d'un vecteur de $C'_Z \backslash C'^\perp_X$ supérieur à ρn. Il suffit de choisir $\alpha < \frac{1}{2}(1 - \frac{4}{m}) + \frac{1}{n}$ puisque dans ce cas $r_Z + \alpha n < \dim(C_X)$. □

Soit $\mathcal{E}$ un effacement. On décompose $\mathcal{E}$ en deux parties :

$$\mathcal{E} = \mathcal{E}_C + \mathcal{E}_P \tag{6.2}$$

où $\mathcal{E}_C$ est la réunion de toutes les composantes connexes qui ne couvre pas de cycles non somme de faces. La partie problématique $\mathcal{E}_P$ de $\mathcal{E}$ est la réunion des autres composantes.

Dans le graphe $G_r(m)$, on définit $g_r(p)$ comme la probabilité que la partie ouverte $\mathcal{E}_r(e)$ couvre un cycle qui n'est pas somme de faces.

Lemme 6.10. *Si $p < p_c(m)$ alors $g_r(p)$ tend vers 0 lorsque r tend vers l'infini.*

Démonstration. Rappelons que $f_r(p)$ est la probabilité que $|\mathcal{E}_r(e)| > r$. Nous allons voir que $g_r(p) \leq f_r(p)$. Il suffit ensuite d'appliquer la proposition 6.8. Si $|\mathcal{E}_r(e)| \leq r$ alors la composante ouverte $\mathcal{E}_r(e)$ de e est incluse dans une boule de rayon r du graphe $G_r(m)$. Cette boule est isomorphe à une boule de même rayon dans le graphe planaire $G(m)$. Or tout cycle d'un graphe planaire est somme de faces. On en déduit que $\mathcal{E}_r(m)$ ne peut couvrir un cycle qui n'est pas somme de faces uniquement lorsque sa taille dépasse r : $\mathcal{E}_r(m) > r$. L'inégalité $g_r(p) \leq f_r(p)$ en découle. □

Remarque : Le même argument que dans la preuve précédente permet de démontrer que tout cycle de longueur inférieure à $2r$ dans le graphe $G_r(m)$ est somme de faces. Ceci prouve que la distance minimale du code quantique $Q_r(m)$ est minorée par $2r$.

Proposition 6.11. *Si l'on considère le canal à effacement quantique de probabilité $p < p_c$ alors $\forall \varepsilon > 0, \exists r_0 \in \mathbb{N}$ tel que si $r \geq r_0$ alors le poids moyen de la partie problématique $\mathcal{E}_P$ de $\mathcal{E}$ vérifie :*

$$\mathbb{E}(|\mathcal{E}_P|) \leq \varepsilon n.$$

Démonstration. Pour toute arête e de $G_r(m)$, on note $X_{r,e}$ la variable aléatoire qui prend la valeur 1, si la composante connexe $\mathcal{E}_r(e)$ de e dans $G_r(m)$ couvre un cycle qui n'est pas somme de faces, et qui prend la valeur 0 dans le cas contraire. Alors on a :

$$|\mathcal{E}_P| = \sum_e X_{r,e}.$$

Pour conclure, on remarque que $\mathbb{E}(X_{r,e}) = g_r(p)$ et on applique le lemme 6.10. □

Le lemme suivant affirme que si un vecteur effacement $\mathcal{E}$ a une grande composante problématique $\mathcal{E}_P$ alors il peut être corrigé par le code amélioré défini dans la proposition 6.9.

Lemme 6.12. *Soit $Q'_r(m)$ l'un des codes quantiques donné par proposition 6.9 et soit d sa distance minimale. Supposons que la composante $\mathcal{E}_P$ du vecteur d'effacement $\mathcal{E}$ est de taille $|\mathcal{E}_P| < d$. Alors $\mathcal{E}$ est corrigible par le code $Q'_r(m)$.*

Démonstration. Soit C_X et C_Z les codes linéaires binaires associés aux codes quantiques $Q_r(m)$ et C'_X, C'_Z leurs sous-codes binaires associés au code quantique $Q'_r(m)$ construit dans la proposition 6.9 en ajoutant des lignes aux matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$ de $Q_r(m)$.

Si le vecteur effacement $\mathcal{E}$ couvre un élément x de $C'_X \backslash C'^{\perp}_Z$ alors x doit appartenir à $C_X \backslash C_Z^{\perp}$ *i.e.* x est un cycle de $G_r(m)$ qui n'est pas somme de faces. La restriction de ce cycle à $\mathcal{E}_C$ défini dans (6.2) est encore un cycle y et par définition de $\mathcal{E}_C$, c'est une somme de faces. On en déduit un cycle $x + y$ inclus dans $\mathcal{E}_P$ avec $y \in C_Z^{\perp} \subset C'^{\perp}_Z$, i.e. $x + y \in C'_X \backslash C'^{\perp}_Z$. C'est une contradiction lorsque la partie $\mathcal{E}_P$ de l'effacement $\mathcal{E}$ est de poids strictement inférieur à la distance minimale d du code amélioré $Q'_r(m)$. □

Nous sommes maintenant en mesure de démontrer la borne sur le seuil de percolation des graphes $G(m)$. Nous utiliserons la fonction de différence des rangs de la famille de codes stabilisateurs $Q'_r(m)$ introduite en définition 4.13.

Théorème 6.13. *Soit $m \geq 5$ et soit $p_c(m)$ le seuil de percolation du graphe $G(m)$. On note $D(p)$ la fonction de différence des rangs de la suite de codes stabilisateurs associée aux graphes $G_r(m)$. Alors pour tout $p < p_c$, on a :*

$$1 - \frac{4}{m} \leq 1 - 2p - D(p).$$

Démonstration. Prenons $p < p_c$ et notons $R = 1 - \frac{4}{m}$. Pour tout α tel que $0 < \alpha < R/2$, la proposition 6.9 nous donne une famille de codes quantiques $Q'(m)$ de distance minimale $d \geq \rho n$ avec $\rho = h^{-1}(\alpha/2)$ et de rendement $R - 2\alpha$. Pour un tel code la probabilité d'erreur après décodage vérifie :

$$P_{err} \leq P(|\mathcal{E}_P| \geq \rho n).$$

Pour tout $\varepsilon > 0$, on peut choisir r suffisamment grand pour appliquer la proposition 6.11. On en déduit grâce à l'inégalité de Markov :

$$P_{err} \leq P(|\mathcal{E}_P| \geq \frac{\rho}{\varepsilon}\varepsilon n) \leq \frac{\varepsilon}{\rho}.$$

Pour tout $\varepsilon > 0$, on peut prendre $\rho = \sqrt{\varepsilon}$. De sorte que $\rho(\varepsilon)$ et $\frac{\varepsilon}{\rho(\varepsilon)}$ convergent simultanément vers 0 lorsque ε tend vers 0. On choisit α tel que $\alpha = 2h(\rho)$ puis on prend une suite décroissante de ϵ qui tend vers 0. On obtient ainsi une famille de codes quantiques améliorés $Q'_r(m)$ dont la probabilité d'erreur après décodage tend vers 0 et dont le rendement $R - 2\alpha$ tend vers R.

On peut donc appliquer le théorème 4.14 à la suite des matrices stabilisatrices des codes $Q'_r(m)$. Nous avons vu que leur rendement tend vers $1 - 4/m$ et comme ces codes $Q'_r(m)$ sont obtenus en ajoutant une proportion négligeable de générateurs au groupe stabilisateur des codes $Q_r(m)$, la fonction $D(p)$ de la famille $Q'_r(m)$ est la même que celle de la famille de codes de surface $Q_r(m)$. □

D'après la proposition 4.19, la fonction $D(p)$ est positive lorsque $\leq 1/2$. On en déduit :

Proposition 6.14. *Pour tout entier $m \geq 5$, le seuil de percolation $p_c(m)$ des graphes $G(m)$ est majoré par :*

$$p_c(m) \leq \frac{2}{m}.$$

En appliquant la borne inférieure sur $D(p)$ obtenue dans la proposition 5.6, on obtient le théorème suivant :

Théorème 6.15. *Le seuil de percolation $p_c(m)$ des graphes $G(m)$ est majoré par p la plus petite solution $p \in [0, 1]$ de l'équation :*

$$1 - \frac{4}{m} = (1 - 2p)\Big(\frac{4}{mp}\Big(1 - (1 - p)^m S_{m-2}(p(1 - p)^{m-2})\Big) - 1\Big).$$

où $S_{m-2}(x) = \sum_{k=0}^{m-2} \frac{a_k}{k+1} x^k$ et les nombres a_k sont les coefficients de la série génératrice T_m.

Table 6.1 – Bornes sur le seuil de percolation de pavages hyperboliques $G(m)$.

m	Borne inf. $p_c(m) \geq \frac{1}{m-1}$:	Borne du th. 6.15 :	Borne de prop. 6.14 $= \frac{2}{m}$:
5	0.25	0.38	0.40
10	0.11	0.16	0.20
20	0.053	0.073	0.100
30	0.035	0.046	0.067
40	0.026	0.033	0.050
50	0.020	0.026	0.040

Grâce à un logiciel de calcul symbolique, on peut évaluer cette borne sur le seuil de percolation. Quelques exemples numériques sont regroupés dans le tableau 6.1. nous utilisons des propriétés classiques des séries génératrices pour calculer les éléments de la suite $(a_k)_k$. On trouvera les résultats classiques sur les séries génératrices et notamment le théorème d'inversion de Lagrange dans les ouvrages [45], [97].

On peut voir que cette nouvelle borne supérieure devient meilleure pour des pavages auto-duaux $G(m)$ dont la longueur des faces grandit. Ceci correspond au fait que l'on énumère un plus grand nombre de composantes connexes dans ce cas.

Conclusion

- La valeur exacte du seuil de percolation des graphes $G(m)$ reste à découvrir. Pour améliorer notre borne, nous devons énumérer un plus grand nombre de composantes connexes de graphe aléatoire de la partie 5.3.2. La difficulté augmente lorsque nous cherchons à énumérer des composantes non arborescentes. Notre méthode fait aussi intervenir un argument de concavité sur la fonction d'écart des rangs. Une alternative à cette borne pourrait nous rapprocher de la véritable valeur du seuil de percolation.
- Les estimations numériques de ces seuils sont difficiles étant donné la croissance exponentielle des boules des graphes hyperboliques. Gu et Ziff ont démontré l'inconsistance de certains résultats numériques [55]. Ceci renforce l'intérêt de notre approche théorique.

Chapitre 7

Décodage des codes topologiques par couplage parfait

Ce dernier chapitre concerne le problème du décodage des codes topologiques sur le canal de dépolarisation. Plusieurs stratégies ont été proposées pour décoder ces codes quantiques. La plus naturelle est d'adapter l'algorithme de décodage itératif des codes LDPC [3, 29, 73, 78]. Ceci permet d'obtenir un algorithme qui fonctionne pour toute famille de codes LDPC quantiques et pas uniquement pour les codes topologiques. La difficulté est de prendre en compte les cycles courts qui apparaissent dans le graphe de Tanner. Ces cycles sont inévitables car ils sont dus aux relations d'orthogonalité.

Deux méthodes particulières à la famille des codes topologiques ont été proposées pour obtenir de meilleures performances : il s'agit du décodage par groupe de renormalisation, inspiré de la physique statistique [16, 40, 85], et du décodage par couplage parfait, basé sur l'algorithme de couplage parfait d'Edmonds [38,46,94,95]. Nous présentons cet algorithme de décodage des codes de surface dans une première partie.

Nous proposons une généralisation aux codes couleur dans la seconde partie. Le résultat principal de ce chapitre est ce nouvel algorithme de décodage des codes couleur par couplage parfait. Cette procédure de décodage passe par la projection d'une erreur qui agit sur le code couleur sur trois erreurs agissant sur trois codes de surface. Ceci permet de transférer des résultats des codes de surface vers les codes couleur. Ce transfert a déjà été entrepris par Bombin, Duclos-Cianci et Poulin qui ont proposé de décomposer un code couleur en deux codes de surface [16]. L'inconvénient de leur décomposition est qu'elle modifie le modèle d'erreur. Au contraire, notre projection des erreurs transforme tout canal de dépolarisation sur un code couleur en un canal de dépolaration sur un code de surface. Il en découle une borne inférieure sur le seuil d'erreur tolérable d'une famille de codes couleur en fonction du seuil d'erreur des codes de surface associés.

Nous avons implémenté cet algorithme et nous avons simulé le décodage d'un code couleur construit sur un pavage hexagonal du tore. En 2012, Raussendorf et Sarvepalli ont obtenu numériquement un seuil d'erreur tolérable 7.8% pour cette famille de codes [85]. Les résultats de nos simulations dépassent ceux de Raussendorf et Sarvepalli et nous obtenons un seuil de 8.5%.

7.1 Décodage des codes de surface

7.1.1 Le problème du décodage

Soit $\mathbf{H} \in \mathcal{M}_{r,n}(\mathcal{P}_1)$ une matrice stabilisatrice et soit σ la fonction syndrome associée. Le syndrome d'un vecteur de $\mathbb{F}_2^r$ est l'information que l'on mesure sur l'erreur, étant donné un état reçu $E|\psi\rangle$. À partir de cette information, nous estimons l'erreur E. Un décodage est donc une application qui à chaque syndrome associe une erreur de Pauli $\tilde{E} \in \mathcal{P}_n$. On appliquera cet opérateur $\tilde{E}$ à l'état reçu $E|\psi\rangle$ pour corriger E.

Lorsque l'on travaille avec le canal de dépolarisation de probabilité p, la probabilité d'apparition d'une erreur $E \in \mathcal{P}_n$ est $\mathbb{P}(E) = p^{|E|}(1-p)^{n-|E|}$. En écrivant cette probabilité sous la forme $\mathbb{P}(E) = \left(\frac{p}{1-p}\right)^{|E|}(1-p)^n$, on observe que choisir une erreur de probabilité $\mathbb{P}(E)$ maximale, c'est choisir une erreur de poids $|E|$ minimum, lorsque $p < 1/2$. Nous arrivons ainsi à une version combinatoire du décodage, c'est le décodage à distance minimale :

Définition 7.1. *Soit $\mathbf{H} \in \mathcal{M}_{r,n}(\mathcal{P}_1)$ une matrice stabilisatrice d'un code $C(S)$. Nous appellerons* décodage de $C(S)$ à distance minimale*, toute application :*

$$\begin{aligned} \mathcal{D} : \mathbb{F}_2^r &\longrightarrow \mathcal{P}_n \\ s &\longmapsto \tilde{E} \end{aligned}$$

où $\tilde{E}$ est une erreur de Pauli de syndrome s et de poids $|\tilde{E}|$ minimum parmi les erreurs de syndrome s.

D'après la remarque qui précède cette définition, ce décodage coïncide avec la recherche de l'erreur la plus probable sur le canal de dépolarisation de probabilité $p < 1/2$. C'est une version simplifiée du *décodage par maximum de vraisemblance* qui consiste dans le cas quantique à chercher la classe $E.S$ la plus probable. Cette dégénérescence est difficile à prendre en compte lors du décodage. Pour contourner cette difficulté nous cherchons l'erreur la plus probable.

Le problème du décodage est difficile comme dans le cas des codes classiques. Il n'existe pas d'algorithme polynomial qui calcule la fonction $\mathcal{D}$ étant donné un code quelconque [61]. Afin de pouvoir décoder en temps raisonnable, nous considérons la famille des codes topologiques. La structure de ces codes nous permet d'espérer un décodage rapide et performant. De plus, nous nous intéressons à une version simplifiée du problème du décodage pour les codes CSS, nous traiterons les erreurs en X et celles en Z de manière indépendante.

Soit $\mathbf{H}_X \in \mathcal{M}_{r_x,n}(\mathbb{F}_2)$ et $\mathbf{H}_Z \in \mathcal{M}_{r_Z,n}(\mathbb{F}_2)$ deux matrices définissant un code CSS. Le syndrome d'une erreur $E = (E_X, E_Z) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ est alors composé de deux vecteurs binaires $s_X = \mathbf{H}_Z E_X^t \in \mathbb{F}_2^{r_Z}$ et $s_Z = \mathbf{H}_X E_Z^t \in \mathbb{F}_2^{r_X}$. Le décodage à distance minimale consiste à déterminer E_X et E_Z de syndromes respectivement s_X et s_Z qui forment une erreur de Pauli E de poids minimum.

Définition 7.2. *Soit* $\mathbf{H}_X \in \mathcal{M}_{r_X,n}(\mathbb{F}_2)$ *et* $\mathbf{H}_Z \in \mathcal{M}_{r_Z,n}(\mathbb{F}_2)$ *deux matrices définissant un code CSS noté* C*. Nous appellerons* décodage de C non corrélé à distance minimale*, toute application :*

$$\begin{aligned}\mathcal{D} : \mathbb{F}_2^{r_X} \times \mathbb{F}_2^{r_Z} &\longrightarrow \mathbb{F}_2^n \times \mathbb{F}_2^n \\ (s_Z, s_X) &\longmapsto (\tilde{E}_X, \tilde{E}_Z)\end{aligned}$$

où $\tilde{E}_X$ *est une erreur de Pauli de syndrome* s_X *et de poids* $w(\tilde{E}_X)$ *minimum parmi les erreurs de syndrome* s_X *et* $\tilde{E}_X$ *est une erreur de Pauli de syndrome* s_X *et de poids* $w(\tilde{E}_X)$ *minimum parmi les erreurs de syndrome* s_X*.*

Ce décodage n'est pas le décodage à distance minimale car les poids de E_X et de E_Z sont minimum mais le poids de l'erreur $E \in \mathcal{P}_n$ ne l'est pas nécessairement. En effet, le poids de E s'exprime en fonction des poids de Hamming des vecteurs binaires E_X et E_Z, c'est $|E| = w(E_X) + w(E_Z) - w(E_X \cap E_Z)$ où le vecteur $E_X \cap E_Z$ est le vecteur de $\mathbb{F}_2^n$ obtenu en faisant le produit composante par composante de E_X et E_Z. De sorte que, pour minimiser le poids de E, on doit considérer les corrélations entre E_X et E_Z. Pour simplifier ce problème, nous considérons un décodage non corrélé. Autrement dit, nous corrigeons indépendamment les erreurs en X et celles en Z.

7.1.2 Décodage des codes de surface par couplage parfait

Soit $G = (V, E, F)$ une surface et soit $G^* = (F, E, V)$ sa surface duale. Cette surface définit un code CSS de longueur $n = |E|$. Nous rappelons dans cette partie le principe du décodage par couplage parfait des codes de surface proposé par Wang, Fowler, Stephens et Hollenberg, [95].

Nous avons introduit les codes de surface dans la définition 2.3 à partir du complexe de chaîne associé à la surface G :

$$C_2 \xrightarrow{\partial_2} C_1 \xrightarrow{\partial_2} C_0$$

Nous disposons aussi d'un complexe de chaîne associé à la surface duale G^* :

$$C_2^* \xrightarrow{\partial_2^*} C_1^* \xrightarrow{\partial_2^*} C_0^*$$

Dans ce chapitre, nous utilisons cette interprétation géométrique pour décoder les codes topologiques.

Une erreur E_Z est donc vue comme un ensemble d'arêtes du graphe G, c'est-à-dire comme un vecteur de C_1 et son syndrome est son bord $s_Z = \partial_1(E_Z) \in C_0$ qui est un ensemble de sommets du graphe G. On cherche à retrouver le vecteur E_Z à une somme de faces près, c'est-à-dire la classe $E_Z + \operatorname{Im}\partial_2$ de E_Z modulo le sous-groupe $\operatorname{Im}\partial_2$. De même, le syndrome de l'erreur E_X, que l'on considère comme un vecteur de C_1^*, est le vecteur $s_X = \partial_1^*(E_X) \in C_0^*$. On cherche alors à retrouver la classe $E_X + \operatorname{Im}\partial_2^*$ à partir du vecteur s_X. Le décodage d'un code de surface se ramène donc à un problème géométrique :

Définition 7.3. *Soit G une surface et soit $\partial_1 : C_1 \longrightarrow C_0$ l'application bord sur ses chaînes d'arêtes. Un* décodage de surface *de graphe G est une application :*

$$\begin{aligned} \mathcal{DS}_G : \operatorname{Im} \partial_1 \subset C_0 &\longrightarrow C_1 \\ s &\longmapsto \tilde{x} \end{aligned}$$

où $\tilde{x}$ est un vecteur de bord $\partial_1(\tilde{x}) = s$ et de poids $w(\tilde{x})$ minimum parmi les vecteurs de bord s.

Le décodage non corrélé à distance minimale du code de surface associé à G est donc composé du décodage de surface G et du décodage de surface G^*.

Nous présentons maintenant un algorithme de calcul d'un décodage de surface. Il nécessite le pré-calcul du graphe des distances et de la fonction géodésique dont les définitions suivent.

Définition 7.4. *Soit $G = (V, E)$ un graphe connexe et soit $V = \{v_1, v_2, \ldots, v_r\}$ l'ensemble de ses sommets. Le* graphe des distances *est le graphe complet à r sommets K_r. Chaque arête $\{i, j\}$ de ce graphe est pondérée par la distance $d(v_i, v_j)$ entre les sommets v_i et v_j dans le graphe G. On le note K_G.*

Définition 7.5. *Soit G un graphe connexe à r sommets et soit $s \in C_0(G)$ un ensemble de sommets de G. Le* graphe excité *associé au vecteur s est le sous-graphe du graphe des distances K_G, induit par les sommets de s. On le note $K_G(s)$.*

Définition 7.6. *Une* fonction géodésique *associée à un graphe connexe $G = (V, E)$ est une application :*

$$\begin{aligned} \mathcal{G} : V \times V &\longrightarrow C_1 \\ (u, v) &\longmapsto \mathcal{G}(u, v) \end{aligned}$$

où $\mathcal{G}(u, v) \in C_1$ est un chemin de longueur minimale joignant u et v.

Ces trois objets vont nous permettre de ramener le problème du décodage de surface à la recherche d'un couplage parfait dans un graphe. Nous commençons par quelques rappels sur l'algorithme de couplage parfait.

Définition 7.7. *Un* couplage parfait *M dans un graphe $G = (V, E)$ est un ensemble d'arêtes $M \subset E$ tel que chaque sommet est contenu dans exactement une arête de M.*

Lorsque le graphe G est pondéré, le poids d'un couplage M est la somme des poids de ses arêtes. Nous nous intéressons au problème du calcul d'un couplage parfait de poids minimum. En 1965, Edmonds a proposé l'algorithme «blossom» qui résout ce problème en temps polynomial [41, 42]. Nous utiliserons l'implémentation «blossom V», due à Kolmogorov en 2009 [67], dont la complexité dans le pire des

cas est en $O(|V|^3|E|)$. En pratique, la complexité typique de cet algorithme est bien meilleure.

La proposition suivante exprime une fonction de décodage de surface en fonction d'un couplage parfait de poids minimum.

Proposition 7.8. *Soit G et soit $V = \{v_1, v_2, \ldots, v_r\}$ l'ensemble de ses sommets. A tout syndrome $s \in \operatorname{Im}\partial_1$ est associé un couplage parfait $M(s)$ de poids minimum dans le graphe excité $K_G(s)$. La fonction :*

$$\mathcal{DS}_G(s) = \sum_{\{i,j\}\in M(s)} \mathcal{G}(v_i, v_j),$$

est une fonction de décodage de surface de graphe G.

Algorithme 1 Décodage non corrélé à distance minimale d'un code de surface G

Entrées: $s \in \operatorname{Im}\partial_1$, le graphe des distances K_G, la fonction géodésique $\mathcal{G}_G$.
Sorties: $\tilde{x} = \mathcal{D}_G(s)$.

1: Extraire le sous-graphe $K_G(s)$ de K_G ;
2: Déterminer un couplage parfait $M(s)$ de poids minimum dans le graphe $K_G(s)$;
3: Retourner $\tilde{x} = \sum_{\{i,j\}\in M(s)} \mathcal{G}(v_i, v_j)$;

Démonstration. Soit $\tilde{x} = \sum_{\{i,j\}\in M(s)} \mathcal{G}(v_i, v_j)$. Nous commençons par démontrer que le bord de $\tilde{x}$ est bien le vecteur s. Nous verrons ensuite que son poids est minimal. Par linéarité de l'application bord ∂_1, le bord de $\tilde{x}$ est la somme des bords des géodésiques $\mathcal{G}(v_i, v_j)$. Par définition de ces géodésiques, un tel bord est $\partial_1(\mathcal{G}(v_i, v_j)) = v_i + v_j$. On arrive donc à l'expression :

$$\partial_1(\tilde{x}) = \sum_{\{i,j\}\in M(s)} (v_i + v_j).$$

Comme $M(s)$ est un couplage parfait, chaque sommet v_i de s apparaît exactement une fois dans cette somme. On a bien $\partial_1(\tilde{x}) = s$.

Soit $x \in C_1$, un vecteur de bord s. Notre objectif est de prouver que le poids de x est au moins égal à celui de $\tilde{x}$. Pour cela nous allons voir que x définit un couplage parfait dans le graphe $K(s)$ de poids inférieur à $w(x)$.
Tout vecteur $x \in C_1$ admet une décomposition en somme de chemins à supports disjoints : $x = \sum \gamma_m$. On peut supposer que les extrémités de ces chemins γ_m sont disjointes. Cette décomposition en chemins du vecteur x définit un couplage des sommets de s et donc un couplage parfait M' du graphe $K_G(s)$. Soit γ_m un chemin de la décomposition de x et soient v_i et v_j ses extrémités. Par définition, la longueur du chemin γ_m est minorée par la longueur de la géodésique $\mathcal{G}(v_i, v_j)$, c'est-à-dire le poids de l'arête $\{i, j\}$ du graphe $K_G(s)$. Comme le poids du vecteur x est la somme des longueurs des chemins γ_m, il est minoré par le poids du couplage parfait M'. Par définition du couplage parfait de poids minimum $M(s)$, on a $w(x) \geq w(M(s)) = w(\tilde{x})$. □

D'après la proposition 7.8, l'algorithme 1 renvoie une estimation $\tilde{x}$ de l'erreur x à partir de son syndrome s. La complexité de cet algorithme est polynomiale.

Nous avons simulé le décodage par couplage parfait des codes de surface hyperboliques. Les performances obtenues ne sont pas satisfaisantes. Les précalculs nécessaires au décodage par couplage parfait nous empêchent de simuler des codes de très grandes longueurs. On peut espérer observer de meilleurs résultats pour de très grandes longueurs en utilisant un algorithme de décodage moins gourmand en précalculs.

7.2 Décodage des codes couleur par couplage parfait

Notre but est maintenant de généraliser ce décodage par couplage parfait aux codes couleur. Ce nouvel algorithme de décodage des codes couleur fournit une alternative au décodage par groupe de renormalisation. De plus, il rapproche le problème du décodage des codes de surface et des codes couleur. Ceci permet notamment de transférer des propriétés de la famille, très étudiée, des codes de surface vers les codes couleur.

Soit $G = (V, E, F)$ une surface telle que le graphe G est trivalent et les faces de G sont 3-coloriables. Cette surface permet de définir un code couleur comme indiqué dans la définition 2.13. Notre algorithme de décodage est basé sur la géométrie du graphe dual. Nous commençons donc par exprimer le syndrome d'un erreur de manière géométrique dans le graphe dual $G^* = (V^*, E^*, F^*)$. Les faces du graphe dual sont toutes de longueur trois car le graphe G est trivalent.

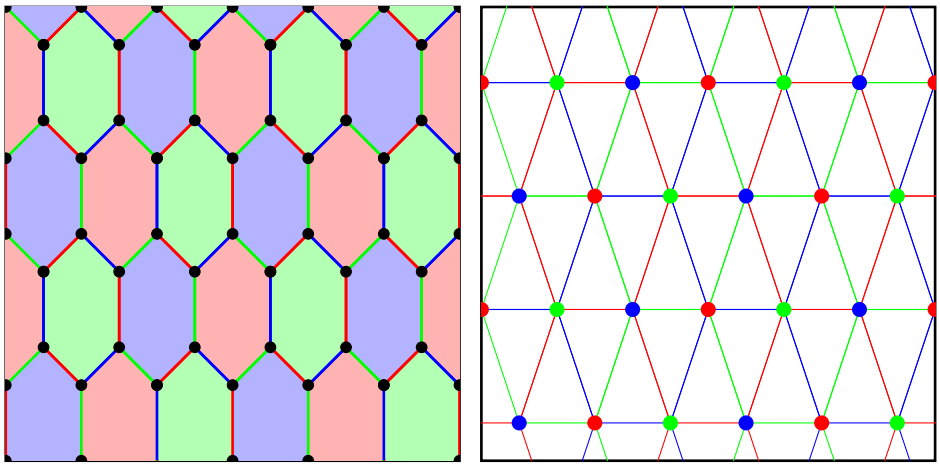


FIGURE 7.1 – Un pavage hexagonal du tore dont les faces sont 3-coloriées et son dual. Les sommets du graphe dual héritent de la 3-coloration.

7.2.1 Le 2-complexe associé au code couleur

Dans cette partie $G = (V, E, F)$ est un pavage de surface définissant un code couleur et $G^* = (V^*, E^*, F^*)$ est son pavage dual. Le graphe G est trivalent donc les

faces du graphe G^* sont toutes composées de trois arêtes, ce sont des triangles. Les faces du graphe G sont 3-coloriées. On en déduit une 3-coloration des sommets du graphe G^*. Un tel pavage ainsi que son dual sont représentés figure 7.1.

Pour étudier le décodage des codes couleur, nous nous plaçons dans le graphe dual G^* que nous regardons comme un hypergraphe $\mathcal{H}$.

Définition 7.9. L'hypergraphe associé à G *est l'hypergraphe* $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ *dont les sommets sont les sommets de* G^* *et dont les hyperarêtes sont les triplets de sommets* $\mathcal{E}(f)$ *incidents à une face* f *de* G^**. On munit cet hypergraphe d'un ensemble d'hyperfaces. Pour tout sommet* v *de* G^**,* $\mathcal{F}(v)$ *est l'ensemble des hyperarêtes de* $\mathcal{H}$ *contenant le sommet* v*. L'ensemble des hyperfaces de* $\mathcal{H}$ *est* $\mathcal{F} = \{\mathcal{F}(v) \mid v \in V^*\}$.

Nous continuerons d'appeler hypergraphe le triplet $\mathcal{H} = (\mathcal{V}, \mathcal{E}, \mathcal{F})$ composé d'un hypergraphe et de ses hyperfaces.

Définition 7.10. *Le* 2-complexe *associé à l'hypergraphe* $\mathcal{H}$ *est le complexe de chaîne formé du triplet :*

$$C_2(\mathcal{H}) = \bigoplus_{f \in \mathcal{F}} \mathbb{F}_2 f, \qquad C_1(\mathcal{H}) = \bigoplus_{e \in \mathcal{E}} \mathbb{F}_2 e, \qquad C_0(\mathcal{H}) = \bigoplus_{v \in \mathcal{V}} \mathbb{F}_2 v$$

et des applications bord $\partial_2^{\mathcal{H}}$ *et* $\partial_1^{\mathcal{H}}$ *qui sont les applications linéaires :*

$$C_2(\mathcal{H}) \xrightarrow{\partial_2^{\mathcal{H}}} C_1(\mathcal{H}) \xrightarrow{\partial_2^{\mathcal{H}}} C_0(\mathcal{H})$$

telles que $\partial_2^{\mathcal{H}}(f) = \sum_{e \in f} e$ *et* $\partial_1^{\mathcal{H}}(e) = \sum_{v \in e} v$.

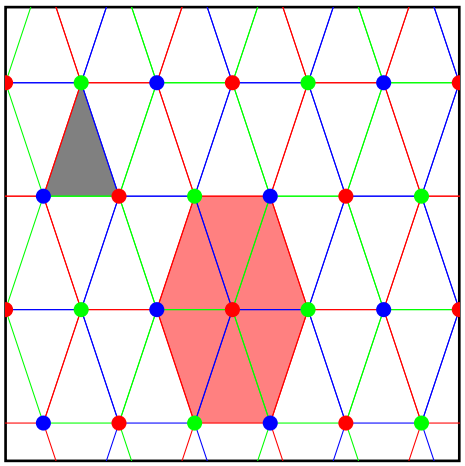


Figure 7.2 – En gris une hyperarête de l'hypergraphe $\mathcal{H}$ associé au pavage dual du pavage hexagonal du tore. En rouge une hyperface de cet hypergraphe.

Comme dans le cas d'un complexe de chaîne associé à un pavage de surface, en appliquant $\partial_1^{\mathcal{H}}$ puis $\partial_2^{\mathcal{H}}$ à une face f de l'hypergraphe, on obtient le vecteur nul.

Proposition 7.11. *La composition des application bord* $\partial_1^{\mathcal{H}}$ *et* $\partial_2^{\mathcal{H}}$ *associées à un code couleur est nulle :* $\partial_1^{\mathcal{H}} \circ \partial_2^{\mathcal{H}} = 0$.

Démonstration. Par linéarité, il suffit de vérifier que l'image d'une hyperface est nulle. Soit $\mathcal{F}(v)$ une hyperface de $\mathcal{H}$ associée à un sommet v du graphe G^*. Cette hyperface est composée de l'ensemble des hyperarêtes de $\mathcal{H}$ incidentes au sommet v de $V(G^*) = \mathcal{V}$. En appliquant $\partial_2^{\mathcal{H}}$ à cette face, on obtient :

$$\partial_2^{\mathcal{H}}(\mathcal{F}(v)) = \sum_{\substack{e \in \mathcal{V} \\ v \in e}} e.$$

Nous devons montrer que ce vecteur de $C_1(\mathcal{H})$ est dans le noyau de $\partial_1^{\mathcal{H}}$. Il suffit de voir que chaque sommet $u \in V$ appartient à un nombre pair d'arêtes e de cet somme. Soit u un sommet apparaîssant dans l'une de ces arêtes. Si $u = v$, c'est le centre de l'hyperface $\mathcal{F}(v)$. Ce sommet du graphe G^* est de degré pair d'après le lemme 2.14. il est donc contenu dans un nombre pair d'hyperarêtes de $\partial_2^{\mathcal{H}}(\mathcal{F}(v))$. Considérons maintenant un sommet u voisin de v dans le graphe. L'arête $\{u, v\}$ du graphe G^* est contenu dans exactement deux faces f et f' du graphe G^*. D'après la définition 7.9, ces faces sont des hyperarêtes de $\mathcal{H}$ contenues dans la face $\mathcal{F}(v)$. Ce sont les seules hyperarêtes de $\mathcal{F}(v)$ contenant u. Ce sommet u est donc inclus dans un nombre pair d'arêtes de $\mathcal{F}(v)$. Aucun autre sommet de l'hypergraphe n'est incident à cette hyperface. Nous avons donc démontré que $\mathcal{F}(v)$ est dans le noyau de $\partial_1^{\mathcal{H}} \circ \partial_2^{\mathcal{H}}$. □

Cette relation nous permet de définir un code quantique en posant $\mathbf{H}_X$ la matrice de l'application linéaire $\partial_1^{\mathcal{H}}$ et $\mathbf{H}_Z$ est la transposée de la matrice de l'application linéaire $\partial_2^{\mathcal{H}}$. Ce code quantique est le code couleur associé au graphe G introduit lors de la définition 2.13. Pour s'en convaincre, il suffit d'exprimer les applications bord en fonction du graphe G.

On peut définir un hypergraphe dual $\mathcal{H}^* = (\mathcal{F}, \mathcal{E}, \mathcal{V})$, permettant de voir l'application $\mathbf{H}_Z$ comme la matrice de l'application bord $\partial_2^{\mathcal{H}^*}$. Comme cet hypergraphe dual est isomorphe à $\mathcal{H}$, on retrouve le fait que les matrices $\mathbf{H}_X$ et $\mathbf{H}_Z$ sont identiques.

Proposition 7.12. *Soit $C_2(\mathcal{H}) \xrightarrow{\partial_2^{\mathcal{H}}} C_1(\mathcal{H}) \xrightarrow{\partial_2^{\mathcal{H}}} C_0(\mathcal{H})$ le 2-complexe associé à un code couleur. Une erreur de Pauli qui agit sur ce code quantique admet une décomposition binaire $(E_X|E_Z) \in C_1(\mathcal{H})^2$. Son syndrome est le vecteur $(s_Z = \partial_1^{\mathcal{H}}(E_Z), s_X = \partial_2^{\mathcal{H}}(E_X)) \in C_0(\mathcal{H})^2$.*

Démonstration. Cette proposition découle de la proposition 1.31. □

Notre objectif est d'estimer l'erreur de Pauli en fonction de son syndrome. Nous traitons séparément les deux composantes binaires de cette erreur. Le syndrome d'un vecteur binaire $x \in C_1(\mathcal{H})$ est le vecteur $\partial_1^{\mathcal{H}}(x) = s \in C_0(\mathcal{H})$. Il nous suffit de savoir estimer x en fonction de s.

Définition 7.13. *Un décodage coloré de graphe G est une application :*

$$\begin{aligned} \mathcal{DC}_G : \operatorname{Im} \partial_1^{\mathcal{H}} \subset C_0(\mathcal{H}) &\longrightarrow C_1(\mathcal{H}) \\ s &\longmapsto \tilde{x} \end{aligned}$$

où $\tilde{x} \in C_1(\mathcal{H})$ est une chaîne d'hyperarêtes telle que $\partial_1^{\mathcal{H}}(\tilde{x}) = s$, de poids $w(\tilde{x})$ minimum parmi les chaînes de syndrome s.

Une fonction de décodage non corrélé à distance minimale d'un code couleur se déduit facilement d'une section minimale du syndrome $\mathcal{DC}_G$. Il suffit de poser $(\tilde{E}_X, \tilde{E}_Z) = (\mathcal{DC}_G(s_X), \mathcal{DC}_G(s_Z))$ où s_X est le syndrome de E_X et S_Z est celui de E_Z. Les vecteurs $\tilde{E}_X$ et $\tilde{E}_Z$ sont alors les estimations des vecteurs erreurs E_X et E_Z.

7.2.2 Projection de l'erreur sur trois codes de surface

La généralisation du décodage par couplage parfait aux codes couleur n'est pas immédiate. Nous pourrions définir un hypergraphe des distances $\mathcal{K}$ et un hypergraphe excité $\mathcal{K}(s)$ pour remplacer le graphe excité $K(s)$ de la définition 7.5, puis chercher un couplage parfait dans cet hypergraphe. Deux difficultés nouvelles apparaissent. La recherche d'un couplage parfait dans un hypergraphe n'est pas en général polynomial. En effet, le problème du couplage tridimensionnel qui est un cas particulier du problème du couplage dans un hypergraphe est un problème NP-complet [63]. De plus, le pré-calcul de l'hypergraphe $\mathcal{K}$ n'est *a priori* pas polynomial.

Notre but est d'estimer une erreur $x \in C_1(\mathcal{H})$ à partir de son syndrome s qui est le bord $s = \partial_1^{\mathcal{H}}(x) \in C_0(\mathcal{H})$. Pour contourner les difficultés liées à la structure d'hypergraphe, nous décomposons ce problème en deux sous-problèmes. L'erreur $x \in C_1(\mathcal{H})$ est une somme d'hyperarêtes, c'est donc aussi une somme de faces du graphe G^*. Dans un premier temps, on cherchera le bord de cette somme de faces. On remplira ensuite ce bord pour obtenir une estimation de x. Pour illustrer cette stratégie, un exemple de décodage sur un code couleur hexagonal est proposé figure 7.4. Nous nous réfèrerons à cet exemple lors des preuves qui nécessitent des outils techniques.

Lemme 7.14. *Soit G un graphe définissant un code couleur, G^* son dual et $\mathcal{H}$ l'hypergraphe associé. On a $C_1(\mathcal{H}) = C_2(G^*)$ et $C_0(\mathcal{H}) = C_0(G^*)$.*

Démonstration. Ce lemme est une conséquence immédiate de la définition de l'hypergraphe $\mathcal{H}$ dont les sommets sont les éléments de $\mathcal{V} = V(G^*)$ et dont les hyperarêtes correspondent aux faces de G^*. □

Ce lemme permet d'appliquer l'opérateur bord $\partial_2^* : C_2(G^*) \to C_1(G^*)$ à tout vecteur x de $C_1(\mathcal{H})$. On obtient ainsi le bord $b = \partial_2^*(x) \in C_1(G^*)$ de l'erreur x dessiné figure 7.4d.

Commençons par estimer le bord b de $x \in C_1(C_2(G^*))$ à partir de son syndrome. Pour cela nous utilisons la 3-coloration des faces du graphe G. Cette coloration induit une 3-coloration des sommets de son dual G^* et une coloration des arêtes de G^*. Une arête $\{u, v\}$ de G^* porte la couleur qui est absente des sommets u est v. Nous allons partitionner les arêtes de $b \in C_1(G^*)$ suivant leur couleur.

Définition 7.15. *Soit $\mathbf{c} \in \{R, V, B\}$ une couleur.* Le graphe $G^*(\mathbf{c})$ *est le sous-graphe de G^* induit par les arêtes de couleur $\mathbf{c}$.*

Ce graphe admet une structure de surface. Un sommet v de G^* de couleur rouge est entouré par un cycle rouge. Ce cycle rouge est le bord de la face $\mathcal{F}(v)$ de l'hypergraphe $\mathcal{H}$. Une telle hyperface et son bord sont représentés sur la figure 7.2. Un graphe G^* et son sous-graphe rouge sont déssinés sur la figure 7.3.

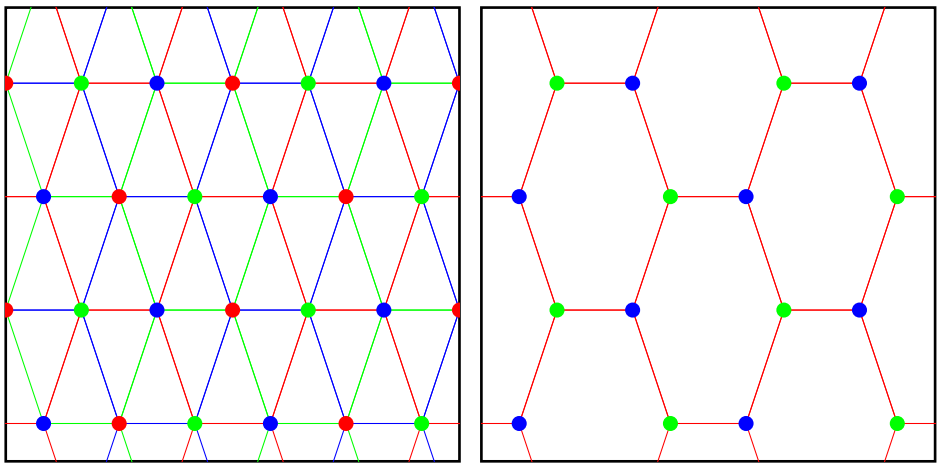


FIGURE 7.3 – Un pavage triangulaire du tore G^* dont les sommets sont 3-coloriés et son sous-graphe induit par les arêtes rouges $G^*(R)$.

Proposition 7.16. *Soit* $\mathbf{c} \in \{R, V, B\}$ *une couleur. Le graphe* $G^*(\mathbf{c})$ *définit un pavage de surface muni des faces* $\partial_2^* \circ \partial_1^{\mathcal{H}}(f)$ *où* $f \in \mathcal{F}$ *est une face de l'hypergraphe* $\mathcal{H}$ *de couleur* $\mathbf{c}$.

Le fonctionnement de l'algorithme de décodage des codes couleur que nous proposons est illustré sur un exemple dans la figure 7.4. Nous partons d'une erreur agissant sur un code couleur torique et à partir de son syndrome nous construisons une estimation valable de l'erreur d'origine. Le reste de ce chapitre est consacré à justifier rigoureusement le fonctionnement du décodage décrit par la figure 7.4.

Il y a une bijection entre les faces de l'hypergraphe de couleur $\mathbf{c}$ et les faces du graphe $G^*(\mathbf{c})$. Chacun de ces pavages de surface définit un code de surface. En se plaçant dans ces trois codes de surface, nous allons pouvoir estimer ce bord b à partir du syndrome s du vecteur x pour le code couleur.

Proposition 7.17. *Soit* $b = \partial_1^*(x)$ *le bord d'une erreur* $x \in C_1(\mathcal{H})$ *pour le code couleur et soit* $s = \partial_1^{\mathcal{H}}(x) \in C_0(\mathcal{H})$ *son syndrome. On note* $b_{\mathbf{c}} \in C_1(G^*(\mathbf{c}))$ *la restriction* b *à* $G^*(\mathbf{c})$. *Le syndrome de* $b_{\mathbf{c}} \in C_1(G^*(\mathbf{c}))$ *pour le code de surface associé au graphe* $G^*(\mathbf{c})$ *est la restriction* $s_{\mathbf{c}}$ *du syndrome* s *au graphe* $G^*(\mathbf{c})$.

Démonstration. Par linéarité, il suffit de démontrer que la propriété est satisfaite lorsque x correspond à une hyperarête de l'hypergraphe $\mathcal{H}$.

Soit e une hyperarête de $\mathcal{H}$. Cette hyperarête est un triplet $e = \{v_R, v_V, v_B\}$ de sommets de $\mathcal{H}$. Ces trois sommets portent chacun une couleur différente indiquée par les indices de ces sommets. Le syndrome de $x = e$ est le vecteur $v_R + v_V + v_B \in C_0(\mathcal{H}) = C_0(G^*)$. La restriction de ce vecteur au graphe $G^*(R)$ est le vecteur

$s_R = v_V + v_B$ car les sommets de ce graphe sont ceux qui ne portent pas la couleur R.

Pour conclure, nous allons prouver que le syndrome de b_R dans le code de surface $G^*(R)$ est bien ce vecteur $v_V + v_B$. Le vecteur $b = \partial_1^*(e)$ est le vecteur $\{v_R, v_V\} + \{v_V, v_B\} + \{v_B, v_R\} \in C_1(G^*)$. Sa restriction au graphe $G^*(R)$ est $b_R = \{v_V, v_B\}$. Le syndrome de b_R dans le code de surface $G^*(R)$ est donc le vecteur $\partial_1(b_R) = v_V + v_B \in C_0(G^*(R))$. On retrouve le vecteur annoncé. Le cas des autres couleurs est identique. Le syndrome de $b_{\mathbf{c}}$ est donc la restriction du syndrome de x pour le code couleur associé au graphe $G^*(\mathbf{c})$. □

Nous cherchons à estimer l'erreur x à partir de son syndrome s. D'après la proposition précédente nous pouvons calculer le syndrome du bord $b_{\mathbf{c}}$ de x restreint au graphe $G^*(\mathbf{c})$ à partir du syndrome s mesuré. On estime alors le bord en appliquant un décodage de surface dans le graphe $G^*(\mathbf{c})$. Cette étape du décodage est illustrée par les figures 7.4b et 7.4c.

Définition 7.18. *Soit $s \in C_0(\mathcal{H}) = C_0(G^*)$ le syndrome d'un vecteur $x \in C_1(\mathcal{H})$ pour le code couleur de graphe G. L'*estimation du bord *de x est le vecteur*

$$\tilde{b} = \tilde{b}_R + \tilde{b}_V = \tilde{b}_B \in C_1(G^*) \quad \textit{tel que} \quad \tilde{b}_{\mathbf{c}} = \mathcal{DS}_{G^*(\mathbf{c})}(s_{\mathbf{c}})$$

où $\mathcal{DS}_{G^*(\mathbf{c})}$ est un décodage de surface associé à $G^*(\mathbf{c})$ et $s_{\mathbf{c}} \in C_1(G^*(\mathbf{c}))$ est la restriction du syndrome s au graphe $G^*(\mathbf{c})$.

Par construction, lorsque ce vecteur $\tilde{b}$ est le bord d'une erreur $\tilde{x}$, le syndrome de cette erreur est s. Nous obtenons ainsi une erreur dont le syndrome est le même que celui de x et dont le bord est de poids minimum.

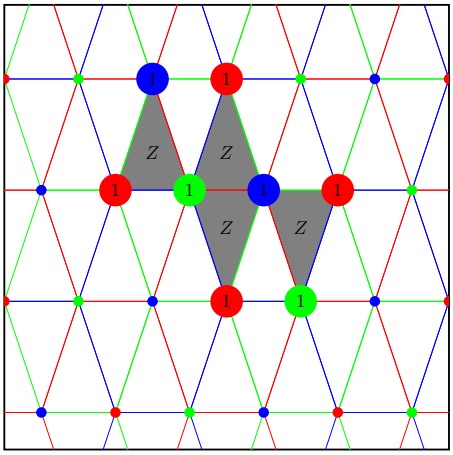
7.2.3 Relèvement du bord de l'erreur

La section précédente nous fournit un procédé d'estimation $\tilde{b} \in C_1(G^*)$ du bord de l'erreur $x \in C_1(\mathcal{H})$. Notre but est de relever ce vecteur $\tilde{b}$ en un vecteur de $C_1(\mathcal{H}) = C_2(G^*)$ lorsque ceci est possible. Nous allons remplir le bord $\tilde{b}$ comme le montre la figure 7.4e.

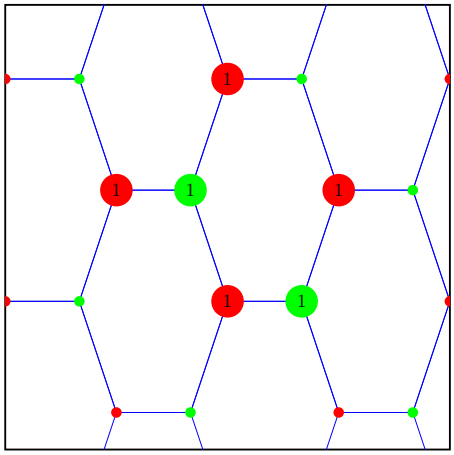
Définition 7.19. *Soit $\tilde{b} \in C_1(G^*)$. On peut voir $\tilde{b}$ comme un ensemble d'arêtes du graphe G et le sous-graphe de G induit par les arêtes de $E \backslash \tilde{b}$ est noté $G_{\tilde{b}}$.*

Définition 7.20. *Soit $C_1, C_2, \dots C_\kappa$ les composantes connexes du graphe $G_{\tilde{b}}$. Le* graphe de composantes *de $G_{\tilde{b}}$ est le graphe de sommets $V = \{1, 2, \dots, \kappa\}$ dont les arêtes sont les couples $\{i, j\}$ tels que les sous-graphes C_i et C_j du graphe G sont reliés par une arête de $\tilde{b}$.*

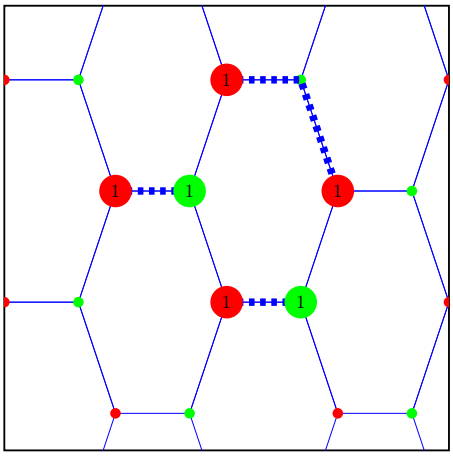
On a $C_1(\mathcal{H}) = C_2(G^*) \simeq C_0(G)$ dont un ensemble de sommets du graphe G définit un vecteur de $C_1(\mathcal{H})$.



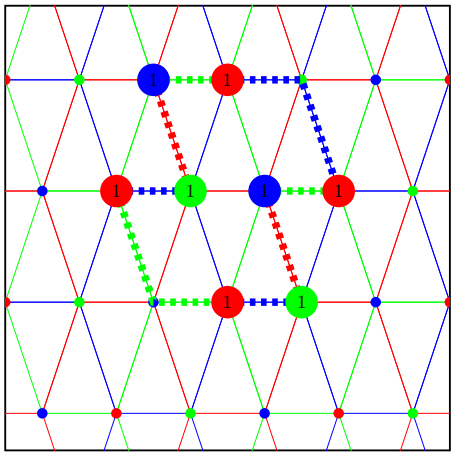
(a) Un vecteur erreur x dont le support est l'ensemble des hyperarêtes grises. Son syndrome est composé de l'ensemble des sommets portant un symbole 1.



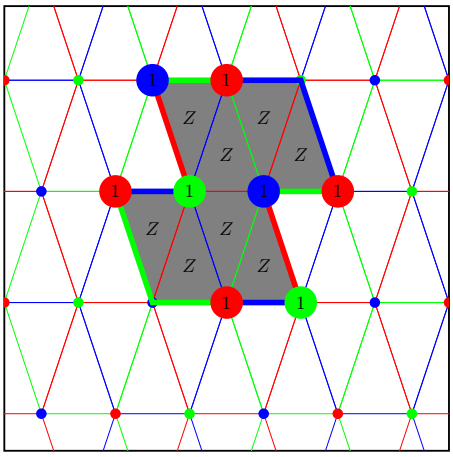
(b) on restreint le syndrome au sous-graphe bleu $G^*(B)$



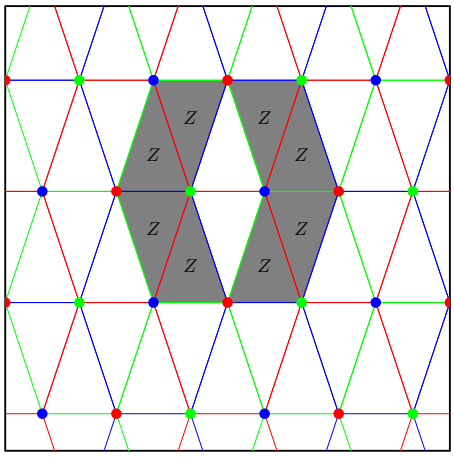
(c) On couple les sommets de syndrome 1 de manière minimale dans le graphe $G^*(B)$. Ceci définit un ensemble $\tilde{b}_B$ d'arêtes bleues ici en pointillés.



(d) On considère la réunion $\tilde{b}$ des ensembles minimaux $\tilde{b}_{\mathbf{c}}$ d'arêtes en pointillés calculés dans les trois sous-graphes $G^*(\mathbf{c})$.



(e) L'estimation $\tilde{x}$ de l'erreur est l'ensemble des hyperarêtes grise. C'est l'ensemble des hyperarêtes contenues dans le cycle $\tilde{b}$.



(f) La somme $x + \tilde{x}$ correspond aux hyperarêtes grises. Cette ensemble est la somme de deux hyperfaces. Le vecteur $\tilde{x}$ est donc une bonne estimation de x.

FIGURE 7.4 – Un exemple de décodage sur un code couleur

Définition 7.21. *Le vecteur $x \in C_1(\mathcal{H})$ défini par une partie $U \subset V(G)$ est le vecteur $x(U) = \sum_{u \in U} x(u)$, où $e(u)$ est l'hyperarête de $\mathcal{H}$ correspondant au sommet $u \in V(G)$.*

Nous sommes désormais en mesure de remplir l'intérieur de $\tilde{b}$. Pour cela nous remplissons des composantes connexes sans jamais remplir deux composantes voisines.

Proposition 7.22. *Soit $\mathcal{C}_{\tilde{b}}$ le graphe de composantes de $G_{\tilde{b}}$. On a $\tilde{b} \in \operatorname{Im} \partial_2^*$ si et seulement si le graphe $G_{\tilde{b}}$ est un graphe biparti. Dans ce cas les sommets de $G_{\tilde{b}}$ sont partitionnés en deux ensembles V_1 et V_2 et on a $\tilde{b} = \partial_2^*(\tilde{x})$ avec $\tilde{x} = x(V_1)$ et $\tilde{x} = x(V_2)$.*

Le choix de $x(V_1)$ ou $x(V_2)$ n'a aucune importance lors du décodage de ce code quantique car ces deux erreurs diffèrent d'une erreur qui fixe le code quantique.

Démonstration. Supposons que le vecteur $\tilde{b}$ soit dans l'espace $\operatorname{Im} \partial_2^*$. Il s'écrit alors $\tilde{b} = \partial_2^*(\tilde{x})$ où $\tilde{x}$ est un vecteur de $C_2(G^*)$. Montrons que l'on peut partitionner les sommets du graphe des composantes de $G_{\tilde{b}}$. Soit C_i et C_j deux composantes du graphe $G_{\tilde{b}}$ séparées par une arête de $\tilde{b}$. On peut regarder $\tilde{x}$ comme un ensemble de sommets du graphe G. Si $\tilde{x}$ contient un sommet v de la composante C_i alors il contient les voisins de x situés dans cette composante. De proche en proche, on prouve que $\tilde{x}$ contient tous les sommets de cette composante connexe. De plus, l'ensemble $\tilde{x}$ ne contient aucun sommet de la composante C_j. Sinon, cet ensemble contient tous les sommets de C_j et le bord de $\tilde{x}$ ne peut pas contenir d'arête séparant ces deux composantes. Pour finir, le vecteur $\tilde{x}$, vu comme un ensemble de sommets de G, est une réunion de composantes connexes C_i. De plus, si deux composantes sont séparées par une arête de $\tilde{b}$ alors x contient exactement l'une de ces composantes. Le vecteur $\tilde{x}$ définit donc une partition des sommets du graphe des composantes qui fait de ce graphe un graphe biparti.
Réciproquement, en partant d'un graphe des composantes biparti, on peut construire un vecteur $\tilde{x}$ convenable en posant $\tilde{x} = x(V_1)$ ou $x(V_2)$ qui correspond à la partition des sommets de $G_{\tilde{b}}$. □

Algorithme 2 Décodage non corrélé à distance minimale d'un code couleur de graphe G

Entrées: $s \in \operatorname{Im} \partial_1^{\mathcal{H}}$.
Sorties: $\tilde{x}$ tel que $\partial_1^{\mathcal{H}}(\tilde{x}) = s$ et $\partial_2^*(\tilde{x})$ de poids minimum ou bien ERREUR.
1: Pour $\mathbf{c} = R, V$ et B calculer la restriction $s_{\mathbf{c}}$ de s à $G^*(\mathbf{c})$;
2: Calculer $\tilde{b} = \sum_{\mathbf{c} \in \{R,V,B\}} \mathcal{DS}_{G^*(\mathbf{c})}(s_{\mathbf{c}})$ grâce à l'algorithme 1 ;
3: Calculer les composantes connexes du graphe $G_{\tilde{b}}$ et les arêtes du graphe $\mathcal{C}_{\tilde{b}}$;
4: Si $G_{\tilde{b}}$ est un graphe biparti retourner ERREUR ;
5: Sinon déterminer une bipartition des sommets $V(G_{\tilde{b}}) = V_1 \cup V_2$;
6: Retourner $\tilde{x} = x(V_1)$;

La complexité de l'algorithme 2, qui permet de décoder les codes couleur, est polynomiale. La détermination du nombre de composantes connexes se fait en temps linéaire $O(|E||V|)$ où $|E|$ est le nombre d'arêtes du graphe G et $|V|$ est le nombre de sommets de ce graphe [60]. L'étape la plus coûteuse est l'appel des trois décodages de surface. La complexité est donc du même ordre de grandeur que celle du décodage de surface.

Afin de comparer l'algorithme 2 à d'autres méthodes de décodage des codes couleur. Nous considérons une famille de codes couleur étudiés par Raussendorf et Sarvepalli en 2012 [85]. Le point de départ est le graphe de Cayley H_r du groupe $\mathbb{Z}/(3r)\mathbb{Z} \times \mathbb{Z}/(3r)\mathbb{Z}$ et de la partie génératrice :

$$\{\pm(1,0), \pm(0,1), \pm(1,-1)\}.$$

Ce graphe se plonge naturellement dans le tore. On peut le munir d'un ensemble de faces triangulaires et ses sommets sont 3-coloriables. C'est le dual d'un pavage hexagonal du tore définissant un code couleur. On obtient une famille de codes couleur de paramètres $[[18.r^2, 4, 4r]]$. En simulant les performances de l'algorithme 1 pour les codes définis par les graphes H_r avec $r = 2^m$, nous observons le seuil d'erreur de cette famille de codes. Ces résultats numériques sont tracés figure 7.5. Le seuil obtenu avec l'algorithme 1 est proche de 8.5%. Cette valeur est supérieure au seuil de Raussendorf et Sarvepalli qui est approximativement 7.8%.

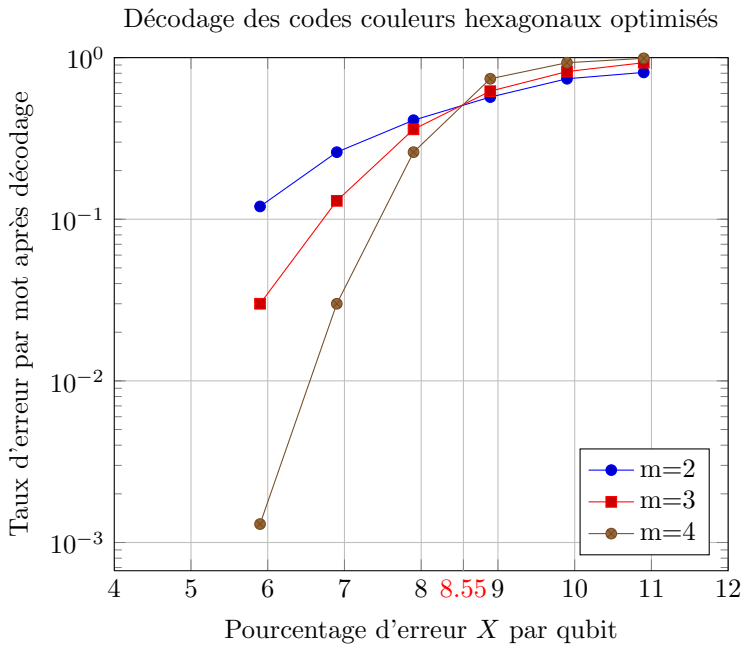


FIGURE 7.5 – Simulation numérique du décodage des codes de couleur hexagonaux de paramètres $[[18.4^m, 4, 4.2^m]]$. En abscisse la probabilité d'une erreur de phase Z (ou d'une erreur de qubit X), en ordonnée la probabilité d'erreur par mots après décodage.

Dans le théorème suivant nous prouvons que cet algorithme de décodage fonctionne lorsque les trois décodages de surfaces renvoient une erreur équivalente à

l'erreur subie. Soit $b_{\mathbf{c}} \in C_1(G^*(\mathbf{c}))$ une erreur pour le code de surface $G^*(\mathbf{c})$ et soit $\tilde{b}_{\mathbf{c}}$ son estimation par l'algorithme 1. On dit que l'erreur $\tilde{b}_{\mathbf{c}}$ corrige $b_{\mathbf{c}}$, si $\tilde{b}_{\mathbf{c}}$ est un vecteur de la classe de $b_{\mathbf{c}}$ modulo le sous-groupe $\operatorname{Im}\partial_2^{G^*(\mathbf{c})}$ car dans ce cas ces vecteurs erreurs ont la même action sur le code quantique et l'on a donc bien identifié la classe $b_{\mathbf{c}} + \operatorname{Im}\partial_2^{G^*(\mathbf{c})}$ de l'erreur subie. De manière analogue un vecteur $\tilde{x} \in C_1(\mathcal{H})$ corrige l'erreur $x \in C_1(\mathcal{H})$ si ces deux erreurs sont équivalentes modulo l'espace $\operatorname{Im}\partial_1^{\mathcal{H}}$ qui correspond aux erreurs du groupe stabilisateur du code couleur.

Théorème 7.23. *Soit $x \in C_1(\mathcal{H})$ et $b = \partial_2^*(x) \in C_1(G^*)$ son bord. On note $b_{\mathbf{c}}$ la restriction de b au graphe $G^*(\mathbf{c})$. Si pour tout $\mathbf{c}$, le décodage de surface $\mathcal{DS}_{G^*(\mathbf{c})}$ corrige $b_{\mathbf{c}}$ alors l'algorithme 2 renvoie une erreur $\tilde{x}$ qui corrige x dans le code couleur.*

Démonstration. Supposons que la correction fonctionne dans les codes de surface $G^*(\mathbf{c})$. Nous avons identifié le bord $b_{\mathbf{c}}$ à une somme de faces du graphe $G^*(\mathbf{c})$ près. On obtient une estimation $\tilde{b}$ du bord b en réunissant les trois vecteurs $\tilde{b}_{\mathbf{c}}$. Les deux vecteurs b et $\tilde{b}$ diffèrent d'un vecteur $\alpha_R + \alpha_V + \alpha_B$ où $\alpha_{\mathbf{c}}$ est une somme de faces du graphe $G^*(\mathbf{c})$. D'après la proposition 7.16 les faces du graphe $G^*(\mathbf{c})$ sont les bords des faces de couleur $\mathbf{c}$ de l'hypergraphe. En remplissant les bords b et $\tilde{b}$ on obtient donc deux erreurs x et $\tilde{x}$ qui diffèrent d'une somme d'hyperarêtes de $\mathcal{H}$. Ces erreurs sont donc équivalentes modulo $\operatorname{Im}\partial_2^{\mathcal{H}}$.

□

7.2.4 Comparaison des seuils des codes couleur et des codes de surface

Nous avons construit un algorithme de décodage des codes couleur qui fait appel à un décodage des codes de surface. Ceci permet de transférer des résultats des codes de surface vers les codes couleur. Dans cette partie, nous comparons les seuils d'erreur de ces deux familles de codes topologiques.

Rappelons que le *seuil d'erreur tolérable* ou seuil d'erreur d'une famille de codes stabilisateurs est le taux de dépolarisation q maximum pour lequel la probabilité d'erreur après décodage tend vers 0. Ce seuil dépend de l'algorithme de décodage utilisé. Nous supposerons que nous utilisons l'algorithme 1 pour les codes de surface et l'algorithme 2 pour les codes couleur. Comme nous travaillons sur des familles de codes CSS, nous considérons non pas la probabilité de dépolarisation q mais la probabilité d'erreur de phase Z (ou d'erreur de qubit X) noté p qui est relié au taux de dépolarisation par la relation $p = 2q/3$. Nous parlerons du *seuil d'erreur de phase Z* (ou d'erreur de qubit X) tolérable.

Théorème 7.24. *Soit $(G_t)_t$ une famille de graphes définissant une famille de codes couleur de seuil d'erreur de phase p_e et soit $p_e(\mathbf{c})$ le seuil d'erreur de phase de la famille des codes de surface $(G_t^*(\mathbf{c}))_t$. Le seuil d'erreur p_e de cette famille de codes couleur est minoré par :*

$$p_e \geq \min_{\mathbf{c}\in\{R,V,B\}} \{1 - \sqrt{1 - p_e(\mathbf{c})}\}.$$

Démonstration. L'algorithme 1 projette une erreur $x \in C_1(\mathcal{H})$ agissant sur le code couleur sur une erreur agissant sur le code de surface $G^*(\mathbf{c})$. Pour démontrer ce théorème, on considère une erreur de Pauli (E_X, E_Z) aléatoire dans le code couleur issue d'un canal de dépolarisation de probabilité p. Le vecteur aléatoire $x = E_X$ suit une loi binomiale de probabilité $p = 2q/3$. Son image dans le code de surface $G^*(\mathbf{c})$ suit une loi binomial de probabilité $2p - p^2$. Cette remarque est basée sur le fait que chaque qubit d'un code de surface $G^*(\mathbf{c})$ correspond à deux qubits du code couleur. La probabilité d'avoir une erreur X sur un qubit du code de surface est donc la probabilité d'erreur sur l'un de ces deux qubits du code couleur mais pas sur les deux.

Lorsque la probabilité $2p - p^2$ dans les codes de surface $G^*(\mathbf{c})$ est située sous le seuil d'erreur de phase de ces trois codes de surface, la probabilité d'erreur en X après décodage tend vers 0 dans ces trois codes. On peut répéter cet argument pour la composante E_Z. En appliquant le théorème 7.23, on conclut que la probabilité d'erreur pour le code couleur tend vers 0. Nous avons démontré que si $2p-p^2 < p_e(\mathbf{c})$ pour les trois couleurs, alors p est sous le seuil d'erreur du code couleur : $p < p_e$. La résolution de l'équation $2p - p^2 = p_e(\mathbf{c})$ termine la preuve. □

Conclusion

- Nous avons proposé un nouvel algorithme de décodage des codes couleur. Cet algorithme est basé sur la projection de l'erreur agissant sur le code couleur sur une erreur agissant sur un code de surface. Il permet d'adapter n'importe quel algorithme de décodage des codes de surface au décodage des codes couleur. Nous avons transformé le décodage des codes de surface par couplage parfait en un décodage des codes couleur.
- Cette procédure de décodage n'est pas toujours en mesure d'estimer l'erreur à distance minimale. En effet, lorsque le bord estimé $\tilde{b}$ n'est pas un vecteur de $\operatorname{Im} \partial_2^*$, l'algorithme 2 renvoie $ERREUR$. Il pourrait être amélioré en considérant ces configurations problématiques. Malgré cela, les performances de l'algorithme 2 appliqué aux codes couleur toriques hexagonaux (Figure 7.5) sont meilleures que celles obtenues récemment par Raussendorf et Sarvepalli [85]. Ceci nous encourage à travailler à l'amélioration de notre algorithme.
- Le décodage des codes couleur passe par la projection de l'erreur sur trois codes de surface. Cette stratégie se rapproche de celle de Bombin, Duclos-Cianci et Poulin [16]. Pour décoder les codes couleur, ils décomposent un code couleur en deux codes de surface. Il ne reste alors plus qu'à décoder les codes de surface pour corriger l'erreur dans le code couleur. L'inconvénient de leur décomposition en codes de surface est que le modèle d'erreur est perturbé. Notre procédure de décodage conserve le modèle d'erreur. On en déduit le théorème 7.24 qui relie les seuils d'erreur de ces deux familles de codes.
- Deux directions sont envisageables pour améliorer les différents algorithmes de décodage des codes quantiques et plus particulièrement des codes topologiques. Le décodage recherché dans ce chapitre est un décodage par maximum de vraisemblance sur les erreurs. Comme l'effet d'une erreur de Pauli sur le code quantique ne dépend que de sa classe modulo le groupe stabilisateur,

nous devrions chercher la classe d'équivalence $E.S$ la plus probable plutôt que l'erreur la plus probable. Cette amélioration du décodage, particulière au cadre quantique, est difficile à mettre en place.
Nous considérons le problème du décodage non-corrélé à distance minimale des codes CSS. Nous cherchons à déterminer les composantes binaires E_X et E_Z de poids minimum qui atteignent un syndrome donné. Ces composantes ne définissent pas, en général, l'erreur de Pauli de poids minimum qui atteint ce syndrome. Nous pouvons espérer atteindre de meilleures performances, en cherchant l'erreur de Pauli de poids minimum qui atteint un syndrome donné. Pour cela nous devons considérer les corrélations entre les composantes binaires E_X et E_Z d'une erreur de Pauli.

Bibliographie

[1] Aly, S. A class of quantum LDPC codes derived from latin squares and combinatorial objects. Tech. rep., Department of Computer Science, Texas A and M University, 2007.

[2] Aly, S. A class of quantum LDPC codes constructed from finite geometries. In *IEEE Global Telecommunications Conference, GLOBECOM 2008* (2008), pp. 1–5.

[3] Andriyanova, I., Maurice, D., and Tillich, J. New constructions of CSS codes obtained by moving to higher alphabets. `http://arxiv.org/abs/1202.3338`, 2012.

[4] Bacon, D. Operator quantum error-correcting subsystems for self-correcting quantum memories. *Physical Review A 73*, 1 (2006), 012340.

[5] Baek, S., Minnhagen, P., and Kim, B. Percolation on hyperbolic lattices. *Physical Review E 79* (2009), 011124.

[6] Barak, O., Burshtein, D., and Feder, M. Bounds on achievable rates of LDPC codes used over the binary erasure channel. *IEEE Transaction on Information Theory 50*, 10 (2004), 2483–2492.

[7] Benjamini, I., and Schramm, O. Percolation beyond Z^d, many questions and a few answers. *Electronic Communications in Probability 1* (1996), 71–82.

[8] Benjamini, I., and Schramm, O. Percolation in the hyperbolic plane. *Selected Works of Oded Schramm* (2011), 729–749.

[9] Bennett, C., and Brassard, G. Quantum cryptography : Public key distribution and coin tossing. In *Proc. of IEEE International Conference on Computers, Systems and Signal Processing* (1984), vol. 175, Bangalore, India.

[10] Bennett, C., DiVincenzo, D., and Smolin, J. Capacities of quantum erasure channels. *Physical Review Letters 78* (1997), 3217–3220.

[11] Bennett, C., DiVincenzo, D., Smolin, J., and Wootters, W. Mixed-state entanglement and quantum error correction. *Physical Review A 54*, 5 (1996), 3824.

[12] Berge, C. *Graphs and Hypergraphs*. Elsevier, 1973.

[13] Berger, M. Systoles et applications selon Gromov. *Astérisque 216* (1993), 279–310.

[14] Bombin, H. Topological subsystem codes. *Physical Review A 81*, 3 (2010), 032301.

[15] BOMBIN, H. Clifford gates by code deformation. *New Journal of Physics 13* (2011), 043005.

[16] BOMBIN, H., DUCLOS-CIANCI, G., AND POULIN, D. Universal topological phase of two-dimensional stabilizer codes. *New Journal of Physics 14*, 7 (2012), 073048.

[17] BOMBIN, H., AND MARTIN-DELGADO, M. Topological quantum distillation. *Physical Review Letters 97* (2006), 180501.

[18] BOMBIN, H., AND MARTIN-DELGADO, M. Homological error correction : Classical and quantum codes. *Journal of Mathematical Physics 48*, 5 (2007), 052105.

[19] BOMBIN, H., AND MARTIN-DELGADO, M. A. Exact topological quantum order in $D = 3$ and beyond : Branyons and brane-net condensates. *Physical Review B 75* (2007), 075103.

[20] BRAVYI, S., DUCLOS-CIANCI, G., POULIN, D., AND SUCHARA, M. Subsystem surface codes with three-qubit check operators. `http://arxiv.org/abs/1207.1443`, 2012.

[21] BRAVYI, S., AND KITAEV, A. Quantum codes on a lattice with boundary. `http://arxiv.org/abs/quant-ph/9811052`, 1998.

[22] BRAVYI, S., LEEMHUIS, B., AND TERHAL, B. Topological order in an exactly solvable 3d spin model. *Annals of Physics 326*, 4 (2011), 839–866.

[23] BRAVYI, S., POULIN, D., AND TERHAL, B. Tradeoffs for reliable quantum information storage in 2D systems. *Physical Review Letters 104*, 5 (2010), 50503.

[24] BRAVYI, S., AND TERHAL, B. A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes. *New Journal of Physics 11*, 4 (2009), 043029.

[25] BRUSS, D., DIVINCENZO, D., EKERT, A., FUCHS, C., MACCHIAVELLO, C., AND SMOLIN, J. Optimal universal and state-dependent quantum cloning. *Physical Review A 57*, 4 (1998), 2368.

[26] BURSHTEIN, D., KRIVELEVICH, M., LITSYN, S., AND MILLER, G. Upper bounds on the rate of LDPC codes. *IEEE Transaction on Information Theory 48*, 9 (2002), 2437–2449.

[27] CALDERBANK, A., RAINS, E., SHOR, P., AND SLOANE, N. Quantum error correction via codes over $GF(4)$. *IEEE Transaction on Information Theory 44*, 4 (1998), 1369–1387.

[28] CALDERBANK, A., AND SHOR, P. Good quantum error-correcting codes exist. *Physical Review A 54*, 2 (1996), 1098.

[29] CAMARA, T., OLLIVIER, H., AND TILLICH, J.-P. A class of quantum LDPC codes : construction and performances under iterative decoding. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2007* (2007), pp. 811–815.

[30] CERF, N. Entropic bounds on coding for noisy quantum channels. *Physical Review A 57*, 5 (1998), 3330.

[31] CERF, N. Pauli cloning of a quantum bit. *Physical Review Letters 84*, 19 (2000), 4497–4500.

[32] COUVREUR, A., DELFOSSE, N., AND ZÉMOR, G. A construction of quantum LDPC codes from cayley graphs. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2011* (2011), pp. 643–647.

[33] COUVREUR, A., DELFOSSE, N., AND ZÉMOR, G. A construction of quantum LDPC codes from cayley graphs. `http://arxiv.org/abs/1206.2656`, 2012.

[34] COVER, T., AND THOMAS, J. *Elements of Information Theory*. Wiley-Interscience, 1991.

[35] DECREUSEFOND, L., AND ZÉMOR, G. On the error-correcting capabilities of cycle codes of graphs. In *Proc. of IEEE International Symposium on Information Theory, ISIT 1994* (1994), p. 307.

[36] DELFOSSE, N., AND ZÉMOR, G. Quantum erasure-correcting codes and percolation on regular tilings of the hyperbolic plane. In *Proc. of IEEE Information Theory Workshop, ITW 2010* (2010), pp. 1–5.

[37] DELFOSSE, N., AND ZÉMOR, G. Upper bounds on the rate of low density stabilizer codes for the quantum erasure channel. `http://arxiv.org/abs/1205.7036`, 2012.

[38] DENNIS, E., KITAEV, A., LANDAHL, A., AND PRESKILL, J. Topological quantum memory. *Journal of Mathematical Physics 43* (2002), 4452.

[39] DIVINCENZO, D., SHOR, P., AND SMOLIN, J. Quantum-channel capacity of very noisy channels. *Physical Review A 57*, 2 (1998), 830.

[40] DUCLOS-CIANCI, G., AND POULIN, D. A renormalization group decoding algorithm for topological quantum codes. In *Proc. of IEEE Information Theory Workshop, ITW 2010* (2010), pp. 1–5.

[41] EDMONDS, J. Maximum matching and a polyhedron with 0-1 vertices. *Journal of Research at the National Bureau of Standards 69B* (1965), 125–130.

[42] EDMONDS, J. Path, trees, and flowers. *Canadian Journal of Mathematics 17* (1965), 449–467.

[43] FETAYA, E. Bounding the distance of quantum surface codes. *Journal of Mathematical Physics 53* (2012), 062202.

[44] FEYNMAN, R. Simulating physics with computers. *International journal of theoretical physics 21*, 6 (1982), 467–488.

[45] FLAJOLET, P., AND SEDGEWICK, R. *Analytic Combinatorics*, 1 ed. Cambridge University Press, 2009.

[46] FOWLER, A., WHITESIDE, A., AND HOLLENBERG, L. Towards practical classical processing for the surface code. *Physical Review Letters 108* (2012), 180501.

[47] FREEDMAN, M., MEYER, D., AND LUO, F. Z2-systolic freedom and quantum codes. *Mathematics of Quantum Computation, Chapman & Hall/CRC* (2002), 287–320.

[48] FRIEDMAN, J., AND TILLICH, J. Generalized alon-boppana theorems and error-correcting codes. *SIAM Journal on Discrete Mathematics 19*, 3 (2006), 700.

[49] GALLAGER, R. *Low Density Parity-Check Codes*. PhD thesis, Massachusetts Institute of Technology, 1963.

[50] GIBLIN, P. *Graphs, surfaces and homology*. Cambridge University Press, 2010.

[51] GOTTESMAN, D. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, 1997.

[52] GRASSL, M., BETH, T., AND PELLIZZARI, T. Codes for the quantum erasure channel. *Physical Review A 56* (1997), 33–38.

[53] GRIMMETT, G. *Percolation*, 2 ed. Springer-Verlag, 1999.

[54] GROMOV, M. Systoles and intersystolic inequalities. *Actes de la Table Ronde de Géométrie Différentielle (Luminy, 1992) 1* (1992), 291–362.

[55] GU, H., AND ZIFF, R. Crossing on hyperbolic lattices. *Physical Review E 85* (2012), 051141.

[56] HAAH, J. Local stabilizer codes in three dimensions without string logical operators. *Physical Review A 83*, 4 (2011), 042330.

[57] HAGIWARA, M., AND IMAI, H. Quantum quasi-cyclic LDPC codes. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2007* (2007), pp. 806–810.

[58] HATCHER, A. *Algebraic topology*. Cambridge University Press, 2002.

[59] HÉNAUT, A., AND YGER, A. *Éléments de géométrie : niveau M1*. Ellipses, 2004.

[60] HOPCROFT, J., AND TARJAN, R. Algorithm 447 : efficient algorithms for graph manipulation. *Communications of the ACM 16*, 6 (1973), 372–378.

[61] HSIEH, M., AND LE GALL, F. NP-hardness of decoding quantum error-correction codes. *Physical Review A 83*, 5 (2011), 052331.

[62] IOFFE, L., AND MÉZARD, M. Asymmetric quantum error-correcting codes. *Physical Review A 75*, 3 (2007), 032345.

[63] JOHNSON, D., AND GAREY, M. Computers and intractability : A guide to the theory of NP-completeness. *Freeman&Co, San Francisco* (1979).

[64] KESTEN, H. The critical probability of bond percolation on the square lattice equals 1/2. *Communications in Mathematical Physics 74* (1980), 41–59.

[65] KIM, I. *Quantum codes on Hurwitz surfaces*. PhD thesis, Massachusetts Institute of Technology, 2007.

[66] KITAEV, A. Fault-tolerant quantum computation by anyons. *Annals of Physics 303*, 1 (1997), 27.

[67] KOLMOGOROV, V. Blossom V : a new implementation of a minimum cost perfect matching algorithm. *Mathematical Programming Computation 1* (2009), 43–67.

[68] LOVÁSZ, L. Submodular functions and convexity. *Mathematical programming : the state of the art* (1983), 235–257.

[69] LUBY, M., MITZENMACHER, M., SHOKROLLAHI, M., AND SPIELMAN, D. Improved low-density parity-check codes using irregular graphs. *IEEE Transaction on Information Theory 47*, 2 (2001), 585–598.

[70] MACKAY, D., MITCHISON, G., AND SHOKROLLAHI, A. More sparse-graph codes for quantum error-correction. `www.inference.phy.cam.ac.uk/mackay/cayley.pdf`, 2007.

[71] MACKAY, D., AND NEAL, R. Good codes based on very sparse matrices. In *Cryptography and Coding. 5th IMA Conference, number 1025 in Lecture Notes in Computer Science* (1995), Springer, pp. 100–111.

[72] MACKAY, D., AND NEAL, R. Good error-correcting codes based on very sparse matrices. *IEEE Transaction on Information Theory* (1999), 399–431.

[73] MACKAY, D. J. C., MITCHISON, G., AND MCFADDEN, P. L. Sparse-graph codes for quantum error correction. *IEEE Transaction on Information Theory 50*, 10 (2004), 2315–2330.

[74] MARGULIS, G. Explicit constructions of graphs without short cycles and low density codes. *Combinatorica 2* (1982), 71–78. 10.1007/BF02579283.

[75] NIELSEN, M., AND CHUANG, I. *Quantum Computation and Quantum Information*, 1 ed. Cambridge University Press, 2000.

[76] OXLEY, J. *Matroid Theory*. Oxford University Press, New York, 1992.

[77] POULIN, D. Stabilizer formalism for operator quantum error correction. *Physical Review Letters 95*, 23 (2005), 230504.

[78] POULIN, D., AND CHUNG, Y. On the iterative decoding of sparse quantum codes. *Quantum Information & Computation 8*, 10 (2008), 987–1000.

[79] PRESKILL, J. Quantum information and computation. `http://theory.caltech.edu/~preskill/ph229/`, 1998.

[80] RAUSSENDORF, R., AND HARRINGTON, J. Fault-tolerant quantum computation with high threshold in two dimensions. *Physical Review Letters 98*, 19 (2007), 190504.

[81] RAUSSENDORF, R., HARRINGTON, J., AND GOYAL, K. Topological fault-tolerance in cluster state quantum computation. *New Journal of Physics 9* (2007), 199.

[82] RICHARDSON, T., SHOKROLLAHI, M., AND URBANKE, R. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Transaction on Information Theory 47* (2001), 619–637.

[83] RICHARDSON, T., AND URBANKE, R. *Modern Coding Theory*, 1 ed. Cambridge University Press, 2008.

[84] SARVEPALLI, K., RÖTTELER, M., AND KLAPPENECKER, A. Asymmetric quantum LDPC codes. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2008* (2008), pp. 305–309.

[85] SARVEPALLI, P., AND RAUSSENDORF, R. Efficient decoding of topological color codes. *Physical Review A 85*, 2 (2012), 022317.

[86] SHOR, P. Algorithms for quantum computation : discrete logarithms and factoring. In *Proc. of IEEE Symposium on Foundations of Computer Science* (1994), pp. 124–134.

[87] SHOR, P. Scheme for reducing decoherence in quantum computer memory. *Physical Review A 52*, 4 (1995), R2493.

[88] SMITH, G., AND SMOLIN, J. Additive extensions of a quantum channel. In *Proc. of IEEE Information Theory Workshop, ITW 2008* (2008), pp. 368–372.

[89] STACE, T., BARRETT, S., AND DOHERTY, A. Thresholds for topological codes in the presence of loss. *Physical Review Letters 102*, 20 (2009), 200501.

[90] STEANE, A. Multiple-particle interference and quantum error correction. *Proc. of the Royal Society of London. Series A : Mathematical, Physical and Engineering Sciences 452*, 1954 (1996), 2551–2577.

[91] TANNER, R. A recursive approach to low complexity codes. *IEEE Transaction on Information Theory 27*, 5 (1981), 533–547.

[92] TILLICH, J.-P., AND ZÉMOR, G. Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$;. In *Proc. of IEEE International Symposium on Information Theory, ISIT 2009* (2009), pp. 799–803.

[93] ŠIRÁŇ, J. Triangle group representations and constructions of regular maps. *Proc. of the London Mathematical Society 82*, 03 (2000), 513–532.

[94] WANG, D., FOWLER, A., HILL, C., AND HOLLENBERG, L. Graphical algorithms and threshold error rates for the 2d color code. *Quantum Information & Computation 10*, 9 (2010), 780–802.

[95] WANG, D., FOWLER, A., STEPHENS, A., AND HOLLENBERG, L. Threshold error rates for the toric and planar codes. *Quantum Information & Computation 10*, 5 (2010), 456–469.

[96] WELSH, D. *Matroid theory*, vol. 5. Academic Press London, 1976.

[97] WILF, H. *Generatingfunctionology*, 3 ed. A K Peters/CRC Press, 2005.

[98] WOOTTERS, W., AND ZUREK, W. A single quantum cannot be cloned. *Nature 299* (1982), 802–803.

[99] ZÉMOR, G. On iterative decoding of cycle codes of graphs. *IMA Volumes in Mathematics and its Applications 123* (2001), 311–326.

[100] ZÉMOR, G. On cayley graphs, surface codes, and the limits of homological coding for quantum error correction. In *Proc. of the 2nd International Workshop on Coding and Cryptology, IWCC 2009* (2009), Springer-Verlag, pp. 259–273.