Cryptographie Quantique : Protocoles et Graphes

Jérôme Javelle

UNIVERSITÉ DE GRENOBLE

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Mathématiques/Informatique**

Arrêté ministériel : 7 août 2006

Présentée par

Jérôme Javelle

Thèse dirigée par **Pablo Arrighi**

préparée au sein du **Laboratoire d'informatique de Grenoble**
et de l' **EDMSTII**

Cryptographie Quantique: Protocoles et Graphes

Thèse soutenue publiquement le **2 juin 2014**,
devant le jury composé de :

Damian Markham
CR1 CNRS, Telecom ParisTech, LTCI, Rapporteur
Ioan Todinca
Prof. Univ. d'Orléans, LIFO, Rapporteur
Emmanuel Jeandel
Prof. Univ. de Lorraine, LORIA, Examinateur
Sophie Laplante
Prof Univ. Paris Diderot, LIAFA, Examinatrice
Frédéric Maffray
DR CNRS, G-SCOP, Examinateur
Pablo Arrighi
MCF UJF, HDR, délégation Inria-Grand-Est, LORIA, Directeur de thèse
Mehdi Mhalla
CR1 CNRS, LIG, Co-Encadrant de thèse
Simon Perdrix
CR1 CNRS, LORIA, Co-Encadrant de thèse
Jean-Louis Roch
MCF Grenoble INP, LIG, Invité

Table des matières

Préambule

Les travaux présentés dans ce document s'inscrivent dans les domaines de la cryptographie quantique et de la théorie des graphes. Nous commençons par introduire quelques notions élémentaires dans ces deux domaines (Chapitre 1).

Dans le Chapitre 2, nous développons des protocoles cryptographiques permettant le partage d'un secret de nature classique puis quantique en utilisant des états quantiques particuliers : les états graphes. Ces résultats reposent sur les travaux suivants :

– Sylvain Gravier, Jérôme Javelle, Mehdi Mhalla, Simon Perdrix *Quantum Secret Sharing with Graph States* Mathematical and Engineering Methods in Computer Science (MEMICS 2012), LNCS, vol 7721, pp 15–31, 2012
– Jérôme Javelle, Mehdi Mhalla, Simon Perdrix *New Protocols and Lower Bound for Quantum Secret Sharing with Graph States* Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC'12), LNCS Vol 7582 pp 1-12, 2013
– Jérôme Javelle, Mehdi Mhalla, Simon Perdrix *Classical versus quantum secret sharing* arXiv 1109.4731, Rapport de recherche

Les structures de ces protocoles nous amènent à considérer des propriétés de théorie des graphes liées en partie à l'opération de complémentation locale et à des problèmes de domination. Dans le Chapitre 3, nous étudions ces problèmes ainsi que leur complexité en utilisant entre autres des méthodes probabilistes et des familles de graphes aux propriétés intéressantes.

Le Chapitre 4 présente l'étude de propriétés des graphes de Paley et fait le lien entre les problèmes étudiés dans le Chapitre 3 et des résultats et conjectures connus en géométrie algébrique. L'essentiel des résultats de ce deux parties ont fait l'objet de la publication :

– Jérôme Javelle, Mehdi Mhalla, Simon Perdrix *On the Minimum Degree Up to Local Complementation : Bounds and Complexity* International Workshop on Graph-Theoretic Concepts in Computer Science (WG'12) LNCS vol 7551 pp 138–147, 2012

La dernière partie du Chapitre 4 est plus exploratoire et propose une nouvelle approche pour l'étude de la structure des graphes de Paley.

Chapitre 1

Introduction

1.1 De la physique à la cryptographie quantique

Une des particularités du domaine de la mécanique quantique est l'aspect peu intuitif des phénomènes qui ont lieu à des échelles de temps et d'espace extrêmement petites. L'idée d'utiliser les atomes, photons, électrons et autres particules dont le comportement se décrit par les lois de la physique quantique en tant que support d'information émerge un peu plus tard. On voit alors émerger un nouveau type d'information qui, lui aussi, possède des propriétés qui n'ont pas leur analogue à notre échelle. On compte parmi elles le principe de superposition, le principe d'incertitude d'Heisenberg, et l'intrication. Un des premiers résultats concernant l'utilisation des principes de la mécanique quantique pour encoder de l'information est proposé par Wiesner à la fin des années 70 [Wie83].

Bien que peu intuitifs, les postulats sur lesquels repose la théorie de l'information quantique se prêtent particulièrement bien à une mise en équation, et on peut exprimer assez simplement les contraintes, évolutions et interactions des états quantiques au cours du temps.

La formalisation mathématique de l'information quantique va de pair avec l'apparition d'une théorie du calcul et de l'algorithmique quantiques. Tout comme en théorie de l'information classique, on définit des machines de Turing quantiques [DD85, BBV93] ou encore des circuits avec des portes logiques quantiques [DD85, Yao93].

L'émergence du domaine de l'information quantique fait apparaître la question de l'existence de "versions quantiques" des algorithmes classiques connus en vue d'en améliorer le temps d'exécution. Ainsi, le problème de la recherche d'un élément dans une liste non triée de taille n peut être résolu en temps linéaire $\Theta(n)$ à l'aide d'un algorithme classique, et cette complexité est optimale. Cependant, on connait un algorithme quantique qui s'exécute en $\mathcal{O}(\sqrt{n})$: l'algorithme de recherche de Grover [Gro96]. Dans certains cas, on constate une amélioration exponentielle des meilleurs algorithmes classiques connus :

c'est la cas du problème de la factorisation des entiers dont les meilleurs algorithmes classiques connus s'exécutent en temps sous-exponentiel $2^{\mathcal{O}\left((logn)^{\frac{1}{3}}(loglogn)^{\frac{2}{3}}\right)}$ (algorithme GNFS inspiré par [LLMP90]) alors que ce problème peut être résolu par un algorithme quantique s'exécutant en temps $\mathcal{O}(n^3)$: l'algorithme de Shor [Sho97]. Il en est de même pour le problème du logarithme discret dont un algorithme quantique polynomial est décrit dans [Sho97] également.

Ces améliorations liées à la nature de l'information quantique portent atteinte à la sécurité des systèmes cryptographiques basés sur la difficulté présumée des problèmes précédents. Ainsi l'algorithme de Shor pour factoriser les entiers remet en cause la sécurité du cryptosystème RSA [RSA78] qui repose sur la difficulté présumée du problème de la factorisation. De même, les cryptosystèmes de Diffie Hellman [DH76], El Gamal [Gam84], ainsi que la cryptographie sur les courbes elliptiques plus récemment étudiée [Was08] ne sont pas sécurisés face à un adversaire quantique (problème du logarithme discret).

Si la théorie de l'information quantique fournit à un attaquant potentiel des méthodes beaucoup plus efficaces que celles utilisées classiquement, on peut également l'utiliser pour fournir une protection plus robuste de l'information classique. Par exemple, le protocole proposé par Bennett et Brassard [BB84] utilise un canal quantique entre deux parties Alice et Bob pour échanger une clé classique. Cet échange possède une sécurité absolue (qui ne dépend pas d'hypothèses calculatoires), et la clé ainsi échangée peut permettre l'établissement d'un "one-time pad" entre Alice et Bob, protocole dont la sécurité est également inconditionnelle. Que ce soit en terme de calcul ou de cryptographie quantique, des outils et méthodes spécifiques sont également utilisés pour manipuler l'information quantique.

Parmi les protocoles de cryptographie quantique existants, on compte notamment les protocoles de partage de secret. Ils consistent en la distribution d'un secret classique ou quantique entre plusieurs personnes qui doivent se concerter pour pouvoir y accéder. Les protocoles de partage de secret constituent une primitive cryptographique dont le cas classique a été largement traité [Sha79, Bla79], mais dont les analogues quantiques laissent la place a plusieurs améliorations.

Certaines familles d'états quantiques présentent un intérêt particulier dans le domaine du calcul et des protocoles quantiques : les états graphes. Ce sont des états représentés par des graphes, objets mathématiques largement utilisés en informatique en général. Ainsi, de nombreuses propriétés quantiques sur les états graphes peuvent être établies en étudiant directement les propriétés des graphes sous-jacents. Les états graphes fournissent un très bon support pour le calcul quantique, notamment pour le calcul par mesure [RB01] ainsi que pour l'établissement de protocoles de calcul à l'aveugle [BFK09].

Les travaux présentés dans ce document traitent de l'utilisation des états graphes dans les protocoles de partage de secret quantique et de l'étude des structures des graphes

associés. Nous étudierons la construction de ces protocoles optimisant les ressources données à chacune des parties, puis nous nous intéresserons aux problèmes structurels de théorie des graphes liés au partage de secret quantique avec des états graphes.

Dans ce document, nous présentons tout d'abord l'étude des protocoles de partage de secret utilisant des états graphes dans le cas d'un secret classique puis quantique et nous proposons des constructions optimisant certains paramètres. Dans un deuxième temps nous étudions des propriétés de théorie des graphes liées à l'utilisation des états graphes comme supports pour le calcul quantique ainsi que pour les protocoles de partage de secret autour de la notion de "complémentation locale". Nous étudions enfin les propriétés locales de la famille des graphes de Paley qui semblent adaptés aux protocoles de partage de secret quantique présentés.

Commençons par donner quelques propriétés de théories des graphes utiles par la suite, ainsi qu'un aperçu des notions fondamentales de théorie de l'information quantique.

1.2 Quelques propriétés de théorie des graphes

Nous donnons ici quelques notions élémentaires de théorie des graphes qui seront utilisées par la suite dans les structures de graphes étudiées.

D'un point de vue formel, on définit un graphe de la façon suivante :

Définition 1.1. *On appelle "graphe" tout couple d'ensembles $G = (V, E)$ vérifiant*
– V est un ensemble fini appelé "ensemble de sommets"
– $E \subseteq V \times V$ et est appelé "ensemble d'arêtes"
La taille de l'ensemble V est appelé "ordre du graphe G".

Dans ce document, on ne considèrera que les graphes non-orientés ($(u, v) \in E \Leftrightarrow (v, u) \in E$) et sans boucles ($\forall u \in V, (u, u) \notin E$). On notera donc les arêtes entre un sommet u et un sommet v de la façon suivante : $\{u, v\}$. Une représentation (dessin) usuelle des graphes est la suivante : chaque sommet est représenté par un point, et chaque arête par une ligne reliant les deux points correspondants aux sommets de l'arête.

Nous donnons à présent la définition du voisinage d'un sommet :

Définition 1.2. *Soit $G = (V, E)$ un graphe et $u \in V$ l'un de ses sommets. On appelle "voisinage de u" l'ensemble*

$$\mathcal{N}(u) = \{v \in V \text{ tel que } \{u, v\} \in E\} \tag{1.1}$$

Un sommet dont le voisinage est l'ensemble des autres sommets du graphe est dit "universel".

Définition 1.3. *Soit $G = (V, E)$ un graphe et $S \subseteq V$ un ensemble de sommets. S est appelé*
– un "stable" lorsqu'il n'existe aucune arête entre les sommets de S
– une "clique" lorsque tous les sommets de S sont reliés par une arête

Le graphe d'ordre n composé d'une clique de taille n est dit "complet" est on le note K_n.

Nous introduisons à présent la notion de "voisinage impair" des sommets d'un graphe, notion centrale dans ce document.

Définition 1.4. *Soit $G = (V, E)$ un graphe. Soit $D \subseteq V$ un ensemble de sommets quelconque. On appelle "voisinage impair de D" l'ensemble suivant :*

$$Odd(D) = \{v \in V \ tq \ |\mathcal{N}(v) \cap D| = 1 \bmod 2\} \tag{1.2}$$

De façon similaire, le "voisinage pair" de D est l'ensemble suivant :

$$Even(D) = \{v \in V \ tq \ |\mathcal{N}(v) \cap D| = 0 \bmod 2\} \tag{1.3}$$

En cas d'ambigüité, on précisera le graphe en question en indice : $Odd_G(D)$ et $Even_G(D)$.

La Figure 1.1 permet de visualiser ces ensembles : les sommets de $Odd(D)$ (resp. $Even(D)$) ont un nombre impair (resp. pair) de voisins dans D. On pourra noter dans la définition précédente que $Odd(D)$ et $Even(D)$ forment toujours une partition de V.

Nous utiliserons dans ce document la notion de différence symétrique sur les arêtes des graphes. En particulier, on utilisera la notation suivante :

Définition 1.5. *Soit $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ deux graphes. On note*

$$G_1 + G_2 = (V_1 \cup V_2, E_1 + E_2) \tag{1.4}$$

où $E_1 + E_2 = (E_1 \cup E_2) \setminus (E_1 \cap E_2)$ désigne la différence symétrique entre les ensembles E_1 et E_2.

La complémentation locale [Kot68] est une opération qui agit sur le voisinage d'un sommet. Voici sa définition :

Définition 1.6. *La complémentation locale d'un graphe G par rapport à l'un de ses sommets u produit le graphe*

$$G * u = G + K_{\mathcal{N}(u)} \tag{1.5}$$

où $+$ dénote la différence symétrique entre les arêtes et $K_{\mathcal{N}(u)}$ représente le graphe complet dont les sommets sont les voisins de u.

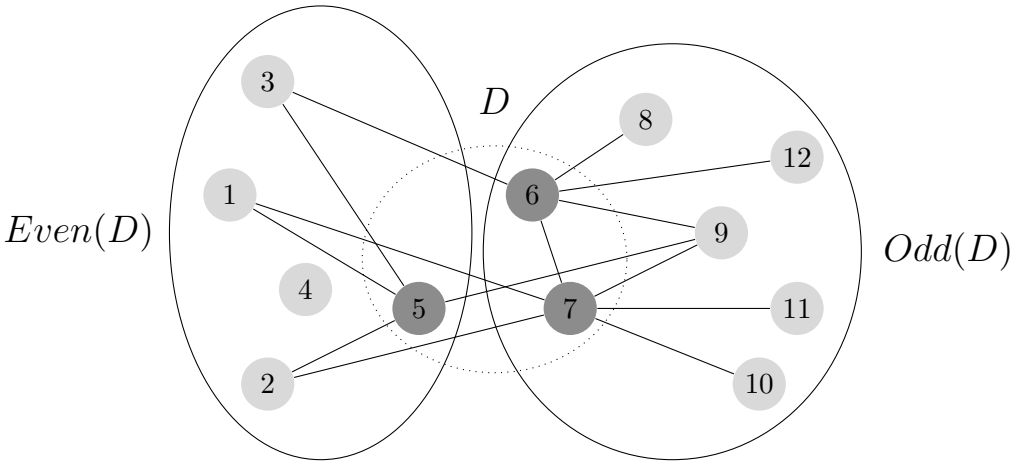

FIGURE 1.1 – Visualisation des ensembles $Odd(D)$ et $Even(D)$ avec $D = \{5, 6, 7\}$. Ces ensembles dépendent uniquement des arêtes dont l'une des extrémités appartient à D (les autres arêtes potentielles sont donc omises dans ce dessin).

Cette opération est notamment utilisée pour donner une caractérisation d'une famille de graphes particulière : les graphes circulaires [Bou90, Bou94, dF81]. On pourra noter que l'application successive de l'opération de complémentation locale sur un même sommet produit le graphe de départ : $(G * u) * u = G$

Dans le cadre de graphe probabilistes, on utilisera le modèle d'Erdös et Renyi [ER59] qui permet d'obtenir une distribution de probabilité sur l'ensemble des graphes possibles à n sommets :

Définition 1.7. *Pour tout $n \in \mathbb{N}$, le graphe $G(n, p) = (V, E)$ est un graphe probabiliste d'ordre n tel que chaque arête potentielle entre deux sommets de V existe avec probabilité p.*

1.3 Introduction à la théorie de l'information quantique

Nous présentons ici quelques notions et concepts généraux de théorie de l'information quantique. Des détails supplémentaires peuvent être trouvés dans l'ouvrage de Nielsen et Chuang [NC00].

1.3.1 Qu'est-ce qu'un bit quantique ?

Le support élémentaire de l'information quantique est l'analogue du bit classique : le bit quantique appelé également "qubit". Il peut être encodé sur le spin d'un photon, les niveaux d'énergie d'un atome, les trajectoires d'un électron soumis à des champs électromagnétiques ou tout autre support obéissant aux lois de la mécanique quantique.

Plus formellement, un bit quantique peut se trouver dans l'un des deux états de base $|0\rangle$ ou $|1\rangle$. Cette notation est appelée "notation de Dirac". L'état $|0\rangle$ sera par exemple associé à un spin horizontal ou à un état fondamental, et l'état $|1\rangle$ à un spin vertical ou à un état excité. Jusqu'ici, on ne constate pas de différence particulière avec les bits classiques qui peuvent valoir soit '0' soit '1'.

Cependant, un bit quantique peut se trouver dans n'importe quel état "intermédiaire" entre ces deux états de base : c'est le *principe de superposition*. Ainsi, en général, un bit quantique dans l'état $|\varphi\rangle$ s'écrit sous la forme $\alpha\,|0\rangle + \beta\,|1\rangle$, une superposition de deux états de base pondérée par α et β, des nombres complexes tels que $|\alpha|^2 + |\beta|^2 = 1$.

1.3.2 Systèmes d'états quantiques

Pour décrire un système physique à n bits quantiques, on représente l'ensemble des états possibles de ce système par les vecteurs unitaires d'un espace de Hilbert $\mathcal{H}$ de dimension 2^n (c'est à dire un espace vectoriel sur $\mathbb{C}$ de dimension 2^n) muni du produit interne

$$\begin{array}{rccl} \langle\ |\ \rangle : & \mathcal{H} \times \mathcal{H} & \to & \mathbb{C} \\ & (\mathbf{x}, \mathbf{y}) & \mapsto & \langle \mathbf{x} | \mathbf{y} \rangle = \mathbf{x}^\dagger \mathbf{y} \end{array} \tag{1.6}$$

où $\mathbf{x}^\dagger$ est le vecteur transposé conjugué de $\mathbf{x}$.

Comme énoncé en 1.3.1, la notation usuelle pour désigner un état quantique est la notation de Dirac $|\varphi\rangle$. Par exemple, lorsque $n = 1$, les états de base sont les vecteurs

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{et} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.7}$$

Ainsi, n'importe quel état $|\varphi\rangle$ s'écrit comme combinaison linéaire de ces états de base :

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{1.8}$$

avec $(\alpha, \beta) \in \mathbb{C}^2$ et $|\alpha|^2 + |\beta|^2 = 1$. On notera également, conformément à la notation de Dirac, le vecteur transposé conjugué de $|\varphi\rangle$ de la façon suivante :

$$\langle\varphi| = \alpha^*\,\langle 0| + \beta^*\,\langle 1| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \tag{1.9}$$

Cette notation est cohérente avec celle du produit interne dans un espace $\mathcal{H}$: pour tout $|\varphi\rangle$, $|\psi\rangle \in \mathcal{H}$ on a $\langle\varphi|\,|\psi\rangle = \langle\varphi|\psi\rangle$.

L'opération mathématique qui correspond à la concaténation de deux systèmes disjoints est le produit tensoriel :

Définition 1.8. *Soit* $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ *un vecteur de taille* n *et* $\mathbf{y}$ *un vecteur de taille* m*. Le produit tensoriel de* $\mathbf{x}$ *et* $\mathbf{y}$ *est le vecteur de taille* nm *défini par*

$$\mathbf{x} \otimes \mathbf{y} = \begin{pmatrix} x_1\mathbf{y} \\ \vdots \\ x_n\mathbf{y} \end{pmatrix} \tag{1.10}$$

Le produit tensoriel de deux matrices $A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$ *et* B *est la matrice définie par blocs*

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,m}B \\ \vdots & \ddots & \vdots \\ a_{n,1}B & \cdots & a_{n,m}B \end{pmatrix} \tag{1.11}$$

Ainsi lorsque l'on considère un système $\mathcal{C}$ composé de deux sous-systèmes $\mathcal{A}$ et $\mathcal{B}$, les états de base de $\mathcal{C}$ sont les produits tensoriels des états de base de $\mathcal{A}$ et ceux de $\mathcal{B}$. Par exemple, pour un système de taille 2, les états de base sont

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{1.12}$$

Si les états de base d'un système s'écrivent sous forme de produits tensoriels des états de bases de ses sous-systèmes comme en (1.12), il existe des états quantiques qui ne vérifient pas cette propriété. Par exemple, l'état de Bell $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ ne peut pas se mettre sous la forme $(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle)$. Ces états sont appelés "états intriqués", et cette notion d'intrication est à l'origine de la supériorité constatée des algorithmes quantiques par rapport aux algorithmes classiques. Les états qui ne sont pas intriqués sont dits "séparables".

Tous les états quantiques décrits jusqu'ici sont aussi appelés "états purs" et peuvent alors s'écrire comme combinaison linéaire des états de base. Ainsi un état quantique $|\varphi\rangle$

sur n qubits se décompose de façon unique de la manière suivante :

$$|\varphi\rangle = \sum_{x\in\{0,1\}^n} \lambda_x |x\rangle \tag{1.13}$$

avec $\lambda_x \in \mathbb{C}$ et $\sum_{x\in\{0,1\}^n} |\lambda_x|^2 = 1$. Cette décomposition illustre ce que l'on appelle le "principe de superposition" d'après lequel on interprète un état quantique comme une superposition des états de base. Par exemple, 1 bit quantique d'information peut contenir une superposition des états $|0\rangle$ et $|1\rangle$ alors qu'un bit classique vaut soit 0 soit 1. Ce principe est à l'origine d'une certaine "parallélisation" des calculs effectués par les algorithmes quantiques.

1.3.3 Matrices de densité et états mixtes

Dans certains cas, un système quantique donné peut être dans un état $|\varphi_1\rangle$ avec probabilité p_1 et dans un état $|\varphi_2\rangle$ avec probabilité p_2. Il ne s'agit pas ici d'une superposition des états $|\varphi_1\rangle$ et $|\varphi_2\rangle$. Un formalisme permet de décrire les systèmes dont les états potentiels suivent une distribution de probabilité : les matrices de densité. Définissons d'abord cette notion pour les états purs :

Définition 1.9. *Soit $|\varphi\rangle$ un état pur sur n qubits. Sa matrice de densité associée est*

$$\rho = |\varphi\rangle \langle\varphi| \in \mathcal{M}_{n,n}(\mathbb{C}) \tag{1.14}$$

Un état qui n'est pas pur ne peut pas s'écrire sous la forme (1.13), en revanche, il possède une matrice de densité calculée de la façon suivante :

Définition 1.10. *On considère un système qui est dans l'état $|\varphi_i\rangle$ avec probabilité p_i pour $i \in E$ où E est un ensemble de taille supérieure ou égale à 2. Sa matrice de densité associée est*

$$\rho = \sum_{i\in E} p_i |\varphi_i\rangle \langle\varphi_i| \tag{1.15}$$

où les états $|\varphi_i\rangle$ sont des états purs.

Les états qui ne sont pas purs sont dits "mixtes". On rencontre des états mixtes notamment lorsque l'on considère un sous-système d'un système intriqué.

Il est possible de calculer la matrice de densité associée à un sous-système grâce à une opération appelée "trace partielle" :

Propriété 1.1. *Soit $\mathcal{E}$ un système dans l'état ρ et $\mathcal{A}$ et $\mathcal{B}$ deux sous-systèmes de $\mathcal{E}$ ($\mathcal{E} = \mathcal{A} \cup \mathcal{B}$). L'état du système $\mathcal{A}$ considéré seul est*

$$\rho^{\mathcal{A}} = tr_B(\rho) = \sum_{|x\rangle\in B} \big(I_A \otimes \langle x|\,\big)\rho\big(I_A \otimes |x\rangle\,\big) \tag{1.16}$$

où les vecteurs $|x\rangle$ parcourent B, une base quelconque de $\mathcal{B}$.

Par exemple, considérons un système $\mathcal{E}$ sur 2 qubits dans l'état de Bell [Bel64] (également connu sous le nom de "paire EPR" [EPR35])

$$|\varphi\rangle_{\mathcal{E}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.17}$$

Cet état est pur et intriqué, comme mentionné précédemment. On appelle $\mathcal{L}$ et $\mathcal{R}$ les deux sous-systèmes de $\mathcal{E}$ sur 1 qubit chacun. Le système $\mathcal{L}$ du premier qubit est alors dans l'état $|0\rangle$ avec probabilité $\frac{1}{2}$ et dans l'état $|1\rangle$ avec probabilité $\frac{1}{2}$ également. D'après la Propriété 1.1, sa matrice de densité associée est

$$\rho^{\mathcal{L}} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \tag{1.18}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{1.19}$$

$$= \frac{I}{2} \tag{1.20}$$

Cet état est un état mixte car sa matrice de densité ne peut pas se mettre sous la forme $|\psi\rangle\langle\psi|$ où $|\psi\rangle$ est un état pur. Un état mixte dont la matrice de densité est $\frac{I}{2}$ est dit "complètement mixte" et correspond à une distribution uniforme sur tous les états possibles.

De façon générale, si $\mathcal{E}$ un système et $\mathcal{A}$ un sous-système qui le composent, on appelle "matrice de densité réduite par rapport à $\mathcal{A}$" la matrice de densité associée à $\mathcal{A}$ et on la note $\rho^{\mathcal{A}}$.

Le formalisme des matrices de densité capture la notion d'information que l'on peut obtenir d'un système. En particulier, deux systèmes qui ont les mêmes matrices de densité sont parfaitement indistingables. Par exemple, le système sur 1 bit quantique qui est dans l'état $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ ou dans l'état $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ avec probabilité $\frac{1}{2}$ est dans l'état mixte

$$\rho = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{I}{2} \tag{1.21}$$

qui est le même que (1.20). Les deux systèmes correspondants sont donc indistingables. En revanche, on peut parfaitement distinguer deux états décrits par leurs matrices de densité ρ et ρ' lorsque l'on a $tr(\rho\rho') = 0$ (voir [NC00], par exemple).

1.3.4 Evolutions et Mesure

L'évolution d'un système quantique est décrite en mécanique quantique par l'équation de Schrödinger, et a pour conséquence que les transformations possibles d'un état quantique isolé $|\varphi\rangle$ sont unitaires. Dans le formalisme précédemment défini, toute matrice unitaire U (c'est-à-dire telle que $U^\dagger U = UU^\dagger = I$) correspond ainsi à une évolution naturelle

de l'état du système. Ces évolutions sont réversibles car $U^{-1} = U^\dagger$ est également une matrice unitaire.

Le principe d'incertitude d'Heisenberg stipule qu'il est impossible de connaître avec précision arbitrairement élevée l'état d'un système sur lequel on ne possède aucune information au préalable. Cependant, il existe des moyens d'obtenir de l'information partielle sur un état donné. Ce processus est appelé "mesure quantique" et est décrit dans la suite.

On définit formellement une mesure de la façon suivante :

Définition 1.11. *On appelle "mesure quantique" d'un état $|\varphi\rangle$ un procédé décrit par un ensemble d'opérateurs $\{M_m\}_{m\in S}$ vérifiant*

$$\sum_{m\in S} M_m^\dagger M_m = I \tag{1.22}$$

Le résultat de la mesure d'un état $|\varphi\rangle$ est un entier m obtenu avec la probabilité

$$p_m = \langle\varphi| M_m^\dagger M_m |\varphi\rangle \tag{1.23}$$

et l'état du système après avoir obtenu la valeur m est

$$\left|\varphi'\right\rangle = \frac{M_m |\varphi\rangle}{\sqrt{p_m}} \tag{1.24}$$

On vérifiera notamment que l'on a bien $\sum_{m\in S} p_m = 1$ grâce à l'expression (1.22).

Dans le cas d'un état mixte ρ, la probabilité de retourner l'entier m s'exprime

$$p_m = tr(M_m^\dagger M_m \rho) \tag{1.25}$$

et l'état obtenu après la mesure est

$$\rho' = \frac{M_m \rho M_m^\dagger}{p_m} \tag{1.26}$$

Ce formalisme est très général et permet notamment d'élargir la notion d'évolution unitaire. En effet, lorsque la mesure comprend un seul opérateur, on est en présence d'une évolution que l'on appellera "isométrie". Ce type d'évolution prend en compte l'ajout éventuel de bits quantiques par rapport au système initial. Une évolution unitaire est une isométrie dont l'opérateur est représenté par une matrice carrée.

Prenons un exemple concret : on souhaite mesurer l'état $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ suivant l'ensemble des opérateurs $\{P_0 = |0\rangle\langle 0|, P_1 = |1\rangle\langle 1|\}$. On peut vérifier que l'on a bien

$P_0^\dagger P_0 + P_1^\dagger P_1 = I$, ainsi à l'issue de la mesure, on obtient la valeur '0' avec probabilité

$$p_0 = \langle\varphi| P_0^\dagger P_0 |\varphi\rangle \tag{1.27}$$
$$= \langle\varphi| |0\rangle \langle 0| |0\rangle \langle 0| |\varphi\rangle \tag{1.28}$$
$$= \alpha^* \langle 0|0\rangle \alpha \langle 0|0\rangle = |\alpha|^2 \tag{1.29}$$

et l'état du système résultant est $|0\rangle$. De façon similaire, on a $p_1 = |\beta|^2$ et lorsque la valeur mesurée est '1' l'état résultant est $|1\rangle$. Ces calculs illustrent bien l'aspect pratique de la notation de Dirac. Les probabilités associées aux résultats des mesures dépendent de l'état mesuré, et on obtient donc de l'information partielle sur cet état.

On remarquera dans ce cas que les opérateurs P_i vérifient $P_i^\dagger P_i = P_i$, ce sont donc des projecteurs. On parlera alors de "mesure projective" :

Définition 1.12. *Soit M un opérateur hermitien qui se décompose sur ses sous-espaces propres de la façon suivante (décomposition spectrale) :*

$$M = \sum_{\lambda_m \in Sp(M)} \lambda_m P_m \tag{1.30}$$

où P_m est le projecteur associé à la valeur propre λ_m. La "mesure projective suivant l'observable M" désigne alors la mesure décrite par les projecteurs P_m (qui vérifient donc $P_m^\dagger P_m = P_m$).

1.3.5 Propriétés

Le théorème de Non-Clonage [WZ82] est un théorème fondamental en théorie de l'information quantique :

Théorème 1.2 (Théorème de Non-Clonage [WZ82])**.** *Soit $\mathcal{H}$ un espace de Hilbert. Il n'existe aucun opérateur unitaire U tel que pour tout $|\varphi\rangle \in \mathcal{H}$,*

$$U(|\varphi_0\rangle \otimes |\varphi\rangle) = |\varphi\rangle \otimes |\varphi\rangle \tag{1.31}$$

avec $|\varphi_0\rangle \in \mathcal{H}$

Démonstration. Supposons qu'un tel opérateur unitaire U existe. Pour tous $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$, on a

$$\langle\varphi|\psi\rangle = \langle\varphi_0|\varphi_0\rangle\langle\varphi|\psi\rangle \tag{1.32}$$
$$= \big(\langle\varphi_0| \otimes \langle\varphi|\big)\big(|\varphi_0\rangle \otimes |\psi\rangle\big) \tag{1.33}$$
$$= \big(\langle\varphi_0| \otimes \langle\varphi|\big)U^\dagger U\big(|\varphi_0\rangle \otimes |\psi\rangle\big) \tag{1.34}$$
$$= \big(\langle\varphi| \otimes \langle\varphi|\big)\big(|\psi\rangle \otimes |\psi\rangle\big) = \langle\varphi|\psi\rangle^2 \tag{1.35}$$

L'équation (1.34) provient de l'unitarité de U ($U^\dagger U = I$) et l'équation (1.35) découle de l'expression (1.31). Ce résultat est absurde, le théorème est donc prouvé. □

Nous introduisons l'opérateur d'Hadamard, une transformation unitaire qui agit sur 1 qubit :

Définition 1.13. *On appelle "opérateur d'Hadamard" l'unitaire H représenté par la matrice :*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.36}$$

Cette opération transforme la base $\{|0\rangle, |1\rangle\}$ en $\{|+\rangle, |-\rangle\}$, et elle permet notamment de créer un superposition uniforme sur n qubits :

$$H^{\otimes n} |0 \cdots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \tag{1.37}$$

Certains opérateurs sur 1 qubit s'avèrent très utiles en calcul quantique : les opérateurs de Pauli. Ce sont des opérateurs unitaires simples largement utilisés en informatique quantique. Ils correspondent à des opérations (ou portes logiques) élémentaires. On les définit de la façon suivante :

Définition 1.14. *On appelle "opérateurs de Pauli" les opérateurs unitaires hermitiens I, X, Y et Z suivants :*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.38}$$

Ces opérateurs ainsi que le scalaire i permettent de construire le "groupe de Pauli" sur 1 qubit :

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm iY, \pm iY, \pm iZ, \pm iZ\} \tag{1.39}$$

Sur n qubits, le groupe G_n est constitué du produit tensoriel de n éléments de G_1. Ce groupe permet de construire une famille d'états particuliers : les "états stabilisables" :

Définition 1.15. *On appelle "état stabilisable" un point fixe commun à n éléments indépendants de G_n qui commutent entre eux.*

Introduisons également un opérateur sur 2 qubits qui ne peut pas être décomposé en 2 opérations sur 1 qubit : l'opérateur $CNOT$ également appelé "contrôle-X" et notée ΛX.

Définition 1.16.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{1.40}$$

De façon intuitive, l'opérateur $CNOT$ agit sur 2 qubit dont le premier est un "qubit de contrôle", c'est à dire que si le premier qubit vaut $|1\rangle$, on applique l'opération X sur le deuxième, et s'il vaut $|0\rangle$ on ne fait rien. On peut également définir des opérations contrôlées à partir de n'importe quel unitaire : par exemple, l'opération "contrôle-Z" (ΛZ) est définie de la façon suivante :

$$\Lambda Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{1.41}$$

Comme nous les avons évoqués au début de ce chapitre, nous considérons une famille d'états quantiques particulière : les états graphes. Ce sont des états quantiques qui peuvent être construits à partir d'un graphe de la façon suivante :

Définition 1.17. *Pour tout graphe $G = (V, E)$ avec $V = \{v_1, \ldots, v_n\}$, l'état graphe associé $|G\rangle$ est un état quantique sur n qubits défini de la façon suivante :*

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{|G[x]|} |x\rangle \tag{1.42}$$

où $|G[x]|$ désigne le nombre d'arêtes du sous-graphe induit $G[x] = (\{v_i \in V \mid x_i = 1\}, \{(v_i, v_j) \in E \mid x_i = x_j = 1\})$.

Les vecteurs x de l'expression (1.42) peuvent également être interprétés comme les vecteurs caractéristiques des ensembles de sommets du graphe G. C'est d'ailleurs cette interprétation qui est traduite dans le sous-graphe induit $G[x]$.

Les états graphes sont un cas particulier d'états stabilisables :

Propriété 1.3. *Soit $G = (V, E)$ un graphe quelconque. Pour tout sommet $u \in V$, nous avons :*

$$X_u Z_{\mathcal{N}(u)} |G\rangle = |G\rangle \tag{1.43}$$

où $Z_{\mathcal{N}(u)} = \bigotimes_{u \in \mathcal{N}(u)} Z_u$

Il est intéressant de noter que les états graphes peuvent être construits exclusivement à partir des deux opérateurs H et ΛZ. Voici le processus de construction de l'état $|G\rangle$ où G est un graphe d'ordre n :

- On commence avec l'état $|0\rangle^{\otimes n}$ sur n qubits numérotés de '1' à 'n' correspondant aux sommets de G.
- On applique l'opérateur $H^{\otimes n}$ L'état obtenu est celui décrit en (1.37).
- Pour toute arête de G entre les sommets i et j, on applique l'opérateur ΛZ sur les qubits i et j. L'état obtenu est l'état graphe $|G\rangle$.

Chapitre 2

Partage de secret quantique à partir d'états graphes

Le partage de secret en général est une primitive cryptographique regroupant plusieurs joueurs dont l'un d'eux, appelé dealer, souhaite partager une information entre les autres joueurs. Dans de tels protocoles, le dealer attribue à chacun des joueurs des données spécifiques. Une fois le partage effectué, certains ensembles de joueurs peuvent reconstruire cette information en mettant en commun leurs données alors que d'autres n'ont aucun moyen d'y accéder. L'information ainsi partagée est appelée le *secret*.

Nous commençons par faire un état de l'art des protocoles de partage de secret classique et quantique, puis nous montrons en quoi l'utilisation d'états graphes permet d'améliorer l'efficacité de ces protocoles et d'en optimiser les ressources. Plusieurs résultats existentiels et constructifs concernant les protocoles de partage de secret quantique à partir d'états graphes sont établis, notamment pour les protocoles à seuil.

2.1 Etat de l'art

2.1.1 Partage de secret classique

Dans un protocole de partage de secret classique, on souhaite partager un nombre secret entre un ensemble de n joueurs auxquels un acteur appelé "dealer" distribue un certain ensemble de données. Certains sous-ensembles de ces n joueurs peuvent, s'ils combinent leurs données d'une certaine façon, réussir à reconstituer le secret partagé. Ces ensembles sont appelés "ensembles autorisés". D'autres sous-ensembles, en revanche, n'ont aucune information sur le secret en question, ce sont les "ensembles interdits". Une troisième catégorie caractérise les sous-ensembles de joueurs qui possèdent une information partielle sur ce secret.

Prenons un exemple élémentaire dans lequel 4 joueurs partagent un bit secret s. Le dealer prépare des bits aléatoires r et r' inconnus des joueurs a priori. Il donne ensuite aux 4 joueurs un bit d'information calculé comme suit :
– joueur 1 : $s \oplus r$
– joueur 2 : $s \oplus r'$
– joueur 3 : $r \oplus r'$
– joueur 4 : r
On constate ici qu'aucun joueur seul ne peut reconstituer le secret. En revanche, les joueurs 1 et 4 ensemble peuvent reconstituer le secret en additionnant leurs données : $s \oplus r \oplus r = s$. De façon similaire, les joueurs $\{2, 3, 4\}$ peuvent reconstituer le secret s. Il est facile de voir que tout ensemble de joueurs qui contient $\{1, 4\}$ ou $\{2, 3, 4\}$ peut reconstituer le secret et que tous les autres n'ont a priori aucun moyen de le faire.

Dans tout protocole de partage de secret, nous distinguons deux types d'ensembles de joueurs : les ensembles autorisés et les ensembles interdits. Nous en donnons une définition formelle :

Définition 2.1. *Pour tout protocole de partage de secret dans lequel un secret s est partagé entre n joueurs, un sous-ensemble B de joueurs est dit*
– autorisé *lorsque les joueurs de l'ensemble B peuvent reconstituer le secret s*
– interdit *lorsque les joueurs de B ne possèdent aucune information sur le secret s*

Cette notion est fondamentale pour les protocoles de partage de secret.

Certains de ces protocoles ont la particularité de ne pas comporter d'ensembles de joueurs disposant d'une information partielle sur le secret : ce sont les protocoles "parfaits" :

Définition 2.2. *Un protocole de partage d'un secret s entre n joueurs est dit "parfait" lorsque pour tout ensemble B de joueurs, exactement une des deux propriétés suivantes est vraie :*
– *B est autorisé*
– *B est interdit*

On désigne par "structure d'accès" l'ensemble des ensembles de joueurs autorisés. On note que la propriété d'être autorisé pour un ensemble de joueurs est stable par sur-ensemble. La description d'une structure d'accès est, en général, de taille exponentielle en n, le nombre de joueurs (car elle est indexée par $\mathcal{P}(\{1, \cdots, n\})$).

Une catégorie de protocoles parfaits a l'avantage de posséder une structure d'accès qui se décrit très simplement : les protocoles de partage de secret à seuil :

Définition 2.3. *On appelle partage de secret classique à seuil (n, k) avec $0 < k \leq n$ un protocole de partage de secret dans lequel :*
– *tout ensemble de k joueurs ou plus est un ensemble autorisé*
– *tout ensemble de $k - 1$ joueurs ou moins est un ensemble interdit*

Les structures des protocoles de partage de secret à seuil sont donc simplement déterminées par la taille des ensembles de joueurs qui la composent.

Shamir propose une solution réalisant un partage de secret classique à seuil (n, k) quelque soit n et quelque soit $k \leq n$ [Sha79]. Cette solution utilise des méthodes classiques d'interpolation polynomiale. Voici la description de ce protocole :

Distribution du secret
- Le secret s est un élément d'un corps fini $\mathbb{F}$ tel que $|\mathbb{F}| > n$
- Le dealer choisit aléatoirement $k-1$ éléments de $\mathbb{F}$ $a_1, \cdots, a_{k-1}$ et construit le polynôme $P(X) = s + a_1 X + \cdots + a_{k-1} X^{k-1}$
- Pour tout $1 \leq i \leq n$, le dealer choisit un élément $x_i \in \mathbb{F}$ et donne la paire $(x_i, P(x_i))$ au joueur i. Les éléments x_i doivent être tous distincts et non nuls.

Une fois le secret partagé, n'importe quel ensemble B de k joueurs est capable de reconstruire le secret de la façon suivante :

Reconstruction du secret
- Soit (x_i, y_i) la paire possédée par le joueur i. On suppose sans perte de généralité que $B = \{1, \cdots, k\}$
- Les k joueurs de B reconstituent le polynôme P avec des méthodes d'interpolation classiques :

$$P(X) = \sum_{i=1}^{k} y_i \left(\prod_{\substack{1 \leq j \leq k \\ i \neq j}} \frac{X - x_j}{x_i - x_j} \right) \tag{2.1}$$

- Les joueurs de B reconstruisent le secret $s = P(0)$.

Les ensembles de taille k peuvent donc reconstituer le secret s, et il se trouve que les ensembles de taille $k-1$, et par conséquents les ensembles de taille inférieure à $k-1$, ne possèdent aucune information sur s. Pour se convaincre de cela, considérons un ensemble de joueurs de taille $k-1$. Les joueurs de cet ensemble possèdent $k-1$ paires (x_i, y_i). Pour tout $x \in \mathbb{F}$, l'ajout d'une $k^{\text{ième}}$ paire arbitraire $(0, x)$ permet l'interpolation d'un polynôme P de degré $k-1$ vérifiant $P(0) = x$. Ainsi, n'importe quel secret x peut avoir été encodé, en d'autres termes l'ensemble de $k-1$ joueurs ne possède pas assez d'information pour exclure certaines valeurs potentielles du secret.

C'est donc le degré du polynôme P qui fixe le seuil associé au partage de secret. Il est donc possible de réaliser de cette façon n'importe quel seuil (k, n) quelque soit n et $k \leq n$.

Le protocole présenté ici se trouve être un protocole de partage de secret parfait, et c'est le cas de tous les protocoles de partage de secret à seuil en général. A titre d'exemple, si on prend $\mathbb{F} = \mathbb{F}_2$, le secret est un bit $s \in \mathbb{F}_2$ choisi uniformément, ainsi pour tout ensemble B de joueurs, on a

1. si $|B| < k$ alors B ne possède aucune information sur s
2. si $|B| \geq k$ alors B peut reconstituer le secret s

Indépendamment, Blakley a proposé un protocole de partage de secret à seuil construit à partir d'hyperplans et de leur intersection [Bla79] permettant de réaliser n'importe quel seuil, tout comme le protocole de Shamir présenté plus haut.

2.1.2 Partage de secret quantique

Nous avons vu comment réaliser un seuil quelconque en partage de secret classique où les parts données à chaque joueur ont une taille de l'ordre de celle du secret [Sha79]. Le problème de l'existence de protocoles de partage de secret quantique à seuil ainsi que celle du partage de secret quantique en général se pose donc naturellement.

Nous considérons ici et dans toute la suite les protocoles de partage de secret quantique construits à partir d'un secret quelconque, présent en une seule copie. Cela correspond au cas le plus général étant donné l'impossibilité de la copie dans le cas d'un secret quantique. Les protocoles basés sur plusieurs copies du secret ne sont pas considérés dans le cadre de ces études.

La question du partage de secret quantique à seuil a été abordée et détaillée par Cleve, Gottesman et Lo dans [CGL99] et [Got00]. Dans ces études, nous voyons apparaître certaines propriétés inhérentes au cas d'un secret quantique. Une première particularité est conséquence du théorème de Non-Clonage rappelé dans le Chapitre 1, un théorème fondamental en Théorie de l'Information Quantique.

L'impact immédiat de ce théorème sur le partage de secret quantique se traduit par le théorème suivant :

Théorème 2.1. *Pour tout protocole de partage de secret quantique* $((n, k))$*, nous avons nécessairement* $n > 2k$*.*

En effet, de façon intuitive, si un protocole $((n, k))$ existait avec $2k \leq n$, on aurait l'existence de deux ensembles de joueurs distincts de taille supérieure au seuil k. Ces deux ensembles seraient alors capables de reconstituer chacun une copie du secret permettant ainsi sa duplication. Le secret quantique étant quelconque et en un seul exemplaire, on obtient une contradiction avec le théorème de Non-Clonage.

Outre cette limitation, la question de l'existence de protocoles de partage de secret quantique à seuil a été résolue. En effet, des constructions explicites de protocoles $((n, k))$ sont données quelque soit $n \in \mathbb{N}^*$ et pour tout $k > \frac{n}{2}$ dans [CGL99] et [Got00]. Cependant, ces protocoles possèdent les deux caractéristiques suivantes :
– les phases de partage et de reconstruction sont assez complexes
– la part donnée à chaque joueur n'est pas bornée : sa taille, en nombre de qubits dépend linéairement du nombre total de joueurs

Comme il sera expliqué dans la section suivante, ce sont ces deux points que l'utilisation d'états graphes permet d'améliorer.

2.1.3 Un protocole $((n, n))$ à partir de l'état GHZ

Un protocole de partage d'un état secret $|\varphi\rangle$ entre n joueurs est proposé par Broadbent, Chouha et Tapp [BCT08]. Le support utilisé pour ce partage est un état GHZ [GHZ89], et les paramètres de ce protocole sont $((n, n))$, c'est-à-dire que la présence des n joueurs est nécessaire pour la reconstruction du secret.

L'avantage de tels protocoles réside entre autres dans le fait que chaque joueur possède 1 qubit, c'est-à-dire une ressource de la taille du secret partagé. En contrepartie, le seuil atteint est très restrictif puisque tous les joueurs doivent être présents pour reconstituer le secret.

Nous décrivons à présent ce protocole dans lequel le dealer souhaite partager le secret

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.2}$$

entre n joueurs numérotés de 1 à n.

Encodage du secret

Voici les étapes de l'encodage du secret :

1. Le dealer chiffre partiellement le secret $|\varphi\rangle$ de la façon suivante : il tire un bit aléatoire $b_X \in \{0, 1\}$. Si le résultat de ce tirage est '0', il ne fait rien, et si le résultat est '1', il applique l'opérateur X au secret. L'état résultant est ainsi

$$\left|\varphi'\right\rangle = X^{b_X}\,|\varphi\rangle \tag{2.3}$$
$$= \alpha'\,|0\rangle + \beta'\,|1\rangle \tag{2.4}$$

2. En utilisant n fois successivement la porte $CNOT$ (appelée aussi "pseudo-copie") à l'état $|\varphi'\rangle$, il produit l'état

$$\left|\varphi''\right\rangle = \alpha'\,|0\rangle^{\otimes n} + \beta'\,|1\rangle^{\otimes n} \tag{2.5}$$

3. Le dealer choisit aléatoirement une chaine de bits $x_1 \cdots x_n$ telle que $\bigoplus_{i=1}^{n} x_i = b_X$ et donne au joueur i le i^{eme} qubit de $|\varphi''\rangle$ ainsi que le bit x_i.

Reconstruction du secret

Il faut tout d'abord choisir le joueur qui recevra le secret. Supposons en toute généralité qu'il s'agit du joueur 1. Les phases de la reconstruction s'articulent de la façon suivante :

1. Tous les joueurs sauf le joueur 1 appliquent l'opérateur d'Hadamard à leur qubit puis mesurent leur qubit dans la base standard. Soit y_i le résultat de la mesure obtenue par le joueur i. L'état du qubit du joueur 1 est alors
$$\alpha' |0\rangle + (-1)^{\bigoplus_{i=2}^{n} y_i} \beta' |1\rangle \tag{2.6}$$
Chaque joueur i envoie au joueur 1 les bits x_i et y_i.
2. Le joueur 1 calcule $y = \bigoplus_{i=2}^{n} y_i$. Si $y = 0$, il ne fait rien, si $y = 1$ il applique l'opérateur Z à son qubit. L'état résultant est alors
$$\alpha' |0\rangle + \beta' |1\rangle = X^{b_X} |\varphi\rangle \tag{2.7}$$
3. Le joueur 1 calcule $b_X = \bigoplus_{i=1}^{n} x_i$. Si $b_X = 0$, il ne fait rien, si $b_X = 1$ il applique l'opérateur X à son qubit. Le qubit résultant du joueur 1 contient le secret $|\varphi\rangle$.

2.1.4 Encodage d'un secret dans un état graphe

Les états graphes décrits dans le Chapitre 1 peuvent être utilisés pour encoder un secret partagé entre plusieurs personnes. Un tel encodage est présenté dans [MS08] et permet de partager un secret classique puis quantique entre n joueurs.

Encodage d'un secret classique

Soit $G = (V, E)$ un graphe d'ordre $n + 1$ et $d \in V$ l'un des sommets de ce graphe. Le sommet d est associé au dealer alors que chacun des autres sommets de G est associé à un joueur différent. Le dealer souhaite encoder un secret $s \in \{0, 1\}$.

On note $G' = G \setminus d$ le graphe obtenu à partir de G après suppression du sommet d.

Si $s = 0$, le dealer prépare l'état $|G'\rangle$. Si $s = 1$, il prépare l'état $Z_{\mathcal{N}(d)} |G'\rangle$. L'état résultant s'écrit alors
$$|G_s\rangle = Z^s_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.8}$$

Encodage d'un secret quantique

Lorsque le secret à partager est un état quantique $|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$ sur 1 qubit, l'encodage s'effectue comme une superposition de l'encodage du secret classique '0' avec celui du secret '1' pondérés par α et β :
$$|G_\varphi\rangle = \alpha \left|G'\right\rangle + \beta Z_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.9}$$

Structures d'accès

Grâce à ces encodages, il n'est en général pas nécessaire que tous les joueurs soient réunis afin de pouvoir reconstituer le secret, comme c'était le cas pour le protocole décrit en 2.1.3. Des conditions suffisantes d'accessibilité au secret sont ainsi établies en fonction des structures des ensembles de joueurs.

Lorsque le secret partagé est un bit classique, les ensembles de joueurs qui peuvent reconstituer les secret sont décrit à partir de structures sur les ensembles de sommets du graphe G utilisant notamment la notion de voisinage impair (Définition 1.4). Le cas d'un secret quantique paragé entre n joueurs se réduit au cas d'un secret classique en terme de structure d'accès décrites sur le graphe G : Markham et Sanders proposent ainsi une descripiton de ces structures [MS08] en faisant intervenir le graphe G et son "graphe complémentaire" qui s'apparente au graphe $G * d$ issu de la complémetation locale de G par rapport au sommet d associé au dealer.

2.2 Partage de secret classique avec états graphes

Comme présentés dans le Chapitre 1, les états graphes sont un excellent support pour le calcul quantique et l'implémentation de protocoles en général. En effet, lors de la construction d'un état graphe à partir d'un graphe G donné, les opérations quantiques utilisés sont sur 2 qubits seulement : l'opération ΛZ appliquée sur chaque paire de qubits correspondant à une arête de G.

L'apparition des états graphes dans les protocoles de partage de secret quantique [MS08] a plusieurs avantages. Tout d'abord, dans un protocole à n joueurs avec un secret quantique sur 1 qubit, on choisit de donner exactement 1 qubit à chaque joueur, correspondant à 1 sommet du graphe sous-jacent. Ainsi, la taille de la part donnée à chaque joueur correspond exactement à la taille du secret. Les ressources sont donc réduites au maximum (quantité élémentaire d'information par joueur).

Enfin, des questions émergent de l'utilisation d'états graphes pour le partage de secret : quelles sont les structures d'accès liées au choix du graphe de départ ? Comment eut-on les décrire à partir des propriétés de ce graphe ? L'étude de ces nouvelles structures d'accès présente des liens avec des questions de théories des graphes, et nous établissons ainsi plusieurs correspondances entre les deux domaines.

2.2.1 Description du protocole et structures d'accès

Markham et Sanders [MS08] proposent une façon de partager un secret classique $s \in \{0, 1\}$ entre n joueurs à partir d'états graphes (Définition 1.17). Dans ces protocoles, chaque joueur possède exactement 1 qubit.

Le protocole de partage d'un secret classique présenté ici est fondé sur l'utilisation d'états multipartis construits à partir d'états graphes. Nous noterons ce type de protocole un protocole "cQSS". Les protocoles cQSS sont paramétrés par un graphe G dont chacun des sommets correspond à un joueur et le dealer se voit attribuer un sommet particulier. On parle alors de protocole cQSS (G, d) avec $d \in V(G)$.

cQSS

Soit G un graphe d'ordre $n+1$. Soit d un sommet de G associé au dealer. Le dealer souhaite partager un secret $s \in \{0,1\}$ entre n joueurs. On note G' le graphe résultant de G après suppression du sommet d.

Partage du secret

1. Le dealer prépare l'état suivant sur n qubits :

$$Z^s_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.10}$$

2. Chacun des n joueurs reçoit un qubit de cet état.

Reconstitution du secret Soit B est un ensemble de joueurs autorisé.

1. Trouver $D \subseteq B$ tel que $|D \cap \mathcal{N}(d)| = 1 \bmod 2$ et $Odd(D) \subseteq B$ (algorithme Figure 2.2)
2. Les joueurs de B mesurent leurs qubits suivant l'observable $(-1)^{G[D]} X_D Z_{Odd(D)}$
3. Le résultat de la mesure fournit le secret s.

FIGURE 2.1 – Protocole de partage de secret classique avec des états graphes cQSS

De façon générale, un ensemble $B \subseteq V$ qui souhaite reconstituer le secret s doit parvenir à distinguer le cas où le secret '0' a été encodé du cas où c'est le secret '1'. Pour décrire cela, on appelle $\rho_B(s)$ l'état mixte possédé par les joueurs de B :

$$\rho^B(s) = tr_{V \setminus B}(|G_s\rangle \langle G_s|) \tag{2.11}$$

Un ensemble B de joueurs peut reconstruire le secret s si et seulement si ils peuvent distinguer parfaitement $\rho^B(0)$ et $\rho^B(1)$, c'est à dire lorsque $tr(\rho^B(0)\rho^B(1)) = 0$. En revanche, l'ensemble B ne possède aucune information sur le secret lorsque les états $\rho^B(0)$ et $\rho^B(1)$ sont indistingables, c'est-à-dire lorsque $\rho^B(0) = \rho^B(1)$.

Des conditions suffisantes sur les ensembles autorisés dans les états graphes ont été prouvées dans [KMMP09]. Nous introduisons d'abord la définition suivante :

Définition 2.4. *Soit $G = (V, E)$ un graphe et $d \in V$ un sommet appelé dealer. Un ensemble $B \subseteq V \setminus \{d\}$ est dit* à noyau impair *lorsque*

$$\exists D \subseteq B \text{ tel que } Odd(D) \subseteq B \text{ et } |D \cap \mathcal{N}(d)| = 1 \bmod 2 \tag{2.12}$$

On parlera ainsi de "noyau impair" pour désigner un ensemble $D \subseteq B$ ayant cette propriété.

Un ensemble $B \subseteq V$ est dit dominé modulo 2 *lorsque*

$$\exists C \subseteq V \setminus B \text{ tel que } Odd(C) \cap B = \mathcal{N}(d) \cap B \tag{2.13}$$

Un algorithme permettant de trouver un ensemble D vérifiant les conditions de l'expression (2.12) dans une ensemble b à noyau impair est donné dans la Figure 2.2.

Algorithme de recherche de noyau impair

Soit $G = (V, E)$ un graphe d'ordre $n+1$, $d \in V$ le dealer et $V' = V \setminus \{d\}$. Soit $B \subseteq V \setminus \{d\}$ un ensemble à noyau impair (Définition 2.4) de taille k.

1. Soit $\Gamma \in \mathcal{M}_n(\mathbb{F}_2)$ la matrice d'adjacence correspondant au graphe G privé du dealer d. On construit la matrice $A \in \mathcal{M}_{n-k+1,k}(\mathbb{F}_2)$ de la façon suivante :
   – Soit Γ_B la matrice de coupe issue de Γ correspondant à l'ensemble B
   – On ajoute à la matrice Γ_B une ligne de '1' pour former la matrice A
2. A l'aide d'un algorithme de résolution de systèmes linéaires, trouver un vecteur $X \in \mathbb{F}_2^k$ solution du système suivant :

$$AX = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \tag{2.14}$$

3. Soit $D \subseteq B$ l'ensemble représenté par le vecteur X. Retourner D.

FIGURE 2.2 – Algorithme de recherche de *noyau impair*

Théorème 2.2. *Soit $G = (V, E)$ un graphe et $d \in V$ l'un de ses sommets. Soit $V' = V \setminus \{d\}$. Pour tout $B \subseteq V'$ à noyau impair, il est possible de trouver un ensemble $D \subseteq B$ vérifiant les conditions de l'expression (2.12) en temps polynomial en l'ordre de G.*

Démonstration. On montre que l'algorithme de la Figure 2.2 retourne un tel ensemble $D \subseteq B$ en temps polynomial.

Soit X une solution du système (2.14) et D l'ensemble représenté par le vecteur X.

Tout d'abord, par construction de la matrice A, on a

$$\Gamma_B X = 0 \tag{2.15}$$

Cela s'interprète de la façon suivante : chaque sommet de $V' \setminus B$ possède un nombre pair de voisins parmi les sommets de D. Ainsi, nous avons

$$V' \setminus B \subseteq Even(D) \tag{2.16}$$

en d'autres termes

$$Odd(D) \subseteq B \tag{2.17}$$

Ensuite, le système (2.14) nous permet d'écrire

$$[1 \cdots 1]\, X = 1 \tag{2.18}$$
$$|X| = 1 \bmod 2 \tag{2.19}$$
$$|D| = 1 \bmod 2 \tag{2.20}$$

Tout noyau impair D correspond ainsi à une solution du système (2.14), et puisque B est un ensemble à noyau impair, un telle solution existe nécessairement, ce qui justifie l'existence de la solution X utilisée dans l'algorithme Figure 2.2.

L'algorithme de résolution usuel d'un système linéaire étant polynomial en la taille du système, on a bien le résultat énoncé. □

Un résultat [KMMP09] établit un lien entre les ensembles à noyau impair dans le graphe de départ et les ensembles de joueurs qui peuvent reconstruire le secret :

Lemme 2.3 ([KMMP09])**.** *Soit $G = (V, E)$ un graphe. Pour tout protocole cQSS (G, d), pour tout $B \subseteq V \setminus \{d\}$:*
– *Si B est à noyau impair, alors B est autorisé.*
– *Si B est dominé modulo 2, alors B est interdit.*

D'après le lemme précédent, il existe une façon pour les ensembles B à noyau impair de reconstruire le secret. Nous détaillons la procédure permettant à un ensemble à noyau impair de retrouver ce secret. Pour cela, on établit d'abord une propriété sur les stabiliseurs des états graphes qui étend la Propriété 1.3 au cas d'un ensemble D quelconque :

Lemme 2.4. *Soit $G = (V, E)$ un graphe et $D \subseteq V$ un ensemble de sommets. Si $|G\rangle$ est l'état graphe associé à G, on a*

$$(-1)^{|G[D]|} X_D Z_{Odd(D)} |G\rangle = |G\rangle \tag{2.21}$$

Démonstration. On considère un état graphe construit à partir d'un graphe $G = (V, E)$. Quelque soit $u, v \in V$, les opérateurs $X_u Z_{\mathcal{N}(u)}$ et $X_v Z_{\mathcal{N}(v)}$ commutent. En effet, si u et v ne sont pas voisins dans G, ces opérateurs agissent sur des bits quantiques disjoints et commutent donc. S'ils sont voisins, l'application de l'opérateur $(X_u Z_{\mathcal{N}(u)})(X_v Z_{\mathcal{N}(v)})$ effectue notamment l'opération $X_u Z_u$ sur le qubit u et $Z_v X_v$ sur le qubit v. On a donc toujours un nombre pair d'opérateurs X et Z qui commutent.

Ainsi, d'après la Propriété 1.3, pour tout ensemble $D \subseteq V$, on a

$$\left(\prod_{u \in D} X_u Z_{\mathcal{N}(u)} \right) |G\rangle = |G\rangle \tag{2.22}$$

On souhaite à présent montrer que

$$\left(\prod_{u\in D} X_u Z_{\mathcal{N}(u)}\right) = (-1)^{|G[D]|} X_D Z_{Odd(D)} \tag{2.23}$$

On raisonne alors par induction sur la taille de l'ensemble D. Le cas initial $|D| = 1$ est donné par la Propriété 1.3 car $Odd(u) = \mathcal{N}(u)$ et $|G[u]| = 0$. Supposons que la propriété (2.23) soit vraie pour un ensemble D de taille quelconque. Alors pour tout $v \in V$, on distingue deux cas :

– Si $v \notin Odd(D)$, alors $|G[D \cup v]| = |G[D]| \bmod 2$ car l'ajout du sommet v ajoute un nombre pair d'arètes par rapport au sous-graphe induit par D (par hypothèse sur v). Ensuite, on a

$$X_{D\cup v} Z_{Odd(D\cup v)} = X_D X_v Z_{Odd(D)} Z_{Odd(v)} \tag{2.24}$$
$$= X_D Z_{Odd(D)} X_v Z_{\mathcal{N}(v)} \tag{2.25}$$

car $v \notin Odd(D)$.

– Si $v \in Odd(D)$, $|G[D \cup v]| = |G[D]| + 1 \bmod 2$ par hypothèse sur v, et puisque les opérateurs X et Z anti-commutent, on a

$$X_{D\cup v} Z_{Odd(D\cup v)} = -X_D Z_{Odd(D)} X_v Z_{\mathcal{N}(v)} \tag{2.26}$$

Dans tous les cas, la propriété (2.23) est vérifiée sur l'ensemble $D \cup v$ et ceci termine la preuve de l'égalité (2.21). □

Le lemme suivant fournit une preuve de la correction de la procédure de reconstruction du secret par un ensemble autorisé dans un protocole cQSS (Lemme 2.3).

Lemme 2.5. *La procédure de reconstitution du secret dans un protocole cQSS décrite dans la Figure 2.1 permet effectivement de reconstituer le secret initial s.*

Démonstration. L'état partagé entre les joueurs de l'ensemble B a noyau impair est $|G'_s\rangle = Z^s_{\mathcal{N}(d)} |G'\rangle$ (2.10). On note aussi

$$\mathcal{O}_D = (-1)^{|G'[D]|} X_D Z_{Odd(D)} \tag{2.27}$$

l'observable associée à la mesure projective effectuée. Afin de trouver les sous-espaces propres associés à $\mathcal{O}_D$, on calcule :

$$\mathcal{O}_D \left|G'_s\right\rangle = (-1)^{|G'[D]|} X_D Z_{Odd(D)} Z^s_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.28}$$
$$= (-1)^{|G'[D]|} X_D Z^s_{\mathcal{N}(d)} Z_{Odd(D)} \left|G'\right\rangle \tag{2.29}$$
$$= (-1)^{|G'[D]|} (-1)^s Z^s_{\mathcal{N}(d)} X_D Z_{Odd(D)} \left|G'\right\rangle \tag{2.30}$$
$$\tag{2.31}$$

car $|D \cap \mathcal{N}(d)| = 1 \bmod 2$, donc il y a un nombre impair d'échanges entre les opérateurs X et Z (qui anti-commutent) sur les qubits associés à $D \cap \mathcal{N}(d)$. On a donc l'apparition d'un signe '$-$' conditionné par la valeur de s. En utilisant le Lemme 2.4 :

$$\mathcal{O}_D \left|G'_s\right\rangle = (-1)^s Z^s_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.32}$$

$$= (-1)^s \left|\varphi\right\rangle \tag{2.33}$$

L'état $|\varphi\rangle$ est donc un vecteur propre de $\mathcal{O}_D$ associé à la valeur propre 1 si $s = 0$ et -1 si $s = 1$. En écrivant

$$\mathcal{O}_D = P_0 - P_1 \tag{2.34}$$

avec $P_0 = \frac{I+\mathcal{O}_D}{2}$ et $P_1 = \frac{I-\mathcal{O}_D}{2}$ les deux projecteurs associés aux sous-espaces propres de $\mathcal{O}_D$. Le résultat de la mesure projective associée à $\mathcal{O}_D$ détermine parfaitement la valeur de s : si la mesure retourne '0', alors $s = 0$ et si elle retourne '1' alors $s = 1$. □

Ce Théorème fournit entre autres une preuve constructive du premier point du Lemme 2.3.

En ce qui concerne le deuxième point du Lemme 2.3, nous pouvons également exprimer le fait qu'un ensemble B de joueurs dominé modulo 2 ne puisse pas obtenir d'information sur le secret $s \in \{0, 1\}$:

Propriété 2.6. *Soit $G = (V, E)$ un graphe, $d \in V$ un sommet et $V' = V \setminus \{d\}$. Pour tout protocole cQSS (G,d), tout ensemble $B \subseteq V'$ dominé modulo 2 est un ensemble interdit.*

Démonstration. Soit $G' = (V', E)$ (voir Figure 2.1) et $\rho^B(s)$ la matrice de densité associée à l'état du système B. On souhaite montrer que $\rho^B(0) = \rho^B(1)$. On pose également

$$\rho(s) = \left|G'_s\right\rangle \left\langle G'_s\right| \tag{2.35}$$

$$= \rho^B(s) \otimes \rho^{V' \setminus B}(s) \tag{2.36}$$

la matrice de densité associée à l'état du système global sans le dealer. B est dominé modulo 2, donc d'après la Définition 2.4 il existe $C \subseteq B$ tel que

$$Odd(C) \cap B = \mathcal{N}(d) \cap B \tag{2.37}$$

On appelle U l'opérateur agissant uniquement sur les qubits de $V' \setminus B$ défini de la façon suivante :

$$U = (-1)^{G[C]} X_C Z_{Odd(C)+\mathcal{N}(d)} \tag{2.38}$$

On écrit alors

$$U\rho(1)U^\dagger = U Z_{\mathcal{N}(d)} \left|G'\right\rangle \left\langle G'\right| Z_{\mathcal{N}(d)} U^\dagger \tag{2.39}$$

$$= \left|G'\right\rangle \left\langle G'\right| \tag{2.40}$$

d'après le Lemme 2.4. Ainsi,

$$U\rho(1)U^\dagger = \rho(0) \tag{2.41}$$

Par définition de l'ensemble C, l'opérateur U agit uniquement sur les qubits de $V' \setminus B$, donc on peut écrire

$$U\rho(1)U^\dagger = \rho^B(1) \otimes U\rho^{V'\setminus B}(1)U^\dagger \tag{2.42}$$
$$= \rho^B(0) \otimes \rho^{V'\setminus B}(0) \tag{2.43}$$

d'après l'égalité (2.41). La trace partielle de l'état précédent par rapport au premier registre donne donc

$$\rho^B(0) = \rho^B(1) \tag{2.44}$$

Les joueurs de l'ensemble B n'ont aucune information sur le secret s. □

Nous montrons à présent que les conditions du Lemme 2.3 sont également des conditions nécessaires d'accessibilité au secret. De plus, nous prouvons que le protocole cQSS est *parfait*, c'est-à-dire que chaque sous-ensemble de joueurs est soit autorisé soit interdit, donc qu'il n'existe aucun ensemble de joueur qui possède une information partielle sur le secret.

Théorème 2.7. *Pour tout graphe $G = (V, E)$ et $d \in V$, pour tout $B \subseteq V \setminus \{d\}$, B vérifie exactement l'une des deux propriétés suivantes :*

1. *B est à noyau impair*
2. *B est dominé modulo 2*

Démonstration. Soit Γ la matrice d'adjacence associée au graphe $G' = G\setminus\{d\}$. On a donc $\Gamma \in \mathcal{M}_{n,n}(\mathbb{F}_2)$ où n est l'ordre de G'. Pour tout ensemble $B \subseteq V \setminus \{d\}$, nous appelons Γ_B la matrice de coupe induite par les sommets de B, c'est-à-dire la sous-matrice de Γ dont les colonnes correspondent aux sommets de B et les lignes correspondent aux sommets de $V \setminus B$.

$$\Gamma = \left[\begin{array}{c|c} * & \Gamma_B \\ \hline \Gamma_B^T & * \end{array}\right] \tag{2.45}$$

En représentant les ensembles X de sommets de V par leurs vecteurs caractéristiques (c'est-à-dire avec un '1' en $i^{\text{ième}}$ position lorsque le sommet i appartient à X), la matrice Γ_B est celle de l'application linéaire suivante :

$$\Gamma_B : \quad X \subseteq B \quad \mapsto \quad \Gamma_B X = Odd(X) \cap V \setminus B \tag{2.46}$$

En effet, si $X = \{u\} \subseteq B$, on a $\Gamma_B X = \mathcal{N}(u) \cap V \setminus B$. Par linéarité, si X contient un nombre quelconque de sommets, les coordonnées non-nulles du vecteur $\Gamma_B X$ sont celles qui correspondent aux sommets de $V \setminus B$ qui appartiennent au voisinage d'un nombre impair de sommets de X. De façon similaire,

$$\Gamma_{V\setminus B} : \ Y \subseteq V \setminus B \ \mapsto \ \Gamma_{V\setminus B} Y = Odd(Y) \cap B \tag{2.47}$$

$\forall Y \subseteq V \setminus B, \Gamma_{V\setminus B} Y = Odd(Y) \cap B$. Notons que Γ est symétrique, d'où $\Gamma_{V\setminus B} = \Gamma_B^T$. Dans la suite de cette preuve, nous identifierons les ensembles de sommets à leurs vecteurs caractéristiques.

On remarque le fait suivant : étant donnés deux ensembles $X \subseteq V$ et $Y \subseteq V$, nous avons $|X \cap Y| \bmod 2 = Y^T X$. Dans l'équation 1, la condition $D \cup Odd(D) \subseteq B$ se traduit ainsi par $\Gamma_B D = 0$, et la condition $|D \cap \mathcal{N}(d)| = 1 \bmod 2$ peut s'écrire $(\mathcal{N}(d) \cap B)^T D = 1$. Ecrites de cette façon, les deux conditions précédentes permettent de relâcher la contrainte $D \subseteq B$. Ainsi, l'équation 1 est vérifiée lorsque

$$\exists D \subseteq V, \quad \left[\begin{array}{c} (\mathcal{N}(d) \cap B)^T \\ \hline \\ \Gamma_B \\ \\ \end{array}\right] D = \left[\begin{array}{c} 1 \\ \hline 0 \\ \vdots \\ 0 \end{array}\right] \tag{2.48}$$

La condition précédente est équivalente à

$$\mathsf{rank} \left[\begin{array}{c} (\mathcal{N}(d) \cap B)^T \\ \hline \\ \Gamma_B \\ \\ \end{array}\right] = \mathsf{rank} \left[\begin{array}{c|c} (\mathcal{N}(d) \cap B)^T & 1 \\ \hline & 0 \\ \Gamma_B & \vdots \\ & 0 \end{array}\right] \tag{2.49}$$

$$= \mathsf{rank} \left[\begin{array}{c|c} 0 & 1 \\ \hline & 0 \\ \Gamma_B & \vdots \\ & 0 \end{array}\right] \tag{2.50}$$

$$= \mathsf{rank}(\Gamma_B) + 1 \tag{2.51}$$

Notons

$$\pi(B) = \mathsf{rank} \left[\begin{array}{c} (\mathcal{N}(d) \cap B)^T \\ \hline \\ \Gamma_B \\ \\ \end{array}\right] - \mathsf{rank}(\Gamma_B) \tag{2.52}$$

Ainsi, pour tout $B \subseteq V$, B est à noyau impair lorsque $\pi(B) = 1$.

De façon similaire, on établit que pour tout $B \subseteq V$, B est dominé modulo 2 lorsque

$$\exists C \subseteq V,\ \Gamma_{V\setminus B}.C = \mathcal{N}(d) \cap B \ \Leftrightarrow\ \mathsf{rank}\left[\ \Gamma_{V\setminus B}\ \middle|\ \mathcal{N}(d)\cap B\ \right] = \mathsf{rank}(\Gamma_{V\setminus B}) \quad (2.53)$$

$$\Leftrightarrow\ \mathsf{rank}\begin{bmatrix}\dfrac{(\mathcal{N}(d)\cap B)^T}{\Gamma_B}\end{bmatrix} = \mathsf{rank}(\Gamma_B) \quad (2.54)$$

$$\Leftrightarrow\ \pi(B) = 0 \quad (2.55)$$

Pour tout ensemble $B \subseteq V$, $\pi(B) \in \{0,1\}$ d'où exactement l'une des deux propriétés énoncées 1 ou 2 est vraie. □

Le théorème précédent fournit ainsi une caractérisation des ensembles autorisés et interdits dans un protocole cQSS :

Corollaire 2.8. *Soit $G = (V, E)$ un graphe. Le protocole cQSS (G, d) est parfait, et pour tout ensemble $B \subseteq V \setminus \{d\}$,*
– *B est autorisé $\Leftrightarrow$ B est à noyau impair*
– *B est interdit $\Leftrightarrow$ B est dominé modulo 2*

Dans cette section, nous avons établi une correspondance directe entre structures graphiques et structures d'accès au secret dans le cadre des protocoles cQSS. Dans de tels protocoles, on peut donc partitionner les ensembles de joueurs selon leur capacité à reconstruire le secret. Le corollaire précédent nous assure que les protocoles de partage de secret cQSS sont parfaits : les ensembles de joueurs qui ne peuvent pas reconstituer le secret ne peuvent en extraire aucune information.

2.2.2 Protocole classique équivalent

Les protocoles cQSS qui utilisent des états graphes afin de partager un secret classique $s \in \{0,1\}$ offrent des structures d'accès spécifiques dépendant des propriétés graphiques des graphes sous-jacents (Définition 2.4 et Corollaire 2.8). Etant donnée l'utilisation d'états quantiques pour réaliser ces structures d'accès pour un secret classique, nous nous posons naturellement la question de l'existence de protocoles exclusivement classiques qui réalisent ces mêmes structures d'accès. Nous proposons ainsi des protocoles classiques à partir de graphes quelconques qui fournissent les mêmes structures d'accès que les protocoles cQSS (Corollaire 2.8). Ces protocoles seront notés cCSS.

On considère ici une famille de protocoles de partage de secret classique construite à partir de n'importe quel graphe $G = (V, E)$. On associe à chaque sommet du graphe un joueur, le secret est un bit classique $s \in \{0,1\}$. Chaque joueur possède une clé secrète k_i ainsi que le secret masqué par les clés secrètes de ses voisins ($c_i = s + \sum_{i' \in \mathcal{N}(i)} k_{i'}$).

La Figure 2.3 est un exemple de protocole cCSS construit à partir du graphe P_5.

Nous donnons une définition formelle de ce protocole dans la Figure 2.4

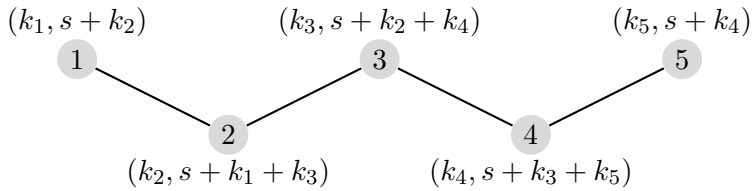

FIGURE 2.3 – Protocole cCSS sur le graphe P_5

Le principe de la reconstruction du secret est d'utiliser les clés des voisins pour supprimer le masque présent sur le secret. On peut ainsi tout d'abord constater qu'un joueur avec ses voisins constituent un ensemble autorisé. Dans la figure précédente, par exemple, les ensembles $\{1, 2\}, \{2, 3, 4\}, \{4, 5\}$ peuvent reconstituer le secret. Il existe cependant des ensembles de joueurs qui peuvent reconstituer les secret mais qui ne sont pas de cette forme. C'est le cas de l'ensemble de joueurs $\{1, 3, 5\}$: en effet, si on ajoute leurs secrets masqués, on obtient

$$(s + k_2) + (s + k_2 + k_4) + (s + k_4) = 3s + 2k_2 + 2k_4 \tag{2.56}$$
$$= s \bmod 2 \tag{2.57}$$

Le secret en clair peut donc être reconstruit. Nous cherchons alors à caractériser les ensembles qui peuvent accéder au secret.

On note c_i la valeur associée au secret s masqué par les voisins du joueur i :

$$c_i = s + \sum_{i' \in \mathcal{N}(i)} k_{i'} \bmod 2 \tag{2.58}$$

Nous avons la propriété suivante :

Propriété 2.9. *Soit $G = (V, E)$ un graphe et $d \in V$. On note $V' = V \setminus \{d\}$. Soit (G, d) le protocole cCSS construit à partir du graphe G avec un dealer d. Tout ensemble de joueurs $B \subseteq V'$ à noyau impair (Définition 2.4) peut reconstruire le secret.*

Démonstration. Soit $B \subseteq V'$ un ensemble à noyau impair. Il existe donc $D \subseteq B$ tel que $|D| = 1 \mod 2$ et $Odd(D) \subseteq B$. On montre maintenant que les joueurs de l'ensemble B

peuvent reconstruire le secret en calculant la quantité $\sum_{i\in D} c_i + \sum_{j\in Odd(D)} k_j \mod 2$.

$$\sum_{i\in D} c_i + \sum_{j\in Odd(D)} k_j = \sum_{i\in D}\left(s + \sum_{i'\in\mathcal{N}(i)} k_{i'}\right) + \sum_{j\in Odd(D)} k_j \tag{2.59}$$

$$= |D|.s + \sum_{i\in D, i'\in\mathcal{N}(i)} k_{i'} + \sum_{j\in Odd(D)} k_j \tag{2.60}$$

$$= |D|.s + \sum_{i'\in V} |\mathcal{N}(i')\cap D|.k_{i'} + \sum_{j\in Odd(D)} k_j \tag{2.61}$$

$$= s \mod 2 \tag{2.62}$$

□

Nous montrons maintenant que tout ensemble dominé modulo 2 ne peut pas obtenir d'information sur le secret.

Théorème 2.10. *Soit $G = (V, E)$ un graphe, $d \in V$ et (G, d) le protocole cCSS associé. Soit $B \subseteq V \setminus \{d\}$ un ensemble de joueurs.*

$$B \text{ est dominé modulo 2} \Rightarrow B \text{ est interdit} \tag{2.63}$$

Démonstration. On note $G' = G \setminus \{d\}$ et $V' = V \setminus \{d\} = V(G')$. Soit B un ensemble de joueurs dominé modulo 2 dans G'.

Chaque joueur $i \in B$ possède le couple (k_i, c_i). On note ainsi $k_B = \{k_i\}_{i\in B}$ et $c_B = \{c_i\}_{i\in B}$.

Nous montrons que les joueurs de B ne possèdent aucune information sur le secret s, c'est à dire :

$$Pr(s|k_B, c_B) = Pr(\overline{s}|k_B, c_B) \tag{2.64}$$

où $\overline{s} = 1 + s \mod 2$.

Tout d'abord, on remarque que pour tout i

$$\overline{c_i} = \overline{s} + \sum_{j\in\mathcal{N}(i)} k_i \tag{2.65}$$

Ainsi, on a

$$Pr(\overline{s}|k_B, c_B) = Pr(s|k_B, \overline{c_B}) \tag{2.66}$$

De plus, d'après les lois fondamentales des probabilités,

$$Pr(s|k_B, c_B) = \frac{Pr(s, c_B|k_B)}{Pr(c_B|k_B)} \tag{2.67}$$

B est dominé modulo 2, ainsi d'après la Définition 2.4, il existe un ensemble $C \subseteq V' \setminus B$ tel que $B \subseteq Odd(C)$. En d'autres termes, pour tout $i \in B$, $|\mathcal{N}(i) \cap C| = 1 \mod 2$.

On exprime à présent la valeur de $\overline{c_i}$ pour tout joueur i en séparant les voisins de i qui appartiennent à C :

$$\overline{c_i} = 1 + s + \sum_{j \in \mathcal{N}(i)} k_j \mod 2 \tag{2.68}$$

$$= 1 + s + \sum_{j \in \mathcal{N}(i) \cap C} k_j + \sum_{j \in \mathcal{N}(i) \cap \overline{C}} k_j \mod 2 \tag{2.69}$$

$$= 1 + s + |\mathcal{N}(i) \cap C| + \sum_{j \in \mathcal{N}(i) \cap C} (k_j - 1) + \sum_{j \in \mathcal{N}(i) \cap \overline{C}} k_j \mod 2 \tag{2.70}$$

$$= s + \sum_{j \in \mathcal{N}(i) \cap C} \overline{k_j} + \sum_{j \in \mathcal{N}(i) \cap \overline{C}} k_j \mod 2 \tag{2.71}$$

où $k_C = \{k_i\}_{i \in C}$.

Ainsi, on peut déduire les deux égalités suivantes :

$$Pr(\overline{c_B}|k_B, k_C) = Pr(c_B|k_B, \overline{k_C}) \tag{2.72}$$

$$Pr(s, \overline{c_B}|k_B, k_C) = Pr(s, c_B|k_B, \overline{k_C}) \tag{2.73}$$

On peut désormais établir l'égalité (2.66) de la façon suivante :

$$Pr(\overline{s}|k_B, c_B) = Pr(s|k_B, \overline{c_B}) \tag{2.74}$$

$$= \frac{P(s, \overline{c_B}|k_B)}{Pr(\overline{c_B}|k_B)} \tag{2.75}$$

$$= \frac{\sum_{k_C \in \{0,1\}^C} P(k_C) P(s, \overline{c_B}|k_B, k_C)}{\sum_{k_C \in \{0,1\}^C} Pr(k_C) Pr(\overline{c_B}|k_B, k_C)} \tag{2.76}$$

$$= \frac{\sum_{k_C \in \{0,1\}^C} \frac{1}{2^{|C|}} Pr(s, c_B|k_B, \overline{k_C})}{\sum_{k_C \in \{0,1\}^C} \frac{1}{2^{|C|}} Pr(c_B|k_B, \overline{k_C})} \tag{2.77}$$

$$= \frac{\sum_{k_C \in \{0,1\}^C} \frac{1}{2^{|C|}} Pr(s, c_B|k_B, k_C)}{\sum_{k_C \in \{0,1\}^C} \frac{1}{2^{|C|}} Pr(c_B|k_B, k_C)} \tag{2.78}$$

$$= \frac{Pr(s, c_B|k_B)}{Pr(c_B|k_B)} \tag{2.79}$$

$$= Pr(s|k_B, c_B) \tag{2.80}$$

□

Tout comme pour le cas des protocoles cQSS définis au début de cette section, la caractérisation des ensembles autorisés pour les protocoles cCSS nous permet d'établir le corollaire suivant :

Corollaire 2.11. *Soit $G = (V, E)$ un graphe. Le protocole cCSS (G, d) est parfait, et pour tout ensemble $B \subseteq V \setminus \{d\}$,*
– *B est autorisé $\Leftrightarrow$ B est à noyau impair*
– *B est interdit $\Leftrightarrow$ B est dominé modulo 2*

Nous avons ainsi construit un protocole intégralement classique qui permet de partager un bit classique secret avec les mêmes structures d'accès que les protocoles cQSS définis précédemment.

cCSS

Soit $G = (V, E)$ un graphe d'ordre $n + 1$. Chaque sommet de G est associé à un joueur. Soit $d \in V$ le dealer qui souhaite partager un secret $s \in \{0, 1\}$ entre n joueurs (numérotés de 1 à n).

Partage du secret
– Pour tout joueur $i \in V \setminus \{d\}$, le dealer choisit une clé secrète k_i qu'il tire aléatoirement uniformément dans $\{0, 1\}$.
– Pour tout i, le dealer calcule la quantité $c_i = s + \sum_{i' \in \mathcal{N}(i)} k_{i'} \bmod 2$.
– Le dealer donne à chaque joueur i le couple (k_i, c_i).

Reconstitution du secret Si B est un ensemble de joueurs à noyau impair :
– Trouver $D \subseteq B$ tel que $Odd(D) \subseteq B$ (algorithme de la Figure 2.2)
– Le secret s est calculé de la façon suivante :

$$s = \sum_{i \in D} c_i + \sum_{j \in Odd(D)} k_j \tag{2.81}$$

FIGURE 2.4 – Protocole classique équivalent cCSS

2.3 Partage d'un secret quantique avec des états graphes

Dans [MS08], les protocoles cQSS sont généralisés au cas des protocoles de partage d'un secret quantique $|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$ à partir d'états graphes que l'on notera désormais "qQSS". Voici la description de ce protocole : à partir d'un graphe $G = (V, E)$ d'ordre $n+1$ et d'un sommet particulier $d \in V$ tel que $\mathcal{N}(d) \neq \varnothing$, on note G' le graphe résultant de G après suppression du sommet d qui représente le dealer. Ce dernier prépare tout d'abord l'état suivant :

$$\left|G'_\varphi\right\rangle = \alpha \left|G'\right\rangle + \beta Z_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.82}$$

On pourra noter que l'état $\left|G'_\varphi\right\rangle$ correspond à une superposition des encodages d'un secret classique 0 ou 1 dans le cas de protocoles cQSS. Soulignons également que la

transformation

$$|\varphi\rangle \mapsto \left|G'_{\varphi}\right\rangle \tag{2.83}$$

est une évolution quantique valide (c'est-à-dire une isométrie) lorsque $|G'\rangle$ et $Z_{\mathcal{N}(d)}|G'\rangle$ sont orthogonaux, ce qui est le cas puisque $\mathcal{N}(d) \neq \varnothing$.Le dealer envoie ensuite chacun des n qubits de l'état $\left|G'_{\varphi}\right\rangle$ à chacun des n joueurs restant.

En ce qui concerne la reconstruction du secret, une caractérisation des ensembles autorisés utilisant le graphe G et son complémentaire est proposée dans [MS08]. Nous la formulons ainsi :

Propriété 2.12 ([MS08])**.** *Soit $G = (V, E)$ un graphe et $d \in V$. Un ensemble $B \subseteq V \backslash \{d\}$ de joueurs est autorisé dans le protocole qQSS associé à (G, d) si et seulement si il est autorisé dans les protocoles cQSS associés à (G, d) et $(G * d, d)$.*

En d'autres termes, et de façon plus intuitive, l'accessibilité à un secret quantique dans un graphe G est "équivalente" à l'accessibilité à un secret classique dans G ainsi que dans $G * d$, le graphe obtenu à partir de G après complémentation locale avec le sommet d (dealer).

Nous introduisons ici une autre caractérisation des ensembles de joueurs autorisés pour un protocole qQSS qui a pour avantage de ne pas faire intervenir le graphe $G * d$. Dans un premier temps, nous établissons un lemme. Précisons pour cela la notation suivante : pour tous graphes $G_1 = (V, E_1)$ et $G_2 = (V, E_2)$ qui partagent le même ensemble de sommets, on définit $G_1 + G_2 = (V, E_1 + E_2)$ où $E_1 + E_2$ désigne la différence symétrique de E_1 et E_2.

Lemme 2.13. *Soit $G = (V, E)$ un graphe, $A \subseteq V$ et $X \subseteq V$ deux ensembles de sommets tels que $|X \cap A| = 1 \bmod 2$.*

$$Odd_{G+K_A}(X) = Odd_G(X) + A \tag{2.84}$$

Démonstration. Soit $u \in V$ un sommet. Si $u \notin A$, on a de façon évidente

$$|\mathcal{N}_G(u) \cap X| = |\mathcal{N}_{G+K_A}(u) \cap X| \tag{2.85}$$

Si $u \in A$, on décompose la quantité $|\mathcal{N}_G(u) \cap X|$ de la façon suivante :

$$\begin{aligned} |\mathcal{N}_G(u) \cap X| &= |\mathcal{N}_G(u) \cap X \cap A| + |\mathcal{N}_G(u) \cap X \cap \overline{A}| && (2.86)\\ &= |X \cap A| - |\mathcal{N}_{G+A}(u) \cap X \cap A| + |\mathcal{N}_{G+K_A}(u) \cap X \cap \overline{A}| && (2.87)\\ &= 1 + |\mathcal{N}_{G+K_A}(u) \cap X| \bmod 2 && (2.88) \end{aligned}$$

par hypothèse.

Ainsi, la parité de $|\mathcal{N}_G(u) \cap X|$ est la même que celle de $|\mathcal{N}_{G+K_A}(u) \cap X|$ si et seulement si $u \notin A$, ce qui se formule comme dans l'équation (2.84). □

On pourra noter l'égalité suivante dans le cas du graphe G et du sommet d : $G * d = G + K_{\mathcal{N}(d)}$.

Théorème 2.14. *Soit $G = (V, E)$ un graphe et $d \in V$ un sommet associé au dealer. Notons $V' = V \setminus \{d\}$. Un ensemble $B \subseteq V'$ est autorisé dans le protocole qQSS (G, d) si et seulement si les deux conditions suivantes sont réalisées :*

1. *B est autorisé dans le protocole cQSS (G, d)*
2. *$V' \setminus B$ est interdit dans le protocole cQSS (G, d)*

Démonstration. D'après le Lemme 2.13, pour tout $X \in V'$, si $|X \cap \mathcal{N}(d)| = 1 \bmod 2$ alors

$$Odd_{G*d}(X) = Odd_G(X) + \mathcal{N}(d) \tag{2.89}$$

Ainsi, pour tout $X, Y \in V'$ avec $|X \cap \mathcal{N}(d)| = 1 \bmod 2$

$$\begin{aligned} Odd_{G*d}(X) \cap Y = \varnothing &\iff (Odd_G(X) + \mathcal{N}(d)) \cap Y = \varnothing && (2.90)\\ &\iff (Odd_G(X) \cap Y) + (\mathcal{N}(d) \cap Y) = \varnothing && (2.91)\\ &\iff Odd_G(X) \cap Y = \mathcal{N}(d) \cap Y && (2.92) \end{aligned}$$

[⇒]
Supposons que B puisse reconstruire un secret quantique dans le protocole qQSS (G, d). B peut alors également reconstruire un secret classique dans le protocole cQSS (G, d) (en effet, le protocole cQSS est un cas particulier du protocole qQSS où le secret est $|0\rangle$ ou $|1\rangle$). Ainsi, par la Propriété 2.12, $\exists D \subseteq B$ tel que $Odd_{G*d}(D) \cap (V' \setminus B) = \varnothing$. L'expression (2.92) implique alors

$$Odd_G(D) \cap V' \setminus B = \mathcal{N}(d) \cap (V' \setminus B) \tag{2.93}$$

D'après le Lemme 2.3, $V' \setminus B$ est donc un ensemble interdit dans le protocole cQSS (G, d).

[⇐]
Supposons que l'ensemble $V' \setminus B$ soit interdit et que l'ensemble B soit autorisé dans le protocole cQSS (G, d). $V' \setminus B$ est interdit, donc il existe alors $C \subseteq B$ tel que $Odd_G(C) \cap V' \setminus B = \mathcal{N}(d) \cap V' \setminus B$ (Lemme 2.3). De même, B est autorisé, donc il existe un ensemble $D \subseteq V'$ tel que $|D \cap \mathcal{N}(d)| = 1 \bmod 2$ et $Odd_G(D) \cap V' \setminus B = \varnothing$. On définit alors l'ensemble C' de la façon suivante :

1. Si $|C \cap \mathcal{N}(d)| = 1 \bmod 2$, alors $C' = C$.
2. Si $|C \cap \mathcal{N}(d)| = 0 \bmod 2$, alors $C' = C + D$.

Montrons que dans les deux cas on a $|C' \cap \mathcal{N}(d)| = 1 \bmod 2$ et $Odd_G(C') \cap V' \setminus B = \mathcal{N}(d) \cap V' \setminus B$:

1. Ce cas est immédiat par définition de C.

2. Calculons la quantité $|C' \cap \mathcal{N}(d)|$:

$$|C' \cap \mathcal{N}(d)| = |(C \cap \mathcal{N}(d)) + (D \cap \mathcal{N}(d))| \tag{2.94}$$
$$= |(C \cap \mathcal{N}(d))| + |(C \cap \mathcal{N}(d))| \tag{2.95}$$
$$= 0 + 1 = 1 \bmod 2 \tag{2.96}$$

Montrons maintenant la deuxième propriété :

$$Odd_G(C') \cap V' \setminus B = (Odd_G(C) \cap V' \setminus B) + (Odd_G(D) \cap V' \setminus B) \tag{2.97}$$
$$= (\mathcal{N}(d) \cap V' \setminus B) + \varnothing \tag{2.98}$$
$$= \mathcal{N}(d) \cap V' \setminus B \tag{2.99}$$

Nous utilisons à présent l'expression (2.92) pour conclure que

$$Odd_{G*d}(C') \cap V' \setminus B = \varnothing \tag{2.100}$$

Par conséquent, B est autorisé dans les protocoles cQSS (G, d) et $(G*d, d)$. La Propriété 2.12 permet donc de conclure que B est autorisé dans le protocole qQSS associé à (G, d). □

A présent nous montrons que le processus de reconstruction d'un secret quantique partagé à l'aide d'un état graphe donné dans la Figure 2.5 permet effectvement de retrouver le secret initial :

Théorème 2.15. *La procédure de reconstitution du secret dans un protocole qQSS décrite dans la Figure 2.5 permet effectivement de reconstituer le secret initial s.*

Démonstration. L'ensemble B est de taille supérieure ou égale à k, donc d'après le Théorème 2.14 les deux ensembles C et D de la Figure 2.5 sont bien définis. L'application de l'isométrie U_D (2.109) à l'état $|\varphi\rangle$ donne l'état

$$|G_\varphi\rangle = U_D |\varphi\rangle \tag{2.101}$$
$$= |0\rangle \otimes P_0 |\varphi\rangle + |1\rangle \otimes P_1 |\varphi\rangle \tag{2.102}$$
$$= \alpha |0\rangle \otimes \left|G'\right\rangle + \beta |1\rangle \otimes Z_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.103}$$

En effet, comme il a été montré dans le Lemme 2.5, le vecteur $|G'\rangle$ est dans le sous-espace propre associé à P_0 et $Z_{\mathcal{N}(d)} |G'\rangle$ est dans le sous-espace propre associé à P_1.

Par définition de l'ensemble D, l'opérateur unitaire V_C (2.112) ne s'applique que sur des qubits de l'ensemble B (car $Odd(C) + \mathcal{N}(d) \in B$). On applique ensuite l'opérateur Λ_{V_C} défini en (2.111) :

$$\Lambda_{V_C} |G_\varphi\rangle = \alpha |0\rangle \otimes \left|G'\right\rangle + \beta |1\rangle \otimes V_C Z_{\mathcal{N}(d)} \left|G'\right\rangle \tag{2.104}$$
$$= \alpha |0\rangle \otimes \left|G'\right\rangle + \beta |1\rangle \otimes (-1)^{|G'[C]|} X_C Z_{Odd(C)} \left|G'\right\rangle \tag{2.105}$$

D'après le Lemme 2.4, on obtient

$$\Lambda_{V_C} |G_\varphi\rangle = \big(\alpha |0\rangle + \beta |1\rangle\big) \otimes \big|G'\big\rangle \tag{2.106}$$
$$= |\varphi\rangle \big|G'\big\rangle \tag{2.107}$$

et le premier registre contient bien l'état secret $|\varphi\rangle$. □

Une conséquence de ce théorème permet d'établir une propriété sur les graphes en général :

Propriété 2.16. *Soit $G = (V, E)$ un graphe et $d \in V$ un sommet. On note $V' = V \setminus \{d\}$. Soit $B \subseteq V'$ à noyau impair.*

$$V' \setminus B \text{ est dominé modulo } 2 \Leftrightarrow B \text{ est à noyau impair dans } G * d \tag{2.108}$$

Démonstration. D'après la Propriété 2.12, B est un ensemble autorisé dans le protocole qQSS (G,d). Le Théorème 2.14 permet de déduire que $V' \setminus B$ est interdit dans le protocole cQSS (G,d). Ainsi, par le Corollaire 2.8, B est à noyau impair dans $G * d$.

Les propriétés utilisées dans cette preuve sont des équivalences, ce qui tremine la preuve de cette propriété. □

Dans n'importe quel protocole de partage de secret pur, c'est-à-dire un protocole dans lequel l'état global des joueurs est un état pur (voir Définition 1.10), un ensemble de joueurs peut reconstituer le secret si et seulement si l'ensemble complémentaire ne possède aucune information sur le secret (voir [Got00]). Nous pouvons tirer de ce fait une conséquence sur les protocoles qQSS :

Corollaire 2.17. *Soit $G = (V, E)$ un graphe et $d \in V$. Pour tout protocole qQSS associé à (G, d), un ensemble de joueurs B est interdit si et seulement si $V' \setminus B$ est autorisé dans le protocole cQSS (G, d) ($V' = V \setminus \{d\}$).*

Nous avons donné plusieurs caractérisations graphiques des ensembles de joueurs autorisés et interdits dans les protocoles qQSS grâce à l'utilisation des propriétés établies pour le cas d'un secret classique (protocoles cQSS). On peut cependant noter une différence majeure avec les protocoles cQSS : l'apparition d'un troisième type d'ensemble de joueurs. En effet, il arrive que certains ensembles de joueurs ne soient ni autorisés, ni interdits.De tels ensembles n'existent pas pour les protocoles cQSS en raison du Théorème 2.7 et du Corollaire 2.8.

Corollaire 2.18. *Soit $G = (V, E)$ un graphe et $d \in V$. Les protocoles qQSS (G, d) et $(G * d, d)$ ont exactement les mêmes structures d'accès.*

Démonstration. Ce corollaire se déduit de l'interchangeabilité des deux graphes dans la Propriété 2.12 et du fait que $(G * d) * d = G$. □

qQSS

Soit $G = (V, E)$ un graphe d'ordre $n+1$ et $d \in V$ un sommet associé au dealer. On note G' le graphe résultant de G après suppression du sommet d. Le dealer souhaite partager un secret $|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$ entre n joueurs.

Partage du secret

1. *Encodage dans un état graphe :* Le dealer encode l'état $|\varphi\rangle$ dans l'état sur n qubits $\alpha |G'\rangle + \beta Z_{\mathcal{N}(d)} |G'\rangle$.
2. *Distribution :* Chaque joueur i reçoit de la part du dealer le qubit i correspondant.

Reconstitution du secret Les joueurs d'un ensemble B de taille supérieure ou égale à k souhaitent reconstituer le secret. Soit $D \subseteq B$ et $C \subseteq B$ tels que :
– $|D \cap \mathcal{N}(d)| = 1 \bmod 2$ et $Odd(D) \subseteq B$
– $Odd(C) \cap (V \setminus B) = \mathcal{N}(d) \cap (V \setminus B)$
Le processus de reconstruction se déroule de la façon suivante :

1. *Registre auxiliaire :* Les joueurs de B appliquent à leurs qubits l'isométrie

$$U_D = |0\rangle \otimes P_0 + |1\rangle \otimes P_1 \tag{2.109}$$

où $\left\{ P_i = \frac{I + (-1)^i \mathcal{O}_D}{2} \right\}$ sont les projecteurs associés à l'observable

$$\mathcal{O}_D = (-1)^{|G'[D]|} X_D Z_{Odd(D)} \tag{2.110}$$

L'état global résultant est $\alpha |0\rangle \otimes |G'\rangle + \beta |1\rangle \otimes Z_{\mathcal{N}(d)} |G'\rangle$

2. *Désintrication du registre auxiliaire :* Les joueurs de l'ensemble B appliquent l'opérateur unitaire

$$\Lambda_{V_C} = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes V_C \tag{2.111}$$

avec

$$V_C = (-1)^{|G'[C]|} X_C Z_{Odd(C)+\mathcal{N}(d)} \tag{2.112}$$

L'état global résultant est alors

$$\big(\alpha |0\rangle + \beta |1\rangle\big) \otimes \big|G'\big\rangle \tag{2.113}$$

Le premier registre contient alors le secret.

FIGURE 2.5 – Description d'un protocole de partage de secret quantique à seuil qQSS de paramètres $((n, k))$

2.4 Partage de secret quantique avec seuil

Nous avons présenté jusqu'ici un protocole permettant de partager un secret classique ainsi qu'un secret quantique à l'aide d'états graphes, et une caractérisation graphique des structures d'accès liée aux graphes sous-jacents a été établie dans ces deux cas. On se pose maintenant la question de l'existence de protocoles de partage d'un secret quantique $|\varphi_s\rangle$ à seuil : existe-t-il des graphes d'ordre n dont les sous-ensembles de sommets autorisés sont exactement ceux de taille supérieure ou égale à k pour un certain $k \leq n$?

2.4.1 Graphes à seuil naturel

Comme présenté dans [MS08], on peut construire un protocole cQSS de paramètres $(5, 3)$ ainsi qu'un protocole qQSS $((5, 3))$ à partir du cycle à 5 sommets.

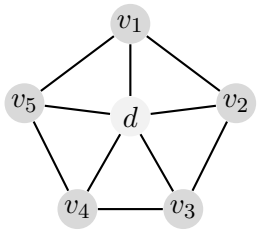

FIGURE 2.6 – Graphe W_6

Théorème 2.19. *Le graphe W_6 constitué d'un graphe C_5 et d'un sommet d (dealer) universel réalise un protocole cQSS de paramètres* $(5, 3)$

Démonstration. On souhaite montrer que, pour le graphe W_6 décrit en Figure 2.6 où le dealer d est le sommet de degré 5, tous les ensembles de sommets autres que d de taille 3 sont à noyau impair (Définition 2.4), et tous les ensembles de taille 2 sont dominés modulo 2.

A isomorphisme près, il existe exactement 2 ensembles de taille 3 différents dans le graphe C_5 : ceux qui sont isomorphes à $\{v_1, v_2, v_3\}$ et ceux qui sont isomorphes à $\{v_1, v_3, v_4\}$:
– $B = \{v_1, v_2, v_3\} \rightarrow D = \{v_2\}$, $Odd(D) = \{v_1, v_3\}$
– $B = \{v_1, v_3, v_4\} \rightarrow D = \{v_1, v_3, v_4\}$, $Odd(D) = \{v_3, v_4\}$
Les ensembles de sommets de taille 3 sont donc autorisés (Lemme 2.3).

A présent, on montre que les ensembles de sommets de taille inférieure sont dominés modulo 2 (Définition 2.4). Tout comme pour les ensembles de taille 3, les ensembles de sommets de taille 2 sont nécessairement isomorphes à $\{v_1, v_2\}$ ou à $\{v_1, v_3\}$.
– $B = \{v_1, v_2\} \rightarrow C = \{v_3, v_5\}$, $Odd(C) = \{v_1, v_2\} = B$
– $B = \{v_1, v_3\} \rightarrow C = \{v_2\}$, $Odd(C) = \{v_1, v_3\} = B$

Les ensembles de sommets de taille 2 sont dominés modulo 2, donc d'après la caractérisation du Lemme 2.3, ce sont des ensembles interdits.

On a donc la présence d'un seuil à partir de la taille 3. □

Etendons maintenant ce résultat aux protocoles qQSS, c'est-à-dire où le secret partagé est un état quantique quelconque :

Théorème 2.20. *Le graphe W_6 de la Figure 2.6 réalise un protocole qQSS de paramètres* $((5,3))$

Démonstration. Dans la preuve du Théorème 2.19, on a montré que les ensembles de sommets de taille 3 sont autorisés pour un protocole cQSS, et les ensembles de taille 2 sont interdits. Or, en faisant abstraction du sommet d de degré 5 dans le graphe W_6, les ensembles de sommets de taille 2 sont les complémentaires de ceux de taille 3.

On utilise à présent le Théorème 2.14. Le graphe W_6 permet donc de réaliser un protocole qQSS de paramètres $((5,3))$ en prenant le sommet de degré 5 comme dealer. □

Notons que ce théorème peut également se prouver en utilisant la caractérisation de la Propriété 2.12 et en constatant que les graphes W_6 et $W_6 * d$ sont isomorphes (d est le sommet de degré 5 comme dans la Figure 2.6).

Le graphe W_6 est donc un exemple de graphe permettant de réaliser un protocole qQSS à seuil $(5,3)$ en choisissant le sommet de degré 5 (le centre de la roue) comme dealer.

Nous pouvons alors nous poser la question suivante : existe-t-il d'autres graphes dont les structures permettent de réaliser d'autres protocoles à seuil ? Nous montrons un peu plus loin dans le Corollaire 2.37 qu'il n'en existe pas à partir de l'ordre 79, et Sarvepalli a montré récemment qu'il n'en existe pas non plus dont les ordres sont compris entre 6 et 79 [Sar12]. Ainsi, le graphe W_6 est le seul graphe qui permet de construire un protocole de partage de secret qQSS à seuil.

2.4.2 One-time pad quantique

Le graphe C_5 est le seul graphe qui permette de réaliser un protocole de partage de secret quantique à seuil non-trivial. Nous proposons ici une modification du protocole initial permettant de générer un protocole de partage de secret à seuil à partir de n'importe quel graphe.

Supposons que le dealer souhaite partager un état $|\varphi_s\rangle$ entre n joueurs à partir d'un graphe G d'ordre n. Soit $k \leq n$ tel que la taille du plus grand ensemble interdit soit $k-1$.

– Le dealer tire aléatoirement 2 bits b_X et b_Z et partage l'état $X^{b_X} Z^{b_Z} |\varphi_s\rangle$ entre les n joueurs

– Le dealer partage les bits b_X et b_Z entre les n joueurs en utilisant un protocole de partage de secret classique [Sha79, Bla79].

De cette façon, le processus de reconstruction du secret s'effectue en 2 étapes : reconstituer l'état $X^{b_X} Z^{b_Z} |\varphi_s\rangle$, puis supprimer le "masque quantique" $X^{b_X} Z^{b_Z}$ en reconstituant les bits classiques b_X et b_Z. Cette méthode est appelée "one-time pad quantique" et est également utilisée par Boykin et Roychowdhury [BR03] et Ambainis, Mosca, Tapp et De Wolf [AMTW00].

Lemme 2.21. *Pour tout qubit dans un état $|\varphi\rangle$ quelconque, l'état résultant de l'application d'un "one-time pad quantique" est complètement mixte.*

Démonstration. Après application d'un one-time pad quantique $X^{b_X} Z^{b_Z}$ sans la connaissance de b_X et b_Z, l'état du qubit considéré s'écrit :

$$\rho = \frac{1}{4}\left[|\varphi\rangle\langle\varphi| + X|\varphi\rangle\langle\varphi|X^\dagger + Z|\varphi\rangle\langle\varphi|Z^\dagger + XZ|\varphi\rangle\langle\varphi|Z^\dagger X^\dagger\right] \tag{2.114}$$

En effet, chacun des opérateurs I, X, Z, et $XZ = -iY$ sont appliqués avec probabilité $\frac{1}{4}$. Posons $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$. L'état ρ s'écrit alors

$$\rho = \frac{1}{4}\left[\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{pmatrix} + \begin{pmatrix} |\beta|^2 & \beta\alpha^* \\ \alpha\beta^* & |\alpha|^2 \end{pmatrix} + \begin{pmatrix} |\alpha|^2 & -\alpha\beta^* \\ -\beta\alpha^* & |\beta|^2 \end{pmatrix} + \begin{pmatrix} |\beta|^2 & -\beta\alpha^* \\ -\alpha\beta^* & |\alpha|^2 \end{pmatrix}\right] \tag{2.115}$$

$$= \frac{I}{2} \tag{2.116}$$

L'état en question est donc complètement mixte. □

Ce lemme montre qu'il est impossible d'extraire de l'information sur $|\varphi\rangle$ lorsque l'on ne connait ni b_X ni b_Z.

La Figure 2.7 résume le protocole qQSS* (partage d'un secret quantique à seuil avec des états graphes et un one-time pad quantique).

2.4.3 Théorie du partage de secret à seuil

Soit $G = (V, E)$ un graphe d'ordre n et $d \in V$ l'un de ses sommets. Nous avons donné une caractérisation graphique des ensembles autorisés et des ensembles interdits dans les protocoles de partage de secret qQSS (Théorème 2.14 et Corollaire 2.8). Nous nous concentrons à présent sur une catégorie de partage de secret très étudiée en lien avec la théorie des codes : le partage de secret à seuil. Tout comme le partage de secret classique présenté en 2.1.1, on notera $((n, k))$ un protocole de partage d'un secret quantique à seuil k entre n joueurs.

Dans le cas d'un protocole de partage de secret quantique où l'état global du système est un état pur (voir Définition 1.10) comme c'est le cas de protocoles qQSS, le seuil, s'il

qQSS*

Soit $G = (V, E)$ un graphe d'ordre $n+1$ et $d \in V$ un sommet associé au dealer. On note G' le graphe résultant de G après suppression du sommet d. Le dealer souhaite partager un secret $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ entre n joueurs.

Partage du secret

1. *Chiffrement du secret :* Le dealer chiffre le secret $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ à l'aide d'un one-time pad quantique : il tire aléatoirement de façon uniforme deux bits classiques b_X et b_Z et applique l'opérateur $X^{b_X}Z^{b_Z}$ sur $|\varphi\rangle$. L'état résultant est alors $|\varphi'\rangle = \alpha|b_X\rangle + \beta(-1)^{b_Z}|\overline{b_X}\rangle$.
2. *Encodage dans un état graphe :* Le dealer encode l'état $|\varphi'\rangle$ dans l'état sur n qubits $\alpha\left|G'_{b_X}\right\rangle + \beta(-1)^{b_Z}\left|G'_{\overline{b_X}}\right\rangle$.
3. *Distribution :* Chaque joueur i reçoit de la part du dealer le qubit i correspondant. De plus, à l'aide d'un partage de secret classique de seuil k comme décrit à la section 4.14, le dealer partage les bits classiques b_X et b_Z entre les n joueurs.

Reconstitution du secret Les joueurs d'un ensemble B de taille supérieure ou égale à k souhaitent reconstituer le secret. Soit $D \subseteq B$ et $C \subseteq B$ tels que :
– $|D \cap \mathcal{N}(d)| = 1 \bmod 2$ et $D \cup Odd(D) \subseteq B$
– $Odd(C) \cap (V \setminus B) = \mathcal{N}(d) \cap (V \setminus B)$
Le processus de reconstruction se déroule en 3 étapes :

1. *Registre auxiliaire :* Les joueurs de B appliquent à leurs qubits l'isométrie

$$U_D = |0\rangle \otimes P_0 + |1\rangle \otimes P_1 \tag{2.117}$$

où $\{P_i\}$ sont les projecteurs associés à l'observable

$$\mathcal{O}_D = (-1)^{G[D]} X_D Z_{Odd(D)} \tag{2.118}$$

En d'autres termes,

$$P_i = \frac{I + (-1)^i \mathcal{O}_D}{2} \tag{2.119}$$

L'état global résultant est $\alpha|b_X\rangle \otimes \left|G'_{b_X}\right\rangle + \beta.(-1)^{b_Z}|\overline{b_X}\rangle \otimes \left|G'_{\overline{b_X}}\right\rangle$

2. *Désintrication du registre auxiliaire :* Les joueurs de l'ensemble B appliquent l'opérateur unitaire contrôlé

$$\Lambda_{V_C} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes V_C \tag{2.120}$$

où $V_C = (-1)^{G[C]} X_C Z_{Odd(C)+\mathcal{N}(d)}$. L'état global résultant est alors

$$\alpha|b_X\rangle \otimes \left|G'\right\rangle + \beta.(-1)^{b_Z}|\overline{b_X}\rangle \otimes \left|G'\right\rangle = \left(\alpha|b_X\rangle + \beta.(-1)^{b_Z}|\overline{b_X}\rangle\right) \otimes \left|G'\right\rangle \tag{2.121}$$

3. *Déchiffrement du secret :* Les joueurs de B retrouvent les bits b_X et b_Z grâce au partage de secret classique. Ils appliquent ensuite X^{b_X} puis Z^{b_Z} sur le qubit du premier registre qui se retrouve alors dans l'état $|\varphi\rangle$.

FIGURE 2.7 – Description d'un protocole de partage de secret quantique à seuil qQSS* $((n, k))$

existe, est nécessairement égal à $\frac{n+1}{2}$ [Got00]. Cette propriété est très restrictive, ainsi nous connaissons un unique protocole qQSS qui soit à seuil : le protocole basé sur un graphe C_5 auquel on ajoute un sommet universel (le dealer). Ce protocole réalise un partage de secret quantique à seuil $((5,3))$.

Cependant, de manière générale, un protocole qQSS correspond à un partage de secret à palier ("ramp secret sharing scheme", voir [OSIY05b]) dans lequel un ensemble de joueurs B vérifie nécessairement l'une des 3 conditions :
– si $|B| \leq n-k$, alors B est interdit et ne peut obtenir aucune information sur le secret
– si $n-k < |B| < k$, alors B possède une information partielle sur le secret
– si $|B| \geq k$, alors B est autorisé et peut reconstruire le secret
pour un entier k donné avec $\frac{n}{2} < k \leq n$.

Nous montrons dans cette section comment ces partages de secret quantique à palier peuvent être transformés en partages de secret à seuil qQSS* à l'aide d'une étape supplémentaire utilisant un protocole de partage de secret classique ([Sha79] par exemple).

Dans un premier temps, nous établissons les propriétés graphiques utilisées dans la caractérisation des structures d'accès et nous donnons ensuite une construction des protocoles qQSS* où le secret est encodé suivant le voisinage du sommet correspondant au dealer. Enfin, nous réduisons l'étude des protocoles qQSS* au cas d'un dealer universel (sommet $d \in V$ universel dans G).

Nous introduisons à présent une quantité centrale pour les protocoles de partage de secret quantique à seuil à partir d'état graphe : le "seuil d'accessibilité quantique" $\kappa_Q(G,d)$ définie pour tout graphe $G=(V,E)$ et tout sommet $d \in V$. Cette quantité est en lien direct avec la valeur du seuil que les graphes considérés permettent de réaliser.

Définition 2.5. *Soit $G=(V,E)$ un graphe d'ordre n et $d \in V$ un sommet au voisinage non vide. On note $V' = V \setminus d$.*

$$\kappa_Q(G,d) = \min_{B \subseteq V'} \left\{ |B| \text{ t.q. } \exists D_B, C_B \subseteq B \left\{ \begin{array}{l} |D_B \cap \mathcal{N}(d)| = 1 \bmod 2 \\ Odd(D_B) \subseteq B \\ Odd(C_B) \cap V \setminus B = \mathcal{N}(d) \cap V \setminus B \end{array} \right. \right\} \tag{2.122}$$

$$= \min_{B \subseteq V'} \left\{ B \text{ est à noyau impair et } V' \setminus B \text{ est dominé modulo } 2 \right\} \tag{2.123}$$

Nous définissons également

$$\overline{\kappa_Q}(G,d) = n - \kappa_Q(G,d) \tag{2.124}$$

Nous omettrons parfois le sommet d dans cette notation, auquel cas $\kappa_Q(G) = \kappa_Q(G \cup d, d)$ où $G \cup d$ est un graphe obtenu à partir de G après ajout d'un sommet universel d. On notera également $\overline{\kappa_Q}(G) = \overline{\kappa_Q}(G \cup d, d)$.

Nous remarquons une propriété sur la quantité définie précédemment :

Propriété 2.22. *Soit $G = (V, E)$ un graphe d'ordre n et $d \in V$ un sommet au voisinage non vide.*

$$\kappa_Q(G, d) = \kappa_Q(G * d, d) \tag{2.125}$$

Il est également possible de caractériser la quantité κ_Q en faisant intervenir les ensembles à noyau impair du graphe $G * d$:

Propriété 2.23. *Soit $G = (V, E)$ un graphe d'ordre n et $d \in V$ un sommet au voisinage non vide. On note $V' = V \setminus d$.*

$$\kappa_Q(G, d) = \min_{B \subseteq V'} \{B \text{ est à noyau impair dans } G \text{ et dans } G * d\} \tag{2.126}$$

Démonstration. D'après la Définition 2.5, la quantité $\kappa_Q(G)$ est un minimum sur les ensembles $B \subseteq V'$ à noyau impair. On utilise alors la Propriété 2.16 afin de remplacer la contrainte "$V' \setminus B$ est dominé modulo 2 dans G" par "B est à noyau impair dans $G * d$". □

Nous arrivons ainsi à un des principaux résultats de ce chapitre :

Théorème 2.24. *Soit $G = (V, E)$ un graphe et $d \in V$ un sommet au voisinage non vide. Pour tout $k > \kappa_Q(G, d)$, pour tout $c \geq 0$, il existe un protocole de partage de secret quantique à seuil $((n + c, k + c))$ dans lequel :*
- *le dealer envoie exactement 1 qubit à n joueurs parmi les $n + c$*
- *le dealer utilise un protocole de partage de secret classique à seuil $(n + c, k + c)$ pour partager 2 bits classiques d'information*

La suite de cette section est dédiée à la preuve de ce théorème. Nous noterons ces protocoles *qQSS**.

Un protocole de partage de secret quantique $((n, n))$ est proposé dans [BCT08] dans lequel l'application conditionnelle d'un opérateur Z est utilisée afin d'interdire à certains ensembles de joueurs de taille inférieure au seuil n d'obtenir de l'information partielle sur le secret. En nous inspirant de ce protocole, nous proposons l'ajout d'une phase de reconstruction "classique" aux protocoles qQSS définis précédemment. De cette façon, les protocoles qQSS qui correspondaient à des protocoles à palier $((n - k, k, n))$ peuvent être transformés en protocoles de partage de secret à seuil $((n, k))$ en assurant que les ensembles de joueurs dont la taille est comprise entre $n - k$ et k n'ont pas d'information sur le secret.

Nous remarquons que le protocole défini dans la sous-section 2.1.3 à partir d'un état GHZ correspond à un protocole qQSS à partir de l'état graphe $|K_n\rangle$ où K_n est le graphe complet sur n sommets. Cette construction se trouve donc étendue à n'importe quel graphe, également avec un chiffrement initial du secret plus général.

Lemme 2.25. *Le protocole qQSS* tel que défini précédemment à partir d'un graphe $G = (V, E)$, d'un sommet $d \in V$ et d'un entier k est un protocole de partage de secret quantique à seuil $((n, k))$ où n est l'ordre de G.*

Démonstration. Soit $|\varphi\rangle$ le secret partagé dans le protocole qQSS* considéré. Le masque classique utilisé dans le protocole qQSS* à l'aide d'un one-time pad quantique assure que pour tout ensemble B de joueurs de taille strictement inférieure à k, B n'a aucune information sur $|\varphi\rangle$. En effet, les bits classiques b_X et b_Z sont partagés entre les joueurs de B avec un protocole de partage de secret classique, ainsi B ne possède aucune information sur ces bits. De plus, d'après le Lemme 2.21, les joueurs de B ne possèdent aucune information sur $|\varphi\rangle$. Tout ensemble B avec $|B| < k$ est donc interdit.

L'observable $\mathcal{O}_D$ agit sur les qubits de $D \cup Odd(D) \subseteq B$. Les projecteurs P_i vérifient

$$P_i |G_s\rangle = \begin{cases} |G_s\rangle & \text{si } i = s \\ 0 & \text{sinon} \end{cases} \tag{2.127}$$

Ainsi, après application de l'isométrie U_{D_B}, l'état résultant est

$$\alpha |b_x\rangle \otimes |G_{b_x}\rangle + \beta.(-1)^{b_z} \left|\overline{b_x}\right\rangle \otimes |G_{\overline{b_x}}\rangle \tag{2.128}$$

Pour la deuxième étape de la reconstruction du secret, on sait par définition de l'ensemble C que

$$Odd(C) \cap V \setminus B = \mathcal{N}(d) \cap V \setminus B \tag{2.129}$$

Ainsi,

$$C \cup (Odd(C) + \mathcal{N}(d)) \subseteq B \tag{2.130}$$

L'opérateur V_C agit donc uniquement sur des qubits de B. Après son application, l'état résultant est

$$\left(\alpha |b_x\rangle + \beta.(-1)^{b_z} \left|\overline{b_x}\right\rangle\right) \otimes |G\rangle \tag{2.131}$$

La phase de déchiffrement qui a lieu ensuite permet aux joueurs de B de reconstruire les bits b_X et b_Z et peuvent ainsi reconstituer l'état $|\varphi\rangle$. □

Preuve du Théorème 2.24.

Démonstration. La correction des protocoles qQSS* donnée dans le Lemme 2.25 prouve l'existence d'un protocole $((n, k))$.

Nous modifions alors ce protocole de la façon suivante : on ajoute c joueurs aux n joueurs initialement présents, et on partage les bits secrets b_x et b_z entre les $n + c$ joueurs au lieu des n premiers seulement à l'aide d'un protocole de partage de secret classique

$(n+c, k+c)$. De cette façon, tout ensemble de taille $n+c$ comprend au moins n joueurs initialement présents qui peuvent donc reconstituer l'état (2.131).

L'état secret $|\varphi\rangle$ est ensuite reconstitué grâce aux bits b_x et b_z, phase que les ensembles de joueurs de taille inférieure à $n+c$ ne peuvent effectuer. □

Dans la suite, nous nous restreignons aux protocoles (G, u) où u est un sommet universel. Ce choix est motivé par le fait que pour tout protocole (G, d) où d est un sommet quelconque au voisinage non vide, il existe un graphe $G' = (V', E')$ permettant de construire un protocole ayant des paramètres similaires à ceux du protocole initial. Ce résultat se formalise de la façon suivante :

Théorème 2.26. *Si $(G \cup \{d\}, d)$ réalise un protocole qQSS* $((n, k))$, alors il existe $G' = (V', E')$ et u un sommet universel tel que $(G' \cup \{u\}, u)$ réalise un protocole qQSS* $((k+\ell, n+\ell))$ avec $\ell = 2n - 2k + 1$.*

Démonstration. Soit $G' = (V', E')$ un graphe construit à partir de $G = (V, E)$ de la façon suivante : on ajoute à G un stable X de taille $n-k$ et une clique Y de taille $n-k+1$ telle que tout sommet de Y est connecté exclusivement aux sommets de X et de $V \setminus \mathcal{N}(d)$ (voir Figure 2.8).

On montre à présent que cette construction vérifie la propriété annoncée. Soit $B \subseteq V'$ tel que $|B| = k + l = 2n - k + 1$. Par construction, on a

$$|B| = k + |X| + |Y| \tag{2.132}$$

Ainsi, l'intersection de B avec les sommets de G vérifie nécessairement

$$|B \cap V| \geq k \tag{2.133}$$

$(G \cup \{d\}, d)$ réalise un protocole $((n, k))$, donc il existe deux ensembles $C, D \subseteq B \cap V$ tels que

$$\begin{cases} |D \cap \mathcal{N}(d)| = 1 \bmod 2 \\ Odd(D) \cap V \subseteq B \cap V \\ (Odd(C) \cap V' \setminus B) \cap V = (\mathcal{N}(d) \cap V' \setminus B) \cap V \end{cases} \tag{2.134}$$

A partir de ces ensembles C et D, on construit des ensembles $C', D' \subseteq V'$ tels que

$$\begin{cases} |D'| = 1 \bmod 2 \\ Odd(D') \subseteq B \\ Odd(C') \cap V' \setminus B = V' \setminus B \end{cases} \tag{2.135}$$

La construction est décrite ici (pour plus de clarté, les notations X et Y désignent à la fois les graphes et leurs sommets).
Pour l'ensemble D' :

– si $|D| = 1 \bmod 2$, on a $|D \cap V' \setminus \mathcal{N}(d)| = 0 \bmod 2$ donc $Odd(D) \cap Y = \varnothing$. De plus, par construction de G', $Odd(D) \cap X = \varnothing$. On prend alors $D' = D$ et on a donc bien $Odd(D') \subseteq B \cap V \subseteq B$.
– si $|D| = 0 \bmod 2$:
  – cas $B \cap X \neq \varnothing$: on a $|D \cap V' \setminus \mathcal{N}(d)| = 1 \bmod 2$ d'où $Y \subseteq Odd(D)$. De plus, pour tout $x \in B \cap X$, $Odd(D \cup \{x\}) = Odd(D) + \mathcal{N}(x) = Odd(D) + Y$. Ainsi, aucun sommet de $Odd(D \cup \{x\})$ n'appartient à Y, et on prend donc $D' = D \cup \{x\}$. On a bien $Odd(D') \subseteq B$.
  – cas $B \cap X = \varnothing$: dans ce cas, $|B| = 2n - k + 1 = |V| + |Y|$ donc $B = V \cup Y = V' \setminus X$. Ainsi, pour tout $u \in V$, $Odd(u) = \mathcal{N}(() u) \subseteq B$. On prend dans ce cas $D' = \{u\}$.

Pour l'ensemble C' :
– si $|C \cap V \setminus \mathcal{N}(d)| = 0 \bmod 2$, $Odd(C) \cap V' \setminus B = \mathcal{N}(d) \cap V' \setminus B$. De plus, pour tout $y \in Y$, $Odd(y) \cap V' \setminus B = \mathcal{N}(y) \cap V' \setminus B = (V \setminus \mathcal{N}(d) \cup X \cup Y) \cap V' \setminus B$. On prend alors $C' = C \cup \{y\}$, et on a $Odd(C') \cup V' \setminus B = (Odd(C) + Odd(u)) \cap V' \setminus B = V' \setminus B$.
– si $|C \cap V \setminus \mathcal{N}(d)| = 1 \bmod 2$:
  – cas $B \cap X \neq \varnothing$: Soit $x \in X$ et $y \in Y$. On pose $C' = C \cup \{x\} \cup \{y\}$. La décomposition du voisinage impair donne

$$\begin{aligned} Odd(C') \cap V' \setminus B &= \big(Odd(C) + \mathcal{N}(x) + \mathcal{N}(y)\big) \cap V' \setminus B && (2.136)\\ &= \big(\mathcal{N}(d) \cap V \cup Y + Y + V \setminus \mathcal{N}(d) + Y + X\big) \cap V' \setminus B && (2.137)\\ &= \big(V + Y + X\big) \cap V' \setminus B && (2.138)\\ &= V' \setminus B && (2.139) \end{aligned}$$

  – cas $B \cap X = \varnothing$: comme précédemment, dans ce cas $B = V' \setminus X$, ainsi pour tout $y \in Y$, $Odd(y) = \mathcal{N}(y) = X$. En posant $C' = \{y\}$, on a $Odd(C') \cap V' \setminus B = X = V' \setminus B$.

□

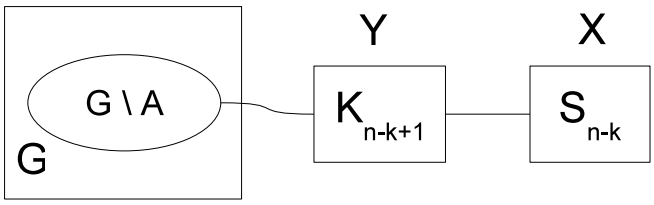

FIGURE 2.8 – Construction du graphe G' pour la réduction au cas d'un dealer universel

2.5 Différentes familles de graphes

Dans cette section, nous considérons des protocoles dans lesquels le dealer associé au sommet d est universel, ainsi nous omettrons de préciser le sommet d dans les notations et

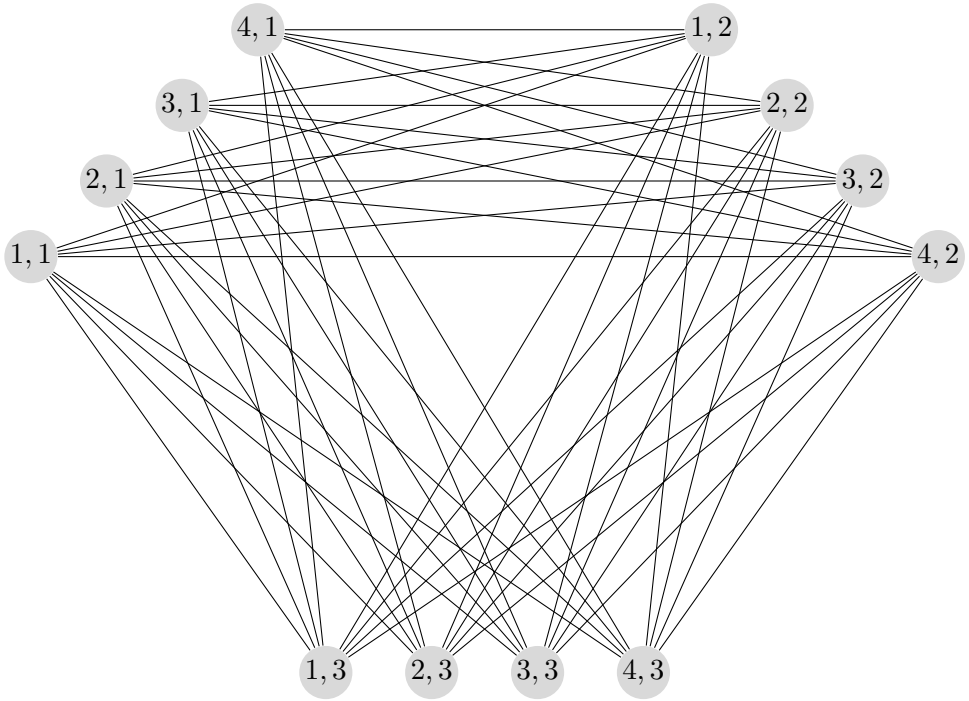

FIGURE 2.9 – Exemple de graphe $G_{p,q}$ avec $p = 4$ et $q = 3$

les graphes considérés n'incluront donc pas le dealer parmi leurs sommets. Par exemple, nous noterons $\kappa_Q(G)$ (resp. $\overline{\kappa_Q}(G)$) au lieu de $\kappa_Q(G, V)$ (resp. $\overline{\kappa_Q}(G, V)$).

Nous présentons alors plusieurs familles de graphes à partir desquels on peut construire des protocoles de partage de secret quantique à seuil aux paramètres intéressants.

2.5.1 p, q Graphes

La famille de graphes présentée ici est appelée p, q-graphes, où p et q sont des entiers positifs. Ainsi, pour tout $p, q \in \mathbb{N}^*$ avec $q \geq 2$, le graphe $G_{p,q}$ est le graphe q-parti complet dont chaque stable est de taille p. Son ordre est donc pq. Un exemple est donné Figure 2.9.

Lemme 2.27. *Pour tout $p \geq 1$ et $q \geq 2$, on note $n = pq$ l'ordre du graphe $G_{p,q}$. On a*

$$\kappa_Q(G_{p,q}) \leq \max\{n - p, n - q\} + 1 \tag{2.140}$$

Démonstration. Soit B un ensemble de sommets de $G_{p,q} = (V, E)$ tel que

$$|B| = \max\{n - p, n - q\} + 1 \tag{2.141}$$

On note $S_1, \cdots, S_q$ les q stables du graphe $G_{p,q}$.

B contient nécessairement l'un des q stables en entier, sinon sa taille doit vérifier

$$|B| \leq q(p-1) = n - q \tag{2.142}$$

ce qui contredit l'égalité (2.141). Sans perte de généralité, on peut supposer que ce stable est S_1. De plus, pour des raisons similaires, B contient au moins un sommet de chaque stable, sinon

$$|B| \leq p(q-1) = n - p \tag{2.143}$$

ce qui contredit également l'égalité (2.141). On appelle alors u_i le sommet de S_i qui appartient également à B.

On pose

$$B_0 = S_1 \cup \{u_1, \cdots, u_q\} \tag{2.144}$$

et on montre à présent les deux propriétés suivantes
– B_0 est à noyau impair
– $V \setminus B_0$ est dominé modulo 2
$V \setminus B_0$ est dominé modulo 2, en effet, si on prend $C = \{u_1\} \subseteq B_0$, on a

$$Odd(C) = S_2 \cup \cdots \cup S_q \tag{2.145}$$

d'où $V \setminus B_0 \subseteq Odd(C)$.

On veut prouver que B_0 est à noyau impair. Séparons 2 cas :
– si $q = 0 \bmod 2$, on prend $D = \{u_2, \cdots, u_q\}$
– si $q = 1 \bmod 2$, on prend $D = \{u_1, \cdots, u_q\}$
Dans les deux cas, on a $|D| = 1 \bmod 2$ et

$$Odd(D) = S_1 \tag{2.146}$$

$$D \cup Odd(D) \subset B_0 \tag{2.147}$$

L'ensemble B_0 est à noyau impair.

Ainsi, la Définition 2.5 permet de prouver l'inégalité (2.140). □

Cette famille de graphes peut être utilisée pour construire un protocole qQSS* avec les paramètres suivants :

Corollaire 2.28. *Pour tout entier $p \leq 2$, le graphe $G_{p,p}$ d'ordre $n = p^2$ réalise un protocole qQSS* de paramètres $((n, n - \sqrt{n}))$.*

Démonstration. D'après l'inégalité (2.140), on a

$$\kappa_Q(G_{p,q}) \leq n - \sqrt{n} \tag{2.148}$$

Le Théorème 2.24 avec $c = 0$ permet donc de construire un protocole qQSS* de paramètres $((n, n - \sqrt{n}))$. □

FIGURE 2.10 – Représentation de l'ensemble B_0 dans le graphe $G_{p,q}$

2.5.2 Construction itérative avec le produit lexicographique

Nous donnons ici une famille infinie de protocoles de partage de secret quantique qQSS* de paramètres $((k,n))$ où $k = n - n^{\frac{log(3)}{log(5)}} + 1 < n - n^{0.68}$. Les graphes G_i qui la composent vérifient alors $\overline{\kappa_Q}(G_i) \geq n_i^{0.68}$ où n_i est l'ordre du graphe G_i. Cette famille utilise des graphes d'ordre non-borné définis récursivement à partir d'une loi de composition : le produit lexicographique (voir [Har91], par exemple). Rappelons la définition de cette loi de composition :

Définition 2.6 ([Har91])**.** *Soit $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ deux graphes. Leur produit lexicographique $G_1 \bullet G_2 = (V, E)$ vérifie :*

$$\begin{cases} V = V_1 \times V_2 \\ E = \left\{ \big((u_1,u_2),(v_1,v_2)\big) \;\middle|\; (u_1,v_1) \in E_1 \text{ ou } (u_1 = v_1 \text{ et } (u_2,v_2) \in E_2) \right\} \end{cases} \tag{2.149}$$

Une vue plus intuitive du produit lexicographique d'un graphe G_1 par un graphe G_2 est la suivante : le graphe $G = G_1 \bullet G_2$ est similaire à un graphe G_1 dont chaque sommet est remplacé par un graphe G_2 et chaque arête est remplacée par une bipartition complète entre les deux graphes G_2 correspondants. Une illustration de cette loi de composition est donnée Figure 2.11.

Rappelons une propriété utile du produit lexicographique :

Propriété 2.29 ([Har91])**.** *Pour tous graphes G_1 et G_2,*

$$\overline{G_1 \bullet G_2} = \overline{G_1} \bullet \overline{G_2} \tag{2.150}$$

Les graphes que nous utilisons ici pour la famille de protocoles qQSS* sont des itérations successives du graphe C_5 par produit lexicographique. Ainsi, le premier graphe G_1 est le graphe C_5, et $G_i = G_{i-1} \bullet C_5 = C_5^{\bullet i}$ (voir Figure 2.13).

Il est possible de trouver une borne sur la valeur de $\overline{\kappa_Q}(G_1 \bullet G_2)$ en fonction des valeurs respectives de $\overline{\kappa_Q}$ pour les deux graphes G_1 et G_2. Cette borne joue un rôle crucial dans la construction de notre famille de protocoles. Elle est explicitée dans le théorème suivant :

Théorème 2.30. *Pour tous graphes G_1, G_2, nous avons*

$$\overline{\kappa_Q}(G_1 \bullet G_2) \geq \overline{\kappa_Q}(G_1).\overline{\kappa_Q}(G_2)$$

Démonstration. Soit $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ et $G = G_1 \bullet G_2 = (V, E)$. Soit $n_1 = |V_1|$, $n_2 = |V_2|$ et $n = |V| = n_1 n_2$.

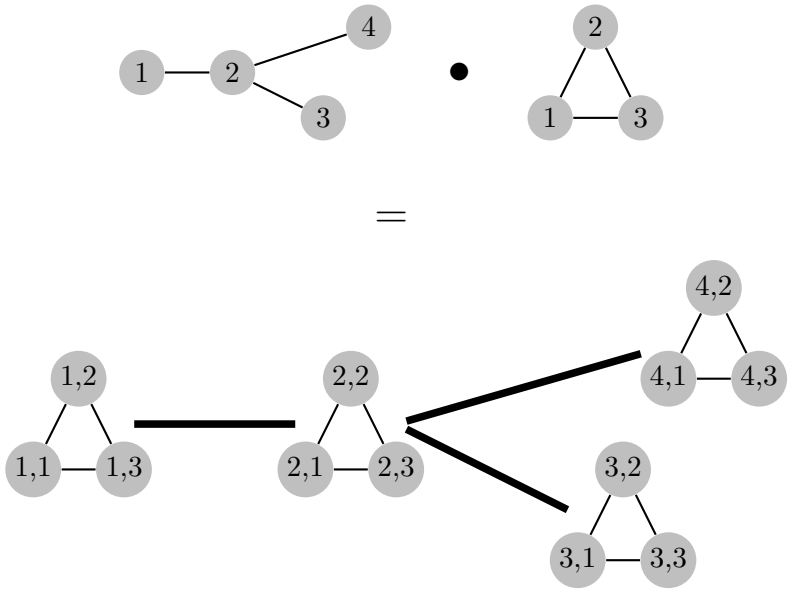

FIGURE 2.11 – Visualisation du produit lexicographique • entre deux graphes. Une ligne épaisse représente une bipartition complète entre deux triangles.

Pour tout ensemble $B \subseteq V$ nous définissons les ensembles suivants :

$$B_2(v_1) = \left\{ v_2 \in V_2 \middle| (v_1, v_2) \in B \right\} \text{ avec } v_1 \in V_1 \tag{2.151}$$

$$B_1 = \left\{ v_1 \in V_1 \middle| |B_2(v_1)| > \kappa_Q(G_2) \right\} \tag{2.152}$$

La principale partie de cette preuve consiste à montrer que tout ensemble $B \subseteq V$ de taille $k = n - \overline{\kappa_Q}(G_1)\overline{\kappa_Q}(G_2) + 1$ contient un noyau impair D_B.

Montrons tout d'abord que pour tout ensemble $B \subseteq V$ tel que $|B| = k$, la taille de l'ensemble B_1 vérifie

$$|B_1| \geq \kappa_Q(G_1) \tag{2.153}$$

Par contraposée, considérons que $|B_1| < \kappa_Q(G_1)$. Nous écrivons l'ensemble B de la façon suivante :

$$B = \bigcup_{\substack{v_1 \in V_1 \\ v_2 \in B_2(v_1)}} \{(v_1, v_2)\} \tag{2.154}$$

L'ensemble V se décompose de la façon suivante :

$$V = \bigcup_{\substack{v_2 \in B_2(v_1) \\ v_1 \in V_1}} \big\{(v_1, v_2)\big\} \cup \bigcup_{\substack{v_2 \in V_2 \setminus B_2(v_1) \\ v_1 \in B_1}} \big\{(v_1, v_2)\big\} \cup \bigcup_{\substack{v_2 \in V_2 \setminus B_2(v_1) \\ v_1 \in V_1 \setminus B_1}} \big\{(v_1, v_2)\big\} \tag{2.155}$$

$$= B \cup \bigcup_{\substack{v_2 \in V_2 \setminus B_2(v_1) \\ v_1 \in B_1}} \big\{(v_1, v_2)\big\} \cup \bigcup_{\substack{v_2 \in V_2 \setminus B_2(v_1) \\ v_1 \in V_1 \setminus B_1}} \big\{(v_1, v_2)\big\} \tag{2.156}$$

Dans l'égalité précédente, on constate que les unions sont disjointes. La taille de B s'exprime alors

$$|B| = \underbrace{|V|}_{=n_1 n_2} - \sum_{v_1 \in B_1} \underbrace{|V_2 \setminus B_2(v_1)|}_{\geq 0} - \sum_{v_1 \in V_1 \setminus B_1} \underbrace{|V_2 \setminus B_2(v_1)|}_{\geq \overline{\kappa_Q}(G_2)} \tag{2.157}$$

$$|B| \leq n_1 n_2 - \underbrace{|V_1 \setminus B_1|}_{\geq \overline{\kappa_Q}(G_1)} (\overline{\kappa_Q}(G_2)) \tag{2.158}$$

$$\leq n - \overline{\kappa_Q}(G_1)\overline{\kappa_Q}(G_2) \tag{2.159}$$

$$< k \tag{2.160}$$

L'inégalité $|V_1 \setminus B_1| \geq \overline{\kappa_Q}(G_1)$ utilisée dans l'équation (2.158) provient de l'hypothèse $|B_1| < k_1$. Nous avons donc une contradiction, ainsi $|B_1| \geq \kappa_Q(G_1)$.

Montrons à présent que dans tout ensemble $B \subseteq V$ de taille k il existe un noyau impair $D \subseteq B$. Considérons pour cela les ensembles D_1, $D_2(v_1)$, $C_2^0(v_1)$ et $C_2^1(v_1)$ avec $v_1 \in B_1$ définis de la façon suivante :

- D_1 : D'après le résultat établi plus haut, $|B_1| \geq \kappa_Q(G_1)$. Par conséquent, B_1 possède un noyau impair D_1.
- $D_2(v_1)$: $v_1 \in B_1$, d'où $|B_2(v_1)| > \kappa_Q(G_2)$. L'ensemble $B_2(v_1)$ possède donc un noyau impair que l'on notera $D_2(v_1)$.
- $C_2^0(v_1)$: De même, $|B_2(v_1)| > \kappa_Q(G_2)$, donc d'après la Définition 2.5, il existe un ensemble $C_2(v_1) \subseteq B_2(v_1)$ tel que $V_2 \setminus B_2(v_1) \subset Odd(C_2(v_1))$. Si $C_2(v_1)$ est de taille paire, on prend $C_2^0(v_1) = C_2(v_1)$, sinon on prend $C_2^0(v_1) = C_2(v_1) + D_2(v_1)$. Dans les deux cas, on a bien $V_2 \setminus B_2(v_1) \subset Odd(C_2^0(v_1))$ où $C_2^0(v_1)$ est de taille paire.
- $C_2^1(v_1)$: Avec un raisonnement similaire, on a l'existence d'un ensemble $C_2^1(v_1) \subseteq B_2(v_1)$ de taille impaire tel que $V_2 \setminus B_2(v_1) \subset Odd(C_2^1(v_1))$.

Enfin, on définit un ensemble $S_2(v_1)$ pour tout sommet $v_1 \in V_1$ construit à partir des 4 ensembles précédemment définis et de la partition de V_1 suivante :

- si $v_1 \in D_1 \cap Even(D_1)$, $S_2(v_1) = D_2(v_1)$
- si $v_1 \in D_1 \cap Odd(D_1)$, $S_2(v_1) = C_2^1(v_1)$
- si $v_1 \in V_1 \setminus D_1 \cap Even(D_1)$, $S_2(v_1) = \varnothing$
- si $v_1 \in V_1 \setminus D_1 \cap Odd(D_1)$, $S_2(v_1) = C_2^0(v_1)$

On construit alors l'ensemble $D \subseteq V$ de la façon suivante :

$$D = \bigcup_{v_1 \in V_1} \{v_1\} \times S_2(v_1) \tag{2.161}$$

Ainsi, en décomposant l'ensemble D suivant la partition de V_1 utilisée précédemment, on obtient

$$\begin{aligned}
|D| = & \sum_{v_1 \in D_1 \cap Even(D_1)} |D_2(v_1)| + \sum_{v_1 \in D_1 \cap Odd_(D_1)} |C_2^1(v_1)| \\
& + \sum_{v_1 \in V_1 \setminus D_1 \cap Even(D_1)} |\varnothing| + \sum_{v_1 \in V_1 \setminus D_1 \cap Odd(D_1)} |C_2^0(v_1)| && (2.162) \\
= & \sum_{v_1 \in D_1 \cap Even(D_1)} 1 + \sum_{v_1 \in D_1 \cap Odd_(D_1)} 1 \\
& + \sum_{v_1 \in V_1 \setminus D_1 \cap Even(D_1)} 0 + \sum_{v_1 \in V_1 \setminus D_1 \cap Odd(D_1)} 0 \mod 2 && (2.163) \\
= & \sum_{v_1 \in D_1} 1 \mod 2 = |D_1| \bmod 2 && (2.164) \\
= & \ 1 \bmod 2 && (2.165)
\end{aligned}$$

D est donc de taille impaire, et on veut maintenant montrer que $D \cup Odd(D) \subseteq B$.

On cherche à prouver que tout sommet $v \in V \setminus B$, on a $v \in Even(B)$. Pour cela, on commence par calculer la parité des tailles de certains sous-ensembles de V_1 que l'on reporte dans le tableau de la Figure 2.12.

$v_1 \in$	$S_2(v_1)$	$\lvert\mathcal{N}_{G_1}(v_1) \cap D_1\rvert$	$\lvert\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)\rvert$	$\lvert\mathcal{N}_{G_1}(v_1) \cap D_1\rvert + \lvert\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)\rvert$
$D_1 \cap Even(D_1)$	$D_2(v_1)$	0	0	0
$D_1 \cap Odd(D_1)$	$C_2^1(v_1)$	1	1	0
$V_1 \setminus D_1 \cap Even(D_1)$	$\varnothing$	0	0	0
$V_1 \setminus D_1 \cap Odd(D_1)$	$C_2^0(v_1)$	1	1	0

FIGURE 2.12 – Définition des ensembles $S_2(v_1) \subset V_2$ par rapport à une partition de V_1

Pour tout $v = (v_1, v_2) \in V \setminus B$, d'après la Définition 2.6, on écrit

$$\mathcal{N}_G(v) \cap D = \Big(\{v_1\} \times \big(\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)\big)\Big) \cup \bigcup_{u_1 \in \mathcal{N}_{G_1}(v_1)} \{u_1\} \times S_2(u_1) \qquad (2.166)$$

On calcule la taille de cet ensemble :

$$|\mathcal{N}_G(v) \cap D| = |\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| + \sum_{u_1 \in \mathcal{N}_{G_1}(v_1)} |S_2(u_1)| \qquad (2.167)$$

D'après la figure 2.12,

$$|\mathcal{N}_G(v) \cap D| = |\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| + \sum_{u_1 \in \mathcal{N}_{G_1}(v_1) \cap D_1} 1 \mod 2 \tag{2.168}$$

$$= |\mathcal{N}_{G_2}(v_2) \cap S_2(v_1)| + |\mathcal{N}_{G_1}(v_1) \cap D_1| \mod 2 \tag{2.169}$$

$$= 0 \mod 2 \tag{2.170}$$

L'équation (2.168) provient du fait que si $v_1 \in V_1 \setminus D_1$, on a $|S_2(v_1)| = 0 \bmod 2$ (voir Figure 2.12). Le passage de l'équation (2.169) à l'équation (2.170) est expliqué par le tableau de la Figure 2.12. Nous avons ainsi établi le fait suivant : pour tout ensemble $B \subseteq V$ de taille k, il existe un ensemble $D \subseteq B$ de taille impaire tel que

$$(\forall v \in V \setminus B) \qquad v \in Even(D) \tag{2.171}$$

ce qui s'écrit aussi

$$D \cup Odd(D) \subset B \tag{2.172}$$

Tout ensemble de sommets de G de taille k est donc à noyau impair.

On montre à présent que pour tout ensemble $B \subseteq V$ de taille k, $V' \setminus B$ est dominé modulo 2. D'après la Propriété 2.16, on peut prouver de façon équivalente que B est à noyau impair dans le graphe $G * d$. Dans ce cas, le dealer d est universel, on veut alors montrer que

$$B \text{ est à noyau impair dans } \overline{G} \tag{2.173}$$

D'après la Propriété 2.29

$$\overline{G} = \overline{G_1 \bullet G_2} \tag{2.174}$$

$$= \overline{G_1} \bullet \overline{G_2} \tag{2.175}$$

Or $\kappa_Q(G_1) = \kappa_Q(\overline{G_1})$ et $\kappa_Q(G_2) = \kappa_Q(\overline{G_2})$. Ainsi, par un raisonnement similaire, on montre la propriété (2.173).

On a donc montré que pour tout ensemble $B \subseteq V$ de taille k, B est à noyau impair et $V \setminus B$ est dominé modulo 2. Ainsi

$$\kappa_Q(G) \leq k \tag{2.176}$$

$$\leq n - \overline{\kappa_Q}(G_1)\overline{\kappa_Q}(G_2) + 1 \tag{2.177}$$

$$\overline{\kappa_Q}(G) \geq \overline{\kappa_Q}(G_1)\overline{\kappa_Q}(G_2) \tag{2.178}$$

□

Ce théorème joue un rôle crucial dans le calcul du seuil réalisé par la famille que nous construisons à présent. Celle-ci est basée sur les itérations successives du produit lexicographique à partir d'un graphe de départ appelé *graine*.

Nous choisissons dans un premier temps le graphe C_5 comme graine et nous déduisons ainsi le résultat suivant :

Théorème 2.31. *Pour tout $i \in \mathbb{N}^*$, le graphe ${C_5}^{\bullet i} = \underbrace{C_5 \bullet C_5 \bullet \cdots \bullet C_5}_{i \text{ times}}$ réalise un protocole $((n, n - n^{\frac{log(3)}{log(5)}} + 1))$ (où $n = 5^i$).*

Démonstration. Un raisonnement par récurrence à partir du Théorème 2.30 permet d'écrire

$$\overline{\kappa_Q}({C_5}^{\bullet i}) \geq \overline{\kappa_Q}(C_5)^i \tag{2.179}$$

Or $\overline{\kappa_Q}(C_5) = 3$, d'où $\overline{\kappa_Q}({C_5}^{\bullet i}) \geq 3^i$. Nous avons $|{C_5}^{\bullet i}| = 5^i$, ainsi en utilisant le Théorème 2.24, on déduit que le graphe ${C_5}^{\bullet i}$ réalise un protocole à seuil de paramètres $((n - n^{\frac{log(3)}{log(5)}} + 1, n))$ (où $n = 5^i$). □

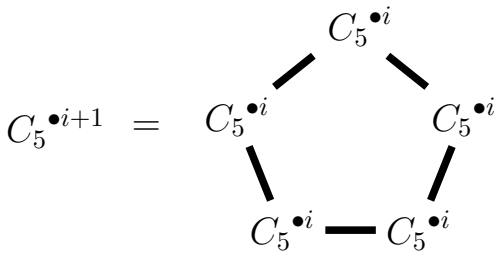

FIGURE 2.13 – Décomposition du graphe ${C_5}^{\bullet i+1}$.

D'une manière plus générale, il est possible de calculer les paramètres des protocoles qQSS* obtenus par ce procédé itératif en fonction des paramètres de la graine G utilisée.

Corollaire 2.32. *Soit G un graphe permettant de réaliser un protocole qQSS* de paramètres $((n_0, k_0))$. Alors pour tout $i \in \mathbb{N}^*$, le graphe $G^{\bullet i}$ réalise un protocole qQSS* de paramètres $((n, k))$ avec*

$$\begin{cases} n = {n_0}^i \\ k = n - n^{\frac{log(n_0 - k_0 + 1)}{log(n_0)}} + 1 \end{cases} \tag{2.180}$$

Démonstration. Ce corollaire se montre de la même façon que le Théorème 2.31 en utilisant un graphe G quelconque au lieu du graphe C_5. □

Les graines qui donnent naissance aux familles itératives de graphes ayant les seuils les plus intéressants (i.e. les plus bas) sont donc les graphes qui réalisent un protocole qQSS* de paramètres $((n,k))$ dont la quantité $\frac{log(n-k+1)}{log(n)}$ est minimale.

Une recherche exhaustive à l'aide de l'outils et `sage` (voir annexe) et de programmes développés en langage `C` jusqu'à l'ordre 11 a confirmé que le graphe C_5 était la graine optimale jusqu'à la taille 11. En revanche, nous avons tourné notre attention vers des graphes qui semblaient être de "bons candidats" à cause de leur régularité et forte régularité. Parmi ces graphes se trouvent les graphes de Paley [Sac62, ER63] qui font également l'objet du Chapitre 4. Ainsi, le graphe de Paley d'ordre 29 (décrit Figure 2.14) fournit la meilleure graine à ce jour pour la construction itérative à partir du produit lexicographique.

Propriété 2.33. *Le graphe de Paley d'ordre* 29 Pal_{29} *réalise un protocole qQSS* de paramètres* $((29,19))$.

Démonstration. Ces paramètres ont été calculés à l'aide d'un algorithme de recherche utilisant le package *nauty*. □

Nous pouvons alors construire un protocole de partage de secret quantique qQSS* à partir du graphe Pal_{29} dont les paramètres sont meilleurs que ceux de la construction itérative à partir du graphe C_5.

Théorème 2.34. *Pour tout* $i \in \mathbb{N}^*$, *le graphe* ${Pal_{29}}^{\bullet i}$ *réalise un protocole de paramètres*

$$((n, \lceil n - n^{0.71} \rceil)) \tag{2.181}$$

(où $n = 29^i$*).*

Démonstration. Le Corollaire 2.32 utilisé avec le graphe Pal_{29} dont les paramètres sont donnés dans la Propriété 2.33 donne lieu à une construction dont les paramètres sont $((n, n - n^{\frac{log(11)}{log(29)}} + 1))$. On utilise ensuite l'inégalité $n^{\frac{log(11)}{log(29)}} \leq n^{0.71}$. □

2.6 Borne inférieure pour l'accessibilité quantique

Comme vu précédemment, le théorème de Non-Clonage implique une borne inférieure sur la taille du seuil des protocoles qQSS*. En effet, pour tout protocole de paramètres $((n,k))$, nous avons nécessairement $k > \frac{n}{2}$ (Théorème 2.1). Dans le cas de protocoles construits à partir d'états graphes tels que nous les avons présentés en 2.4, nous établissons une borne plus restrictive liée à la structure des protocoles qQSS et qQSS*.

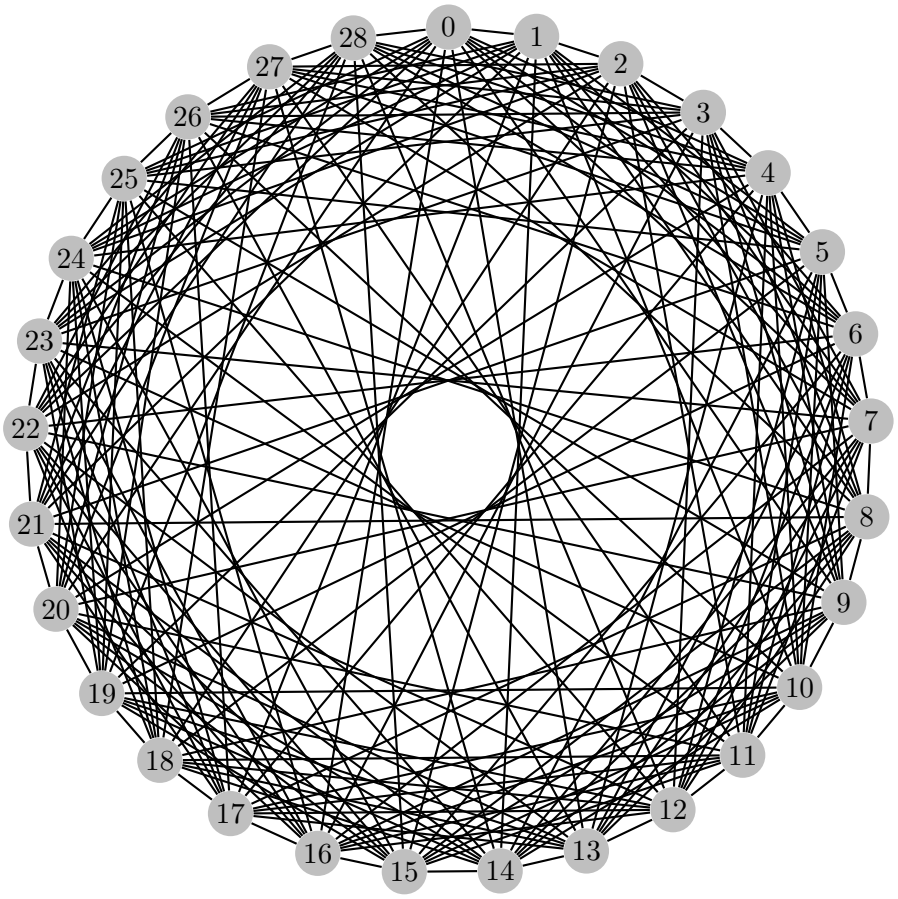

FIGURE 2.14 – Graphe de Paley d'ordre 29

Lemme 2.35. *Soit $G = (V, E)$ un graphe réalisant un protocole qQSS* de paramètres $((n, k))$. Alors pour tout $B \subseteq V$ de taille k, il existe un ensemble $X \subseteq V$ de taille*

$$|X| \leq \frac{2}{3}(n - k + 1) \tag{2.182}$$

qui vérifie l'une des deux conditions suivantes :

1. $X \cup Odd(X) \subseteq B$ *et* $|X| = 1 \bmod 2$
2. $B \subseteq Odd(X)$

Démonstration. Dans la matrice d'adjacence de G, considérons la matrice de coupe $\Gamma_B \in \mathcal{M}_{k,n-k}(\mathbb{F}_2)$ associée à l'ensemble de sommets $B \subseteq V$. Γ_B peut être interprétée comme l'application linéaire qui envoie un ensemble $D \subseteq B$ (sous sa représentation vectorielle) sur son voisinage impair dans $V \setminus B$ (voir expression 2.46). Ainsi, tout ensemble D qui vérifie $Odd(D) \subseteq B$ correspond à une combinaison linéaire nulle des colonnes de Γ_B. Le noyau de Γ_B s'exprime alors ainsi :

$$Ker(\Gamma_B) = \{D \subseteq B,\, Odd(D) \subseteq B\} \tag{2.183}$$

Nous amalgamons ici, ainsi que dans la suite de cette preuve, la notation ensembliste et la notation vectorielle.

Soit $t = dim(Ker(\Gamma_B))$. La formule du rang nous permet d'écrire :

$$t = k - dim(Im(\Gamma_B)) \tag{2.184}$$
$$\geq 2k - n \tag{2.185}$$

Considérons les ensembles suivants :
– $\mathcal{D}_1 = \left\{D \subseteq B \;\middle|\; |D| = 1 \bmod 2 \text{ et } Odd(D) \subseteq B\right\}$
– $\mathcal{C} = \left\{C \subseteq B \;\middle|\; V \setminus B \subseteq Odd(C)\right\}$
En termes vectoriels, $\mathcal{D}_1$ est constitué des éléments de $Ker(\Gamma_B)$ de taille impaire et $\mathcal{C}$ est constitué des antécédents du vecteur $(1, \cdots, 1)^T$ par Γ_B. $\mathcal{D}_1$ et $\mathcal{C}$ sont des espaces affines partageant le même espace vectoriel sous-jacent :

$$\mathcal{D}_0 = \left\{D \subseteq B \;\middle|\; |D| = 0 \bmod 2 \text{ and } D \cup Odd(D) \subseteq B\right\} \tag{2.186}$$

En remarquant que $Ker(\Gamma_B) = \mathcal{D}_1 \sqcup \mathcal{D}_0$, nous avons $dim(\mathcal{D}_0) = t - 1$. Il existe donc un ensemble X_0 de taille $t - 1$ tel que l'on puisse trouver $D_1 \in \mathcal{D}_1$ et $C \in \mathcal{C}$ qui n'ont aucune intersection commune avec X_0 : $X_0 \cap D_1 = X_0 \cap C = \varnothing$. Ainsi,

$$|C \cup D_1| \leq k - t + 1 \leq n - k + 1 \tag{2.187}$$

Nous écrivons alors

$$2|D_1 \cup C| = |D_1| + |C| + |D_1 + C| \tag{2.188}$$
$$\leq 2(n - k + 1) \tag{2.189}$$

Cette inégalité implique que l'un des trois ensembles D_1, C et $D_1 + C$ est de cardinalité inférieure ou égale à $\frac{2}{3}(n - k + 1)$. Or ces ensembles ont les propriétés suivantes :

– $D_1 : D_1 \cup Odd(D_1) \subseteq B$ and $|D_1| = 1 \bmod 2$
– $C : B \subseteq Odd(C)$
– $D_1 + C : B \subseteq Odd(D_1 + C)$

□

Ce lemme nous garantit que dans tout graphe qui peut être utilisé pour réaliser un protocole $((n, k))$, tout ensemble de taille k contient soit un noyau impair, soit un dominant de taille inférieure ou égale à $\frac{2}{3}(n - k + 1)$.

Ainsi, nous utilisons cette condition nécessaire des ensembles autorisés ainsi qu'un argument de dénombrement pour établir la borne suivante :

Théorème 2.36. *Il n'existe aucun graphe G qui permette de réaliser un protocole qQSS* de paramètres $((n, k))$ avec $k < \frac{n}{2} + \frac{n}{157}$.*

Démonstration. Considérons un graphe $G = (V, E)$ qui réalise un protocole qQSS* de paramètres $((n, k))$. Tout ensemble de taille $n - k$ est donc dominé modulo 2, ainsi tout ensemble $D \subseteq V$ avec $|D| = 1 \bmod 2$ vérifie $|D \cup Odd(D)| \geq n - k + 1$, car un ensemble de sommets ne peut pas être à la fois dominé modulo 2 et posséder un noyau impair (Théorème 2.7).

Par conséquent, pour tout ensemble $D \subseteq V$ de taille impaire, il existe au plus $\binom{n-(n-k+1)}{k-(n-k+1)} = \binom{k-1}{2k-n-1}$ ensembles B de taille k qui contiennent $D \cup Odd(D)$. En effet, on peut compléter $D \cup Odd(D)$ en choisissant des sommets parmi les sommets restants qui sont au plus $n - (n - k + 1)$ pour arriver à un ensemble de taille k.

De façon similaire, pour tout ensemble $C \subseteq V$ nous avons

$$|C \cup Even(C)| \geq n - k + 1 \tag{2.190}$$

Dans le cas contraire, on aurait l'existence d'ensembles de taille supérieure ou égale à k dominés modulo 2, ce qui est impossible dans un protocole qQSS* $((n, k))$.

Ainsi, étant donné un ensemble $C \subseteq V$, le nombre d'ensembles B de taille k contenant C et tels que $C \cup Even(C) \subseteq B$ est au plus $\binom{k-1}{2k-n-1}$. On remarque ici une symétrie avec le cas des noyaux impairs D.

Le lemme 2.35 établi précédemment garantit que pour tout ensemble $B \subseteq V$ de taille k, il existe nécessairement un ensemble C ou un ensemble D de taille inférieure ou égale à $\frac{2}{3}(n - k + 1)$ avec
– $D \cup Odd(D) \subseteq B$
– $C \cup Even(C) \subseteq B$
Dans le graphe G, on majore le nombre de coupes de taille k en comptant deux fois tous les ensembles de sommets de taille inférieure ou égale à $\frac{2}{3}(n - k + 1)$ et en comptant le

nombre de façons de les compléter. On obtient alors l'inégalité suivante :

$$\binom{n}{k} \leq 2 \sum_{i=1}^{\frac{2}{3}(n-k+1)} \binom{n}{i}\binom{k-1}{2k-n-1} \tag{2.191}$$

Une analyse numérique effectuée à l'aide de `sage` (voir annexe) montre que cette inégalité implique

$$k > \frac{n}{2} + \frac{n}{157} \tag{2.192}$$

lorsque $n \to \infty$. □

Ce théorème montre que pour la famille des protocoles qQSS* il existe une borne plus restrictive que celle obtenue avec le théorème de Non-Clonage. Nous apportons également une réponse quand à l'existence de protocoles de partage de secret quantique à seuil sans utilisation du one-time pad quantique pour les protocoles qQSS :

Corollaire 2.37. *Il n'existe pas de protocole qQSS à seuil construit à partir d'un graphe* $G = (V, E)$ *avec* $|V| \geq 79$.

Démonstration. La caractérisation des protocoles à seuil donnée par Gottesman [Got00] implique que tout protocole de partage de secret à seuil qQSS a pour paramètres $((2k-1, k))$. De plus, grâce au Théorème 2.36, nous avons $k \geq n/2 + n/157$. En combinant ces deux résultats, nous avons $k \leq \frac{159}{4}$, ainsi $n < 79$. □

Chapitre 3

Domination impaire faible

Les protocoles de partage de secret quantique à partir d'états graphes (cQSS, qQSS et qQSS*) font apparaître des liens entre ensembles de joueurs qui peuvent accéder au secret et structures des graphes sous-jacents (Corollaire 2.8 et Théorème 2.14). Les questions d'accessibilité à seuil se traduisent également en terme de propriétés graphiques.

Nous étudions dans ce chapitre des quantités définies à partir de structures simples sur les sommets de graphes. Plus précisément, les résultats présentés ici s'articulent autour de la notion de complémentation locale, et plus précisément le degré minimum d'un graphe par complémentation locale. Nous formalisons ensuite les conséquences de ces propriétés sur les états graphes, en terme de partage de secret ou comme support de calcul quantique plus généralement. Les études présentées ici répondent également à des questions de théorie des graphes a priori sans lien avec le domaine de l'information quantique.

Dans un premier temps, nous définissons pour tout graphe G les quantités $\kappa(G)$ et $\kappa'(G)$ et rappelons la définition du degré minimum par complémentation locale $\delta_{loc}(G)$. Une caractérisation de la quantité $\kappa_Q(G)$ définie dans le Chapitre 2 (Définition 2.5) utilisant κ et κ' est également établie.

Ensuite, nous étudions la complexité des problèmes de décision associés aux quantités κ, κ', κ_Q et δ_{loc}. Les méthodes mises en œuvre pour cela comprennent entre autres des techniques de réduction classiques à des problèmes dont les complexités sont connues, notamment le problème de l'existence de codes parfaits dans un graphe ainsi que la recherche du plus petit mot d'un code linéaire [Var97].

Enfin, nous utilisons des méthodes probabilistes ainsi que le Lemme Local de Lovász [Lov75] pour prouver entre autres l'existence de familles infinies de graphes dont le degré minimum par complémentation locale est linéaire en l'ordre du graphe. Un résultat similaire est également prouvé pour la quantité κ_Q, garantissant ainsi l'existence de protocoles de partage de secret quantique qQSS* dont le seuil représente une proportion constante du nombre de joueurs impliqués.

3.1 Ensembles dominés et degré minimum par complémentation locale

3.1.1 Quelques définitions

Nous nous intéressons dans ce chapitre à la notion de "complémentation locale" (voir Définition 1.6).

Deux graphes G et G' sont dits "localement équivalents" lorsqu'il est possible d'obtenir le graphe G' à partir de G en effectuant une suite de complémentations locales par rapports aux sommets de G :

Définition 3.1. *Soit G et G' deux graphes.*

$$G \equiv_{LC} G' \Longleftrightarrow \exists \{u_1, \cdots, u_k\} \subseteq V(G) \text{ } t.q. \text{ } G' = G * u_1 * \cdots * u_k \tag{3.1}$$

On remarquera que cette relation est une relation d'équivalence (car $(G * u) * u = G$), et les graphes sont donc partitionnés en classes par rapport à cette relation.

La question de la distinction de ces classes à été traitée par Bouchet [Bou87, Bou91] : il donne un algorithme polynomial qui décide si deux graphes donnés appartiennent à la même classe d'équivalence. Nous nous intéressons ici à la valeur du degré minimal des graphes d'une classe donnée, appelé "degré minimal par complémentation locale" :

Définition 3.2. *Soit G un graphe.*

$$\delta_{loc}(G) = min \left\{ \text{ } \delta(G') \text{ } \middle| \text{ } G \equiv_{LC} G' \text{ } \right\} \tag{3.2}$$

où $\delta(G')$ dénote le degré minimum de G'.

Pour tout graphe G, la quantité $\delta_{loc}(G)$ est caractérisée graphiquement [HMP06] en utilisant les voisinages impairs de certains sous-ensembles des sommets de G (voir Définition 1.4). Le degré minimum par complémentation locale est directement lié à la taille du plus petit ensemble de la forme $D \cup Odd(D)$:

Propriété 3.1 ([HMP06])**.** *Soit G un graphe.*

$$\delta_{loc}(G) = \min \left\{ \text{ } |D \cup Odd(D)| \text{ } \middle| \text{ } D \neq \varnothing, D \subseteq V(G) \text{ } \right\} - 1 \tag{3.3}$$

Cette propriété présente notamment l'avantage de pouvoir caractériser le degré minimum par complémentation locale d'une classe à partir de n'importe lequel de ses représentants.

Une autre notion essentielle de ce chapitre est la "domination impaire faible" (WOD : Weak Odd Domination). Elle se formalise ainsi :

Définition 3.3. *Soit $G = (V, E)$ un graphe. Un ensemble de sommets $B \subseteq V$ est dit "WOD" lorsqu'il existe un ensemble $C \subseteq V \setminus B$ tel que*

$$B \subseteq Odd(C) \tag{3.4}$$

Tout comme l'énonce le Théorème 2.7 avec les ensembles à noyau impair et les ensembles dominés modulo 2, nous avons ici une caractérisation des ensembles non-WOD :

Propriété 3.2. *Soit $G = (V, E)$ un graphe. Si un ensemble $B \subseteq V$ de sommets n'est pas WOD (non-WOD), alors il existe $D \subseteq B$ avec $|D| = 1 \bmod 2$ tel que*

$$Odd(D) \subseteq B \tag{3.5}$$

On remarque que les sous-ensembles des ensembles WOD sont également WOD. Ainsi, nous introduisons les quantités qui correspondent à la taille du plus grand ensemble WOD et celle du plus petit non-WOD :

Définition 3.4. *Pour tout graphe G,*

$$\kappa(G) = \max_{B \ WOD} |B| \tag{3.6}$$

$$\kappa'(G) = \min_{B \ non\text{-}WOD} |B| \tag{3.7}$$

Cette notion coïncide avec les ensembles "dominés modulo 2" définis dans le Chapitre 2 (Définition 2.4) dans le cas d'un graphe avec un dealer universel. De même, les ensembles non-WOD coïncident avec les ensembles "à noyau impair". De cette façon, la quantité $\kappa'(G)$ est la taille du plus petit ensemble de joueurs capables d'accéder à un secret classique dans un protocole construit à partir d'états graphes (voir Chapitre 2, protocoles cQSS). De même, $\kappa(G)$ est la taille du plus grand ensemble qui n'a pas accès au secret dans ces protocoles.

Illustrons cette définition par le calcul de ces valeurs pour la famille des graphes $G_{p,q}$ précédemment introduits en 2.5.1. Pour tout $p, q \in \mathbb{N}^*$ où $q \geq 2$, le graphe $G_{p,q}$ est le graphe d'ordre pq q-parti complet dont chaque stable est de taille p. On décompose alors $G_{p,q} = (V, E)$ en q stables :

$$V = V_1 \cup \cdots \cup V_q \tag{3.8}$$

Toutes les paires de sommets $\{u, v\}$ sont donc reliées lorsque u et v n'appartiennent pas au même stable V_i.

Propriété 3.3. *Pour tout $p, q \in \mathbb{N}$ avec $q \geq 2$ et $n = pq$ l'ordre du graphe $G_{p,q}$,*
– Si $q = 1 \bmod 2$

$$\begin{cases} \kappa(G_{p,q}) = n - p \\ \kappa'(G_{p,q}) = q \end{cases} \tag{3.9}$$

– *Si* $q = 0 \bmod 2$

$$\begin{cases} \kappa(G_{p,q}) = \max(n-p, n-q) \\ \kappa'(G_{p,q}) = p+q+1 \end{cases} \tag{3.10}$$

Démonstration. Nous distinguons 2 cas en fonction de la parité de q.
– Si $q = 1 \bmod 2$
  – $[\kappa(G_{p,q}) \geq n-p]$: On considère l'ensemble $B = V_2 \cup \cdots \cup V_q$. Tout sommet $u \in V_1$ vérifie

$$B \subseteq Odd(\{u\}) \tag{3.11}$$

  donc d'après la Définition 3.3, B est WOD et $|B| = n-p$. Ainsi, $\kappa(G_{p,q}) \geq n-p$.
  – $[\kappa(G_{p,q}) \leq n-p]$: Soit $B \subseteq V$ un ensemble quelconque tel que $|B| > n-p$. La contrainte sur la taille de B assure que B contient au moins 1 sommet u_i dans chaque stable V_i. On note ainsi $D = \{u_1, \cdots, u_q\}$ et on remarque que $|D| = q = 1 \bmod 2$. Chaque sommet $x \in V \setminus D$ est connecté à tous les sommets de D sauf celui qui est dans le même stable V_i que lui. x a donc $q-1 = 0 \bmod 2$ voisins dans D, d'où

$$Odd(D) = \varnothing \tag{3.12}$$

  Par conséquent, B est non-WOD et $\kappa(G_{p,q}) \leq n-p$.
  – $[\kappa'(G_{p,q}) \leq q]$: Soit B un ensemble de taille q composé d'un sommet u_i de chaque stable V_i. Comme il a été prouvé dans le point précédent, B est non-WOD, donc $\kappa'(G_{p,q}) \leq q$.
  – $[\kappa'(G_{p,q}) \geq q]$: Pour tout ensemble $B \subseteq V$ tel que $|B| < q$, il existe un stable V_i tel que $B \cap V_i = \varnothing$. Soit u un sommet quelconque de V_i. Tout sommet $x \in B$ vérifie alors

$$x \subseteq Odd(\{u\}) \tag{3.13}$$

  D'après la Définition 3.3, B est WOD, donc $\kappa'(G_{p,q}) \geq q$.
– Si $q = 0 \bmod 2$
  – $[\kappa(G_{p,q}) \geq max(n-p, n-q)]$: On prouve que $\kappa(G_{p,q}) \geq n-p$ de la même façon que pour le cas $q = 1 \bmod 2$. Soit $C \subseteq V$ un ensemble de sommets de taille q composé d'exactement un sommet de chacun des ensembles V_i. Considérons à présent l'ensemble $B = V \setminus C$. Chaque sommet de B est connecté à exactement $q-1 = 1 \bmod 2$ sommets de U. Par conséquent,

$$B \subseteq Odd(C) \tag{3.14}$$

  donc B est un ensemble WOD de taille $n-q$. On a ainsi $\kappa(G_{p,q}) \geq n-q$.
  – $[\kappa(G_{p,q}) \leq max(n-p, n-q)]$: Tout ensemble B tel que $|B| > max(n-p, n-q)$ contient à la fois un stable V_{i_0} en entier et au moins un sommet u_i dans chacun des ensembles V_i. On pose $D = \{u_1, \cdots, u_{i_0-1}, u_{i_0+1}, \cdots, u_q\}$. $D \subseteq B$ est donc une

clique de taille $q - 1 = 1 \bmod 2$. Tout sommet $u \in V \setminus B$ est connecté à tous les sommets de D sauf un (celui appartenant au même ensemble V_i que lui). On a donc

$$Odd(D) \subseteq B \tag{3.15}$$

d'où $\kappa(G_{p,q}) \leq max(n-p, n-q)$.

– $[\kappa'(G_{p,q}) \leq p + q - 1]$: Soit B un ensemble de taille $p + q - 1$ composé de l'union de V_1 et d'un sommet u_i de chaque stable V_i. Comme pour le point précédent, en prenant $D = B \setminus V_1$ on a bien $|D| = q - 1 = 1 \bmod 2$ et

$$Odd(D) \subseteq B \tag{3.16}$$

Par conséquent B est non-WOD donc $\kappa'(G_{p,q}) \leq p + q - 1$.

– $[\kappa'(G_{p,q}) \geq p + q - 1]$: Soit $B \subseteq V$ avec $|B| < p + q - 1$. S'il existe un stable V_i tel que $B \cap V_i = \varnothing$, alors pour tout sommet $u \in V_i$ on a

$$B \subseteq Odd(\{u\}) \tag{3.17}$$

donc B est WOD. Si B intersecte tous les ensembles V_i, alors par contrainte de taille il ne peut contenir aucun des V_i en entier. On pose ainsi $C = \{u_1, \cdots, u_q\}$ où $u_i \in V_i \setminus B$. Tout sommet de B possède exactement $q - 1 = 1 \bmod 2$ voisins dans C :

$$B \subseteq Odd(C) \tag{3.18}$$

Dans les deux cas, on a bien $\kappa'(G_{p,q}) \geq p + q - 1$.

□

3.1.2 Propriétés de κ et κ'

Les quantités κ et κ' définies précédemment possèdent plusieurs propriétés utiles par la suite.

Tout d'abord, nous montrons que pour un graphe G donné, la somme de $\kappa(G)$ et $\kappa'(\overline{G})$ est toujours supérieure ou égale à l'ordre de G. Cette propriété est une conséquence de la correspondance entre les ensembles WOD dans G et ceux qui ne sont pas WOD dans $\overline{G}$. Cette dualité apparaît à plusieurs reprises.

Commençons par établir le lemme suivant :

Lemme 3.4. *Soit $G = (V, E)$ un graphe et $B \subseteq V$ un ensemble de sommets.*

$$B \text{ non-WOD dans } G \quad \Rightarrow \quad V \setminus B \text{ WOD dans } \overline{G} \tag{3.19}$$

Démonstration. Soit B un ensemble non-WOD dans G. D'après la Propriété 3.2 il existe alors $D \subseteq B$ avec $|D| = 1 \bmod 2$ tel que

$$Odd_G(D) \subseteq B \tag{3.20}$$

En d'autres termes, pour tout sommet $v \in V \setminus B$

$$|\mathcal{N}_G(v) \cap D| = 0 \bmod 2 \tag{3.21}$$

Puisque D est de taille impaire, cette égalité s'écrit dans le graphe complémentaire

$$|\mathcal{N}_{\overline{G}}(v) \cap D| = 1 \bmod 2 \tag{3.22}$$

Ainsi,

$$V \setminus B \subseteq Odd_{\overline{G}}(D) \tag{3.23}$$

□

Nous arrivons alors au résultat annoncé :

Théorème 3.5. *Pour tout graphe G d'ordre n*

$$\kappa'(G) + \kappa(\overline{G}) \geq n \tag{3.24}$$

Démonstration. La Définition 3.4 assure l'existence d'un ensemble $B \subseteq V$ non-WOD de taille $\kappa'(G)$. D'après le Lemme 3.4, $V \setminus B$ est WOD dans $\overline{G}$, par conséquent

$$n - |B| \leq \kappa(\overline{G}) \tag{3.25}$$

$$n - \kappa'(G) \leq \kappa(\overline{G}) \tag{3.26}$$

□

Pour tout graphe G, une première borne liant les degré maximum et minimum de G aux valeurs de $\kappa(G)$ et $\kappa'(G)$ peut être donnée :

Lemme 3.6. *Soit G un graphe de degré minimum δ et de degré maximum Δ.*

1. $\kappa(G) \geq \Delta$
2. $\kappa'(G) \leq \delta + 1$

Démonstration. Pour tout sommet v de G, son voisinage ouvert $\mathcal{N}(v)$ est un ensemble WOD car $Odd(v) = \mathcal{N}(v)$ (Définition 4.14). En revanche, son voisinage fermé $\mathcal{N}[v]$ est un ensemble non-WOD car $\mathcal{N}(v) = \{v\} \cup Odd(v)$. La première inégalité est obtenue en prenant v un sommet de degré Δ et la deuxième en prenant v de degré δ. □

Nous nous intéressons à présent à la recherche d'une borne supérieure pour $\kappa(G)$ et d'une borne inférieure pour $\kappa'(G)$.

Lemme 3.7. *Pour tout graphe G d'ordre n et de degré maximum Δ, nous avons*

$$\kappa(G) \leq \frac{n.\Delta}{\Delta + 1} \tag{3.27}$$

Démonstration. Soit $G = (V, E)$ et $B \subseteq V$ n ensemble WOD. D'après la Définition 4.14, il existe un ensemble $C \subseteq V \setminus B$ tel que $B \subseteq Odd(C)$. Ainsi nous avons

$$|C| \leq n - |B| \tag{3.28}$$

et

$$|B| \leq |Odd(C)| \leq \Delta.|C| \tag{3.29}$$

d'où

$$|B| \leq \Delta(n - |B|) \tag{3.30}$$

$$|B| \leq \frac{n.\Delta}{\Delta + 1} \tag{3.31}$$

La dernière inégalité est vérifiée quelque soit B WOD, donc par définition de $\kappa(G)$ (Définition 3.4), la borne (3.27) est vérifiée. □

Dans certains cas, la borne précédente est atteinte. Il est possible de caractériser les graphes qui réalisent le cas d'égalité par la présence ou non d'une structure appelée "code parfait" définie de la façon suivante :

Définition 3.5. *Soit $G = (V, E)$ un graphe. On appelle "code parfait" un ensemble de sommets $C \subseteq V$ tel que*
– C est un stable
– Tous les sommets de $V \setminus C$ ont exactement un voisin dans C

Une illustration de la notion de "code parfait" est donnée Figure 3.1.

Nous prouvons alors une caractérisation qui établit un lien entre le paramètre κ et l'existence d'un code parfait dans un graphe G :

Théorème 3.8. *Pour tout graphe G d'ordre n et de degré maximum Δ,*

$$\kappa(G) = \frac{n\Delta}{\Delta + 1} \iff G \text{ possède un code parfait } C \text{ tel que } \forall v \in C,\ d(v) = \Delta \tag{3.32}$$

Démonstration. [⇐]
Soit C un code parfait de G vérifiant $\forall v \in C$, $\delta(v) = \Delta$. Par définition d'un code parfait, chaque sommet de $V \setminus C$ possède un nombre impair de voisins dans C, d'où

$$Odd(C) = V \setminus C \tag{3.33}$$

Ainsi, $V \setminus C$ est un ensemble WOD.

Ensuite, chaque sommet de $V \setminus C$ possède exactement un voisin dans C, et chaque sommet de C possède exactement Δ voisins dans $V \setminus C$ par hypothèse. Cette propriété implique une contrainte sur la taille de $V \setminus C$:

$$|V \setminus C| = \frac{n\Delta}{\Delta + 1} \tag{3.34}$$

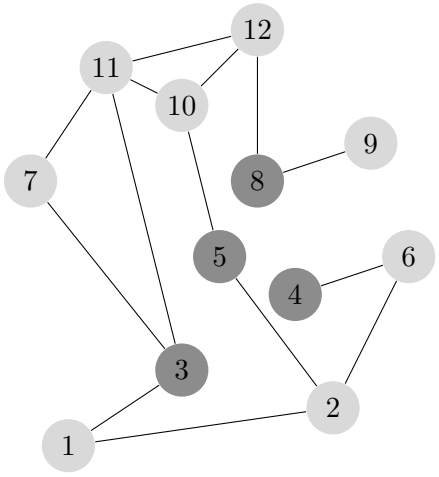

FIGURE 3.1 – Exemple de code parfait : les sommets $\{3, 4, 5, 8\}$ constituent un code parfait.

Par conséquent,

$$\kappa(G) \geq \frac{n.\Delta}{\Delta + 1} \tag{3.35}$$

En combinant cette borne avec celle du Lemme 3.7, on obtient bien le cas d'égalité annoncé.

[⇒]
Supposons que $\kappa(G) = \frac{n\Delta}{\Delta+1}$. Soit B un ensemble WOD de taille $\frac{n\Delta}{\Delta+1}$. Il existe $C \subseteq V \setminus B$ tel que $B \subseteq Odd(C)$ (Définition 2.4). La taille de C vérifie alors

$$|C| \leq n - \frac{n\Delta}{\Delta + 1} = \frac{n}{\Delta + 1} \tag{3.36}$$

De plus, $B \subseteq Odd(C) \subseteq \mathcal{N}(C)$ et $|\mathcal{N}(C)| \leq |C|\Delta$. Nous en déduisons

$$\frac{n\Delta}{\Delta + 1} = |B| \leq |C|\Delta \tag{3.37}$$

$$\frac{n}{\Delta + 1} \leq |C| \tag{3.38}$$

Ainsi, les inégalités (3.36) et (3.38) impliquent

$$|C| = \frac{n}{\Delta + 1} \tag{3.39}$$

donc $C = V \setminus B$.

Montrons que C est un code parfait dont tous les sommets sont de degré Δ. La taille de l'ensemble B vérifie

$$|B| = |B \cap Odd(C)| \tag{3.40}$$
$$\leq \sum_{v \in C} d(v) \tag{3.41}$$
$$\leq \Delta |C| = |B| \tag{3.42}$$

Les inégalités sont donc nécessairement des égalités. Si C n'est pas un code parfait, l'inégalité (3.41) est stricte, et s'il existe un sommet $v \in C$ tel que $d(V) < \Delta$, l'inégalité (3.42) est stricte. Par conséquent, C est un code parfait et $\forall v \in C$, $d(v) = \Delta$. □

La restriction de cette caractérisation au cas des graphes réguliers permet de relâcher la contrainte de régularité du code parfait présent dans le graphe :

Corollaire 3.9. *Soit G un graphe Δ-régulier d'ordre n.*

$$\kappa(G) = \frac{n\Delta}{\Delta + 1} \Leftrightarrow G \text{ possède un code parfait} \tag{3.43}$$

On pourra noter que dans ce cas, la seule taille possible pour un code parfait est $\frac{n}{\Delta+1}$.

Nous nous intéressons maintenant à la recherche d'une borne inférieure pour la valeur de $\kappa'(G)$ où G est un graphe quelconque.

Lemme 3.10. *Pour tout graphe G de degré minimum δ,*

$$\kappa'(G) \geq \frac{n}{n - \delta} \tag{3.44}$$

Démonstration. D'après le Théorème 3.5, $\kappa'(G) \geq n - \kappa(\overline{G})$. De plus, le Lemme 3.7 permet d'écrire

$$n - \kappa(\overline{G}) \geq n - \frac{n\Delta(\overline{G})}{\Delta(\overline{G}) + 1} \tag{3.45}$$
$$\tag{3.46}$$

On remarque que $\Delta(\overline{G}) = n - 1 - \delta(G)$, d'où

$$n - \kappa(\overline{G}) \geq n - \frac{n(n - 1 - \delta(G))}{n - \delta(G)} = \frac{n}{n - \delta} \tag{3.47}$$

□

On considère le lemme suivant qui établit un lien entre les ensembles *Odd* et *Even* dans un graphe G et son complémentaire $\overline{G}$: Une propriété notable de ces ensembles par rapport au graphe complémentaire est la suivante :

Lemme 3.11. *Soit $G = (V, E)$ un graphe et $D \subseteq V$ un ensemble de sommets. On note $\overline{G}$ le graphe complémentaire de G.*
– *si* $|D| = 0 \bmod 2$

$$\begin{cases} Odd_{\overline{G}}(D) = Odd_G(D) \\ Even_{\overline{G}}(D) = Even_G(D) \end{cases} \tag{3.48}$$

– *si* $|D| = 1 \bmod 2$

$$\begin{cases} Odd_{\overline{G}}(D) = Even_G(D) \\ Even_{\overline{G}}(D) = Odd_G(D) \end{cases} \tag{3.49}$$

Démonstration. On traite seulement le cas du calcul de $Odd_{\overline{G}}(D)$ lorsque $|D| = 1 \bmod 2$, les autres cas se prouvent de façon similaire.

$[\subseteq]$
On a donc $|D| = 1 \bmod 2$. Soit $v \in Odd_{\overline{G}}(D)$. D'après la Définition 1.4, v possède un nombre impair de voisins dans D dans le graphe $\overline{G}$. D est de taille impaire, ainsi il y a un nombre pair de sommets de D qui n'appartiennent pas au voisinage de v dans $\overline{G}$. Par conséquent, dans le graphe G, v possède un nombre pair de voisins dans D, d'où $v \in Even_G(D)$.

$[\supseteq]$
Ce cas se traite de manière similaire.

On a donc $Odd_{\overline{G}}(D) = Even_G(D)$. □

Tout comme pour la borne établie au Lemme 3.7, nous montrons que la borne inférieure du Lemme précédent est atteinte dans certains cas. En particuliers, les graphes réguliers qui atteignent cette borne sont ceux dont le graphe complémentaire possède un code parfait :

Théorème 3.12. *Soit G un graphe δ-régulier d'ordre n tel que $\frac{n}{n-\delta}$ est un entier impair.*

$$\kappa'(G) = \frac{n}{n-\delta} \iff \overline{G} \text{ possède un code parfait} \tag{3.50}$$

Démonstration. $[\Leftarrow]$
Soit C un code parfait dans $\overline{G}$. Comme nous avons pu le voir dans l'équation (3.39),

$$|C| = \frac{n}{\Delta(\overline{G}) + 1} \tag{3.51}$$

$$= \frac{n}{n-\delta} = 1 \bmod 2 \text{ par hypothèse} \tag{3.52}$$

De plus, on a

$$V \setminus C \subseteq Odd_{\overline{G}}(C) \tag{3.53}$$

En utilisant le Lemme 3.11 puis en prenant les ensembles complémentaires, on obtient

$$V \setminus C \subseteq Even_G(C) \tag{3.54}$$
$$C \supseteq Odd_G(C) \tag{3.55}$$

Ainsi, C est un ensemble non-WOD dans G, donc

$$\kappa'(G) \leq \frac{n}{n-\delta} \tag{3.56}$$

Le Lemme 3.10 combiné à l'inégalité précédente permet de déduire $\kappa'(G) = \frac{n}{n-\delta}$.

[⇒]
Soit B un ensemble non-WOD (à noyau impair) de taille $\frac{n}{n-\delta}$ in G. Par définition, il existe $D \subseteq B$ tel que $|D| = 1 \bmod 2$ et $Odd_G(D) \subseteq B$. D'après le Lemme 3.4, $V \setminus B \subseteq Odd_{\overline{G}}(D)$, par conséquent

$$|Odd_{\overline{G}}(D)| \geq |V \setminus B| \tag{3.57}$$
$$\geq n - \frac{n}{n-\delta} = \frac{n(n-\delta-1)}{n-\delta} \tag{3.58}$$
$$\geq \Delta(\overline{G})\frac{n}{n-\delta} \tag{3.59}$$

L'inégalité (3.59) utilise la propriété : $\Delta(\overline{G}) = n-1-\delta$. Or $|Odd_{\overline{G}}(D)| \leq |D|\Delta(\overline{G})$, d'où

$$|D| \geq \frac{n}{n-\delta} \tag{3.60}$$

D est contenu dans l'ensemble B de taille $\frac{n}{n-\delta}$, nous avons donc $D = B$ et

$$|D| = \frac{n}{n-\delta} \tag{3.61}$$

Puisque $V \setminus B \subseteq Odd_{\overline{G}}(D)$, tous les sommets de $V \setminus B$ sont connectés à des sommets de D, donc il y a au moins $|V \setminus D|$ arêtes entre D et $V \setminus D$. De plus, $|V \setminus D| = \Delta(\overline{G})|D|$, donc il y a au maximum $|V \setminus D|$ arêtes entre D et $V \setminus D$ (car $\overline{G}$ est un graphe $\Delta(\overline{G})$-régulier). Ainsi, il y a exactement $\Delta(\overline{G})|D|$ arêtes entre D et $V \setminus D$, ce qui implique les deux faits suivants :
– il n'y a aucune arête à l'intérieur de D (sinon un des sommets de D serait de degré strictement supérieur à $\Delta(\overline{G})$)
– chaque sommet de $V \setminus D$ est relié à un et un seul sommet de D (sinon le nombre d'arêtes entre D et $V \setminus D$ serait strictement supérieur à $|V \setminus D|$)
Nous avons donc montré que D est un code parfait dans $\overline{G}$. □

3.1.3 Lien entre κ, κ' et κ_Q

Dans le Chapitre 2, nous avons utilisé une quantité κ_Q introduite dans la Définition 2.5. Si on considère le cas d'un dealer (sommet d) universel, il est possible d'établir un lien entre les quantités κ, κ' et κ_Q sur un graphe G quelconque.

Dans le but de prouver la difficulté du problème de décision associé à κ_Q, nous établissons la caractérisation suivante :

Lemme 3.13. *Soit $G = (V, E)$ un graphe d'ordre n. On a*

$$\kappa_Q(G) = \max\big(\kappa(G), n - \kappa'(G)\big) \tag{3.62}$$

Démonstration. On remarque d'abord que la Propriété 2.23 montrée dans le Chapitre 2 s'écrit dans la cas d'un dealer universel :

$$\kappa_Q(G) = \max\big(\kappa(G), \kappa(\overline{G})\big) \tag{3.63}$$

D'après le Lemme 3.4, on a l'inégalité

$$\kappa(\overline{G}) \geq n - \kappa'(G) \tag{3.64}$$

On veut montrer que lorsque la valeur de $\kappa_Q(G)$ n'est pas donnée par la valeur de $\kappa(G)$, on a nécessairement une égalité entre $\kappa(\overline{G})$ et $n - \kappa'(G)$ (où $\overline{G}$ désigne le graphe complémentaire de G). En d'autres termes, on veut montrer

$$\kappa(G) < \kappa(\overline{G}) \quad \Rightarrow \quad \kappa(\overline{G}) = n - \kappa'(G) \tag{3.65}$$

Supposons que $\kappa(G) < \kappa(\overline{G})$. Il existe alors un ensemble $B \subseteq V$ de taille $\kappa(\overline{G})$ WOD dans $\overline{G}$ par un ensemble $C \subseteq V \setminus B$.

L'ensemble C vérifie $|C| = 1 \bmod 2$, car dans le cas contraire, dans le graphe G, chaque sommet de B possèderait un nombre impair de voisins dans C et B serait donc dominé modulo 2 dans G. On aurait dans ce cas $\kappa(G) \geq \kappa(\overline{G})$, ce qui contredit la supposition.

Par conséquent, l'ensemble $V \setminus B$ contient $C \cup Odd(C)$ dans le graphe G et il est donc non-WOD d'après le Lemme 3.2. Ainsi, on a

$$\kappa'(G) \leq |V \setminus B| \tag{3.66}$$

ce qui s'écrit également

$$\kappa(\overline{G}) \leq n - \kappa'(G) \tag{3.67}$$

En combinant cette inégalité avec l'inégalité (3.64), on obtient l'égalité souhaitée :

$$\kappa(\overline{G}) = n - \kappa'(G) \tag{3.68}$$

Par conséquent, et d'après l'équation (3.63), on obtient bien la caractérisation (3.62).

□

Profitons de ce lemme pour faire une remarque : les équations (3.62) et (3.63) impliquent le corollaire suivant :

Corollaire 3.14. *Pour tout graphe G, on a*

$$\max\big(\kappa(G), \kappa(\overline{G})\big) = \max\big(\kappa(G), n - \kappa'(G)\big) \tag{3.69}$$

Par ailleurs, on peut noter les trois faits suivants :
– la valeur de ce maximum n'est pas toujours donnée par $\kappa(G)$
– il n'y a pas forcément d'égalité entre $\kappa(\overline{G})$ et $n - \kappa'(G)$
– il y a une symétrie entre G et $\overline{G}$ pour ces propriétés (interchangeabilité)
On peut déduire de cela que parmi les trois quantités $n - \kappa'(G)$, $\kappa(G)$ et $\kappa(\overline{G})$, les deux plus grandes sont nécessairement égales. Un aspect intéressant de cette propriété est qu'elle concerne des quantités définies sur les graphes, mais que l'étape principale qui nous permet de l'établir appartient au domaine de la théorie de l'information quantique : la Propriété 2.23.

Grâce à la caractérisation établie dans le Lemme 3.13, on peut retrouver la valeur de κ_Q des graphes $G_{p,q}$ évoqués précédemment. On s'intéresse notamment au cas $p = q$. Pour tout $p \geq 2$ avec $p = 0 \bmod 2$, le graphe $G_{p,p}$ d'ordre $n = p^2$ vérifie d'après l'expression (3.10) :

$$\begin{aligned} \kappa_Q(G_{p,p}) &= \max\big(\kappa(G), n - \kappa'(G)\big) && (3.70)\\ &= \max\big(n - p, n - 2p - 1\big) && (3.71)\\ &= n - \sqrt{n} && (3.72) \end{aligned}$$

d'après l'équation Lorsque $p = 1 \bmod 2$, on pourra vérifier que l'expression (3.9) donne également

$$\kappa_Q(G_{p,p}) = n - \sqrt{n} \tag{3.73}$$

Cette valeur est bien en accord avec la borne calculée en (2.148).

3.2 Complexité des problèmes associés à κ, κ', κ_Q et δ_{loc}

Après avoir défini les valeurs $\kappa(G)$ et $\kappa'(G)$ pour un graphe G donné et en avoir étudié certaines propriétés, bornes et caractérisations, nous abordons ici les problèmes de décision associés à ces deux quantités. Comme il sera vu plus loin, ces deux problèmes de théorie des graphes jouent aussi un rôle dans les protocoles de partage de secret quantique à partir d'états graphes. Leur complexité est étudiée ici.

Nous appelons **MAX_WOD** le problème de décision associé à $\kappa(G)$ (voir Figure 3.2)

Théorème 3.15. MAX_WOD *est NP-complet.*

MAX_WOD

Entrée
– un graphe G d'ordre n
– un entier $k \geq 0$

Sortie
– **OUI** si $\kappa(G) \geq k$
– **NON** sinon

FIGURE 3.2 – Problème de décision associé à $\kappa(G)$

Démonstration. Tout d'abord, **MAX_WOD** est dans la classe NP car tout ensemble B WOD de taille k est un certificat du OUI. En effet, il existe un algorithme polynomial décidant si un ensemble B est WOD (Figure 2.2).

Pour montrer que **MAX_WOD** est NP-Difficile, nous effectuons une réduction au problème **PERFECT_CODE** qui consiste à décider si un graphe donné possède un code parfait (Définition 3.5). Ce dernier a été prouvé NP-difficile sur les graphes 3-réguliers (voir [Kra87] et [KMP02]).

Soit G un graphe 3-régulier d'ordre n. On utilise l'oracle pour **MAX_WOD** instancié par le graphe G et l'entier $k = \frac{3}{4}n$. On montre alors que l'oracle répond "OUI" si et seulement si le graphe G possède un code parfait.

[⇒]
Si l'oracle répond "OUI", alors $\kappa(G) \geq \frac{3}{4}n$. Or, d'après le Lemme 3.7

$$\kappa(G) \leq \frac{n\Delta}{\Delta + 1} = \frac{3}{4}n = k \tag{3.74}$$

d'où $\kappa(G) = \frac{3}{4}n = \frac{n\Delta}{\Delta+1}$. D'après le Corollaire 3.9, G possède un code parfait.

[⇐]
Le Corollaire 3.9 étant une équivalence, on obtient de façon immédiate : si G possède un code parfait, alors $\kappa(G) = \frac{3}{4}n$ donc l'oracle de **MAX_WOD** répond "OUI".

Le problème **MAX_WOD** se réduit ainsi au problème **PERFECT_CODE** sur les graphes 3 réguliers. □

Le problème de décision associé à $\kappa'(G)$ est également NP-complet. Sa formulation précise à partir d'un graphe G et d'un entier k est donnée dans la Figure 3.3.

Théorème 3.16. MIN_¬WOD *est NP-complet.*

Démonstration. Le problème **MIN_¬WOD** est dans la classe NP. En effet, un ensemble non-WOD de taille k est un certificat pour la réponse OUI.

MIN_¬WOD

Entrée
– un graphe G d'ordre n
– un entier $k \geq 0$

Sortie
– **OUI** si $\kappa'(G) \leq k$
– **NON** sinon

FIGURE 3.3 – Problème de décision associé à $\kappa'(G)$

Nous montrons à présent que **MIN_¬WOD** est NP-difficile. Soit G un graphe 3-régulier d'ordre n. On distingue 2 cas suivant la parité de $\frac{n}{4}$.

Si $\frac{n}{4} = 1 \bmod 2$, alors $\overline{G}$ est un graphe régulier vérifiant

$$\frac{n}{n - \Delta(\overline{G})} = \frac{n}{4} = 1 \bmod 2 \tag{3.75}$$

D'après le Théorème 3.12, G possède un code parfait si et seulement si $\kappa'(\overline{G}) = \frac{n}{4}$. Ainsi, en utilisant l'oracle pour **MIN_¬WOD** sur le graphe $\overline{G}$, on peut décider de l'existence d'un code parfait dans G.

Si $\frac{n}{4} = 0 \bmod 2$, on considère cette fois le graphe $G' = G \cup K_4$ construit à partir de G en ajoutant un graphe complet sur 4 sommets. G' est d'ordre $n' = n + 4$ et est également un graphe 3-régulier.

$$\frac{n'}{n' - \Delta(\overline{G'})} = \frac{n'}{4} = \frac{n}{4} + 1 = 1 \bmod 2 \tag{3.76}$$

On constate que G' admet un code parfait si et seulement si G admet un code parfait. Ainsi, l'oracle pour **MIN_¬WOD** sur le graphe $\overline{G'}$ permet de décider de l'existence d'un code parfait sur G.

Le problème pour **MIN_¬WOD** est donc réduit au problème **PERFECT_CODE** sur les graphes 3-réguliers et est donc NP-difficile. □

La complexité paramétrée de ce problème ainsi que du précédent on été étudiées par Cattanéo et Perdrix [CP13] à la suite de ces travaux.

3.2.1 Problème QKAPPA et implications sur le partage de secret quantique

Nous montrons dans cette section que le problème consistant à décider, étant donné un graphe G et un entier $k \geq 0$, si $\kappa_Q(G) \geq k$ est NP-complet (Theorem 3.18). Pour cela,

nous utilisons le deux ingrédients suivants : une caractérisation alternative de κ_Q faisant intervenir les quantités κ et κ' (Lemme 3.13) ainsi que l'évaluation de κ et κ' sur des constructions de graphes particulières (Lemme 3.17).

Nous calculons les valeurs de κ et κ' d'une construction récursive à partir d'un graphe G en vue d'une réduction dans la preuve de complexité qui suivra.

Lemme 3.17. *Pour tout graphe G et pour tout entier $r > 0$ on a*

$$\begin{cases} \kappa(G^r) = r.\kappa(G) \\ \kappa'(G^r) = \kappa'(G) \end{cases} \tag{3.77}$$

où G^r représente le graphe constitué de r copies de G.

Démonstration. On note $G = (V, E)$.
$[\kappa(G^r) = r.\kappa(G)]$
Pour prouver cette première égalité, on considère un ensemble B WOD de sommets de G de taille $\kappa(G)$. Il existe donc un ensemble $C \subseteq V$ tel que

$$B \subseteq Odd(C) \tag{3.78}$$

On construit alors l'ensemble $B_r \subseteq V(G^r)$ qui consiste en l'union des ensembles B dans les r copies de G. L'ensemble C_r est construit de manière similaire en utilisant les ensembles C précédents. Par construction du graphe G^r, on a

$$B_r \subseteq Odd(C_r) \tag{3.79}$$

Ainsi, B_r est WOD dans G^r d'où

$$\kappa(G^r) \geq r\kappa(G) \tag{3.80}$$

Pour prouver l'inégalité dans l'autre sens, on considère un ensemble $B_0 \subseteq V(G^r)$ quelconque de taille supérieure à $r.\kappa(G)$. Il existe alors nécessairement une copie de G dans le graphe G^r dans laquelle

$$|B_0 \cap G| > \kappa(G) \tag{3.81}$$

L'ensemble $B_0 \cap G$ est donc non-WOD dans cette copie de G, il est donc également non-WOD dans G^r par construction. Par conséquent

$$\kappa(G^r) \leq r.\kappa(G) \tag{3.82}$$

On obtient l'égalité souhaitée en combinant les inégalités (3.80) et (3.82).

$[\kappa'(G^r) = \kappa'(G)]$
Pour cette égalité, on considère un ensemble $B \subseteq V$ non-WOD de taille $\kappa'(G)$. De façon immédiate, si on considère B comme un ensemble de sommets de $V(G^r)$ contenu dans

une des copies de G, on voit que B est non-WOD dans G^r. En effet, les r copies de G sont séparées. De cette façon, on a

$$\kappa'(G^r) \leq \kappa'(G) \tag{3.83}$$

On considère à présent un ensemble $B_0 \subseteq V(G^r)$ tel que $|B_0| < \kappa'(G)$. L'intersection de B' avec chacune des copies de G du graphe G^r vérifie alors

$$|B_0 \cap G| < \kappa'(G) \tag{3.84}$$

Pour chacune des r copies de G dans G^r, on a donc l'existence d'un ensemble de sommets C_i $(1 \leq i \leq r)$ tel que $B_0 \subseteq Odd(C_i)$. Par construction, on a alors

$$B_0 \subseteq Odd(\bigcup_{i=1..r} C_i) \tag{3.85}$$

B_0 est donc un ensemble WOD dans G^r, d'où

$$\kappa'(G^r) \geq \kappa'(G) \tag{3.86}$$

(3.83) et (3.86) terminent la preuve de la deuxième égalité. □

3.2.2 QKAPPA est NP-complet

L'objet de cette partie est l'étude de la difficulté du problème de décision associé à la quantité κ_Q (caractérisée dans le Lemme 3.13) de graphes quelconques.

De façon plus formelle, on considère le problème **QKAPPA** qui prend en entrée un graphe G d'ordre n et un entier $k \geq 0$ et décide si $\kappa_Q(G) \geq k$, c'est à dire si $\kappa(G) \geq k$ ou $\kappa'(G) \leq n - k$ (Figure 3.4).

QKAPPA

Entrée
– un graphe G d'ordre n
– un entier $k \geq 0$

Sortie
– **OUI** si $\kappa_Q(G) \geq k$
– **NON** sinon

FIGURE 3.4 – Problème de décision associé à $\kappa_Q(G)$

Théorème 3.18. QKAPPA *est NP-complet.*

Démonstration. Nous utilisons la caractérisation de la quantité κ_Q établie dans le Lemme 3.13.

QKAPPA appartient à la classe NP. En effet, un ensemble WOD de taille k ou un ensemble non-WOD de taille $n-k$ est un certificat du OUI.

Afin de prouver que **QKAPPA** est NP-difficile, nous proposons une réduction au problème **MIN_¬WOD**. Pour tout graphe G et tout entier $k \geq 0$, on a (Lemme 3.13)

$$\kappa_Q(G^{k+1}) \geq (k+1)n - k \quad \Leftrightarrow \quad \Big(\kappa(G^{k+1}) \geq (k+1)n - k \text{ ou } \kappa'(G^{k+1}) \leq k\Big) \tag{3.87}$$

$$\Leftrightarrow \quad \Big(\kappa(G) \geq n - 1 + \frac{1}{k+1} \text{ ou } \kappa'(G) \geq k\Big) \tag{3.88}$$

$$\Leftrightarrow \quad \Big(\kappa(G) > n - 1 \text{ ou } \kappa'(G) \geq k\Big) \tag{3.89}$$

Dans l'expression (3.89), la première inégalité $\kappa(G) > n-1$ est toujours fausse (Lemme 3.7). On a donc l'équivalence

$$\kappa_Q(G^{k+1}) \geq (k+1)n - k \quad \Leftrightarrow \quad \kappa'(G) \geq k \tag{3.90}$$

Ainsi, pour le problème **MIN_¬WOD** paramétré par les graphe G et l'entier k, on utilise l'oracle pour **QKAPPA** instancié par le graphe G et l'entier $(k+1)n-k$. La réponse donnée par l'oracle est utilisée pour répondre au problème **MIN_¬WOD**.

D'après le Théorème 3.16, le problème **MIN_¬WOD** est NP-complet, par conséquent, **QKAPPA** est NP-complet. □

Une conséquence de la NP-complétude du problème **QKAPPA** est l'absence d'un algorithme efficace (sauf si $P = NP$) qui permettrait de déterminer le seuil que pourrait atteindre un protocole de partage de secret quantique qQSS* à partir d'un graphe quelconque.

3.2.3 Difficulté de la recherche du degré minimum par complémentation locale

Après nous être intéressés aux problèmes de décision liés aux quantités κ, κ' et κ_Q, nous abordons le cas du degré minimum par complémentation locale. Ainsi, nous montrons que pour tout graphe G et tout entier d, décider si $\delta_{loc}(G) \leq d$ est NP-complet, même en nous restreignant aux graphes bipartis.

Ce résultat est établi grâce à une réduction au problème **SHORTEST_CODEWORD** qui consiste à trouver le plus petit mot d'un code linéaire et qui est NP-complet [Var97]. La preuve que nous proposons a la particularité d'utiliser une famille de graphe dont l'existence est prouvée dans le Théorème 3.24.

Montrons tout d'abord un lemme lié à la structure des graphes bipartis.

Lemme 3.19. *Soit $G = (V, E)$ un graphe biparti. Soit $V = V_1 \cup V_2$ où V_1 et V_2 sont les deux stables maximaux de G. Il existe alors $D_0 \subseteq V$ tel que*

$$\delta_{loc}(G) + 1 = |D_0 \cup Odd(D_0)| \tag{3.91}$$

et où D_0 vérifie

$$D_0 \subseteq V_1 \qquad ou \qquad D_0 \subseteq V_2 \tag{3.92}$$

Démonstration. Soit $D \subseteq V$ tel que $|D \cup Odd(D)| = \delta_{loc}(G) + 1$. La caractérisation du Lemme 3.1 assure l'existence d'un tel ensemble D. On écrit

$$D = D_1 \cup D_2 \tag{3.93}$$

avec $D_1 = D \cap V_1$ et $D_2 = D \cap V_2$. $D \neq \varnothing$ donc on suppose sans perte de généralité que $D_1 \neq \varnothing$.

G est un graphe biparti, par conséquent

$$\begin{cases} Odd(D_1) \subseteq V_2 \\ Odd(D_2) \subseteq V_1 \end{cases} \tag{3.94}$$

Ainsi on peut écrire

$$Odd(D_1 \cup D_2) = Odd(D_1) \cup Odd(D_2) \tag{3.95}$$

On revient au degré minimum par complémentation locale de G :

$$\begin{aligned} \delta_{loc}(G) + 1 &= |D \cup Odd(D)| && (3.96)\\ &= |D_1 \cup Odd(D_1) \cup D_2 \cup Odd(D_2)| && (3.97)\\ &\geq |D_1 \cup Odd(D_1)| && (3.98)\\ &\geq \delta_{loc}(G) + 1 && (3.99) \end{aligned}$$

La deuxième égalité est obtenue grâce à l'équation (3.95) et l'inégalité (3.99) provient de la caractérisation du Lemme 3.1. Les deux bornes précédentes sont égales, ainsi toutes les inégalités sont des égalités, notamment

$$\delta_{loc}(G) + 1 = |D_1 \cup Odd(D_1)| \tag{3.100}$$

On termine la preuve en prenant $D_0 = D_1$. □

Ce lemme assure que pour le calcul du degré minimum par complémentation locale d'un graphe biparti grâce à la caractérisation du Lemme 3.1, il suffit de considérer les sous-ensembles de sommets situés intégralement dans l'un ou l'autre des stables du graphe.

Nous introduisons la notion de double biparti d'un graphe G [Wal76] qui consiste en la transformation d'un graphe G en graphe biparti dont l'ordre est doublé et le degré minimum par complémentation locale est le même que celui du graphe G.

MIN_LOCAL_DEGREE

Entrée
– un graphe G d'ordre n
– un entier $d \geq 0$

Sortie
– **OUI** si $\delta_{loc}(G) \leq d$
– **NON** sinon

FIGURE 3.5 – Problème de décision associé à $\delta_{loc}(G)$

Définition 3.6. *Soit $G = (V, E)$. On appelle "double biparti de G" le graphe biparti*

$$G^{\oplus 2} = (V_1 \cup V_2, E') \tag{3.101}$$

où V_1 et V_2 sont deux copies des sommets de V et $E' = \{(u, v) \in V_1 \times V_2 \mid (u, v) \in E\}$.

Le double biparti $G^{\oplus 2}$ est également le produit tensoriel du graphe G et du graphe K_2 (le graphe complet d'ordre 2).

Montrons alors la propriété annoncée sur les doubles bipartis :

Lemme 3.20. *Pour tout graphe G, on a*

$$\delta_{loc}(G^{\oplus 2}) \geq \delta_{loc}(G) \tag{3.102}$$

Démonstration. Soit $G = (V, E)$ et $G^{\oplus 2} = (V_1 \cup V_2, E')$. D'après le Lemme 3.19, il existe $D_0 \subseteq V_1$ tel que

$$\delta_{loc}(G^{\oplus 2}) + 1 = |D_0 \cup Odd_{G^{\oplus 2}}(D_0)| \tag{3.103}$$

On écrit alors

$$\begin{aligned} \delta_{loc}(G^{\oplus 2}) + 1 &= |D| + |Odd_{G^{\oplus 2}}(D)| && (3.104)\\ &= |D| + |Odd_G(D)| && (3.105)\\ &\geq |D \cup Odd_G(D)| && (3.106)\\ &\geq \delta_{loc}(G) + 1 && (3.107) \end{aligned}$$

□

A présent, nous établissons la NP-complétude du problème **MIN_LOCAL_DEGREE** formalisé Figure 3.5.

Théorème 3.21. *Etant donné un graphe G et un entier d, le problème* **MIN_LOCAL_DEGREE** *consistant à décider si*

$$\delta_{loc}(G) \leq d \tag{3.108}$$

est NP-complet sur la famille des graphes bipartis.

Démonstration. Le problème **MIN_LOCAL_DEGREE** est dans NP car un ensemble de la forme $D \cup Odd(D)$ avec $D \neq \varnothing$ et $|D \cup Odd(D)| \leq d+1$ est un certificat du OUI. Pour la NP-complétude, on effectue une réduction au problème **SHORTEST_CODEWORD** consistant à trouver la taille du plus petit mot d'un code linéaire.

Soit $A \in \mathcal{M}_{n+k,k}(\mathbb{F}_2)$ la matrice génératrice d'une code linéaire. On souhaite trouver le plus petit mot de A en faisant appel à un oracle pour **MIN_LOCAL_DEGREE**.

Si $dim(Ker(A)) \neq 0$, alors on a

$$\min_{X \in \mathbb{F}_2^k, X \neq 0} \{w(AX)\} = 0 \tag{3.109}$$

où w est la fonction qui retourne le poids de Hamming d'un vecteur, c'est à dire le nombre de coordonnées non-nulles de ce vecteur. En effet, dans ce cas, le vecteur nul est un mot de code.

Dans l'autre cas, lorsque la matrice A est de rang plein, on peut écrire A sous la forme

$$\begin{pmatrix} I_k \\ A' \end{pmatrix} \tag{3.110}$$

où A' est de taille $n \times k$. Le membre de gauche de l'équation (3.109) s'écrit alors

$$\min_{X \in \mathbb{F}_2^k, X \neq 0} \{w(AX)\} = \min_{X \in \mathbb{F}_2^k, X \neq 0} \{w(X) + w(A'X)\} \tag{3.111}$$

On construit maintenant un graphe biparti G (décrit Figure 3.6) sur lequel on appellera l'oracle. Cette construction est détaillée à présent.

On définit d'abord deux graphes auxiliaires $G_{A'}$ et G_B :
- Soit $G_{A'} = (V_{A'_1} \cup V_{A'_2}, E_{A'})$ un graphe biparti défini de la façon suivante : les ensembles $V_{A'_1}$ et $V_{A'_2}$ sont les deux "parties" de la bipartition et ils vérifient $|V_{A'_1}| = k$ et $|V_{A'_2}| = n$. Pour tout $(x, x') \in V_{A'_1} \times V_{A'_2}$, il y a une arête entre x et x' si et seulement si $A'_{x',x} = 1$.
- Soit $G_B = Pal_p^{\oplus 2}$, où m est le plus petit nombre premier vérifiant $p > n^2$ et $p = 1 \bmod 4$. Pal_p est le graphe de Paley d'ordre p et $Pal_p^{\oplus 2}$ son double biparti. D'après le Lemme 3.20, on a $\delta_{loc}(Pal_p^{\oplus 2}) \geq \delta_{loc}(Pal_p)$ et le Théorème 4.4 assure que $\delta_{loc}(Pal_p) > \sqrt{p} - \frac{2}{3}$. Ainsi,

$$\delta_{loc}(Pal_p^{\oplus 2}) \geq n \tag{3.112}$$

Les ensembles V_{B_1} et V_{B_2} dénotent les deux "parties" de la bipartition des sommets de G_B.

Soit u un sommet quelconque de V_{B_1}. On considère le graphe $G = (V_1 \cup V_2, E)$ (Figure 3.6) défini comme suit : pour l'ensemble V_1 :

$$V_1 = V_{1L} \cup V_{1R} \text{ avec } \begin{cases} V_{1L} = V_{A'_1} \times \{u\} \\ V_{1R} = V_{A'_2} \times V_{B_2} \end{cases} \tag{3.113}$$

L'ensemble V_2 vérifie

$$V_2 = V_{A'_2} \times V_{B_1} \tag{3.114}$$

D'un point de vue formel, l'ensemble E d'arêtes de G est défini ainsi : pour tout $(x, y) \in V_1$ et $(x', y') \in V_2$

$$\Big((x,y),(x',y')\Big) \in E \quad \Leftrightarrow \quad \Big(y = y' \text{ et } (x,x') \in E_{A'}\Big) \text{ ou } \Big(x = x' \text{ et } (y,y') \in E_B\Big) \tag{3.115}$$

De façon plus intuitive, le graphe G est construit à partir d'un graphe $G_{A'}$ auquel on attache une copie du graphe G_B à chacun des sommets de la partie de $G_{A'}$ de taille n. Il n'existe aucune arête à l'intérieur de V_1 ni de V_2, G est donc un graphe biparti dont les ensembles indépendants maximaux sont V_1 et V_2. On note $V = V_1 \cup V_2$.

D'après le Lemme 3.19, il existe un ensemble non vide $D_0 \subseteq V$ tel que

$$\delta_{loc}(G) + 1 = |D_0 \cup Odd(D_0)| \tag{3.116}$$

et $D_0 \subseteq V_1$ ou $D_0 \subseteq V_2$.

On suppose que $D_0 \subseteq V_2$. On peut alors écrire

$$\begin{aligned} \delta_{loc}(G) &= |D_0 \cup Odd(D_0)| - 1 && (3.117)\\ &\geq \delta_{loc}(G_B) && (3.118)\\ &> n + 1 && (3.119)\\ &\geq \delta(G) + 1 && (3.120)\\ &\geq \delta_{loc}(G) && (3.121) \end{aligned}$$

L'inégalité (3.118) est vérifiée car l'intersection de $D_0 \cup Odd(D_0)$ avec une des copies de G_B est également un ensemble du type $D \cup Odd(D)$ dans cette copie de G_B. L'inégalité (3.119) provient de la propriété de G_B donnée en (3.112). Cette dernière étant stricte, on a une contradiction, donc $D_0 \subseteq V_1$.

On suppose que $D_0 \cap V_{1R} \neq \varnothing$. Il existe alors un sommet $v \in D_0 \cap V_{1R}$. Dans ce cas on peut écrire

$$\begin{aligned} \delta_{loc}(G) &= |D_0 \cup Odd(D_0)| - 1 && (3.122)\\ &\geq |\{v\} \cup Odd(\{v\})| - 1 && (3.123)\\ &\geq \delta_{loc}(G_B) > \delta_{loc}(G) && (3.124) \end{aligned}$$

La première inégalité de (3.124) s'explique de façon similaire à (3.118). Ceci aboutit également à une contradiction, donc $D_0 \cap V_{1R} = \varnothing$.

On a donc nécessairement $D_0 \subseteq V_{1L}$. Par construction du graphe G, on remarque que l'ensemble $Odd(D_0)$ dans G correspond exactement à l'ensemble $Odd(D_0)$ dans le graphe $G_{A'}$ utilisé dans la construction de G (voir Figure 3.6).

La matrice de coupe entre les deux stables maximaux de $G_{A'}$ se trouve être, par construction, la matrice A'. Ainsi, dans le graphe G, on a la correspondance

$$|Odd(D_0)| = w(A'X_{D_0}) \tag{3.125}$$

où X_{D_0} est le vecteur caractéristique de l'ensemble D_0. De plus, V_{1L} est un stable donc

$$\begin{aligned} |D_0 \cup Odd(D_0)| &= |D_0| + |Odd(D_0)| && (3.126)\\ &= w(X_{D_0}) + w(A'X_{D_0}) && (3.127) \end{aligned}$$

D'après les équations (3.111) et (3.116), on peut donc écrire

$$\delta_{loc}(G) + 1 = \min_{X \in \mathbb{F}_2^k, X \neq 0} \{w(AX)\} \tag{3.128}$$

Le degré minimum par complémentation locale de G est donc égal (à '1' près) à la taille du plus petit mot du code linéaire décrit par la matrice A. On a donc réduit le problème de la recherche du degré minimum par complémentation locale au problème **SHORTEST_CODEWORD** qui est NP-complet [Var97].

□

On pourra noter que les caractérisations des quantités δ_{loc} (Propriété 3.1) et κ' (Propriété 3.2) sont très similaires : elles ne diffèrent que par la contrainte de parité pour κ'

$$\left\{ \begin{array}{rcl} \delta_{loc}(G) & = & \min \left\{ \; |D \cup Odd(D)| \;\middle|\; D \subseteq V(G), D \neq \varnothing \; \right\} - 1 \\ \kappa'(G) & = & \min \left\{ \; |D \cup Odd(D)| \;\middle|\; D \subseteq V(G), |D| = 1 \bmod 2 \; \right\} \end{array} \right. \tag{3.129}$$

Il est alors intéressant de constater que les problèmes de décision qui leur sont associés sont tous les deux NP-complets, mais les preuves qui sont proposées ici utilisent des techniques totalement différentes.

Il est difficile de calculer le degré minimum par complémentation d'un graphe en général, cependant nous pouvons nous demander s'il est possible d'approximer cette quantité : existe-t-il une constante $l \in \mathbb{R}$ qui garantisse l'existence d'un algorithme de l-approximation pour ce problème ?

Nous prouvons alors le résultat suivant :

Théorème 3.22. *Il n'existe pas d'algorithme d'approximation avec un facteur constant pour le problème du calcul du degré minimum par coplémentation locale, même sur la famille des graphes bipartis, à moins que P=NP.*

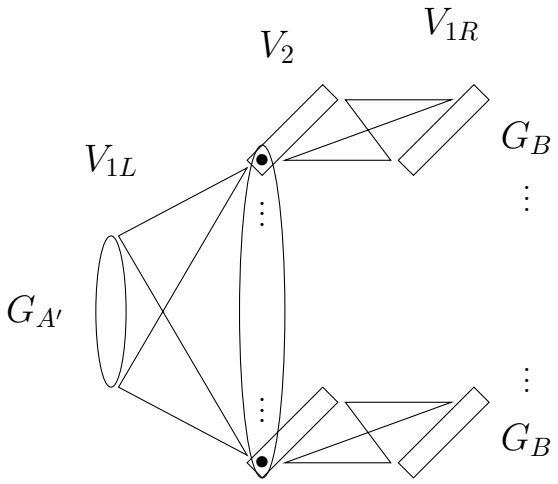

FIGURE 3.6 – Construction du graphe G à partir du graphe biparti $G_{A'}$ (ellipses) et plusieurs copies du graphe biparti G_B (rectangles). $V_1 = V_{1L} \cup V_{1R}$

Démonstration. Dans la preuve du Théorème 3.21 le graphe biparti G construit à partir de la matrice génératrice A d'un code linéaire quelconque (Figure 3.6) est tel que la valeur de $\delta_{loc}(G)$ est la même (à '1' près) que la taille du plus petit mot du code A (3.128). Cette construction étant valable pour un code A quelconque, quelque soit $l \in \mathbb{R}$, n'importe quel algorithme de l-approximation de $\delta_{loc}(G)$ fournit directement une l-approximation du poids de Hamming du plus petit mot de A. Or sous l'hypothèse $P = NP$, le problème du calcul de la taille du plus petit mot d'un code linéaire n'admet aucun algorithme d'approximation à un facteur constant près de complexité polynomiale [DMS03]. Par conséquent, il n'existe aucun algorithme d'approximation à un facteur constant près pour le calcul du degré minimum par complémentation locale d'un graphe, même pour la famille des graphes bipartis. □

3.3 Méthodes probabilistes et graphes probabilistes

Les résultats précédents montrent qu'il est difficile de calculer les quantités $\kappa(G)$ et $\kappa'(G)$ pour un graphe G en général. Le degré minimum par complémentation locale étant lié à ces quantités, il est également difficile de le calculer.

Si nous pouvons facilement construire des graphes dont le degré minimum par complémentation locale est petit (graphes avec un sommet de petit degré), il semble en revanche plus délicat de construire des graphes avec un δ_{loc} relativement grand. Une question se pose aussi naturellement : quelle est le plus grand degré minimum par complémentation locale atteignable pour une taille de graphe donnée ?

Nous utilisons ici des méthodes probabilistes basées sur l'utilisation du modèle d'Erdös-

Renyi [ER59] permettent de démontrer l'existence de familles infinies de graphes dont le degré minimum par complémentation locale est une fraction constante du nombre de sommets. Cette propriété est vraie également si on se restreint au cas des graphes bipartis, même si la constante que nous atteignons sans cette restriction reste meilleure.

3.3.1 Définitions

Le principe des méthodes probabilistes utilisées ici est le suivant : on souhaite prouver l'existence d'un objet parmi un ensemble $\mathcal{E}$ ayant une propriété $\mathcal{P}$. On construit donc une loi probabiliste pour tirer au hasard les objets de $\mathcal{E}$, et on établit un ensemble $\mathcal{A}$ de "mauvais événements" tel que si aucun des événements de $\mathcal{A}$ n'ont lieu, la propriété $\mathcal{P}$ est respectée. On montre ensuite que la probabilité qu'aucun des événements de $\mathcal{A}$ ne se produise est non nulle.

Le résultat que nous utilisons pour formaliser cette méthode est la version asymétrique du Lemme Local de Lovász [Lov75].

Lemme 3.23 (Lemme Local de Lovász Asymétrique)**.** *Soit $\mathcal{A} = \{A_1, \cdots, A_n\}$ un ensemble de "mauvais événements" dans un univers quelconque. Soit $\Gamma(A)$ un sous-ensemble de $\mathcal{A}$ tel que A est indépendant de tous les événements en dehors de A et $\Gamma(A)$. Si pour tout A_i il existe $\sigma(A_i) \in [0, 1)$ tel que*

$$Pr(A_i) \leq \sigma(A_i) \prod_{B_j \in \Gamma(A_i)} (1 - \sigma(B_j)) \tag{3.130}$$

alors on a

$$Pr(\overline{A_1}, \cdots, \overline{A_n}) \geq \prod_{A_j \in \mathcal{A}} (1 - \sigma(A_j)) \tag{3.131}$$

3.3.2 Existence de graphes avec un δ_{loc} linéaire

Cas de graphes bipartis

Nous utilisons le Lemme Local de Lovász (Lemme 3.23) sur les graphes bipartis aléatoires afin de prouver l'existence d'une famille infinie de graphes bipartis dont de degré minimum par complémentation local est linéaire par rapport au nombre de sommets.

Théorème 3.24. *Il existe $\nu_0 \in \mathbb{N}$ tel que pour tout $\nu > \nu_0$ il existe un graphe biparti G_ν d'ordre $n = 2\nu$ vérifiant*

$$\delta_{loc}(G_\nu) \geq 0.110n \tag{3.132}$$

Démonstration. Soit $G_B = (V, E)$ un graphe biparti d'ordre $n = 2\nu$ dont les deux ensembles indépendants V_1 et V_2 sont de taille ν. Chaque arête possible entre V_1 et V_2 existe avec probabilité $\frac{1}{2}$:

$$\forall (u_1, u_2) \in V_1 \times V_2, \quad Pr(\{u_1, u_2\} \in E) = \frac{1}{2} \tag{3.133}$$

Nous cherchons la plus grande valeur de c telle que

$$Pr\left(\delta_{loc}(G_B) \geq cn\right) > 0 \tag{3.134}$$

D'après la Propriété 3.1, cette inégalité est équivalente à la réalisation des événements

$$\text{“}|D \cup Odd(D)| > cn\text{”} \tag{3.135}$$

pour tout $D \subseteq V$.

Ici, le graphe G_B est biparti, et nous montrons alors que l'on peut se restreindre aux ensembles $D \subseteq V$ tels que $D \subseteq V_2$ ou $D \subseteq V_2$. En effet, pour tout ensemble $D \subseteq V$, on pose $D_1 = D \cap V_1$ et $D_2 = D \cap V_2$. G_B est biparti, donc $Odd(D_1) \subseteq V_2$. On a donc

$$D \cup Odd(D) = \big(D_1 \cup Odd(D_1)\big) \cup \big(D_2 \cup Odd(D_2)\big) \tag{3.136}$$

$$|D \cup Odd(D)| \geq |D_1 \cup Odd(D_1)| \tag{3.137}$$

de même $|D \cup Odd(D)| \geq |D_2 \cup Odd(D_2)|$. Ainsi, d'après la Propriété 3.1, on peut considérer uniquement les ensembles $D_1 \subseteq V_1$ et $D_2 \subseteq V_2$.

Dans le but d'appliquer le Lemme 3.23, on considère les “mauvais événements” suivants :

$$\begin{cases} A^1_D(\text{avec } D \subseteq V_1) : |D \cup Odd(D)| \leq cn \\ A^2_D(\text{avec } D \subseteq V_2) : |D \cup Odd(D)| \leq cn \end{cases} \tag{3.138}$$

On souhaite calculer $Pr(A^1_D)$ avec $D \subseteq V_1$. On pose $|D| = d\nu$ avec $0 < d < 1$. Par définition de G_B, pour tout $u \in V_2$ on a

$$Pr(\text{“}u \in Odd(D)\text{”}) = \frac{1}{2} \tag{3.139}$$

L'ensemble $D \subseteq V_1$ étant fixé, les événements “$u \in Odd(D)$” avec $u \in V_2$ sont mutuellement indépendants. Si l'événement “$|Odd(D)| \leq x$” est vrai, il y a au plus x sommets dans V_2 qui appartiennent à $Odd(D)$. Or on compte ν sommets dans V_2, d'où

$$Pr(\text{“}|Odd(D)| \leq x\text{”}) = \left(\frac{1}{2}\right)^{\nu} \sum_{k=0}^{x} \binom{\nu}{k} \tag{3.140}$$

$$\leq \left(\frac{1}{2}\right)^{\nu} 2^{\nu H\left(\frac{x}{\nu}\right)} \tag{3.141}$$

où la fonction $H : t \mapsto -t\log_2(t) - (1-t)\log_2(1-t)$ dénote l'entropie binaire. Pour revenir aux événements A^1_D, on a

$$Pr(A^1_D) = Pr(\text{“}|D \cup Odd(D)| \leq cn\text{”}) \tag{3.142}$$
$$= Pr(\text{“}|D| + |Odd(D)| \leq cn\text{”}) \tag{3.143}$$
$$= Pr(\text{“}|Odd(D)| \leq cn - |D|\text{”}) \tag{3.144}$$
$$\leq 2^{\nu(H(2c-d)-1)} \tag{3.145}$$

d'après l'expression (3.141).

On choisit à présent une pondération des mauvais événements de la forme

$$\sigma(A^1_D) = \sigma(A^1_D) = \frac{1}{r\binom{\nu}{d\nu}} \tag{3.146}$$

où r sera déterminé plus loin. Soit $p = \prod_{D' \in V_1, D'' \in V_2}(1 - \sigma(A^1_{D'}))(1 - \sigma(A^2_{D''}))$. On cherche à obtenir l'inégalité suivante pour pouvoir utiliser le Lemme 3.23 :

$$Pr(A^1_D) \leq \sigma(A^1_D)p \tag{3.147}$$

Réécrivons pour cela le produit p en regroupant les ensembles D' par leur taille :

$$p = \prod_{|D'|=1}^{\nu} \left(1 - \frac{1}{r\binom{\nu}{|D'|}}\right)^{2\binom{\nu}{|D'|}} \tag{3.148}$$
$$= \left[\prod_{|D'|=1}^{\nu} \left(1 - \frac{1}{r\binom{\nu}{|D'|}}\right)^{r\binom{\nu}{|D'|}}\right]^{\frac{2}{r}} \tag{3.149}$$

La fonction $f : x \mapsto \left(1 - \frac{1}{x}\right)^x$ vérifie $f(x) \geq \frac{1}{4}$ lorsque $x \geq 2$. Ains, quelque soit $r \geq 2$ on peut déduire

$$p \geq \left(\frac{1}{4}\right)^{\nu * \frac{2}{r}} = 2^{-\frac{4\nu}{r}} \tag{3.150}$$

En utilisant la borne $\binom{\nu}{d\nu} \leq 2^{\nu H\left(\frac{d\nu}{\nu}\right)}$, on remarque que

$$\sigma(A^1_D)p \geq \frac{1}{r\binom{\nu}{d\nu}} 2^{-\frac{4\nu}{r}} \tag{3.151}$$
$$\geq \frac{1}{r2^{\nu H\left(\frac{d\nu}{\nu}\right)}} 2^{-\frac{4\nu}{r}} = \frac{1}{r} 2^{-\frac{4\nu}{r} - \nu H(d)} \tag{3.152}$$

En combinant les inégalités (3.145) et (3.152), on obtient une condition suffisante pour réaliser la contrainte (3.147). Cette condition suffisante s'écrit de cette façon :

$$2^{\nu(H(2c-d)-1)} \leq \frac{1}{r} 2^{-\frac{4\nu}{r} - \nu H(d)} \tag{3.153}$$

En effet, le membre de gauche de cette inégalité est supérieur ou égal à $Pr(A_D^1)$ et le membre de droite et inférieur ou égal à $\sigma(A_D^1)p$. On applique la fonction logarithme à l'inégalité précédente puis on divise par ν. La condition suffisante devient

$$\frac{\log_2 r}{\nu} + H(d) + H(2c-d) - 1 + \frac{4}{r} \leq 0 \tag{3.154}$$

Prenons $r = \nu$ and $\nu \to +\infty$. La condition (3.154) devient alors asymptotiquement

$$H(d) + H(2c-d) - 1 \leq 0 \tag{3.155}$$

Cette inégalité doit être vérifiée quelque soit $d \in]0,1]$, donc également lorsque la fonction $d \mapsto H(d)+H(2c-d)-1$ est minimale. Des techniques usuelles montrent que ce minimum est atteint lorsque $d = c$. On a désormais un seul paramètre : le réel c. Une analyse numérique effectuée à l'aide du programme `sage` (voir annexe) montre que la valeur $c = 0.110$ satisfait la condition (3.147) lorsque $\nu > \nu_0$.

On raisonne de façon similaire pour montrer que

$$Pr(A_D^2) \leq \sigma(A_D^2)p \tag{3.156}$$

pour tout $D \subseteq V_2$.

A présent, on peut utiliser le Lemme Local de Lovasz (Lemme 3.23). Ainsi, on déduit

$$Pr\left(\{\overline{A_D^1} \mid D \in V_1\}, \{\overline{A_D^2} \mid D \in V_2\}\right) \geq p > 0 \tag{3.157}$$

d'où

$$Pr\left(\delta_{loc}(G_B) \geq cn\right) > 0 \tag{3.158}$$

pour tout $c \leq 0.110$ et pour $\nu > \nu_0$.

Nous avons donc prouvé l'existence d'au moins un graphe biparti G_B d'ordre n tel que

$$\delta_{loc}(G_B) \geq 0.110n \tag{3.159}$$

□

Cas général

Dans le cas général, les graphes tirés aléatoirement sans la contrainte de bipartition permettent d'améliorer la constante obtenue :

Théorème 3.25. *Il existe $n_0 \in \mathbb{N}$ tel que pour tout $n > n_0$ il existe un graphe G d'ordre n tel que*

$$\delta_{loc}(G) \geq 0.189n \tag{3.160}$$

Démonstration. Soit $G = (V, E)$ un graphe d'ordre n choisi aléatoirement de la façon suivante :

$$\forall (u, v) \in V^2, Pr(\{u, v\} \in E) = \frac{1}{2} \tag{3.161}$$

Nous cherchons la plus grande valeur de c telle que

$$Pr\left(\delta_{loc}(G) \geq cn\right) > 0 \tag{3.162}$$

et donc, par conséquent, telle que pour tout $D \subseteq V$,

$$|D \cup Odd(D)| > cn \tag{3.163}$$

d'après la Propriété 3.1.

Afin d'utiliser le Lemme Local de Lovász (Lemme 3.23), les événements que l'on souhaite éviter sont les suivants :

$$A_D : |D \cup Odd(D)| \leq cn \tag{3.164}$$

De façon évidente, nous ne considèrerons ici que les événements A_D avec $D \leq cn$.

Pour tout ensemble D tel que $|D| \leq cn$, nous établissons une borne supérieure pour la quantité $Pr(A_D)$. Soit $|D| = dn$ avec $d \in (0, c]$. Les arêtes de G sont choisies uniformément aléatoirement avec probabilité $\frac{1}{2}$, ainsi pour tout $u \in V \setminus D$,

$$Pr(\text{“}u \in Odd(D)\text{”}) = \frac{1}{2} \tag{3.165}$$

L'ensemble D étant fixé, les événements “$u \in Odd(D)$” avec $u \in V \setminus D$ sont indépendants. Ainsi, si l'événement A_D est vrai, il y a au plus $(c - d)n$ sommets dans $V \setminus D$ qui appartiennent à $Odd(D)$. Or on compte $(1 - d)n$ sommets dans $V \setminus D$, d'où

$$Pr(A_D) = \left(\frac{1}{2}\right)^{(1-d)n} \sum_{k=0}^{(c-d)n} \binom{(1-d)n}{k} \tag{3.166}$$

$$\leq \left(\frac{1}{2}\right)^{(1-d)n} 2^{(1-d)nH\left(\frac{c-d}{1-d}\right)} \tag{3.167}$$

$$\leq 2^{(1-d)n\left[H\left(\frac{c-d}{1-d}\right)-1\right]} \tag{3.168}$$

L'inégalité (3.167) est obtenue en utilisant une borne classique sur la somme des coefficients binomiaux.

Nous choisissons à présent les poids associés aux événements A_D pour utiliser le Lemme 3.23. Soit

$$\sigma(A_D) = \frac{1}{r\binom{n}{|D|}} \tag{3.169}$$

où r est un paramètre que l'on fixera ultérieurement. On pose également $p = \prod_{|D'|\leq cn}(1-\sigma(A_{D'}))$. On cherche à obtenir l'inégalité suivante :

$$Pr(A_D) \leq \sigma(A_D)p \tag{3.170}$$

Réécrivons le produit p :

$$p = \prod_{|D'|=1}^{cn} \left(1 - \frac{1}{r\binom{n}{|D'|}}\right)^{\binom{n}{|D'|}} \tag{3.171}$$

$$= \left[\prod_{|D'|=1}^{cn} \left(1 - \frac{1}{r\binom{n}{|D'|}}\right)^{r\binom{n}{|D'|}}\right]^{\frac{1}{r}} \tag{3.172}$$

De plus, la fonction $f : x \mapsto \left(1-\frac{1}{x}\right)^x$ vérifie $f(x) \geq \frac{1}{4}$ lorsque $x \geq 2$. Nous avons donc

$$p \geq \left(\frac{1}{4}\right)^{\frac{cn}{r}} \tag{3.173}$$

$$\geq 2^{-\frac{2cn}{r}} \tag{3.174}$$

pour tout $r \geq 2$. En utilisant la borne $\binom{n}{dn} \leq 2^{nH\left(\frac{dn}{n}\right)}$, on remarque que

$$\sigma(A_D)p \geq \frac{1}{r\binom{n}{|D|}} 2^{-\frac{2cn}{r}} \tag{3.175}$$

$$\geq \frac{1}{r2^{nH\left(\frac{dn}{n}\right)}} 2^{-\frac{2cn}{r}} = \frac{1}{r} 2^{-\frac{2cn}{r} - nH\left(\frac{dn}{n}\right)} \tag{3.176}$$

En combinant les inégalités (3.168) et (3.176), nous obtenons une condition suffisante pour réaliser la condition (3.170). Elle s'exprime ainsi :

$$2^{(1-d)n\left[H\left(\frac{c-d}{1-d}\right)-1\right]} \leq \frac{1}{r} 2^{-\frac{2cn}{r} - nH\left(\frac{dn}{n}\right)} \tag{3.177}$$

En effet, le membre de gauche de cette inégalité est supérieur ou égal à $Pr(A_D)$ et le membre de droite et inférieur ou égal à $\sigma(A_D)p$. Posons $r = n$, la condition précédente s'écrit alors

$$(1-d)\left[H\left(\frac{c-d}{1-d}\right) - 1\right] + H(d) + \frac{2c}{n} + \frac{\log_2 n}{n} \leq 0 \tag{3.178}$$

asymptotiquement, on a

$$(1-d)\left[H\left(\frac{c-d}{1-d}\right) - 1\right] + H(d) \leq 0 \tag{3.179}$$

Une analyse numérique effectuée à l'aide de `sage` (voir annexe) montre que cette condition est vraie lorsque $c \leq 0.189$ et pour tout d qui vérifie $0 < d \leq cn$. Ainsi, en prenant

par exemple $c = 0.189$, nous avons $Pr(A_D) \leq \sigma(A_D)p$ et nous pouvons utiliser le Lemme 3.23 pour déduire :

$$Pr\left(\left\{ \overline{A_D} \;\middle|\; |D| \leq cn \right\}\right) \geq p > 0 \tag{3.180}$$

La probabilité qu'aucun des "mauvais événements" A_D choisis au départ n'arrivent est donc non nulle, et nous pouvons conclure l'existence d'un graphe G d'ordre n tel que $\delta_{loc}(G) \geq 0.189n$ □

3.3.3 Existence de graphes avec un "petit" κ_Q

Précédemment, nous avons établi la NP-completude du problème **QKAPPA** (voir Figure 3.4), nous posons alors la question de l'existence de graphes dont la quantité κ_Q est "relativement petite". Dans le chapitre 2, nous avons construit une famille de graphes d'ordre n dont la valeur de κ_Q est inférieure à $n - n^{0.71}$ approximativement. Existe-t-il une famille infinie de graphes dont la valeur de κ_Q est inférieure à cn avec $c < 1$?

Nous prouvons dans cette partie l'existence d'une famille infinie de graphes $\{G_i\}$ tels que $\kappa_Q(G_i) \leq 0.811n_i$ où n_i est l'ordre de G_i. Tout comme dans la section 3.3, cette preuve s'appuie sur le Lemme Local de Lovász (Lemme 3.23). Dans un deuxième temps, nous montrons qu'un graphe G choisi au hasard vérifie avec forte probabilité $\kappa_Q(G) \leq c_0 n$ où $(c_0 < 1)$.

Prouvons tout d'abord le lemme suivant.

Lemme 3.26. *Soit $G = (V, E)$ un graphe et k un entier vérifiant $0 \leq k \leq n$. Si pour tout ensemble $D \subseteq V$ non vide on a*

$$\begin{cases} |D \cup Odd(D)| > n - k \\ |D \cup Even(D)| > n - k \end{cases} \tag{3.181}$$

alors

$$\kappa_Q(G) < k \tag{3.182}$$

Démonstration. D'après la première inégalité de (3.181) on peut écrire

$$\kappa'(G) > n - k \tag{3.183}$$

Soit $B \subseteq V$ tel que $|B| \geq k$. Supposons que B est non-WOD. Il existe alors un ensemble $C \subseteq V \setminus B$ tel que $B \subseteq Odd(C)$. Ainsi $Even(C) \subseteq V \setminus B$, ce qui se traduit par

$$|C \cup Even(C)| \leq n - k \tag{3.184}$$

Cela contredit la deuxième inégalité de (3.181). B est donc un ensemble WOD de taille k, ainsi

$$\kappa(G) < k \tag{3.185}$$

La caractérisation donnée dans le Lemme 3.13 permet de conclure. □

Etablissons à présent le résultat principal de cette section à l'aide du Lemme 3.23 :

Théorème 3.27. *Il existe une famille infinie de graphes $\{G_i\}$ tels que*

$$\kappa_Q(G_i) \leq 0.811 n_i \tag{3.186}$$

où n_i est l'ordre de G_i.

Démonstration. Soit $G(n, \frac{1}{2}) = (V, E)$ un graphe aléatoire tiré de la façon suivante : V est un ensemble de sommet de taille n. On souhaite montrer que pour tout ensemble de sommets $D \subseteq V$ et pour une constante $c < 1$ que l'on déterminera on a

$$Pr\left(\text{“}\kappa_Q(G) < cn\text{”}\right) > 0 \tag{3.187}$$

Afin d'utiliser le Lemme 3.23, on construit les “mauvais événements” suivants : pour tout $D \subseteq V$, on définit

$$\begin{cases} A_D = \text{“}|D \cup Odd(D)| \leq (1-c)n\text{”} \\ A'_D = \text{“}|D \cup Even(D)| \leq (1-c)n\text{”} \end{cases} \tag{3.188}$$

D'après le Lemme 3.26, si aucun des événements A_D et A'_D n'a lieu, on a bien $\kappa_Q(G) < cn$. On remarque tout d'abord que lorsque $|D| > (1-c)n$ on a $Pr(A_D) = Pr(A'_D) = 0$. Il suffit donc de considérer seulement les événements A_D et A'_D pour lesquels $|D| \leq (1-c)n$.

Pour tout $D \subseteq V$ tel que $|D| \leq (1-c)n$, essayons d'obtenir une borne supérieure pour la quantité $Pr(A_D)$ (on raisonnera de façon similaire pour $Pr(A'_D)$. On note $|D| = dn$ pour une certaine constant $d \in]0, 1-c]$. Les arêtes de $G(n, \frac{1}{2})$ étant tirées indépendamment avec probabilité $\frac{1}{2}$, on a, pour tout $u \in V \setminus B$

$$Pr(\text{“}u \in Odd(D)\text{”}) = \frac{1}{2} \tag{3.189}$$

Pour un ensemble D fixé, les événements “$u \in Odd(D)$” sont indépendants. Ainsi, l'événement A_D est vérifié lorsque au plus $(1-c-d)n$ sommets de $V \setminus D$ sont contenus dans $Odd(D)$. Or on compte $(1-d)n$ sommets dans $V \setminus D$, on peut donc écrire

$$Pr(A_D) = \left(\frac{1}{2}\right)^{(1-d)n} \sum_{k=0}^{(1-c-d)n} \binom{(1-d)n}{k} \tag{3.190}$$

$$\leq \left(\frac{1}{2}\right)^{(1-d)n} 2^{(1-d)nH\left(\frac{1-c-d}{1-d}\right)} \tag{3.191}$$

$$\leq 2^{(1-d)n\left[H\left(\frac{c}{1-d}\right)-1\right]} \tag{3.192}$$

où H est la fonction d'entropie binaire présentée dans la preuve des Théorèmes 3.24 et 3.25. On montre de même que

$$Pr(A'_D) \leq 2^{(1-d)n\left[H\left(\frac{c}{1-d}\right)-1\right]} \tag{3.193}$$

On choisit d'associer à chaque événement la pondération suivante : pour tout ensemble D tel que $0 < |D| \leq (1-c)n$, on pose

$$\sigma(A_D) = \sigma(A'_D) = \frac{1}{r\binom{n}{|D|}} \tag{3.194}$$

En faisant appel à des méthodes similaires à celles utilisées dans la preuve des Théorèmes 3.24 et 3.25, on montre que la condition asymptotique

$$(1-d)\left[H\left(\frac{c}{1-d}\right) - 1\right] + H(d) \leq 0 \tag{3.195}$$

obtenue en prenant en prenant $r = n$ est une condition suffisante pour assurer que

$$\begin{cases} Pr(A_D) \leq \sigma(A_D) \prod_{|D'| \leq (1-c)n} (1 - \sigma(A_{D'}))(1 - \sigma(A'_{D'})) \\ Pr(A'_D) \leq \sigma(A'_D) \prod_{|D'| \leq (1-c)n} (1 - \sigma(A_{D'}))(1 - \sigma(A'_{D'})) \end{cases} \tag{3.196}$$

Des méthodes d'analyse numérique ainsi que l'utilisation du programme `sage` (voir annexe) montrent que la condition (3.195) est vérifiée pour tout $c > 0.811$ ainsi que pour tout $d \in]0, 1-c]$. On peut ainsi utiliser le Lemme 3.23 pour déduire que pour tout $c > 0.811$,

$$Pr(\kappa_Q(G) < cn) > 0 \tag{3.197}$$

Il existe donc une famille infinie de graphes G_i d'ordre n_i tels que

$$\kappa_Q(G_i) \leq 0.811 n_i \tag{3.198}$$

□

3.3.4 κ_Q d'un graphe aléatoire

De récents travaux [Sar12] ont établi une correspondance entre le protocoles de partage de secret construits à partir d'états graphes et les codes quantiques. Ces résultats combinés avec la borne de Gilbert Varshamov sur les codes stabilisateurs [FM04] peuvent fournir une preuve alternative au Théorème 3.27. L'utilisation du Lemme Local de Lovász [Lov75] et des méthodes probabilistes utilisées ici présentent quant à eux plusieurs avantages : les preuves effectuées sont basées sur des arguments purement graphiques et présentent une extension potentielle pour construire de "bons" protocoles de partage de secret quantique, notamment grâce aux avancées récentes sur une version algorithmique du Lemme Local de Lovász [MT10].

De plus, l'utilisation de méthodes probabilistes offrent déjà un moyen de générer des protocoles de partage de secret quantique possédant un seuil particulièrement bas en ajustant les paramètres du Lemme Local de Lovász :

Théorème 3.28. *Il existe $n_0 \in \mathbb{N}$ tel que pour tou $n > n_0$ un graphe aléatoire $G\left(n, \frac{1}{2}\right)$ vérifie*

$$Pr\left(\kappa_Q\left(G\left(n, \frac{1}{2}\right)\right) \leq 0.811n\right) \leq 1 - \frac{1}{n} \tag{3.199}$$

avec probabilité supérieure à $1 - \frac{1}{n}$.

Démonstration. On notera $G = G\left(n, \frac{1}{2}\right)$ pour une meilleure lisibilité.

Nous utilisons des techniques similaires à celles utilisées dans la preuve du Théorème 3.27. On choisit de même les mauvais événement A_D et A'_D de l'expression (3.188) et les pondérations associées sont celles de l'expression (3.194). La condition suffisante pour l'application du Lemme 3.23 que l'on obtient est la suivante :

$$(1-d)\left[H\left(\frac{c}{1-d}\right) - 1\right] + H(d) + \frac{4(1-c)}{r} + \frac{\log(r)}{n} \leq 0 \tag{3.200}$$

On fixe les paramètres c et r de la façon suivante :

$$\begin{cases} c = 0.811 \\ r = 4\ln(2)(1-c)n^2 \end{cases} \tag{3.201}$$

Une analyse numérique effectuée à l'aide de `sage` (voir annexe) montre que pour tout $n \geq 26681$, la condition (3.200) est vérifiée. Ainsi pour tout ensemble D de sommets de $G\left(n, \frac{1}{2}\right)$ tel que $0 < |D| \leq (1-c)n$ la condition (3.196) est vérifiée et on peut donc appliquer le Lemme 3.23. On obtient donc

$$Pr\left(\text{“}\kappa_Q(G) \leq 0.811n\text{”}\right) \geq p \tag{3.202}$$

où $p = \prod_{|D'| \leq (1-c)n}(1 - \sigma(A_{D'}))(1 - \sigma(A'_{D'}))$. L'expression (3.202) s'écrit ainsi

$$Pr\left(\text{“}\kappa_Q(G) \leq 0.811n\text{”}\right) \geq \left(\frac{1}{4}\right)^{\frac{2}{r}(1-c)n} \tag{3.203}$$

$$\geq \left(\frac{1}{4}\right)^{\frac{1}{2n\ln(2)}} \tag{3.204}$$

$$\geq e^{-\frac{1}{n}} \geq 1 - \frac{1}{n} \tag{3.205}$$

□

Ce théorème fournit donc une méthode pour construire un graphe d'ordre n dont la valeur de la quantité κ_Q est inférieure à $0.811n$ avec forte probabilité (qui tend vers 1 lorsque $n \to \infty$). Cependant, puisque le problème **QKAPPA** est NP-complet (Théorème 3.18), il est impossible de fournir un algorithme déterministe efficace qui vérifie si un graphe G quelconque vérifie effectivement la propriété attendue $\kappa_Q(G) \leq 0.811n$, sauf si $P = NP$.

3.4 Conclusion

Après avoir défini et établi des propriétés générales des quantités κ et κ', nous avons montré un lien avec les seuils atteignables par les protocoles qQSS* définis dans le Chapitre 2. Ces quantités permettent également de déterminer le plus petit degré par complémentation locale d'un graphe donné, quantité étudiée dans le domaine de la théorie des graphes et également utile en calcul quantique [RB01, BFK09].

Nous avons montré que les problèmes de décision associés à toutes ces quantités sont NP-complets, et il n'existe également pas d'algorithme d'approximation pour le calcul du plus petit degré par complémentation locale, sauf si P=NP.

L'utilisation de méthodes probabilistes montre l'existence de famille infinies de graphes dont le degré minimum par complémentation locale est linéaire en l'ordre du graphe. Nous avons également montré, grâce à ces méthodes, l'existence de protocoles qQSS* dont le seuil représente une proportion constante du nombre de joueurs impliqués.

Ces derniers résultats semblent prometteurs puisqu'ils ouvrent la possibilité de construction de familles explicites qui possèdent ces mêmes propriétés. Le chapitre suivant présente d'ailleurs une famille de graphes qui semblent être de bons candidats pour ces propriétés.

Chapitre 4

Etude de propriétés locales des graphes de Paley

Ce chapitre présente l'étude de certaines propriétés des graphes de Paley. Cette famille peut être exploitée dans le domaine du partage de secret quantique (Chapitre 2) et représente un support particulièrement intéressant pour la question de la recherche du degré minimum par complémentation locale (Chapitre 3). Ces graphes sont également intéressants en terme d'intrication quantique [AM13].

Dans un premier temps, nous prouvons que les graphes de Paley représentent la famille explicite ayant le plus grand degré minimum par complémentation locale connu à ce jour. De plus, une conjecture de géométrie algébrique laisse à penser qu'une sous famille de ces graphes est candidate pour atteindre un degré minimum par complémentation locale linéaire en l'ordre du graphe.

Enfin, cette étude utilise une quantité définie pour chaque ensemble de sommets appelée "déséquilibre" qui présente un lien direct avec le seuil que ces graphes permettent d'atteindre en terme de protocoles de partage de secret quantique à seuil à partir d'états graphes.

Les résultats présentés dans les trois premières sections ont été publiés [JMP12b]. La dernière section présente un aspect plus exploratoire : nous proposons une approche liant dépendances linéaires et propriétés algébriques pour le calcul des valeurs du déséquilibre des ensembles de sommets des graphes de Paley. Son objectif est l'amélioration de la borne que nous avons établie [JMP12b] et présentée en section 4.2.

4.1 Introduction

Les graphes de Paley ont été introduits indépendamment par Sachs [Sac62] et Erdös et Renyi [ER63]. Ils sont définis algébriquement à partir des résidus quadratiques dans les

corps finis. Nous rappelons quelques définitions préalables.

Définition 4.1. *Pour tout p premier, soit $\mathbb{F}_p$ le corps fini à p éléments. Un élément $a \in \mathbb{F}_p$ est dit "résidu quadratique" lorsque*

$$\exists x \in \mathbb{F}_p \text{ tel que } x^2 = a \tag{4.1}$$

Définition 4.2. *Soit p un entier premier. Le caractère de Legendre χ_L désigne le morphisme suivant :*

$$\chi_L : \mathbb{F}_p \to \{-1, 0, 1\} \tag{4.2}$$

$$x \mapsto x^{\frac{p-1}{2}} \tag{4.3}$$

Ce caractère est utilisé pour déterminer si un élément de $\mathbb{F}_p$ est un résidu quadratique ou non. En effet, nous avons la propriété suivante :

Propriété 4.1. $\forall x \in \mathbb{F}_p$,

$$\begin{cases} \chi_L(x) = 1 \Leftrightarrow x \text{ est un résidu quadratique non nul} \\ \chi_L(x) = -1 \Leftrightarrow x \text{ n'est pas un résidu quadratique} \\ \chi_L(x) = 0 \Leftrightarrow x = 0 \end{cases} \tag{4.4}$$

Le caractère de Legendre est un caractère multiplicatif :

Propriété 4.2. $\forall a, b \in \mathbb{F}_p$,

$$\chi_L(ab) = \chi_L(a)\chi_L(b) \tag{4.5}$$

La famille des graphes de Paley d'ordre p est définie à partir des résidus quadratiques dans $\mathbb{F}_p$:

Définition 4.3. *Soit p un entier premier tel que $p = 1 \bmod 4$. Le graphe de Paley $Pal_p = (V, E)$ est le graphe d'ordre p défini de la façon suivante :*
– $V = \mathbb{F}_p$
– $\forall (a, b) \in V^2$, $\{a, b\} \in E \Leftrightarrow \chi_L(b - a) = 1$

La contrainte $p = 1 \bmod 4$ nous assure que pour tout $(a, b) \in \mathbb{F}_p^2$, $\chi_L(b - a) = \chi_L(a - b)$. Le graphe de Paley Pal_p ainsi défini est donc un graphe non orienté et sans boucle.

Il est à noter qu'environ la moitié des entiers premiers p vérifient la condition $p = 1 \bmod 4$.

Parmi les propriétés des graphes de Paley, on notera les suivantes :

Propriété 4.3. *Le graphe de Paley Pal_p est fortement régulier de paramètres $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$. Cela signifie :*
– *Pal_p est d'ordre p*

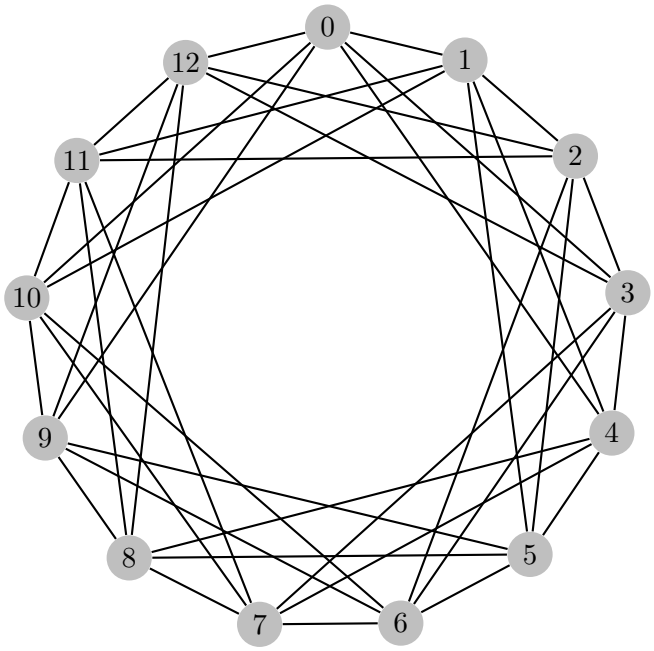

FIGURE 4.1 – Graphe de Paley d'ordre 13 : les résidus quadratiques dans $\mathbb{F}_{13}$ sont ± 1, ± 3 et ± 4, ainsi le sommet x est relié aux sommets $x \pm 1$, $x \pm 3$ et $x \pm 4$.

- *Chaque sommet est de degré* $\frac{p-1}{2}$
- *Deux sommets voisins ont toujours* $\frac{p-5}{4}$ *voisins communs*
- *Deux sommets non-voisins ont toujours* $\frac{p-1}{4}$ *voisins communs*

La Figure 4.1 décrit le graphe de Paley d'ordre 13.

4.2 Degré minimum par complémentation locale des graphes de Paley

4.2.1 Borne inférieure pour $\delta_{loc}(Pal_p)$

Il est difficile de construire des graphes dont le degré minimum par complémentation locale (Définition 3.2) est "relativement élevé". A titre d'exemple, le degré minimum par complémentation locale des hypercubes a été calculé dans [HMP06] et se trouve être logarithmique en l'ordre de l'hypercube. Une construction étendue à partir des hypercubes a permis de construire une famille de graphes dont le degré minimum par complémentation locale est polylogarithme en n, l'ordre du graphe.

Nous considérons ici la famille des graphes de Paley d'ordre p (Pal_p) où p est un entier premier vérifiant $p = 1 \bmod 4$. Nous montrons ici que le degré minimum par

complémentation locale de Pal_p est supérieur à $\sqrt{p}$. Cette valeur est une borne inférieure, et on ne sait pas si elle est atteinte.

Les graphes de Paley constituent, à notre connaissance, la famille constructive de graphes dont le degré minimum par complémentation locale est le plus élevé :

Théorème 4.4. *Pour tout entier premier p qui vérifie $p = 1 \bmod 4$,*

$$\delta_{loc}(Pal_p) > \sqrt{p} - \frac{3}{2} \tag{4.6}$$

Les résultats que nous établissons dans la suite de cette section permettront de prouver ce théorème.

Rappelons tout d'abord que le degré minimum par complémentation locale d'un graphe G est lié à ses sous-ensembles de sommets D de la façon suivante (Propriété 3.1) :

$$\delta_{loc}(G) = \min \left\{ \ |D \cup Odd(D)| \ \middle| \ D \neq \varnothing, D \subseteq V(G) \ \right\} - 1 \tag{4.7}$$

Il suffit alors de donner, dans les graphes de Paley, une borne sur les ensembles de la forme $S \cup Odd(S)$ où $S \subseteq \mathbb{F}_p$ est un ensemble de sommets de Pal_p afin d'obtenir une borne sur $\delta_{loc}(Pal_p)$. Le résultat suivant établit un premier lien entre la taille des ensembles de cette forme.

Au préalable, pour tout ensemble $S \subseteq \mathbb{F}_p$ nous définissons le polynôme $f_S \in \mathbb{F}_p[X]$:

$$f_S(X) = \prod_{j \in S} (X - j) \tag{4.8}$$

Lemme 4.5. *Soit $S \subseteq \mathbb{F}_p$ un ensemble de sommets de Pal_p, le graphe de Paley d'ordre p. L'égalité suivante est alors vérifiée :*

$$\left| \sum_{i=0}^{p-1} \chi_L \left(f_S(i) \right) \right| = \big| \, |S \cup Odd(S)| - |S \cup Even(S)| \, \big| \tag{4.9}$$

Démonstration. La multiplicativité du caractère de Legendre (Propriété 4.2) permet d'écrire

$$\left| \sum_{i=0}^{p-1} \chi_L \left(f_S(i) \right) \right| = \left| \sum_{i=0}^{p-1} \prod_{j \in S} \chi_L(i-j) \right| \tag{4.10}$$

Si $i \in S$, la quantité $\prod_{j \in S} \chi_L(i-j)$ est nulle. Les termes restants dans la somme du membre de droite de l'équation précédente sont donc ceux pour lesquels $i \notin S$.

D'après la Propriété 4.1, $\chi_L(i-j) = 1$ lorsque $i-j$ est un résidu quadratique, c'est-à-dire lorsque les sommets i et j sont voisins dans le graphe de Paley Pal_p. Ainsi,

$$\left| \sum_{i=0}^{p-1} \chi_L \left(f_S(i) \right) \right| = \left| \sum_{i \notin S} (-1)^{|S| - |\mathcal{N}(i) \cap S|} \right| \tag{4.11}$$

Si $i \in Even(S) \setminus S$, $|S| - |\mathcal{N}(i) \cap S| = |S| \bmod 2$. Si $i \in Odd(S) \setminus S$, $|S| - |\mathcal{N}(i) \cap S| = |S| + 1 \bmod 2$. L'équation (4.11) s'écrit alors

$$\left|\sum_{i=0}^{p-1} \chi_L\left(f_S(i)\right)\right| = \left|\sum_{i \in Even(S)\setminus S} (-1)^{|S|} - \sum_{i \in Odd(S)\setminus S} (-1)^{|S|}\right| \tag{4.12}$$

$$= \big|\, |Even(S) \setminus S| - |Odd(S) \setminus S| \,\big| \tag{4.13}$$

Cette dernière expression s'écrit aussi

$$\left|\sum_{i=0}^{p-1} \chi_L\left(f_S(i)\right)\right| = \big|\, |S \cup Odd(S)| - |S \cup Even(S)| \,\big| \tag{4.14}$$

□

Nous avons établi un lien entre le polynôme $f_S \in \mathbb{F}_p[X]$ défini en (4.8) et les voisinages pair et impair de l'ensemble S associé sur le graphe Pal_p.

L'équation (4.9) fait intervenir la différence de cardinalité entre le voisinage impair et le voisinage pair d'un ensemble $S \subseteq \mathbb{F}_p$ d'un graphe de Paley. Nous introduisons ainsi la notion de "déséquilibre" d'un tel ensemble S :

Définition 4.4. *Pour tout $S \subseteq \mathbb{F}_p$, on appelle "déséquilibre" de S la quantité*

$$T(S) = \sum_{x \in \mathbb{F}_p} \chi_L(f_S(x)) \tag{4.15}$$

A présent, nous tirons parti du fait que les graphes de Paley sont définis algébriquement (Définition 4.3) pour établir un lien entre ces graphes et des résultats de géométrie algébrique. L'étude des courbes hyperelliptiques sur les corps finis permet, de cette façon, de déduire des propriétés liées aux sous-ensembles de sommets des graphes de Paley.

Rappelons brièvement la définition d'une courbe hyperelliptique :

Définition 4.5. *Soit $\mathbb{K}$ un corps et $P \in \mathbb{K}[X]$ un polynôme de degré supérieur ou égal à 4. On appelle* courbe hyperelliptique *sur $\mathbb{K}$ l'ensemble de paires $(x, y) \in \mathbb{K}^2$ qui vérifient*

$$y^2 = P(x) \tag{4.16}$$

Pour tout entier premier p fixé et pour tout ensemble $S \subseteq \mathbb{F}_p$, on considère alors la courbe hyperelliptique Γ_S d'équation

$$y^2 = f_S(x) \tag{4.17}$$

où f_S est le polynôme défini en (4.8).

Le calcul du nombre de points des courbes elliptiques et hyperelliptiques est une question fondamentale en géométrie algébrique, et une borne inférieure a été prouvée dans [Wei48]. Il s'agit d'ailleurs d'un résultat primordial sur les courbes elliptiques et hyperelliptiques.

La Proposition 1 de [Joy06] propose une reformulation de cette borne. Elle s'exprime alors de la façon suivante en y incluant la notation de la Définition 4.4 :

Lemme 4.6 ([Joy06], Proposition 1)**.** *Pour tout ensemble non-vide $S \subseteq \mathbb{F}_p$, on a*

$$|T(S)| \leq (|S| - 1)\sqrt{p} + 1 \tag{4.18}$$

Nous utilisons ce lemme afin de prouver une borne sur les ensembles de sommets du type $S \cup Odd(S)$ et $S \cup Even(S)$ avec $S \subseteq \mathbb{F}_p$ dans les graphes de Paley.

Lemme 4.7. *Soit Pal_p le graphe de Paley d'ordre p. Pour tout $S \subseteq \mathbb{F}_p$, $S \neq \varnothing$, on a*

$$\min\left\{ |S \cup Odd(S)|, |S \cup Even(S)| \right\} > \sqrt{p} - \frac{1}{2} \tag{4.19}$$

Démonstration. Supposons que l'on ait $|S \cup Odd(S)| \leq |S \cup Even(S)|$ (dans le cas contraire, un raisonnement similaire est utilisé). On souhaite alors montrer que

$$\sqrt{p} - \frac{1}{2} < |S \cup Odd(S)| \tag{4.20}$$

On remarque tout d'abord que

$$|S \cup Odd(S)| + |S \cup Even(S)| = p + |S| \tag{4.21}$$

en effet, l'ensemble S est compté deux fois car il correspond à l'intersection des deux ensembles dont on somme les cardinaux.

Ensuite, d'après le Lemme 4.5,

$$|S \cup Odd(S)| - |S \cup Even(S)| = -|T(S)| \tag{4.22}$$

En additionnant les deux égalités (4.21) et (4.22), on obtient

$$p + |S| - |T(S)| = 2|S \cup Odd(S)| \tag{4.23}$$

Le Lemme 4.6 permet alors d'écrire

$$p + |S| - (|S| - 1)\sqrt{p} - 1 \leq 2|S \cup Odd(S)| \tag{4.24}$$

Si $|S| < \sqrt{p}$, le membre de gauche de l'égalité (4.24) peut être minoré :

$$\begin{aligned} p + |S| - (|S| - 1)\sqrt{p} - 1 &= p + |S|(1 - \sqrt{p}) + \sqrt{p} - 1 && (4.25)\\ &> p + \sqrt{p}(1 - \sqrt{p}) + \sqrt{p} - 1 && (4.26)\\ &> 2\sqrt{p} - 1 && (4.27) \end{aligned}$$

Dans ce cas on obtient bien l'inégalité (4.20).

Si $|S| \geq \sqrt{p}$, l'inégalité (4.20) est trivialement vérifiée.

□

Revenons à présent à la preuve du **Théorème 4.4 :**

Preuve du Théorème 4.4. Le Lemme 4.7 ainsi que l'équation (4.7) nous permettent de conclure sur la valeur du degré minimum par complémentation locale des graphes de Paley :

$$\delta_{loc}(Pal_p) > \sqrt{p} - \frac{3}{2} \tag{4.28}$$

Cela termine donc la preuve du Théorème 4.4. □

Les graphes de Paley constituent la famille de graphes possédant le plus grand degré par complémentation locale connue.

L'existence de graphes dont le degré minimum par complémentation locale est linéaire en l'ordre du graphe a été prouvée dans le Chapitre 3. Nous pouvons ainsi nous demander si les graphes de Paley représentent de bons candidats pour cette propriété.

4.3 Conjecture de Bazzi-Mitter et partage de secret

Nous explicitons une relation entre le degré minimum par complémentation locale et une quantité définie algébriquement, le "déséquilibre" (Définition 4.4), dans les graphes de Paley.

Il est à noter que l'ensemble $\mathbb{F}_p$ est l'ensemble des sommets de Pal_p, ainsi tout ensemble $S \subseteq \mathbb{F}_p$ désigne également un ensemble de sommets de Pal_p.

L'équation (4.23) ainsi que la caractérisation du degré minimum par complémentation locale rappelée en (4.7) permettent d'exprimer une relation entre le degré minimum par complémentation locale de Pal_p et le déséquilibre $T(S)$ des sous-ensembles de $\mathbb{F}_p$:

$$\frac{p + |S| - |T(S)|}{2} = |S \cup Odd(S)| \tag{4.29}$$

sous l'hypothèse $|S \cup Odd(S)| \leq |S \cup Even(S)|$. Dans le cas contraire on a

$$\frac{p + |S| - |T(S)|}{2} = |S \cup Even(S)| \tag{4.30}$$

$$\leq |S \cup Odd(S)| \tag{4.31}$$

On peut donc déduire la borne suivante :

$$\delta_{loc}(Pal_p) \geq \frac{1}{2}\left(\min_S\{p + |S| - |T(S)|\}\right) - 1 \tag{4.32}$$

$$\geq \frac{p}{2} - \frac{1}{2}\max_S\left\{|T(S)| - |S|\right\} - 1 \tag{4.33}$$

De cette façon, l'étude du déséquilibre des ensembles $S \subseteq \mathbb{F}_p$ fournit une borne inférieure sur la valeur de $\delta_{loc}(Pal_p)$.

4.3.1 Conjecture de Bazzi-Mitter

Nous avons prouvé dans la section 4.2 que le degré minimum par complémentation locale des graphes de Paley est supérieur à $\sqrt{p}$ où p est l'ordre du graphe. Est-il alors possible d'améliorer cette borne inférieure ? De façon plus précise, la valeur de $\delta_{loc}(Pal_p)$ est-elle linéaire en p ?

Une conjecture de géométrie algébrique, la conjecture de Bazzi-Mitter [BM06], nous laisse penser qu'une sous-famille infinie des graphes de Paley possède un degré minimum par complémentation locale linéaire en l'ordre des graphes. Détaillons cette connexion.

La conjecture de Bazzi-Mitter peut se formuler de la façon suivante :

Conjecture 4.1 ([BM06])**.** *Il existe un réel $c < 2$ tel qu'une infinité de premiers p vérifient :*

$$\forall S \subseteq \mathbb{F}_p, \quad |\Gamma_S| \leq cp \tag{4.34}$$

où Γ_S désigne la courbe définie en (4.8).

Tout comme il est rappelé dans [Joy06], le nombre de points rationnels de Γ_S est lié au déséquilibre $T(S)$ de la façon suivante :

Propriété 4.8 ([Wei48])**.** *Pour tout p premier et $S \subseteq \mathbb{F}_p$,*

$$T(S) = \begin{cases} -p - 2 + |\Gamma_S| & \textit{si } |S| \textit{ est pair} \\ -p - 1 + |\Gamma_S| & \textit{si } |S| \textit{ est impair} \end{cases} \tag{4.35}$$

D'après cette propriété, pour tout $S \subseteq \mathbb{F}_p$ nous pouvons écrire

$$T(S) \leq -p + |\Gamma_S| \leq (c-1)p \tag{4.36}$$

Sous la Conjecture 4.1 (Bazzi-Mitter), si $p = 1 \bmod 4$, nous avons une relation entre la valeur de $|T(S)|$ et la valeur de $\delta_{loc}(Pal_p)$ dans l'équation (4.32), ainsi sous la Conjecture 4.1

$$\delta_{loc}(Pal_p) \geq \frac{p + |S| - (c-1)p}{2} \tag{4.37}$$

$$\geq \frac{2-c}{2}p \tag{4.38}$$

Puisque $c < 2$, on a $0 < \frac{2-c}{2}$.

Nous émettons alors une conjecture qui découle de l'expression (4.38) ainsi que de la Conjecture 4.1 (Bazzi-Mitter) en ajoutant la contrainte $p = 1 \bmod 4$:

Conjecture 4.2. *Il existe une infinité de nombres premiers p avec $p = 1 \bmod 4$ et une constante $\alpha > 0$ tels que*

$$\delta_{loc}(Pal_p) \geq \alpha p \tag{4.39}$$

Par conséquent, l'utilisation de cette même famille pour l'établissement de protocoles de partage de secret quantique avec des états graphes présentés dans le Chapitre 2 permettrait d'atteindre un seuil de la forme $((p, \beta p))$ où $\beta = 1 - \alpha < 1$. En effet, le graphe Pal_p vérifie $\overline{Pal_p} = Pal_p$. De plus, la correspondance entre la quantité κ et le seuil d'un protocole cQSS énoncée dans le Chapitre 3 ainsi que l'inégalité $\delta_{loc}(G) \leq \kappa(G)$ pour tout graphe G permettent de réaliser un protocole de partage de secret quantique de seuil βp.

4.4 Propriétés sur les sous-ensembles de sommets des graphes de Paley

Dans la section précédente, nous avons présenté un lien entre le degré minimum par complémentation locale des graphes de Paley et le déséquilibre de leurs sous-ensembles de sommets (Définition 4.4). Cette partie est donc consacrée à l'étude de cette quantité.

Dans toute cette section, p désigne un entier premier vérifiant $p = 1 \bmod 4$. On notera également Q l'ensemble des résidus quadratiques non nuls et N l'ensemble des non-résidus :

$$\mathbb{F}_p = Q \cup N \cup \{0\} \tag{4.40}$$

4.4.1 Premières Propriétés

Nous cherchons ici à étudier le déséquilibre $T(S)$ pour tous les ensembles $S \subseteq \mathbb{F}_p$. Il est possible de calculer $T(S)$ pour certains ensembles S particuliers, et cette partie est dédiée à ces calculs.

Nous introduisons deux quantités utilisées dans la suite :

$$\begin{cases} T_Q(S) &= \sum_{x \in Q} \chi_L\big(f_S(x)\big) \\ T_N(S) &= \sum_{x \in N} \chi_L\big(f_S(x)\big) \end{cases} \tag{4.41}$$

Elles représentent les sommes partielles des caractères de legendre sur les ensembles Q et N. On a notamment

$$T(S) = T_Q(S) + T_N(S) + \chi_L\big(f_S(0)\big) \tag{4.42}$$

Commençons par établir le lemme suivant :

Lemme 4.9. *Soit $S \subseteq \mathbb{F}_p$.*

$$T(S) = \sum_{x \notin S} \chi_L\big(f_S(x)\big) \tag{4.43}$$

Démonstration. Revenons à la définition de $T(S)$ (Définition 4.4) :

$$T(S) = \sum_{x \in \mathbb{F}_p} \chi_L\big(f_S(x)\big) \tag{4.44}$$

$$= \sum_{x \in S} \chi_L\big(f_S(x)\big) + \sum_{x \notin S} \chi_L\big(f_S(x)\big) \tag{4.45}$$

Par construction de f_S (4.8), si $x \in S$ alors $f_S(x) = 0$. La Définition 4.2 du caractère de Legendre permet donc de vérifier l'équation (4.43) □

Calculons la valeur de $T(S)$ lorsque S est un singleton :

Propriété 4.10. *Soit $a \in \mathbb{F}_p$.*

$$T(a) = 0 \tag{4.46}$$

où $T(a)$ désigne $T(\{a\})$ afin d'alléger la notation.

Démonstration. Revenons à la définition :

$$T(a) = \sum_{x \in \mathbb{F}_p} \chi_L\big(x - a\big) \tag{4.47}$$

$$= \sum_{x \in \mathbb{F}_p} \chi_L\big(x\big) \tag{4.48}$$

$$= |Q| - |N| \tag{4.49}$$

L'équation (4.48) est obtenue suite à un changement de variable. En théorie des nombres, il est connu que $|Q| = |N|$ (voir [IR90] par exemple) On peut donc déduire l'équation (4.46). □

D'après la Définition 4.4 et l'équation (4.9), la quantité $T(S)$ désigne, en valeur absolue, la différence entre la taille du voisinage impair et celle du voisinage pair de l'ensemble S. Une interprétation de la Propriété 4.10 est que chaque sommet du graphe Pal_p possède

autant de voisins que de non-voisins. Ceci est expliqué par le fait que Pal_p est un graphe $\frac{p-1}{2}$-régulier d'ordre p (Propriété 4.3).

Regardons à présent le cas de l'ensemble complémentaire du précédent, c'est-à-dire lorsque $S = \mathbb{F}_p \setminus \{a\}$.

Propriété 4.11. *Soit $a \in \mathbb{F}_p$.*

$$T(\overline{a}) = 1 \tag{4.50}$$

où $\overline{a}$ désigne $\mathbb{F}_p \setminus \{a\}$.

Démonstration.

$$T(\overline{a}) = \sum_{x \in \mathbb{F}_p} \prod_{u \neq a} \chi_L\big(x - u\big) \tag{4.51}$$

$$\tag{4.52}$$

D'après le Lemme 4.9, seul le terme correspondant à a est non nul :

$$T(\overline{a}) = \prod_{u \neq a} \chi_L\big(a - u\big) \tag{4.53}$$

$$= \prod_{u \in \mathbb{F}_p^*} \chi_L\big(u\big) \tag{4.54}$$

$$= (-1)^{|N|} = 1 \tag{4.55}$$

En effet, $p = 1 \bmod 4$ donc $|N| = \frac{p-1}{2} = 0 \mod 2$. □

A présent, afin de calculer la valeur de T sur les ensembles de taille supérieure, nous établissons un lemme sur les quantités T_Q et T_N définies en (4.41) :

Lemme 4.12. *Pour tout $a \in \mathbb{F}_p^*$,*

$$T_Q(a) = \frac{-1 - \chi_L\big(a\big)}{2} \tag{4.56}$$

$$T_N(a) = \frac{1 - \chi_L\big(a\big)}{2} \tag{4.57}$$

Démonstration. Soit g un générateur du groupe multiplicatif $\mathbb{F}_p^*$. On remarque tout d'abord que les quantités T_Q et T_N sont invariantes sur Q et N, c-à-d :
– si $a \in Q$

$$\begin{cases} T_Q(a) = T_Q(1) \\ T_N(a) = T_N(1) \end{cases} \tag{4.58}$$

– si $a \in N$

$$\begin{cases} T_Q(a) = T_Q(g) \\ T_N(a) = T_N(g) \end{cases} \tag{4.59}$$

En effet, un changement d'indice approprié permet de réécrire les sommes présentes dans la définition de T_Q et T_N. On détaille par exemple la première équation de (4.59). Soit a un non-résidu quadratique de $\mathbb{F}_p$. Il existe alors $k \in \mathbb{N}$ tel que $a = g^{2k+1}$.

$$T_Q(a) = \sum_{x \in Q} \chi_L\big(x - a\big) \tag{4.60}$$

$$= \sum_{x \in Q} \chi_L\big(g^{2k}\big)\chi_L\big(g^{-2k}x - g^{-2k}a\big) \tag{4.61}$$

$$= \sum_{x \in Q} \chi_L\big(g^{-2k}x - g\big) \tag{4.62}$$

A présent on effectue le changement de variable $x \to g^{2k}x$. Ainsi, lorsque x parcourt Q, $g^{2k}x$ parcourt Q également. On peut donc écrire

$$T_Q(a) = \sum_{x \in Q} \chi_L\big(x - g\big) = T_Q(g) \tag{4.63}$$

Les 3 autres cas se traitent de façon similaire.

On a donc 4 inconnues à calculer : $T_Q(1)$, $T_N(1)$, $T_Q(g)$ et $T_N(g)$. La suite de cette preuve consiste alors en l'établissement de 4 équations linéaires libres faisant intervenir ces quantités.

Première équation : On calcule $T_Q(1) + T_N(1)$

$$T_Q(1) + T_N(1) = \sum_{x \in Q} \chi_L\big(x - 1\big) + \sum_{x \in N} \chi_L\big(x - 1\big) \tag{4.64}$$

$$= \sum_{x \neq 0} \chi_L\big(x - 1\big) \tag{4.65}$$

$$= T(1) - \chi_L\big(-1\big) \tag{4.66}$$

D'après la Propriété 4.10, on obtient

$$T_Q(1) + T_N(1) = -1 \tag{4.67}$$

Deuxième équation :

$$\sum_{x \in N} T_Q(x) = \sum_{x \in N} \sum_{y \in Q} \chi_L\big(x - y\big) \tag{4.68}$$

$$= \sum_{y \in Q} \sum_{x \in N} \chi_L\big(y - x\big) \tag{4.69}$$

$$= \sum_{y \in Q} T_N(y) \tag{4.70}$$

Or, comme prouvé précédemment, les quantités T_N et T_Q sont invariantes sur N et Q. On en déduit donc

$$\frac{p-1}{2}T_Q(g) = \frac{p-1}{2}T_N(1) \tag{4.71}$$

$$T_Q(g) = T_N(1) \tag{4.72}$$

Troisième équation : De manière similaire à la première équation, on calcule $T_Q(g) + T_N(g)$:

$$T_Q(g) + T_N(g) = \sum_{x\in Q}\chi_L\big(x-g\big) + \sum_{x\in N}\chi_L\big(x-g\big) \tag{4.73}$$

$$= \sum_{x\neq 0}\chi_L\big(x-g\big) \tag{4.74}$$

$$= T(g) - \chi_L\big(-g\big) \tag{4.75}$$

d'où

$$T_Q(g) + T_N(g) = 1 \tag{4.76}$$

Quatrième équation : On exprime $T_Q(1)$ d'une autre façon :

$$T_Q(1) = \sum_{x\in Q}\chi_L\big(x-1\big) \tag{4.77}$$

$$= \sum_{x\in Q}\chi_L\big(g\big)\chi_L\big(gx-g\big) \tag{4.78}$$

$$= -\sum_{x\in Q}\chi_L\big(gx-g\big) \tag{4.79}$$

L'équation (4.78) est obtenue en multipliant chaque terme par $\chi_L\big(g\big)^2$. On effectue ensuite le changement de variable $x \to g^{-1}x$ et on remarque que lorsque x parcourt Q, gx parcourt N.

$$T_Q(1) = -\sum_{x\in N}\chi_L\big(x-g\big) \tag{4.80}$$

$$T_Q(1) = -T_N(g) \tag{4.81}$$

Les équations (4.67), (4.72), (4.76) et (4.81) se traduisent par un système de Cramer :

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} T_Q(1) \\ T_Q(g) \\ T_N(1) \\ T_N(g) \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{4.82}$$

Les techniques de résolutions usuelles d'un tel système donnent

$$\begin{cases} T_Q(1) = -1 \\ T_Q(g) = 0 \\ T_N(1) = 0 \\ T_N(g) = 1 \end{cases} \tag{4.83}$$

En utilisant l'invariance de T_Q et T_N sur Q et N traduite en (4.58) et (4.59), on constate que cette solution coïncide avec les formules (4.56) et (4.57).

□

Lorsque S est un ensemble de taille 2, la valeur de $T(S)$ est constante :

Propriété 4.13. *Soit $a, b \in \mathbb{F}_p$ avec $a \neq b$.*

$$T(\{a,b\}) = -1 \tag{4.84}$$

Démonstration.

$$T(\{a,b\}) = \sum_{x\in\mathbb{F}_p} \chi_L\big((x-a)(x-b)\big) \tag{4.85}$$

$$= \sum_{x\in\mathbb{F}_p} \chi_L\big(x(x+a-b)\big) \tag{4.86}$$

$$= \sum_{x\in\mathbb{F}_p} \chi_L\big(x(x-1)\big) \tag{4.87}$$

On obtient l'équation (4.87) après changement d'indice $x \to (b-a)x$. A présent, on sépare la somme selon la partition $\mathbb{F}_p = \{0\} \cup Q \cup N$:

$$T(\{a,b\}) = \sum_{x\in Q} \chi_L\big(x(x-1)\big) + \sum_{x\in N} \chi_L\big(x(x-1)\big) \tag{4.88}$$

$$= \sum_{x\in Q} \chi_L\big(x-1\big) - \sum_{x\in N} \chi_L\big(x-1\big) \tag{4.89}$$

$$= T_Q(1) - T_N(1) \tag{4.90}$$

En utilisant le Lemme 4.12, on obtient

$$T(\{a,b\}) = \frac{-1-\chi_L\big(1\big)}{2} - \frac{1-\chi_L\big(1\big)}{2} = -1 \tag{4.91}$$

□

L'équation (4.87) traduit notamment le fait que $T(\{a,b\}) = T(\{0,1\})$ lorsque $a \neq b$.

Propriété 4.14. *Soit* $(a, b) \in \mathbb{F}_p$.

$$T\left(\overline{\{a,b\}}\right) = 2\chi_L\big(a-b\big) \tag{4.92}$$

Démonstration. D'après le Lemme 4.9,

$$T\left(\overline{\{a,b\}}\right) = \sum_{x\in\mathbb{F}_p} \chi_L\left(f_{\overline{\{a,b\}}}(x)\right) \tag{4.93}$$

$$= \chi_L\left(\prod_{x\neq a,b}(x-a)\right) + \chi_L\left(\prod_{x\neq a,b}(x-b)\right) \tag{4.94}$$

On remarque que χ_L est un caractère d'ordre 2, i.e. $\chi_L^2 = id$. De plus, $\chi_L\big(a-b\big) = \chi_L\big(b-a\big)$. On multiplie donc le terme de droite de l'équation (4.94) par $\chi_L\big(a-b\big)^2$:

$$T\left(\overline{\{a,b\}}\right) = \chi_L\left(\prod_{x\neq a}(x-a)\right)\chi_L\big(a-b\big) + \chi_L\left(\prod_{x\neq b}(x-b)\right)\chi_L\big(a-b\big) \tag{4.95}$$

On reconnaît l'expression de la fonction T pour des ensembles de taille $p-1$, ainsi on peut écrire

$$T\left(\overline{\{a,b\}}\right) = T\left(\overline{\{a\}}\right)\chi_L\big(a-b\big) + T\left(\overline{\{b\}}\right)\chi_L\big(a-b\big) \tag{4.96}$$

D'après la Propriété 4.11, on conclut l'équation (4.92). □

Les deux propriétés qui suivent sont des résultats déjà connus énoncés dans [Joy06]. Ils concernent la valeur de T sur l'ensemble des résidus quadratiques puis sur les non-résidus.

Propriété 4.15.

$$T(Q) = \frac{p-1}{2}\chi_L\big(2\big) + 1 \tag{4.97}$$

Démonstration. Le polynôme f_Q a pour racines l'ensemble des résidus quadratiques modulo p. Tout résidu quadratique x vérifie

$$\chi_L\big(x\big) = 1 \tag{4.98}$$

$$x^{\frac{p-1}{2}} - 1 = 0 \tag{4.99}$$

$$\tag{4.100}$$

Tous les éléments de Q sont racines du polynôme $X^{\frac{p-1}{2}} - 1$ de degré $\frac{p-1}{2}$, or $|Q| = \frac{p-1}{2}$. Ainsi

$$f_Q(X) = X^{\frac{p-1}{2}} - 1 \tag{4.101}$$

On peut alors écrire

$$T(Q) = \sum_{x\in\mathbb{F}_p} \chi_L\left(x^{\frac{p-1}{2}} - 1\right) \tag{4.102}$$

$$= \sum_{x\in Q} \chi_L\big(\chi_L(x) - 1\big) + \sum_{x\in N} \chi_L\big(\chi_L(x) - 1\big) + \chi_L(-1) \tag{4.103}$$

$$= \frac{p-1}{2}\chi_L(2) + 1 \tag{4.104}$$

□

Un résultat similaire existe également lorsque l'on considère l'ensemble N :

Propriété 4.16.

$$T(N) = \frac{p-1}{2}\chi_L(2) + 1 \tag{4.105}$$

Démonstration. La preuve est similaire à celle de la Propriété 4.15 en faisant intervenir le polynôme $X^{\frac{p-1}{2}} + 1$ □

Notons également la valeur de la fonction T sur l'ensemble $\mathbb{F}_p$ tout entier :

Propriété 4.17.

$$T(\mathbb{F}_p) = 0 \tag{4.106}$$

Démonstration. Le Lemme 4.9 donne directement le résultat énoncé. □

On notera également par convention $T(\varnothing) = p$.

4.4.2 Graphe des ensembles et système linéaire

Les quantités $T(S)$ définies en (4.15) sont en lien direct avec le calcul du nombre de points des courbes hyperelliptiques correspondantes Γ_S. Bien que ce domaine fasse usuellement intervenir des méthodes de géométrie algébrique, nous proposons ici l'utilisation d'équations linéaires entre les valeurs de la fonction T pour différents ensembles S.

Nous souhaitons, dans cette partie, établir des liens entre les valeurs de T sur tous les sous-ensembles S de $\mathbb{F}_p$ afin d'établir un système d'équations linéaires.

Pour cela, considérons le graphe $\mathcal{H}_p$ que nous définissons ainsi :

Définition 4.6. *Soit $p \in \mathbb{N}^*$. Le graphe $\mathcal{H}_p = (V, E)$ est défini de la façon suivante :*

$$V = \mathcal{P}(\mathbb{F}_p) \tag{4.107}$$

$$(A, B) \in E \Leftrightarrow |A + B| = 1 \tag{4.108}$$

L'opération '+' entre deux ensembles désigne ici leur différence symétrique, et non la somme usuelle entre les éléments de $\mathbb{F}_p$ qu'ils contiennent.

En d'autres termes, deux parties de $\mathbb{F}_p$ sont voisines lorsqu'elles diffèrent d'exactement un élément.

On remarquera que le graphe $\mathcal{H}_p$ est isomorphe à l'hypercube d'ordre p pour le morphisme associant un ensemble à son vecteur caractéristique. Par exemple, pour $p = 3$ le graphe $\mathcal{H}_3$ est isomorphe à l'hypercube d'ordre 3, c'est-à-dire le cube (voir Figure 4.2).

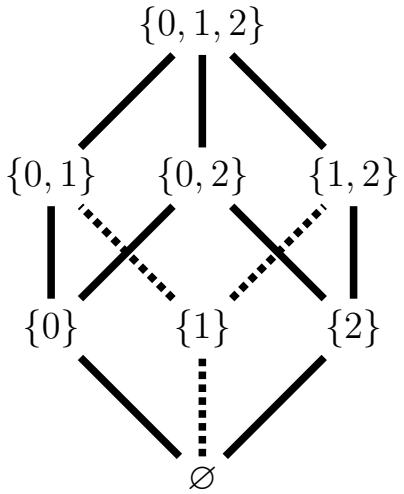

FIGURE 4.2 – Graphe $\mathcal{H}_3$ isomorphe au cube : une arête est présente entre 2 ensembles A et B lorsqu'ils diffèrent d'exactement 1 élément. Pour tout sommet, chacune de ses 3 arêtes adjacentes correspond à l'opération de différence symétrique avec chacun des 3 éléments de $\mathbb{F}_3$.

Dans cette partie, toute notion de voisinage d'un ensemble est relative au voisinage dans le graphe $\mathcal{H}_p$.

A tout sommet S est associé la quantité $T(S)$ ainsi qu'une quantité $V(S)$ définie de cette façon :

$$U(S) = \sum_{x \in S} \chi_L\big(f_{S\setminus\{x\}}(x)\big) \tag{4.109}$$

Cette quantité $U(S)$ correspond à la somme des valeurs de χ_L sur les produits de toutes les différences possibles sauf une des éléments de S.

Pour chaque sommet de $\mathcal{H}_p$ nous cherchons à établir une équation linéaire faisant intervenir les quantités T et U. Pour cela, montrons tout d'abord le lemme suivant :

Lemme 4.18. *Soit $S \subseteq \mathbb{F}_p$ et $a \in S$. On a l'égalité suivante :*

$$T(S \setminus \{a\}) = \chi_L\left(f_{S\setminus\{a\}}(a)\right) + \sum_{x\in\mathbb{F}_p} \chi_L\big(f_S(x)(x-a)\big) \tag{4.110}$$

Démonstration. On utilise la définition de $T(S \setminus \{a\})$ et on décompose la somme en écartant l'élément a :

$$T(S \setminus \{a\}) = \chi_L\left(f_{S\setminus\{a\}}(a)\right) + \sum_{x\neq a} \chi_L\left(f_{S\setminus\{a\}}(x)\right) \tag{4.111}$$

Lorsque $x \neq a$, on a $1 = \chi_L\big(x-a\big)^2$. On peut donc écrire

$$T(S \setminus \{a\}) = \chi_L\left(f_{S\setminus\{a\}}(a)\right) + \sum_{x\neq a} \left[\chi_L\left(f_{S\setminus\{a\}}(x)\right)\chi_L\big(x-a\big)^2\right] \tag{4.112}$$

$$= \chi_L\left(f_{S\setminus\{a\}}(a)\right) + \sum_{x\neq a} \chi_L\big(f_S(x)(x-a)\big) \tag{4.113}$$

Le polynôme $f_S(X)(X-a)$ s'annule en a, on peut donc sommer sur $\mathbb{F}_p$ tout entier et on obtient bien l'égalité (4.110). □

Nous pouvons à présent établir l'équation suivante relative à l'ensemble S qui constitue un résultat central dans cette partie :

Théorème 4.19. *Soit $S \subseteq \mathbb{F}_p$. L'équation suivante est vérifiée :*

$$\sum_{x\in\mathbb{F}_p} T(S+\{x\}) = U(S) \tag{4.114}$$

Démonstration. On sépare la somme de l'équation (4.114) selon la taille des ensembles A :

$$\sum_{x\in\mathbb{F}_p} T(S+\{x\}) = \sum_{a\in S} T(S\setminus\{a\}) + \sum_{a\notin S} T(S\cup\{a\}) \tag{4.115}$$

$$\tag{4.116}$$

D'après le Lemme 4.18, on a

$$\sum_{x\in\mathbb{F}_p} T(S+\{x\}) = \sum_{a\in S}\left[\chi_L\left(f_{S\setminus\{a\}}(a)\right) + \sum_{x\in\mathbb{F}_p}\chi_L\big(f_S(x)(x-a)\big)\right] + \sum_{a\notin S}\sum_{x\in\mathbb{F}_p}\chi_L\left(f_{S\cup\{a\}}(x)\right) \tag{4.117}$$

Lorsque $a \notin S$ le polynôme $f_{S\cup\{a\}}(X)$ s'écrit aussi $f_S(X)(X-a)$. Ainsi, on a

$$\sum_{x\in\mathbb{F}_p} T(S+\{x\}) = \sum_{a\in S}\chi_L\left(f_{S\setminus\{a\}}(a)\right) + \sum_{a\in\mathbb{F}_p}\sum_{x\in\mathbb{F}_p}\chi_L\left(f_S(x)(x-a)\right) \tag{4.118}$$

On identifie le premier terme de cette somme avec la quantité $V(S)$ définie en (4.109). Il reste donc à prouver que le deuxième terme est nul.

On exprime le deuxième terme de (4.118) en effectuant tout d'abord le changement de variable $y = x - a$. Quelque soit $a \in \mathbb{F}_p$, lorsque x parcourt $\mathbb{F}_p$, il en est de même de y.

$$\sum_a \sum_x \chi_L\left(f_S(x)(x-a)\right) = \sum_a \sum_y \chi_L\left(f_S(y+a)y\right) \tag{4.119}$$

$$= \sum_a \left[\sum_{y\in Q} \chi_L\left(f_S(y+a)\right) - \sum_{y\in N} \chi_L\left(f_S(y+a)\right) \right] \tag{4.120}$$

A présent, on permute les sommes (c'est autorisé car les sommes sont finies) :

$$\sum_a \sum_x \chi_L\left(f_S(x)(x-a)\right) = \sum_{y\in Q} \sum_a \chi_L\left(f_S(y+a)\right) - \sum_{y\in N} \sum_a \chi_L\left(f_S(y+a)\right) \tag{4.121}$$

$$= \sum_{y\in Q} T(-y) - \sum_{y\in N} T(-y) \tag{4.122}$$

$$= 0 \tag{4.123}$$

car $|Q| = |N|$ et la quantité T est invariante sur les singletons (voir Propriété 4.10).

En utilisant ce résultat dans l'équation (4.118), on trouve l'équation (4.114) de l'énoncé. □

A présent, on montre que la quantité U précédemment introduite (4.109) est égale à la quantité T de l'ensemble complémentaire :

Lemme 4.20. *Soit $S \in \mathbb{F}_p$. On note $\overline{S} = \mathbb{F}_p \setminus S$.*

$$U(S) = T(\overline{S}) \tag{4.124}$$

Démonstration. On introduit la notation vectorielle $t(S) \in \{-1, 0, 1\}^p$:

$$t(S) = \begin{pmatrix} \chi_L\left(f_S(0)\right) \\ \vdots \\ \chi_L\left(f_S(p-1)\right) \end{pmatrix} \tag{4.125}$$

On remarque que l'on a $T(S) = ||t(S)||_1$. De même on définit $u(S) \in \{-1, 0, 1\}^p$ de la façon suivante :

$$u(S) = \begin{pmatrix} \chi_L\left(f_{S\setminus\{0\}}(0)\right) \mathbb{1}_S(0) \\ \vdots \\ \chi_L\left(f_{S\setminus\{p-1\}}(p-1)\right) \mathbb{1}_S(p-1) \end{pmatrix} \tag{4.126}$$

Il est facile de vérifier de façon similaire que $U(S) = ||u(S)||_1$.

Pour tout $a \in \mathbb{F}_p$, on souhaite montrer que $u(S)_a = t(\overline{S})_a$. On note θ la quantité

$$\theta = u(V)_a \times t(\overline{S})_a \tag{4.127}$$
$$= \chi_L\left(f_{V\setminus\{a\}}(a)\right)\chi_L\big(f_{\overline{S}}(a)\big) \tag{4.128}$$

On veut montrer que $\theta = u(S)_a$.

Si $a \in S$, on peut écrire $f_{V\setminus\{a\}} = f_{S\setminus\{a\}} f_{\overline{S}}$. Ainsi

$$\theta = \chi_L\left(f_{S\setminus\{a\}}(a)\right)\chi_L\big(f_{\overline{S}}(a)\big)^2 \tag{4.129}$$

Or $\chi_L\big(f_{\overline{S}}(a)\big)^2 = 1$ car $a \in S$, d'où

$$\theta = \chi_L\left(f_{S\setminus\{a\}}(a)\right) = u(S)_a \tag{4.130}$$

Si $a \in \overline{S}$, $\chi_L\big(f_{\overline{S}}(a)\big) = 0$, donc l'équation (4.128) donne

$$\theta = 0 = u(S)_a \tag{4.131}$$

Quelque soit $a \in \mathbb{F}_p$, on a donc

$$\theta = u(S)_a \tag{4.132}$$

Pour tout $a \in \mathbb{F}_p$, on a

$$u(V)_a = \chi_L\left(\prod_{x\neq a}(x-a)\right) \tag{4.133}$$
$$= \chi_L\left(\prod_{x\neq 0} x\right) = 1 \tag{4.134}$$

car $p = 1 \bmod 4$.

Ainsi, les équations (4.127) et (4.132) permettent de déduire

$$u(S)_a = t(\overline{S})_a \tag{4.135}$$

□

En utilisant le lemme précédent dans le Théorème 4.19 on obtient le corollaire :

Corollaire 4.21. *Pour tout $S \in \mathbb{F}_p$.*

$$\sum_{x\in\mathbb{F}_p} T(S+\{x\}) = T(\overline{S}) \tag{4.136}$$

Nous nous affranchirons désormais de la quantité V qui a été introduite en (4.109) dans l'unique but d'établir le Corollaire 4.21.

Ensuite, nous considérons les ensembles à distance 2 au lieu des voisins directs d'un sommet S dans le graphe $\mathcal{H}_p$. Nous prouvons alors le résultat suivant :

Propriété 4.22. *Pour tout $S \subseteq \mathbb{F}_p$*

$$(1-p)T(S) = 2 \sum_{d(S,A)=2} T(A) \tag{4.137}$$

où d désigne la distance dans le graphe $\mathcal{H}_p$.

Démonstration. D'après le Corollaire 4.21, on peut écrire

$$T(S) = \sum_{x \in \mathbb{F}_p} T(S + \{x\}) \tag{4.138}$$

On itère en appliquant encore une fois le Corollaire 4.21 :

$$T(S) = \sum_x \sum_y T(S + \{x\} + \{y\}) \tag{4.139}$$

$$= \sum_{x<y} T(S + \{x,y\}) + \sum_{x>y} T(S + \{x,y\}) + \sum_x T(S) \tag{4.140}$$

$$= 2 \sum_{d(S,A)=2} T(A) + pT(S) \tag{4.141}$$

On obtient ainsi le résultat voulu. □

Cette propriété a l'avantage d'être plus "locale" que le Corollaire 4.21 car elle fait intervenir les ensembles à distance 2 de l'ensemble S choisi au lieu de l'ensemble $\overline{S}$. Les sommets à distance 2 dans l'hypercube $\mathcal{H}_p$ correspondent au voisinage direct dans $\mathcal{H}_p^2$.

La Propriété 4.22 peut ainsi se traduire matriciellement en un système linéaire à 2^p variables dont la matrice correspond à la matrice d'adjacence du graphe $\mathcal{H}_p^2$ dans laquelle on ajoute une diagonale de '$\frac{p-1}{2}$'. Dans une optique de recherche de solution, ce système est certes de taille exponentielle, mais sa matrice associée est creuse (seulement $\binom{p}{2}$ coordonnées non-nulles parmi 2^p). De plus, chaque équation correspond à des dépendances locales dans le graphe $\mathcal{H}_p^2$, ainsi nous pouvons envisager une approche consistant en la propagation de solutions.

Nous pouvons remarquer quelques propriétés supplémentaires. Etablissons ainsi la première qui regroupe tous les ensembles de taille impaire fixée :

Propriété 4.23. *Pour tout $k \in \mathbb{N}$*

$$\sum_{|S|=2k+1[2]} T(S) = 0 \tag{4.142}$$

Démonstration. Soit a un élément de N.

$$\sum_{|S|=2k+1[2]} T(S) = \frac{1}{2}\left[\sum_{|S|=2k+1[2]} T(S) + \sum_{|S|=2k+1[2]} T(aS)\right] \tag{4.143}$$

où aS désigne l'ensemble $\{ax | x \in S\}$. En effet, le découpage précédent est vérifié car lorsque S parcourt tous les ensembles de taille $2k+1$, il en est de même de aS.

En utilisant l'expression (4.15),

$$T(aS) = \sum_x \prod_{u\in aS} \chi_L(x-u) \tag{4.144}$$

$$= \sum_x \chi_L(a)^{|S|} \prod_{u\in S} \chi_L(a^{-1}x-u) \tag{4.145}$$

$$= \chi_L(a)^{|S|} \sum_x \prod_{u\in S} \chi_L(x-u) \tag{4.146}$$

$$= \chi_L(a)^{|S|} T(S) \tag{4.147}$$

Ici, $a \in N$ d'où, pour reprendre l'expression (4.143),

$$\sum_{|S|=2k+1[2]} T(S) = \frac{1}{2}\left[\sum_{|S|=2k+1[2]} T(S) - \sum_{|S|=2k+1[2]} T(S)\right] = 0 \tag{4.148}$$

□

Nous pouvons également remarquer que les valeurs que peut prendre la quantité T sont entièrement parcourues si on considère uniquement les ensembles qui contiennent les éléments 0 et 1. En effet, si on considère un ensemble $S = \{u_1, u_2, \cdots, u_k\}$, un changement de variable par translation implique

$$T(S) = \sum_x \chi_L\big((x-u_1)(x-u_2)\cdots(x-u_k)\big) \tag{4.149}$$

$$= \sum_x \chi_L\big(x(x-u_2+u_1)\cdots(x-u_k+u_1)\big) \tag{4.150}$$

$$= T(\{0, u_1-u_2, \cdots, u_k-u_2\}) \tag{4.151}$$

Le calcul de T se réduit donc aux ensembles de la forme $S = \{0, u_1, u_2, \cdots, u_k\}$.

A présent, un changement de variable $x \to u_1 x$ permet d'écrire

$$|T(S)| = \left|\sum_x \chi_L\big(x(x-u_1)(x-u_2)\cdots(x-u_k)\big)\right| \tag{4.152}$$

$$= \left|\sum_x \chi_L\big(x(x-1)(x-u_2u_1^{-1})\cdots(x-u_ku_1^{-1})\big)\right| \tag{4.153}$$

$$= \left|T\left(\left\{0, 1, u_2u_1^{-1}, \cdots, u_ku_1^{-1}\right\}\right)\right| \tag{4.154}$$

Il suffit donc de considérer, pour le calcul de T, uniquement les ensembles de la forme $S = \{0, 1, u_1, \cdots, u_k\}$.

4.5 Conclusion et pistes de recherche

Nous avons présenté une famille de graphes définis algébriquement, les graphes de Paley, et nous avons étudié les propriétés locales de cette famille de graphes en terme de plus petit degré par complémentation locale (voir Chapitre 3).

Ainsi, nous avons prouvé que la valeur de $\delta_{loc}(Pal_p)$ est supérieure à $\sqrt{p}$ où p est l'ordre du graphe, ce qui fait des graphes de Paley la famille de graphes constructive dont le degré minimum par complémentation locale est le plus élevé. De plus, ces graphes peuvent être utilisés comme support pour le partage de secret quantique (Chapitre 2) et réalisent ainsi des protocoles qQSS* de paramètres $((p, k))$ avec $k = \Omega(p - \sqrt{p})$.

Dans un deuxième temps, une conjecture de géométrie algébrique, la conjecture de Bazzi-Mitter, nous laisse penser qu'il existe une sous-famille infinie des graphes de Paley dont le degré minimum par complémentation locale est linéaire. Les graphes de Paley semblent donc être de bons candidats pour cette propriété. Sous cette conjecture, il serait donc possible d'expliciter une famille infinie de graphes ayant à la fois un degré minimum par complémentation locale linéaire dont nous avions prouvé l'existence dans le Théorème 3.25. Cette famille pourrait également servir de support à des protocoles de paramètres $((p, k))$ où $k \sim_{+\infty} cp$ avec $c < 1$.

Enfin, nous avons établi et exploité des connexions entre les propriétés locales des sous-ensembles de sommets des graphes de Paley et une quantité définie algébriquement : le déséquilibre T (Définition 4.4). Nous avons donc établi un système d'équations linéaires montrant les dépendances entres les valeurs de $T(S)$ où S est un sous-ensemble de sommets de Pal_p dans le but de calculer une meilleure borne sur la valeur de $\delta_{loc}(Pal_p)$.

Nous espérons par la suite parvenir à mieux comprendre la structure de la quantité T et considérer des familles particulières de nombres premiers pouvant mener à de meilleures bornes et faire apparaître des valeurs particulières de cette quantité. Nous comptons par exemple considérer les premiers de Fermat ou les premiers de Mersenne, par exemple.

Une autre piste de recherche que nous considérons est l'étude des graphes de Paley sur les extensions des corps de base ($\mathbb{F}_{p^k}$ pour p premier et $k \in \mathbb{N}$) et proposer une construction de graphes non orientés à partir des graphes de Paley orientés lorsque $p = 3 \mod 4$.

Chapitre 5

Conclusion

Dans le domaine du calcul et de la cryptographie quantique, les graphes sont à la base d'un support de calcul : les états graphes, états quantiques intriqués. Ils peuvent notamment être utilisés pour construire des protocoles de partage de secret dans lesquels un "dealer" répartit un état quantique secret $|\varphi_s\rangle$ entre n joueurs de telle sorte que certains ensembles de joueurs peuvent reconstruire $|\varphi_s\rangle$ alors que d'autres n'ont aucune information sur ce secret.

Si la question du partage d'un secret quantique à seuil a déjà été couverte [Sha79, Bla79], le cas d'un secret quantique comprend des limitations liées à la nature quantique de l'information manipulée, notamment l'impossibilité de dupliquer un état quantique arbitraire [WZ82]. La famille des protocoles de partage de secret étudiés dans ce document sont également soumises à ces contraintes.

Les structures d'accès des protocoles de partage de secret à partir d'états graphes [MS08] sont caractérisées par des propriétés sur les graphes associés à ces protocoles (Corollaire 2.8 et Théorème 2.14). Nous avons alors utilisé ces propriétés pour proposer la construction de protocoles qQSS* de partage de secret quantique à seuil à partir d'états graphes à l'aide d'une loi de composition sur les graphes itérée (Corollaire 2.32). Nous réalisons alors des protocoles de seuil $n - n^{\alpha} + 1$ avec $\alpha \approx 0.71$ parmi n joueurs (Théorème 2.34).

L'utilisation de méthodes probabilistes nous a également permis de prouver l'existence de protocoles qQSS* réalisant un seuil $0.811n$ entre n joueurs (Théorème 3.27). De plus, le seuil réalisé par des graphes probabilistes tirés selon le modèle d'Erdös Renyi [ER59] permettent d'atteindre un seuil linéaire cn avec $c < 1$ avec forte probabilité (Théorème 3.28).

Nous avons également montré une borne inférieure plus restrictive que celle issue du théorème de non-clonage (Théorème 1.2) sur les seuils réalisables par les protocoles qQSS* au moyen de techniques combinatoires. Ainsi, il est impossible de construire un tel protocole avec n joueurs dont le seuil est inférieur à $\frac{n}{2} + \frac{n}{157}$ (Théorème 2.36).

Les structures graphiques liées à la construction de protocoles de partage de secret quantique à partir d'états graphes font intervenir la notion de domination impaire (Définition 3.3) et notamment la taille du plus grand ensemble dominé modulo 2 et du plus petit ensemble à noyau impair. Nous nous sommes alors tournés vers l'étude de ces minima et maxima ainsi que de leurs problèmes de décision associés dont nous avons prouvé la NP-complétude (Théorème 3.15 et Théorème 3.16) au moyen de réductions au problème de la recherche d'un code parfait dans un graphe [Kra87] et [KMP02].

Ces problèmes évoquent également l'étude du degré minimum par complémentation locale, quantité étudiée en théorie des graphes (Définition 3.2) et ayant des applications dans la préparations des états graphes [HMP06]. Bien que similaire aux problèmes précédents (à une contrainte de parité près), la preuve de la NP-complétude de la recherche du degré minimum d'un graphe par complémentation locale que nous proposons (Théorème 3.21) fait intervenir une réduction au problème de la recherche de la distance d'un code linéaire [Var97].

Tout comme pour le seuil des protocoles qQSS*, nous utilisons les méthodes probabilistes pour prouver l'existence de graphes bipartis dont le degré minimum par complémentation locale est linéaire en l'ordre du graphe. De tels graphes bipartis sont notamment utilisés dans la preuve de NP-complétude du problème de décision lié au degré minimum par complémentation locale.

L'étude de la complexité des problèmes présentés dans ce document a été poursuivie après ces travaux [CP13], notamment en ce qui concerne la complexité paramétrée.

La famille des graphes de Paley (Définition 4.3) présente des propriétés de régularité qui laissent penser qu'ils représentent de bons candidats pour la construction de protocoles qQSS* avec n joueurs et réalisant un seuil en cn avec $c < 1$. De même, on constate également sur les premiers exemples que ces graphes semblent avoir un degré minimum par complémentation locale relativement élevé. C'est d'ailleurs le graphe de Paley d'ordre 29 qui fournit la meilleur "graine" pour la construction itérative de protocole qQSS* présentée en 2.5.2.

Nous montrons que le graphe de Paley d'ordre p possède un degré minimum par complémentation locale de l'ordre de $\sqrt{p}$, ce qui constitue la famille explicite ayant le plus fort degré par complémentation locale à notre connaissance, et nous faisons un lien avec la conjecture de Bazzi-Mitter dans le domaine de la géométrie algébrique pour conjecturer l'existence d'une sous-famille des graphes de Paley dont le degré minimum par complémentation locale est linéaire en l'ordre du graphe.

Enfin, nous présentons une partie plus exploratoire visant l'établissement d'un système linéaire sur les sous-ensembles de sommets des graphes de Paley en montrant des égalités issues de la nature algébrique de la définition des graphes de Paley. L'objectif de ce système est, à terme, de pouvoir donner une borne inférieure sur le degré minimum par complémentation locale du graphe de Paley d'ordre p pour certains premiers p particuliers.

Bibliographie

[ACS98] Ashok T. Amin, Lane H. Clark, and Peter J. Slater. Parity dimension for graphs. *Discrete Mathematics*, 187(1-3) :1 – 17, 1998.

[ADB05] Hans Aschauer, Wolfgang Dur, and Hans J. Briegel. Multiparticle entanglement purification for two-colorable graph states. *Physical Review A*, 71 :012319, 2005.

[AM13] Anurag Anshu and Mehdi Mhalla. Pseudo-telepathy games and genuine ns k-way nonlocality using graph states. *Quantum Information and Computation*, 13(9-10) :833–845, 2013.

[AMTW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald De Wolf. Private quantum channels. *PROCEEDINGS OF THE 41ST ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE*, pages 547–553, 2000.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography : Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[BBV93] Ethan Bernstein, Ethan Bernstein, and Umesh" Vazirani. Quantum complexity theory. *IN PROC. 25TH ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING, ACM*, pages 11–20, 1993.

[BCG+11] Salman Beigi, Isaac Chuang, Markus Grassl, Peter Shor, and Bei Zeng. Graph concatenation for quantum codes. *Journal of Mathematical Physics*, 52, 2011.

[BCT08] Anne Broadbent, Paul Robert Chouha, and Alain Tapp. The ghz state in secret sharing and entanglement simulation. 10 2008.

[Bel64] John Bell. On the einstein podolsky rosen paradox. *Physics*, 1(3) :195–200, 1964.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Proceedings of FOCS*, pages 517–526, 2009.

[Bla79] George Robert Blakley. Safeguarding cryptographic keys. In *Proceedings of the National Computer Conference*, pages 313–317. American Federation of Information Processing Societies, 1979.

[BM84] George Robert Blakley and Catherine Meadows. Security of ramp schemes. In *Advances in Cryptology, Proceedings of CRYPTO 84*, volume 196, pages 242–268. Springer, 1984.

[BM06] L. M. J. Bazzi and Sanjoy K. Mitter. Some randomized code constructions from group actions. *IEEE Transactions on Information Theory*, 52(7) :3210–3219, 2006.

[Bou87] André Bouchet. Digraph decompositions and eulerian systems. *SIAM J. Algebraic Discrete Methods*, 8 :323–337, July 1987.

[Bou88] André Bouchet. Transforming trees by successive local complementations. *Journal of Graph Theory*, 12(2) :195–207, 1988.

[Bou90] André Bouchet. κ-transformations, local complementations and switching. *Cycles and Rays*, 1990.

[Bou91] André Bouchet. An efficient algorithm to recognize locally equivalent graphs. *Combinatorica*, 11(4) :315–329, 1991.

[Bou94] André Bouchet. Circle graph obstructions. *J. Comb. Theory Ser. B*, 60 :107–144, January 1994.

[BR03] P. Oscar Boykin and Vwani Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67(4), 2003.

[CGL99] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Physical Review Letters*, 83(3) :648–651, 1999.

[CK03] Y. Caro and W. Klostermeyer. The odd domination number of the odd domination number of a graph. In *J. Comb. Math Comb. Comput.*, volume 44, pages 65–84, 2003.

[CP13] David Cattanéo and Simon Perdrix. Parameterized complexity of weak odd domination problems. *Fundamentals of Computation Theory*, 8070 :107–120, 2013.

[DD85] David Deutsch and David" Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. 400 :97–117, 1985.

[dF81] Hubert de Fraysseix. Local complementation and interlacement graphs. *Discrete Mathematics*, 33(1) :29–35, 1981.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6) :644–654, November 1976.

[DMS03] Ilya Dumer, Daniele Micciancio, and Madhu Sudan. Hardness of approximating the minimum distance of a linear code. *IEEE Transactions on Information Theory*, 49(1) :22–37, January 2003. Preliminary version in FOCS 1999.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete ? *Physical Review*, 47(10) :777–780, 1935.

[ER59] Pal Erdös and Alfréd Rényi. On random graphs. *Publications Mathematicae*, 6 :290, 1959.

[ER63] Paul Erdős and Alfred Renyi. Asymmetric graphs. *Acta Mathematica Hungaria*, 1963.

[FM04] Keqin Feng and Zhi Ma. A finite gilbert-varshamov bound for pure stabilizer quantum codes. *IEEE Transactions on Information Theory*, 50(12) :3323–3325, 2004.

[Gam84] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and David Chaum, editors, *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer, 1984.

[GHZ89] D. M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond bell's theorem, 1989.

[GJMP12] Sylvain Gravier, Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. Quantum secret sharing with graph states. In Antonín Kucera, Thomas A. Henzinger, Jaroslav Nesetril, Tomás Vojnar, and David Antos, editors, *MEMICS*, volume 7721 of *Lecture Notes in Computer Science*, pages 15–31. Springer, 2012.

[Got00] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61 :042311, Mar 2000.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *STOC*, pages 212–219. ACM, 1996.

[Har91] Frank Harary. *Graph theory.* Addison-Wesley, 1991.

[HEB04] Marc Hein, Jens Eisert, and Hans J Briegel. Multi-party entanglement in graph states. *Physical Review A*, 69, 2004.

[HKT99] Magnús M. Halldórsson, Jan Kratochvíl, and Jan Arne Telle. Mod-2 independence and domination in graphs, 1999.

[HMP06] Peter Høyer, Mehdi Mhalla, and Simon Perdrix. Resources required for preparing graph states. In *Proceedings of ISAAC'06*, pages 638–649, 2006.

[IR90] Kenneth Ireland and Michael Ira Rosen. *A Classical Introduction to Modern Number Theory.* Graduate Texts in Mathematics. Springer, 1990.

[JMP11] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. Classical versus quantum graph-based secret sharing. *arXiv :1109.4731*, 09 2011.

[JMP12a] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. New protocols and lower bounds for quantum secret sharing with graph states. In *TQC*, pages 1–12, 2012.

[JMP12b] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. On the minimum degree up to local complementation : Bounds and complexity. In Martin Charles Golumbic, Michal Stern, Avivit Levy, and Gila Morgenstern, editors, *WG*, volume 7551 of *Lecture Notes in Computer Science*, pages 138–147. Springer, 2012.

[Joy06] David Joyner. On quadratic residue codes and hyperelliptic curves. *ArXiv Mathematics e-prints*, September 2006.

[KFMS10] Adrian Keet, Ben Fortescue, Damian Markham, and Barry C. Sanders. Quantum secret sharing with qudit graph states. *Phys. Rev. A*, 82 :062315, 2010.

[KMMP09] Elham Kashefi, Damian Markham, Mehdi Mhalla, and Simon Perdrix. Information flow in secret sharing protocols. *EPTCS 9, 2009, pp. 87-97*, 09 2009.

[KMP02] Sandi Klavzar, Uros Milutinovic, and Ciril Petr. 1-perfect codes in sierpinski graphs. *Bulletin of the Australian Mathematical Society*, 66 :369–384, 2002.

[Kot68] Anton Kotzig. Eulerian lines in finite 4-valent graphs and their transformations. In *Colloqium on Graph Theory*, pages 219–230. Academic Press, 1968.

[Kra87] Jan Kratochvil. Perfect codes in general graphs. *7th Hungarian colloqium on combinatorics, Eger*, 1987.

[LLMP90] Arjen K. Lenstra, Hendrik W. Lenstra, Mark S. Manasse, and J. M. Pollard. The number field sieve. In *ACM Symposium on Theory of Computing*, pages 564–572, 1990.

[Lov75] László Lovász. Problems and results on 3-chromatic hypergraphs and some related questions. In *Colloquia Mathematica Societatis Janos Bolyai*, pages 609–627, 1975.

[MM12] Anne Marin and Damian Markham. On the equivalence between sharing quantum and classical secrets, and error correction. 05 2012.

[MP07] Mehdi Mhalla and Simon Perdrix. Finding optimal flows efficiently. In *Proceedings of 35th ICALP*, pages 857–868, 09 2007.

[MS08] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78 :042309, 2008.

[MT10] Robin A. Moser and Gábor Tardos. A constructive proof of the general lovász local lemma. *J. ACM*, 57(2), 2010.

[MVdNB07] Guifre Vidal Maarten Van de Nest, Wolfgang Dür and Hans J. Briegel. Classical simulation versus universality in measurement based quantum computation. *Physical Review A*, 75 :012337, 2007.

[NC00] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 1 edition, 2000.

[OSIY05a] Tomohiro Ogawa, Akira Sasaki, Mitsugu Iwamoto, and Hirosuke Yamamoto. Quantum secret sharing schemes and reversibility of quantum operations. *Phys. Rev. A*, 72 :032318, Sep 2005.

[OSIY05b] Tomohiro Ogawa, Akira Sasaki, Mitsugu Iwamotoand, and Hirosuke Yamamoto. Quantum secret sharing schemes and reversibility of quantum operations. *Physical Review A*, 72(3), 2005.

[Oum08] Sang-Il Oum. Approximating rank-width and clique-width quickly. *ACM Trans. Algorithms*, 5 :10 :1–10 :20, December 2008.

[RB01] Robert Raussendorf and Hans Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22) :5188–5191, 2001.

[RB02] Robert Raussendorf and Hans Briegel. Computational model underlying the one-way quantum computer. *Quantum Information and Computation*, 6 :433, 2002.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2) :120–126, February 1978.

[Sac62] Horst Sachs. Über selbstkomplementäre graphen. *Publicationes Mathematicae Debrecen*, 1962.

[Sar12] Pradeep Sarvepalli. Nonthreshold quantum secret-sharing schemes in the graph-state formalism. *Physical Review A*, 86(4), 2012.

[Sch04] Wolfgang M. Schmidt. *Equations over finite fields : an elementary approach.* Kendrick Press, 2nd edition, 2004.

[Sev06] Simone Severini. Two-colorable graph states with maximal schmidt measure. *Physics Letters A*, 356 :99, 2006.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11) :612–613, 1979.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5) :1484–1509, 1997.

[Sut89] Klaus Sutner. Linear cellular automata and the garden-of-eden. *The Mathematical Intelligencer*, 11 :49–53, 1989. 10.1007/BF03023823.

[Sut90] K. Sutner. The σ-game and cellular automata. In *Amer. Math. Monthly*, pages 24–34, 1990.

[SW01] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Physical Review A*, 65, 2001.

[Tel94] J.A. Telle. Complexity of domination-type problems in graphs. In *Nordic Journal of Computing*, volume 1, pages 157–171, 1994.

[Var97] Alexander Vardy. Algorithmic complexity in coding theory and the minimum distance problem. In *STOC*, pages 92–109, 1997.

[Wal76] Derek A. Waller. Double covers of graphs. *Bulletin of the Australian Mathematical Society*, 14 :233–248, 4 1976.

[Was08] Lawrence C. Washington. *Elliptic Curves : Number Theory and Cryptography, Second Edition.* Chapman & Hall/CRC, 2 edition, 2008.

[Wei48] André Weil. On some exponential sums. In *Proceedings of the National Academy of Sciences*, volume 34, pages 204–207, 1948.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1) :78–88, January 1983.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886) :802–803, October 1982.

[Yao93] Andrew Chi-Chih Yao. Quantum circuit complexity. In *FOCS*, pages 352–361. IEEE Computer Society, 1993.