Modélisation graphique et simulation en traitement d'information quantique

David Cattaneo

Communauté
UNIVERSITÉ Grenoble Alpes

THÈSE

Pour obtenir le grade de

DOCTEUR DE LA COMMUNAUTÉ UNIVERSITÉ GRENOBLE ALPES

Spécialité : Informatique

Arrêté ministériel : 25 mai 2016

Présentée par

David CATTANEO

Thèse dirigée par **Pablo ARRIGHI**
et codirigée par **Simon PERDRIX**
préparée au sein du **Laboratoire d'Informatique de Grenoble**
dans **l'École Doctorale Mathématiques, Sciences et technologies de l'information, Informatique**

Modélisation graphique et simulation en traitement d'information quantique

Graph modeling and simulation in quantum information processing

Thèse soutenue publiquement le **4 décembre 2017**,
devant le jury composé de :

Monsieur PABLO ARRIGHI
PROFESSEUR, UNIVERSITE AIX-MARSEILLE, Directeur de thèse
Monsieur PAUL DORBEC
MAITRE DE CONFERENCES, UNIVERSITE DE BORDEAUX, Rapporteur
Monsieur EMMANUEL JEANDEL
PROFESSEUR, UNIVERSITE DE LORRAINE, Examinateur
Monsieur MATHIEU LIEDLOFF
MAITRE DE CONFERENCES, UNIVERSITE D'ORLEANS, Rapporteur
Madame MYRIAM PREISSMANN
DIRECTRICE DE RECHERCHE, CNRS DELEGATION ALPES, Président
Monsieur SIMON PERDRIX
CHARGE DE RECHERCHE, CNRS DELEGATION CENTRE-EST, Examinateur

Modélisation combinatoire en traitement de l'information quantique

David Cattanéo

Notations concernant les ensembles

Complémentaire $\overline{X}$

Étant donné une partie X d'un ensemble E, $E \setminus X = \{x \in E | x \notin X\}$ est le complémentaire de X dans E. On notera simplement $\overline{X}$ quand l'ensemble E est clairement défini par le contexte.

Ensembles PAIR/IMPAIR

PAIR est l'ensemble des entiers naturels pairs défini par PAIR$= \{2n | n \in \mathbb{N}\}$. IMPAIR est l'ensemble des entiers naturels impairs défini par IMPAIR$= \{2n + 1 | n \in \mathbb{N}\}$.

Corps fini à q éléments $\mathbb{F}_q$

On défini pour tout $q \in \mathbb{N}$ puissance de premier $\mathbb{F}_q$ comme étant le corps fini à q éléments muni des opérations d'addition et de multiplication.

Différence symétrique $\oplus$

Étant données deux parties A et B d'un ensemble X, $A \oplus B$ est la différence symétrique de A et B définie par $A \oplus B = \{a | a \in A, a \notin B\} \cup \{b | b \in B, b \notin A\}$.

Entiers non-nuls $\mathbb{N}^*$

On note $\mathbb{N}^*$ l'ensemble des entiers non-nuls défini par $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Notations concernant les graphes

Remarque générale : Dans ce document on considèrera un graphe simple non-orienté quand on parlera d'un graphe sauf noté explicitement.

Complémentaire $\overline{X}$

Étant donné un graphe $G = (V, E)$, $\overline{G}$ est le complémentaire de G, défini par $\overline{G} = (V, \{(u, v) | u \in V, v \in V, u \neq v, (u, v) \notin E\})$.

Relation de voisinage

Étant donné un graphe $G = (V, E)$, $\sim_G$ dénote la relation de voisinage de G i.e. $\forall u, v \in V$, $u \sim_G v \Leftrightarrow \{u, v\} \in E$. On pourra aussi noter $\sim$ si aucune ambiguïté n'est possible pour le graphe.

Voisinage ouvert $N(v)$ et degrés $\delta(v)$, Δ_G, δ_G

Étant donné un graphe $G = (V, E)$ et $v \in V$ un sommet, $N(v)$ est le voisinage **ouvert** de v défini par $N(v) = \{u | u \neq v \text{ et } u \sim_G v\}$ (noté aussi $N_G(C)$ si préciser le graphe est nécessaire).
Le degré $\delta(v)$ du sommet v est la taille de son voisinage : $\delta(v) = |N(v)|$ (noté aussi $delta_G(v)$ si préciser le graphe est nécessaire).
Le degré maximum du graphe G noté Δ_G est le plus grand degré sur tous les sommets de G : $\delta_G = max(\{\delta_G(v) | v \in V\})$.
Le degré minimum du graphe G noté δ_G est le plus petit degré de tous les sommets de G : $\delta_G = min(\{\delta_G(v) | v \in V\})$.

Nombre de couverture par sommets

Étant donné un graphe $G = (V, E)$, $\tau(G)$ est son nombre de couverture par sommets de G, *i.e.* la taille du plus petit ensemble de sommets $S \subseteq V$ tel que si $u \sim v$, alors $u \in S$ ou $v \in S$: $\tau(G) = min(\{|S| | S \subseteq V, \forall uv \in E \; u \in S \text{ ou } v \in S\})$.

Voisinage pair/impair $Even(C)/Odd(C)$

Étant donné un graphe $G = (V, E)$ et $C \subseteq V$ un ensemble de sommets :

- $Odd(C)$ est le voisinage impair de C défini par $Odd(C) = \{u \in V | |N(u) \cap C| = 2k + 1, k \in \mathbb{N}\}$ (noté aussi $Odd_G(C)$ si préciser le graphe est nécessaire).
- $Even(C)$ est le voisinage pair de C défini par $Even(C) = \{u \in V | |N(u) \cap C| = 2k, k \in \mathbb{N}\}$ (noté aussi $Even_G(C)$ si préciser le graphe est nécessaire).

Table des matières

Introduction

La complexité paramétrée est une approche récente pour contourner l'impossibilité de résoudre en temps polynomial les problèmes NP-complets sous l'hypothèse $P \neq NP$, un sujet d'étude majeur en informatique. Les problèmes de domination impaire faible et de degré minimum par complémentation locale sont des problèmes de graphes classiques liés à des problématiques de traitement de l'information quantique. Plus généralement, cette approche peut être utilisée pour résoudre des cas de problèmes de domination généralisée.

Dans le cadre de cette étude, nous commencerons par décrire le traitement de l'information quantique dans son contexte de recherche théorique. Nous introduirons uniquement les notions principales nécessaires à la compréhension des résultats obtenus, pour une introduction complète se référer à [53].

Notion de qubit : En informatique classique, l'information est portée par les bits (0 ou 1) alors qu'en informatique quantique, celle-ci est portée par les qubits, qui recouvrent l'espace vectoriel complexe généré par les deux états de bases 0 et 1.

Définition 1. *Étant donné* $|0\rangle$ *et* $|1\rangle$ *des vecteurs,* $(|0\rangle, |1\rangle)$ *formant une base, un qubit est défini par :*
$\alpha |0\rangle + \beta |1\rangle$ *avec* α *et* β *des scalaires complexes et* $|\alpha|^2 + |\beta|^2 = 1$

Un qubit ayant des amplitudes complexes, il peut ainsi contenir une information a priori infinie car un complexe est constitué de deux réels. Cependant, cette information n'est pas entièrement accessible par la mesure.

Un ensemble de n bits permet de générer toutes les configurations de tailles n. Un système à n qubits quant à lui est une superposition des états classiques sur n bit : $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$, avec $\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$.

Le traitement de l'information quantique consiste donc à manipuler les qubits dans les buts principaux d'effectuer des calculs et de transmettre de l'information de façon sécurisée.

Résultats principaux de l'informatique quantique : Ces résultats peuvent être séparés en deux catégories : ceux liés au calcul quantique et ceux liés à la cryptographie quantique.

Parmi les résultats principaux concernant le calcul quantique, on peut citer les algorithmes de Grover [36] et de Shor [60]. L'algorithme de Grover permet d'effectuer une recherche dans une liste non-triée de taille n en temps $\mathcal{O}(\sqrt{n})$,

alors que dans le modèle de calcul classique tous les éléments doivent être traités (en temps n). L'algorithme de Shor factorise un entier de taille n en temps $\mathcal{O}(n^3)$, alors qu'en utilisant le modèle classique les meilleurs algorithmes sont super-polynomiaux.

De la même manière pour la cryptographie quantique, on peut citer les protocoles BB84 [3] et E91 [27].

Deux modèles de calcul principaux, universels pour le calcul quantique et équivalents, sont utilisés en traitement de l'information quantique : les circuits quantiques et le *one-way quantum computing* [58]. Par exemple, les algorithmes de Grover et de Shor ont été pensés en terme de circuit. Dans ce travail, nous nous intéresserons principalement aux états-graphes qui sont un support de l'implémentation du *one-way quantum computing*.

État-graphes : Les états graphes forment un sous-ensemble des états quantiques, en bijections avec les graphes. Ils sont définis dans [38] de la manière suivante :

Étant donné un graphe $G = (V, E)$ de sommets $v_1, \ldots, v_n$, on défini l'état graphe associé de la façon suivante :

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

avec $q(x)$ le nombre d'arêtes dans le sous-graphe induit $G[x] = (\{v_i \in V | x_i = 1\}, \{(x_i, x_j) \in E | x_i = x_j = 1\})$.

Le modèle de calcul associé aux états-graphes est le *one-way quantum computing*, introduit par Raussendorf et Briegel dans [58]. Pour un problème P donné, le *one-way quantum computing* sur un état-graphe consiste dans un premier temps à associer à chaque instance I de P un état-graphe $|G_I\rangle$. On défini également un algorithme de mesures à effectuer, où chaque nouvelle mesure dépend du résultat des précédentes. Chaque nouvelle mesure détruit le qubit sur lequel elle s'effectue, et le résultat final sera ainsi donné par la mesure du dernier qubit.

Complémentation Locale : La LU-équivalence, (LU pour Local Unitary) est une équivalence entre deux états stabilisables qui sont un sous-ensemble des états quantiques incluant les états-graphes. Soit deux états-graphes $|G_1\rangle$ et $|G_2\rangle$, alors $|G_1\rangle \equiv_{LU} |G_2\rangle$ ($|G_1\rangle$ LU-équivalent à $|G_2\rangle$) signifie que $|G_1\rangle$ est transformable en $|G_2\rangle$ (et inversement) par une séquence d'opérations unitaires locales, et ainsi cette transformation est facilement implémentable..

La LC-équivalence entre deux graphes G_1 et G_2 est définie comme la possibilité de transformer G_1 en G_2 (et inversement) par une série de complémentations locales définies par Kotzig dans [46] comme suit : dans un graphe G, la complémentation locale de G par rapport à un de ses sommets u est l'application $G \mapsto G \star u$ telle que $v \sim_{G \star u} w$ si et seulement si $(v \sim_G w)$ xor $(u \sim_G v \wedge u \sim_G w)$. Une propriété fondamentale prouvée par Bouchet [6] est le temps polynomial pour déterminer la LC-équivalence de deux graphes.

Il a été montré par Van Den Nest que deux graphes LU-équivalents étaient LC-équivalents [64]. De plus, comme la LU-équivalence et la LC-équivalence

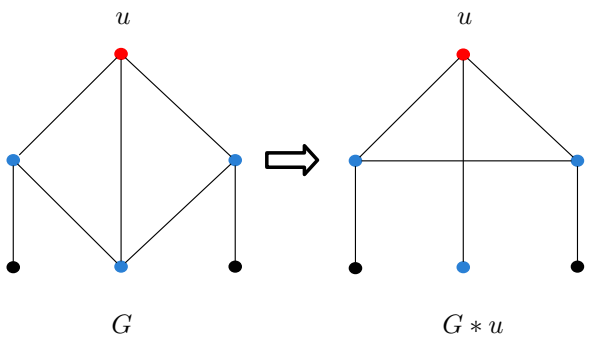


FIGURE 1 – Exemple de complémentation locale

coïncident pour certaines classes de graphes [63, 65], il a été conjecturé que c'était vrai pour tous les états-graphes (D.Schlingemann : Local equivalence of graph states in [47]). Cependant, un contre-exemple a été donné dans [44] en utilisant une méthode assistée par ordinateur.

De nombreuses études ont été menées sur la LC-équivalence des graphes, en particulier par Bouchet [8, 9] et Oum [54]. Une propriété intéressante liée à la LC-équivalence est le degré minimum par complémentation locale d'un graphe G, ce qui correspond au plus petit degré minimum parmi tous les graphes LC-équivalents à G. Dans [43], des bornes pour le degré minimum par complémentation locale ont été montrées, ainsi que les complétudes pour NP et APX du problème associé. C'est dans ce contexte que s'inscrit la partie de ce travail de thèse portant sur la LC-équivalence.

Partage de secret : Une autre application des états graphes est le partage de secrets quantiques. Introduit par Shamir dans [59], le partage de secret est un protocole de cryptographie dont le but est de partager un secret entre plusieurs personnes, ceci de façon à ce qu'un certain nombre partageant leurs connaissances puissent retrouver ce secret. Un protocole de partage de secret de seuil (n, k) consiste ainsi à distribuer à un nombre n de dépositaires une partie d'une information (le secret) pour que k ou plus dépositaires (dits acesseurs) puissent le reconstituer alors qu'un nombre inférieur n'en soit pas capable.

Le partage de secrets classiques en utilisant des canaux quantiques [40] permet de vérifier la non-compromission de l'information. Le partage de secret quantique introduit dans [20], a l'avantage par rapport à la version classique, de permettre que tout ensemble de dépositaires non-acesseurs n'ait aucune information sur le secret.

Dans ce contexte, les état-graphes permettent de définir un nouveau type de protocole, le partage de secret quantique à l'aide d'état-graphe. Ces derniers ont

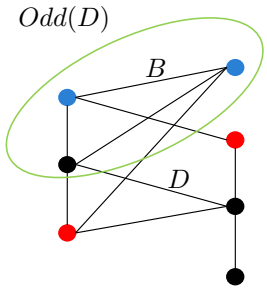


FIGURE 2 – Domination impaire faible

pour avantage d'impliquer exclusivement des opérateurs locaux (s'appliquant sur un seul qubit), plus faciles à implémenter.

Dans [49], Markham et Sanders définissent un protocole de partage de secret à l'aide d'état-graphe. Dans ce protocole, l'implication d'un ensemble de propriétés graphiques dites de domination impaire faible a été montrée par Perdrix *et al.* dans [43].

Domination impaire faible (WOD) : Étant donné un graphe $G = (V, E)$ un ensemble de sommets $B \subseteq V$ est dominé de façon impaire faible ou WOD pour Weak Odd Dominated si et seulement si il existe un ensemble de sommets $D \subseteq V \setminus B$ tel que B appartient au voisinage impair de D *i.e.* les sommets ayant un nombre impair de voisins dans D. Le seuil du protocole de Markham et Sanders est défini comme le maximum entre la taille du plus grand ensemble dominé de façon impaire faible et la taille du graphe moins celle du plus petit ensemble non-dominé de façon impaire faible.

Le problème de décision associé au seuil de ce protocole a été démontré NP-complet dans [43], et plusieurs bornes concernant les diverses quantités associées ont été montrées dans ce même article. C'est dans la continuité de ces travaux que s'inscrit ce travail de thèse, en particulier sur l'aspect de la complexité paramétrée de ce problème.

La WOD est un type particulier de domination et il est intéressant d'élargir l'étude de la complexité paramétrée au cas général de la domination.

(σ, ρ)-domination : La (σ, ρ)-domination, introduite par Telle dans [62], est un cadre général de domination défini de la façon suivante : étant donnés σ et ρ deux ensembles d'entiers naturels et $G = (V, E)$ un graphe :
Un ensemble de sommets $D \subseteq V$ est (σ, ρ)-dominant si et seulement si :

- $\forall d \in D,\ |N(d) \cap D| \in \sigma$
- $\forall u \in V \setminus D,\ |N(u) \cap D| \in \rho$

Ainsi, avec la (σ, ρ)-domination, le problème classique de domination s'ex-

prime en $(\mathbb{N}, \mathbb{N}^+)$-domination (pas de contrainte dans le dominant et au moins un voisin pour les autres), le problème Code Parfait devient $(\{0\}, \{1\})$-domination et la domination impaire devient $(\mathbb{N}, IMPAIR)$-domination.

Les problèmes de (σ, ρ)-domination ont été fortement étudiés dans le cadre de la complexité paramétrée [33, 45, 50]. En particulier, Domination est $W[2]$-complet [25] et Code parfait est $W[1]$-complet [14].

Complexité paramétrée : Ce type de complexité, définie par Downey et Fellows [28], raffine les problèmes NP-complets par l'ajout d'un paramètre fixe dans les données du problème. En particulier, ce cadre permet de mettre en évidence les problèmes dit FPT (pour Fixed Parameter Tractable) qui, bien que NP-complets, peuvent être résolus en temps $f(k)p(x)$, avec f une fonction quelconque, k le paramètre fixe, p un polynôme, et x la taille de l'entrée du problème. On peut citer comme exemple de problème FPT celui de la couverture par sommets [30].

Ce cadre définit aussi la hiérarchie W qui, pour tout $i \in \mathbb{N}$, associe une classe $W[i]$ définie par la complexité minimum des circuits permettant de résoudre les problèmes qui lui appartiennent. Cette hiérarchie a également la propriété d'inclusion suivante : $W[i] \subseteq W[i+1]$, FPT pouvant être vu comme $W[0]$.

L'étude des problèmes de graphe en terme de complexité paramétrée a donné lieu à de nombreux résultats (pour une liste non-exhaustive voir [16], [25] ou [52]), et en particulier pour les problèmes de domination qui s'inscrivent dans le cadre de cette thèse voir le tableau 1.4.1.

Ce travail se divise en trois chapitres, le premier sur la domination généralisée introduisant également la complexité paramétrée, le second sur la WOD et le dernier sur le degré minimum par complémentation locale.

Chapitre 1 : Domination généralisée Ce travail commence par un chapitre consacré à l'étude de la complexité paramétrée de problèmes de domination généralisée. Tout d'abord les problèmes de domination généralisée seront définis et plus particulièrement la (σ, ρ)-domination définie par Telle [62]. Dans un graphe $G = (V, E)$ étant donné σ et ρ deux ensembles d'entiers, un ensemble D sera dit (σ, ρ)-dominant si et seulement si pour tout $u \in D$ la taille de son voisinage dans D appartient à σ et pour tout $u \in V \setminus D$ la taille de son voisinage dans D appartient à ρ.

On définira ensuite le cadre de la complexité paramétrée. Dans ce chapitre, on s'intéressera plus particulièrement aux classes FPT, $W[1]$ et $W[2]$ étant les classes auxquelles appartiennent la plupart des problèmes de graphes [33, 25, 16].

Enfin, on définira la méthode par machine de Turing de Cesati [15] qui servira de base à notre principal outil de démonstration du chapitre. Il s'agit d'exhiber une exécution courte d'une machine de Turing résolvant un problème afin de montrer son appartenance à $W[1]$ et $W[2]$ selon que la machine soit respectivement simple ou multi-bandes.

Le corps de ce chapitre sera ensuite constitué de la présentation de la méthode par machine de Turing aveugle 1.3 et de son utilisation pour montrer la complexité paramétrée de nombreux problèmes de domination généralisée.

La présentation de la définition du problème d'exécution courte de machine de Turing aveugle introduira cette partie. Une machine de Turing aveugle est une version de machine de Turing multi-bandes à laquelle on ajoute un nouveau type de transition ne dépendant pas de l'état de la bande. Suivra la démonstration de l'appartenance du problème d'exécution courte de machine de Turing aveugle à $W[2]$.

Le résultat majeur de cette partie sera la preuve de l'appartenance du problème de (σ, ρ)-domination à $W[2]$ pour tout σ et tout ρ récursifs (c-à-d. l'appartenance à σ et ρ est calculable). Celle-ci sera effectuée par réduction au problème d'exécution courte de machine de Turing aveugle.

On terminera par l'utilisation de l'exécution courte de machine de Turing aveugle pour résoudre d'autres problèmes de dominations et de théorie des codes.

Chapitre 2 : Domination impaire faible. Dans ce second chapitre on étudiera les problèmes de domination impaires faibles. Dans un graphe $G = (V, E)$ un ensemble de sommets $B \subseteq V$ est faiblement dominé si et seulement si il existe un autre ensemble de sommets $D \subseteq V \setminus B$ tel que B appartient au voisinage impaire de D. On cherchera la taille $\kappa(G)$ du plus grand ensemble faiblement dominé de façon impaire (WOD pour Weak Odd Dominated) car, étant donné B un ensemble WOD, alors tout sous-ensemble de B l'est également. On cherchera aussi la taille $\kappa'(G)$ plus petit ensemble non-WOD car étant donné B un ensemble non-WOD pour tout sommet $v \in V$ $B \cup v$ est non-WOD. Enfin, on cherchera $\kappa_Q(G)$ le maximum de κ et $|V| - \kappa'(G)$.

Ces trois problèmes viennent du partage de secret à l'aide d'états graphes, $\kappa(G)$ correspondant au plus grand ensemble de joueurs non-accesseur d'un protocole de partage de secret classique, $\kappa'(G)$ au plus petit ensemble de joueurs accesseur et enfin $\kappa_Q(G)$ au seuil d'accessibilité d'un protocole de partage de secret quantique. On commencera donc par présenter ces différents protocoles et leur utilité pour définir précisément les problèmes puis ces derniers seront associés à un état de l'art sur les différentes bornes et constructions existantes pour ces différentes valeurs.

La suite de ce chapitre correspondra ensuite au travail effectué et apportant de nouveaux résultats publiés dans [11].

Dans un premier temps, on améliorera les bornes existantes pour les valeurs de κ et κ' par une méthode non-déterministe. Il s'agit de choisir de façon aléatoire un ensemble D, chaque sommet ayant une probabilité $1 - q$ d'appartenir à D, d'estimer la taille de son voisinage impair $Odd(D)$, et enfin d'optimiser l'espérance de celle-ci en variant q.

Ensuite, étant donné que les problèmes liés à à la détermination des différentes valeurs κ, κ' et κ_Q ont été montrés NP-complets dans [43], on s'intéressera à la complexité paramétré de ces problèmes. On commencera par déterminer la bonne paramétrisation à adopter. En particulier, on montrera que la paramétrisation standard par la taille de l'ensemble cherché n'est pas satisfaisante menant à des algorithmes FPT mais de noyaux linéaires dans la taille de l'entrée. On adoptera donc la paramétrisation duale, le paramètre devenant la taille du reste du graphe, et montrera par un cycle de FPT-réductions la FPT-

équivalence de ces problèmes avec Ensemble impair un problème classique de domination avec parité montré $W[1]$-difficile et appartenant à $W[2]$ dans [33].

Enfin on s'intéressera à la complexité en approximation des valeurs de κ, κ' et κ_Q et les problèmes associés seront montrés APX-complets pour κ et κ'. Pour le problème associé à κ_Q, seule l'appartenance à APX sera montrée.

Chapitre 3 : Degré minimum par complémentation locale. Le dernier chapitre consiste en une étude du degré minimum par complémentation locale. On commencera par l'introduction de la complémentation locale, une transformation sur les graphes, puis de la LC-équivalence qui est l'équivalence de deux graphes par une série de complémentation locale. Ensuite, on introduira les notions de LU-équivalence et d'équivalence de rang de coupe. Celles-ci sont liés à la LC-équivalence et à des propriétés très étudiées, en particulier dans le domaine de l'informatique quantique. Puis on introduira la notion clef du chapitre, le degré minimum par complémentation locale, qui est le plus petit ensemble de sommets constitué par un sous-ensemble de sommets et son voisinage impair. Le nom de degré minimum par complémentation locale vient de la possibilité par une série de complémentations locales de transformer un tel ensemble en un sommet et ses voisins, et donc le plus petit degré minimum des graphes dans l'orbite LC du graphe de départ.

Suite à l'introduction de ces notions essentielles, le reste de ce chapitre sera consacré aux nouveaux résultats obtenus et publiés dans [13].

En utilisant la borne de Plotkine [56], on montre tout d'abord une borne supérieur par le nombre de couverture par sommet qui amène la borne suivante pour les graphes biparties : $\delta_{loc}(G) < \frac{n}{4} + log_2 n$ 21, puis cette borne est ramenée à $\delta_{loc}(G) < \frac{3n}{8} + log_2 n$ 22 pour le cas général.

Ensuite une étude de la complexité paramétrée de problème de degré minimum par complémentation locale sera présentée. La paramétrisation se fera de façon classique par la taille de l'ensemble. On ne considère ici que la complexité paramétrée car il a été montré dans [43] que le problème de degré minimum par complémentation locale est NP-complet et APX-complet. Le résultat principal est la démonstration de la FPT-équivalence de ce problème avec Ensemble pair un problème classique de domination avec parité appartenant à $W[2]$ [33].

Enfin, on construira un algorithme exact en temps exponentiel à partir des bornes montrées précédemment. Cet algorithme a une complexité en $\mathcal{O}^*(1.938^n)$ et est ensuite raffiné à $\mathcal{O}^*(1.466^n)$ pour les graphes bipartis.

Chapitre 1

Complexité paramétrique de problèmes de domination généralisée

Dans ce chapitre, on s'intéresse aux problèmes de domination généralisée, définis par Telle dans [62] de la façon suivante :

Étant donné un graphe $G = (V, E)$ et deux ensembles d'entiers σ et ρ, un ensemble de sommets $D \subseteq V$ est (σ, ρ)-dominant si :

- $\forall d \in D, |N(d) \cap D| \in \sigma$
- $\forall d \in V \setminus D, |N(d) \cap D| \in \rho$

De nombreux problèmes classiques de domination comme Ensemble dominant ou Ensemble indépendant entrent dans le cadre de la domination généralisée et deviennent ainsi Ensemble $(\mathbb{N}, \mathbb{N}^+)$-dominant et Ensemble $(\{0\}, \mathbb{N})$-dominant. La plupart de ces problèmes étant NP-complets pour les graphes en général, leur complexité paramétrée a été étudiée pour établir les liens entre les variations de σ et ρ et la difficulté des problèmes [33, 45, 50].

Nous commencerons par définir une nouvelle méthode de preuve d'appartenance à $W[2]$ grâce à une machine de Turing dite "aveugle", pour ensuite démontrer l'appartenance à $W[2]$ du problème de domination généralisée pour tout σ et ρ récursifs ainsi que pour des problèmes de codes linéaires. Ce chapitre regroupe les résultats publiés lors de la conférence TAMC de 2014 [12].

1.1 Complexité paramétrée

1.1.1 Principes et classe FPT

Cette notion a été introduite par Downey et Fellows dans [24]. Il s'agit d'extraire un paramètre, le plus souvent un entier, appelé paramètre, des entrées

d'un problème. il s'agira ensuite de considérer la complexité du problème en fonction de la taille des entrées et aussi de ce paramètre. La complexité paramétrée a pour but de raffiner la classe NP. Par exemple ces deux problèmes donné dans [28] : l'existence d'un transversal de taille k et d'un dominant de taille k définis par :

Transversal de taille au plus k
Entrée : Un graphe $G = (V, E)$, un entier k.
Question : Existe-t-il un sous-ensemble V' de V de taille au plus k tel que pour toute arête uv de E, u ou v appartiennent à V' ?

Ensemble dominant de taille au plus k
Entrée : Un graphe $G = (V, E)$, un entier k.
Question : Existe-t-il un sous-ensemble D de V de taille au plus k tel que tout sommet v de $V \setminus D$ a au moins un voisin dans D ?

Bien que ces deux problèmes appartiennent à la classe NP on peut remarquer qu'avec le choix de k la taille de la solution comme paramètre on a une grande différence entre la complexité de ces problèmes. En effet, le meilleur algorithme connu pour résoudre le problème de transversal est en $\mathcal{O}(1.271^k + kn)$ [19] alors que l'on reste sur une exploration de tous les sous-ensembles possibles pour la domination, soit un algorithme en $\mathcal{O}(n^{k+1})$. Cette différence devenant significative si l'on considère un k assez petit où le transversal peut être calculé en temps raisonnable [18]. Cette différence mène donc aux définitions suivantes des problèmes FPT pour Fixed Parameter Tractable (décidable à paramètre fixe) :

Définition 2. *Un langage paramétré est un sous-ensemble $L \subseteq \Sigma^* \times \Sigma^*$ (Σ étant le vocabulaire). Si (x, k) est un langage paramétré alors on considère x comme la partie principale et k comme le paramètre.*

Il est à noter ici que le paramètre n'est pas forcément un entier même ci cela représente la majorité des cas étudiés.

Définition 3. *Un langage paramétré L est dit FPT si l'on peut déterminer si $(x, k) \in L$ en temps $f(|k|)q(n)$, avec $|x| = n$, q est un polynôme en n et f est une fonction quelconque.*

Dans la définition de FPT, $q(n)$ est un polynôme en n et ne dépend pas de k, sont donc exclus les temps d'exécution en n^k.

1.1.2 Réduction paramétrée et hiérarchie W

Dans la section précédente, on a défini FPT la classe des problèmes paramétrés pouvant se résoudre en temps polynomial (hors paramètre). Se pose maintenant la question de savoir si cette classe ne représente pas en fait l'intégralité des problèmes paramétrés.

Tout d'abord il faut définir la notion de réduction polynomiale en complexité paramétrée. Pour qu'une réduction paramétrée soit polynomiale il faut que celle-ci se fasse en temps $f(|k|)q(n)$ (comme pour la définition de FPT) mais aussi que le nouveau paramètre k' dépende exclusivement de k (par une fonction quelconque), ce qui donne la définition suivante dans [24] :

Définition 4. *Une réduction polynomiale d'un langage paramétré L à un langage paramétré L' est un algorithme qui avec comme entrée (x, k) produit (x', k') tel que :*

- *$(x, y) \in L$ si et seulement si $(x', k') \in L'$.*
- *$k' = g(k)$ est fonction de k seul.*
- *le calcul s'effectue en temps $f(|k|)q(n)$ avec $n = |x|$, f est une fonction quelconque et $q(n)$ un polynôme en n ne dépendant pas de k.*

Pour la suite, on nommera ces réductions polynomiales entre langages paramétrés réductions-FPT.

De manière analogue à la complexité classique, on va partir du problème d'arrêt d'une machine de Turing dont le paramètre va être le temps d'exécution, défini dans [24] par :

Exécution courte d'une machine de Turing non-déterministe simple
Entrée : Une machine de Turing non-déterministe simple, un mot w sur l'alphabet Σ, un entier k.
Paramètre : k.
Question : Existe-t-il une exécution de M sur w qui atteint un état acceptant en au plus k étapes ?

La classe de ce problème est $W[1]$, or Exécution courte d'une machine de Turing non-déterministe simple est difficile pour $W[1]$ [25], donc que le problème d'exécution courte est plus difficile que tout problème appartenant à $W[1]$. De manière analogue à la complexité classique, la réponse à $FPT = W[1]$ reste ouverte. Il est à noté que cette question repose sur la question de complexité classique $P \neq NP$ [24].

En revanche, il a été remarqué qu'en revenant à l'exemple de départ de problème difficile en complexité paramétré Ensemble dominant de taille au plus k, on ne trouve pas de réduction de ce problème à l'exécution courte de machine de Turing. En effet, en complexité paramétrée, il existe une infinité de classes $W[i]$ pour tout i entier naturel avec $W[i] \subseteq W[i+1]$, FPT étant égale à $W[0]$, la question de l'égalité entre chacune de ces classes revenant à la question $FPT = W[1]$. Dans [24] Ensemble dominant de taille au plus k est montré complet pour $W[2]$, on a donc que Ensemble dominant de taille au plus k n'est pas FPT et donc qu'il n'existe pas d'algorithme en temps $f(|k|)q(n)$ qui résout ce problème, à moins que la hiérarchie W ne s'effondre dans FPT.

Chacune des classes $W[i]$ est définie dans [23] à l'aide des circuits mixtes définis comme :

Définition 5. *Un circuit mixte de décision est un circuit booléen ayant un nombre non borné d'entrées et une seule sortie avec deux types de portes :*
- *les* **petites portes** *sont des portes ET et OU ayant deux entrées.*
- *les* **grandes portes** *sont des portes ET et OU ayant un nombre non borné d'entrées.*

Définition 6. La profondeur *d'un circuit mixte est le nombre maximum de portes (petites et grandes portes) se trouvant sur un chemin entrée/sortie.*
La largeur de trame *d'un circuit mixte est le nombre maximum de grandes portes se trouvant sur un chemin entrée/sortie.*

Définition 7. *Étant donné F une famille de circuits mixtes de décision de profondeur maximale h et de largeur de trame maximale i, L_F est le problème paramétrique de circuit défini par : $L_F = \{(C, k) : C \in F$ accepte une entrée de poids $k\}$, poids d'une entrée étant le nombre d'entrées du circuit à 1.*

La définition des classes $W[i]$ est donc :

Définition 8. *Un problème L appartient à $W[i]$ si L se réduit uniformément au problème de circuit paramétrique L_F pour la famille $F_{h,i}$ de circuits mixtes de décision.*

Il est à noter que cette définition revient à déterminer si l'on peut résoudre le problème L avec un circuit de taille $f(|k|)q(n)$ (car il s'agit d'une réduction), de profondeur bornée (ne dépendant donc ni de n ni de k) et de largeur de trame i.

On utilisera aussi ici une autre hiérarchie avec les classes $W^*[i]$, celles-ci sont analogues aux classes $W[i]$ et correspondent donc aux classes de problèmes pouvant être résolus à l'aide de circuits mixtes de largeur de trame i mais avec une profondeur dépendant du paramètre k (au lieu d'une profondeur fixe dans le cas des $W[i]$). Le principal résultat concernant ces classes étant les égalités $W[1] = W^*[1]$ et $W[2] = W^*[2]$ [23].

1.2 Méthode par machine de Turing

1.2.1 Définition

Pour démontrer l'appartenance d'un problème L à une classe $W[i]$, pour $i \geq 1$ on a trois possibilités :
- soit effectuer une réduction de L à partir du problème canonique associé à la classe $W[i]$, le problème de circuit $L_{F(i,h)}$ avec $F(i, h)$ la famille des circuits mixtes de trame i et de profondeur h une constante quelconque, c'est à dire résoudre le problème à l'aide de circuits de taille polynomiale en n, de profondeur constante et trame i (pour rappel la trame est la profondeur du circuit en ne comptant que les "grandes portes").
- soit comme pour la complexité classique une réduction à des problèmes connus existants.

– soit par exécution courte de machine de Turing non-déterministe [15].
En effet, dans [25], Downey et Fellows ont montré que le problème d'exécution courte de machine de Turing simple est complet pour $W[1]$, ce qui permet d'avoir un outil pratique permettant de montrer l'appartenance à $W[1]$. En particulier, une démonstration simple de l'appartenance à $W[1]$ de Code parfait a été donnée par Cesati [14]. Le problème associé à la machine simple est défini comme :

Exécution courte d'une machine de Turing non-déterministe simple
Entrée : Une machine de Turing non-déterministe à une seule bande, un mot w sur l'alphabet Σ, un entier k.
Paramètre : k.
Question : Existe-t-il une exécution de M sur w qui atteint un état accepteur en au plus k étapes ?

Cesati a ensuite étendu cette méthode à $W[2]$ en prouvant la complétude pour $W[2]$ de la version multi-bandes du problème de l'arrêt qui permet par exemple de montrer l'appartenance à $W[2]$ de la version paramétrée du problème d'Arbre de Steiner [15]. Le problème associé à la machine multi-bandes est défini comme :

Exécution courte d'une machine de Turing non-déterministe multi-bandes
Entrée : Une machine de Turing non-déterministe à m bandes, un mot w sur l'alphabet Σ, un entier k.
Paramètre : k.
Question : Existe-t-il une exécution de M sur w qui atteint un état acceptant en au plus k étapes ?

1.2.2 Exemple d'application : Domination classique

Ici on montre un exemple d'application de la méthode par machine de Turing multi-bandes au problème classique de domination Ensemble dominant de taille au plus k défini comme suit :

Ensemble dominant de taille au plus k
Entrée : Un graphe $G = (V, E)$, un entier k.
Paramètre : k.
Question : Existe-t-il un sous-ensemble D de V de taille au plus k tel que tout sommet v de $V \setminus D$ a au moins un voisin dans D ?

La description complète de la machine de Turing non-déterministe à $n+1$ bandes est la suivante : $M = (Q, \Gamma, \Delta, \Sigma, b, q_I, Q_A)$, avec :
$\Gamma = \{\square, 0, 1, v_1, \ldots, v_n\}$ l'alphabet, $b = \square$ le symbole blanc, $\Sigma = \varnothing$ l'alphabet d'entrée vide ici, $Q = \{q_{r,s} \mid r \in [1, n+1], s \in [0, k]\} \cup \{q_s^{\text{ret}} \mid s \in [1, k+1]\} \cup \{q_{i,s}^{\text{sig}} \mid i \in [1, n], s \in [0, k]\} \cup \{q^{\text{sig}}, q^{\text{end}}, q^{\text{read}}, q_A\}$, $q_I = q_{1,0}$ l'ensemble des états et $Q_A = \{q_A\}$ l'ensemble des états accepteurs. L'ensemble des transitions Δ

étant par la suite, un exemple d'exécution est aussi donné 1.1.

Étape 1 – Initialisation de D

$\langle \square\square^n, q_{r,s}, v_i\square^n, q_{i+1,s+1}, (+1)0^n \rangle$ $\quad i \in [1,n], r \in [1,n], s \in [0,k]$
$\langle \square\square^n, q_{r,s}, \square\square^n, q_{r,s+1}, 00^n \rangle$ $\quad r \in [1,n+1], s \in [0,k]$
$\langle \square\square^n, q_{r,k}, \square\square^n, q^{\text{end}}, (-1)0^n \rangle$ $\quad r \in [1,n+1]$
$\langle v_i\square^n, q^{\text{end}}, v_i\square^n, q^{\text{end}}, (-1)0^n \rangle$ $\quad i \in [1,n]$
$\langle \square\square^n, q^{\text{end}}, \square\square^n, q^{\text{end}}, (-1)0^n \rangle$
$\langle \square\square^n, q^{\text{end}}, \square\square^n, q^{\text{read}}, (+1)0^n \rangle$

Atteindre l'état $q_{r,s}$ signifie que $s-1$ sommets parmi $v_1, \ldots, v_{r-1}$ ont déjà été choisis sur la première bande, son utilisation nous permet de ne pas effectuer deux fois le même choix de sommet dans D étant donné que, dans la table de transitions celles ayant $q_{r,s}$ pour état initial ne permettent pas l'écriture de sommets d'indices inférieurs à r.

Atteindre l'état q^{end} signifie que l'initialisation de D est terminée et que les têtes de lecture sont revenues aux cellules non-vides (contenant un autre symbole que le symbole blanc $\square$) les plus à gauche sur chaque bande.

Étape 2 : Exploration du voisinage

$$\langle v_i\square^n, q^{\text{read}}, v_i s_1 \ldots s_n, q^{\text{read}}, (+1)d_1 \ldots d_n \rangle \quad i \in [1,n], \text{où } d_t = \begin{cases} +1 & \text{si } v_t \in N[v_i] \\ 0 & \text{sinon} \end{cases}$$

Avec $N[v]$ le voisinage fermé de v : $N[v] = N(v) \bigcup \{v\}$

Ici, on explore un par un les sommets de l'ensemble choisi D sur la première bande. Pour chaque sommet de D, on va inscrire 1 sur toutes les bandes associées aux sommets de son voisinage fermé pour marquer sa domination, décaler la tête de lecture sur la droite pour garantir que toutes les têtes lisent bien $\square$ (pour éviter l'explosion du nombre de transitions), et passer au sommet de D suivant.
Étape 3 : Vérification

$\langle \square\square^n, q^{\text{read}}, \square\square^n, q_f, 0(-1)^n \rangle$
$\langle \square 1^n, q^{\text{read}}, \square 1^n, q_A, 00^n \rangle$

Enfin, on se contente de revenir une fois à gauche sur toutes les bandes sauf la première : si un sommet est dominé par au moins un élément de l'ensemble alors il y aura un 1 sinon un $\square$. L'ensemble choisi est donc dominant si et seulement si toutes les têtes de lectures sauf la première pointent sur des 1.

1.2.3 Limite : Domination impaire

Prenons maintenant un autre exemple de problème de domination appartenant à $W[2]$ avec Ensemble dominant impair de taille au plus k (prouvé dans [33]) défini comme suit :

Ensemble dominant impair de taille au plus k
Entrée : Un graphe bipartie $G = (R, B, E)$, un entier k.

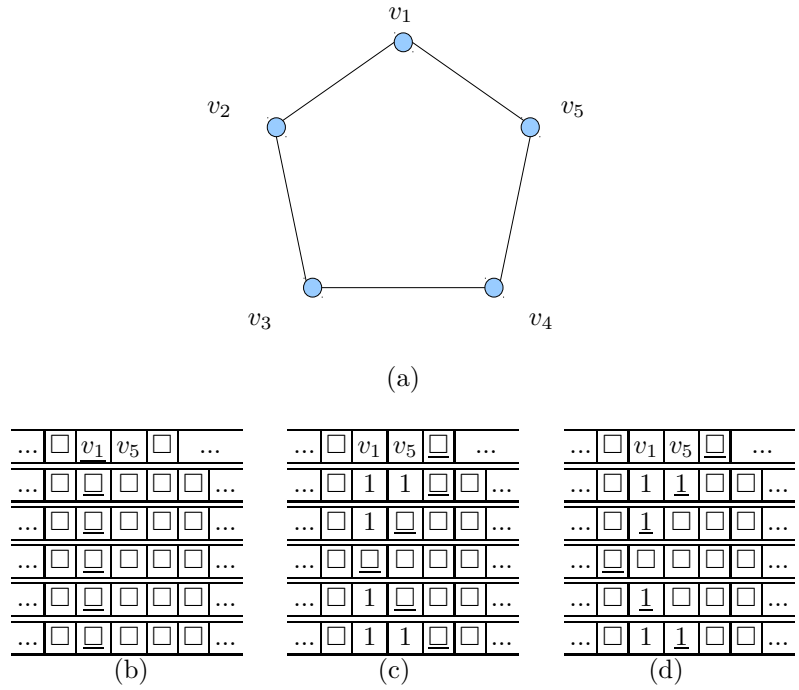


FIGURE 1.1 – Calcul de ENSEMBLE DOMINANT DE TAILLE AU PLUS k sur une machine de Turing multi-bandes avec $k = 2$ pour un C_5. (a) Graphe d'entré ; (b) État de la machine à la fin de la phase (1) : l'ensemble D choisi est sur la première bande, les autres sont vides ; (c) Fin de la phase (2) : on a inscrit sur la bande associée à chaque sommet le nombre de sommets de D dans son voisinage fermé ; (d) Fin de la phase (3) : on fait revenir toutes les têtes de lecture (symbole souligné) d'une position à gauche, v_1, v_2, v_4 et v_5 lisent 1 et sont donc dominés mais pas v_3, l'ensemble n'est pas dominant. Pour illustrer le fonctionnement, on a choisi $\{v_1, v_5\}$ qui n'est pas dominant. La machine étant non-déterministe aurait choisit un dominant comme $\{v_1, v_4\}$.

Paramètre : k.
Question : Existe-t-il un sous-ensemble R' de R de taille au plus k tel que tout sommet b de B a un nombre impair de voisins dans R' ?
Ici, on a la difficulté d'avoir la parité de chaque sommet. Pour appliquer une méthode similaire à celle de l'exemple précédant, on peut imaginer une machine à $|B|+1$ bandes, la première servant à tirer R' et ensuite une bande pour chaque sommet de B. À ce moment, on peut capturer la parité en inscrivant celle-ci sur la bande par une alternance de 0 et de 1 pour ensuite décaler la tête de lecture de chaque bande associée à un sommet du voisinage lors du parcours de R'. Cette solution résout bien le problème mais ne correspond pas à une réduction paramétrée car elle nécessite un nombre exponentiel de transitions. En effet, si à la fin du parcours il est simple de vérifier la parité si toutes les têtes de lecture pointent vers 1, à un instant donné du parcours toutes les configurations de parité de chacun des sommets sont possibles il faut donc une table de transition de taille $2^{|B|}$. D'autres solutions simples sont possibles mais aboutissent soit à une explosion du nombre de configurations soit à un nombre de transitions trop grand. Étant donné la difficulté pour $W[2]$ du problème d'exécution de la machine, une réduction existe mais on voit bien une limite de cette méthode en tant qu'outil pour faciliter la démonstration de l'appartenance à $W[2]$.

1.3 Machine de Turing aveugle

1.3.1 Définition

L'exemple du problème de domination impaire (voir le paragraphe 1.2.3) nous montre une limite de la méthode par machine de Turing. Dans cet exemple, l'impossibilité d'inscrire la parité de chaque sommet sur sa bande sans faire exploser le nombre de transitions interdit l'utilisation d'une machine similaire à celle de la domination classique.

En revanche, on peut se rendre compte que l'on peut inscrire à l'avance cette parité sur chacune des bandes par une alternance de symboles (voir la figure 1.2) et faire non plus du nombre de symboles mais de la position de la tête de lecture la marque du nombre de domination de chaque sommet, en décalant à gauche la tête de lecture de chaque voisin des sommets du dominant. Ainsi, la lecture de la configuration courante n'est plus nécessaire qu'à la fin, au moment de la vérification où la configuration doit être uniformément impaire.

Avec cette méthode, l'explosion du nombre de configurations persiste toujours, mais en ajoutant un nouveau type de transition qui ne dépend pas du symbole lu sur certaines bandes, on peut résoudre ce problème. On crée donc de nouvelles transitions qui ne dépendent plus (ou partiellement plus) de la configuration courante de la machine, c'est ce type de transition que l'on appelle transition "aveugle".

Pour plus de clarté, on ne va pas définir un nouvel ensemble de transitions, mais introduire dans l'alphabet un nouveau symbole neutre "␣" qui s'il se situe en partie gauche de la transition signifie "quelque soit le symbole lu" et en

partie droite "le même symbole que celui lu" sur cette bande. Ainsi la transition $\langle \sqcup^k, q, \sqcup^k, q', +1^k \rangle$ signifie que dans l'état q, quelque soit la configuration, on la laisse, puis on passe à l'état q' et on décale toutes les têtes de lecture à droite.

La définition d'une machine de Turing aveugle sera donc aussi un septuplet $M = (Q, \underline{\Gamma}, \Delta, \Sigma, b, q_0, Q_F)$ avec Q l'ensemble des états, $\underline{\Gamma} = \Gamma \cup \{\sqcup\}$ l'ensemble des symboles de travail et l'ajout du symbole neutre "$\sqcup$" pour les transitions aveugles, $\Delta \subseteq (\underline{\Gamma}^m \times Q \times \underline{\Gamma}^m \times Q \times \{\text{-}1^m, 0^m, 1^m\})$ l'ensemble des transitions, Σ l'ensemble des symboles inscrits sur les bandes ($\Sigma = \underline{\Gamma} \setminus \{b, \sqcup\}$), b le symbole blanc, q_0 l'état initial, et Q_F l'ensemble des états accepteurs. Pour prouver l'appartenance d'un problème à $W[2]$, la méthode par machine de Turing aveugle se fera, comme pour la méthode classique, en effectuant une réduction vers un problème d'exécution courte avec une machine de Turing donc en définissant une machine qui résout le problème. On défini donc le problème d'exécution courte de la façon suivante :

Exécution courte d'une machine de Turing aveugle non-déterministe multi-bandes
Entrée : Une machine de Turing aveugle non-déterministe à m bandes, un mot w sur l'alphabet Σ, un entier k.
Paramètre : k.
Question : Existe-t-il une exécution de M sur w qui atteint un état accepteur en au plus k étapes ?

1.3.2 $W[2]$-complétude

La difficulté pour $W[2]$ est induite par la complétude pour $W[2]$ du cas classique [15], la machine classique étant un cas particulier de machine aveugle n'utilisant jamais le symbole neutre. Pour obtenir la complétude il reste donc à prouver l'appartenance à $W[2]$.

Comme pour le cas classique, il s'agit en fait d'une appartenance à $W^*[2]$ défini dans [23] comme étant la classe des problèmes pouvant être résolus par un circuit mixte de trame 2 (profondeur ne comptant que les portes de taille d'entrée non-bornée) et de profondeur bornée par une fonction de k (au lieu d'être constante pour $W[2]$). Comme l'égalité $W^*[2] = W[2]$ est aussi montrée dans [23], on obtient notre appartenance à $W[2]$.

L'appartenance à $W^*[2]$ se montre directement en exhibant pour toute machine de Turing aveugle M et tout entier k un circuit mixte de trame 2 et de profondeur bornée par une fonction de k qui résout Exécution courte d'une machine de Turing aveugle non-déterministe multi-bandes de (M, k).

Théorème 1. Exécution courte d'une machine de Turing aveugle non-déterministe multi-bandes *est complet pour* $W[2]$.

Démonstration. Dans un premier temps, M est transformée en une machine qui si elle atteint un état accepteur en au plus k étapes l'atteint aussi en exactement k étapes. Pour cela, les états accepteurs de M sont fusionnés en un seul état q_A et on ajoute une transition aveugle $\langle \sqcup^m, q_A, \sqcup^m, q_A, 0^m \rangle$ qui boucle sur l'état

accepteur sans lire ni modifier la configuration. Ainsi, si on atteint un état accepteur en k étapes on atteint q_A en k étapes, et si on l'atteint avant on reste sur q_A jusqu'à la $k^{ème}$ étape.

Dans la suite, C est un circuit mixte de largeur de trame 2 de façon à ce que les entrées qui renvoient vrai correspondent aux séquences de k transitions d'une machine M de l'état initial à l'état accepteur.

L'ensemble Δ des transitions de M est indexé par $j \in [1, |\Delta|]$. Les symboles de $\underline{\Gamma}$ sont indexés par $s \in [0, |\Gamma|]$, où 0 et $|\Gamma|$ sont respectivement l'indice du symbole blanc et l'indice du symbole neutre '␣'. Soit $x[i, j]$ pour tout $i \in [1, k], j \in [1, |\Delta|]$ et $x[-1, -1]$ les entrées du circuit. Pour tout $i \in [1, k], j \in [1, |\Delta|]$, $x[i, j]$ est vrai si et seulement si la $i^{ème}$ transition de la séquence d'exécution de la machine est la transition d'index j, $x[-1, -1]$ représentant la constante 0.

Les portes suivantes encodent les informations sur les transitions de M : $\forall i \in [1, k], \forall q \in [1, |Q|], \forall s \in [0, |\Gamma|], \forall t \in [1, m], \forall d \in \{\text{-}1, 0, 1\}$,

- $\tau_o(i, q)$ renvoie vrai ssi l'état initial de la $i^{ème}$ transition est q :

$$\tau_o(i, q) := \bigvee_{j \in J_q} x[i, j]$$

  où $J_q = \Delta \cap (\underline{\Gamma}^m \times \{q\} \times \underline{\Gamma}^m \times Q \times \{\text{-}1, 0, 1\}^m)$
- $\tau_n(i, q)$ renvoie vrai ssi l'état terminal de la $i^{ème}$ transition est q :

$$\tau_n(i, q) := \bigvee_{j \in J'_q} x[i, j]$$

  où $J'_q = \Delta \cap (\underline{\Gamma}^m \times Q \times \underline{\Gamma}^m \times \{q\} \times \{\text{-}1, 0, 1\}^m)$
- $\sigma_o(i, s, t)$ renvoie vrai ssi à la $i^{ème}$ transition, soit le symbole lu sur bande t est s, soit on ne lit pas le symbole sur la bande t dans le cas "aveugle" $(s = |\Gamma|)$:

$$\sigma_o(i, s, t) := \bigvee_{j \in J_{s,t}} x[i, j]$$

  où $J_{s,t} = \Delta \cap (\underline{\Gamma}^{t-1} \times \{s\} \times \underline{\Gamma}^{m-t} \times Q \times \underline{\Gamma}^m \times Q \times \{\text{-}1, 0, 1\}^m)$
- $\sigma_n(i, s, t)$ renvoie vrai ssi à la $i^{ème}$ transition, soit le symbole écrit sur la bande t est s, soit il n'y a pas de réécriture sur la bande t dans le cas "aveugle" $(s = |\Gamma|)$:

$$\sigma_n(i, s, t) := \bigvee_{j \in J'_{s,t}} x[i, j]$$

  où $J'_{s,t} = \Delta \cap (\underline{\Gamma}^m \times Q \times \underline{\Gamma}^{t-1} \times \{s\} \times \underline{\Gamma}^{m-t} \times Q \times \{\text{-}1, 0, 1\}^m)$
- $\mu(i, d, t)$ renvoie vrai ssi à la $i^{ème}$ transition, la tête t a pour mouvement d :

$$\mu(i, d, t) := \bigvee_{j \in J_{d,t}} x[i, j]$$

  où $J_{d,t} = \Delta \cap (\underline{\Gamma}^m \times Q \times \underline{\Gamma}^m \times Q \times \{\text{-}1, 0, 1\}^{t-1} \times \{d\} \times \{\text{-}1, 0, 1\}^{m-t})$

On remarque que la plupart de ces portes sont dans le cas général des portes OU de taille d'entrée non bornées. On voit aussi que ces portes sont indépendantes, et par conséquent qu'aucun chemin allant d'une entrée à la sortie ne passe par deux de ces portes.

Les portes suivantes encodent les positions des têtes et tous les symboles de chaque cellule sur les bandes, ces bandes sont de taille non bornée mais sur une exécution courte d'au plus k étapes, les cellules visitées sont aussi éloignées d'au plus k positions de la position initiale. Ces portes garantissent que l'exécution est correcte. $\forall i \in [1,k], \forall l \in [\text{-}k,k], \forall t \in [1,m], \forall s \in [0,|\Gamma|-1]$:

– $\beta(i,l,t)$ renvoie vrai si et seulement si la tête t est à la position l avant l'étape i, pour ce faire on vérifie si la position à l'étape $i-1$: $\beta(i-1,*,t)$ ainsi que le mouvement de la tête à l'étape $i-1$: $\mu(i-1,*,t)$ correspondent à un mouvement vers la position l (ou une absence de mouvement depuis la position l). Comme la séquence de transitions est de longueur k, l est compris dans l'intervalle $[\text{-}k,k]$. La porte est définie par :

$$\begin{aligned}
\beta(0,l,t) &:= \begin{cases} 1 & \text{si } l = 0 \\ 0 & \text{sinon} \end{cases} \\
\beta(i,l,t) &:= (\beta(i{-}1,l,t) \wedge \mu(i{-}1,0,t)) \\
&\quad \vee (\beta(i{-}1,l{-}1,t) \wedge \mu(i{-}1,1,t)) \\
&\quad \vee (\beta(i{-}1,l{+}1,t) \wedge \mu(i{-}1,\text{-}1,t))
\end{aligned}$$

– $\sigma(i,l,s,t)$ renvoie vrai ssi le symbole de la cellule l de la bande t avant l'étape i est s. Soit w le mot initial de la machine, situé sur la première bande.

$$\begin{aligned}
\sigma(0,l,s,t) &:= \begin{cases} 1 & \text{si } \big((s \text{ est l'indice de } w[l]) \wedge (t=1) \wedge (0 \le l < |w|)\big) \\ 1 & \text{si } \big((s=0) \wedge (t \neq 1 \vee l < 0 \vee l \ge |w|)\big) \\ 0 & \text{sinon} \end{cases} \\
\sigma(i,l,s,t) &:= (\neg\beta(i-1,l,t) \wedge \sigma(i-1,l,s,t)) \\
&\quad \vee (\beta(i-1,l,t) \wedge \sigma_n(i-1,s,t)) \\
&\quad \vee (\beta(i-1,l,t) \wedge \sigma_n(i-1,|\Gamma|,t) \wedge \sigma(i-1,l,s,t))
\end{aligned}$$

Dans la définition de $\sigma(i,l,s,t)$ pour $i > 0$, trois cas apparaissent : soit la tête n'était pas sur la case l, donc le symbole est inchangé ; soit la tête était sur l, et il s'agit du symbole écrit ; soit la tête était sur l mais la transition était aveugle, donc le symbole reste encore inchangé.

On remarque que toutes ces portes ont un nombre borné d'entrées, et que si la définition de ces portes est récursive celle-ci porte sur le nombre de transition, donc la profondeur de ces portes est bornée par une fonction de k. On remarque aussi que ces portes sont en nombre polynomial car il y a $k \cdot 2k \cdot m$ portes β et

$k \cdot 2k \cdot |\underline{\Gamma}| \cdot m$ portes σ.

Toutes les informations sur l'exécution de la machine ont été encodées, il ne reste donc que la vérification de la validité de la séquence de transitions :

- $E := E_0 \wedge E_1 \wedge E_2 \wedge E_3 \wedge E_4$ est la porte finale du circuit. Il en résulte que, pour toute entrée acceptée, les conditions suivantes $E_0, \ldots, E_4$ doivent être satisfaites.
- $E_0 := \neg x[\text{-}1, \text{-}1]$ défini $x[\text{-}1, \text{-}1]$ comme la constante 0, donc $\neg x[\text{-}1, \text{-}1]$ devient 1, ces constantes étant utilisées par différentes portes du circuit.
- E_1 défini que pour tout $i \in [0, k]$, au plus un fil du bloc $x[i, 1], \ldots, x[i, |\Delta|]$ est vrai, ce qui signifie qu'à chaque étape au plus une transition est effectuée. Pour cela, on regarde chaque couple et on vérifie qu'au moins un des deux est faux. E_1 est définie comme :

$$E_1 := \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{|\Delta|} \bigwedge_{j'=1, j' \neq j}^{|\Delta|} (\neg x[i, j] \vee \neg x[i, j'])$$

- E_2 vérifie que l'état initial de chaque transition est l'état final de la transition précédente. E_2 est définie comme :

$$E_2 := \bigwedge_{i=2}^{k} \bigwedge_{q=1}^{|Q|} (\neg \tau_n(i-1, q) \vee \tau_o(i, q))$$

  À noter qu'il s'agit de la transcription logique de la formule :
  $\forall i \in [2, k], \forall q \in [1, |Q|], \tau_n(i-1, q) \Rightarrow \tau_o(i, q)$.
- E_3 vérifie que sur chaque bande le symbole lu de la transition est bien celui inscrit, et dans le cas d'une transition aveugle renvoie vrai. E_3 est définie comme :

$$E_3 := \bigwedge_{i=1}^{k} \bigwedge_{t=1}^{m} \bigwedge_{l=-k}^{k} \bigwedge_{s=0}^{|\Gamma|-1} (\neg \beta(i, l, t) \vee \neg \sigma(i, l, s, t) \vee \sigma_o(i, s, t) \vee \sigma_o(i, |\Gamma|, t))$$

  À noter qu'il s'agit de la transcription logique de la formule :
  $\forall i \in [1, k], \forall l \in [-k, k], \forall s \in [0, |\Gamma|], \forall t \in [1, m], (\beta(i, l, t) \wedge \sigma(i, l, s, t)) \Rightarrow (\sigma_o(i, s, t) \vee \sigma_o(i, |\Gamma|, t))$.
- E_4 vérifie que l'état initial de la première transition est q_0, l'état initial de M d'indice 0, et que l'état final de la dernière est q_A d'indice $|Q| - 1$. Donc E_4 est définie comme :

$$E_4 := \tau_o(0, 0) \wedge \tau_n(k-1, |Q| - 1)$$

Toutes les portes $E_i, i \in [0, 4]$ sont indépendantes, donc tout chemin allant d'une entrée à la sortie passe donc par au plus une de ces portes de taille d'entrée non bornée. Comme les seules autres portes de taille d'entrée non bornée sont celles qui encodent les transitions et sont elles aussi indépendantes, ce circuit est de trame 2.

Comme les seules portes définies de façon récursive le sont sur le nombre de transitions, la profondeur du circuit est bornée par une fonction du paramètre. De plus, ces portes sont en nombre polynomial en $|M|$.

Le circuit renvoie vrai si et seulement si M une séquence d'au plus k transitions de l'état initial à un état final sur le mot w, i.e. si et seulement si M possède un chemin d'exécution accepteur de taille k sur w. Par conséquent, Exécution courte d'une machine de Turing aveugle non-déterministe multi-bandes appartient à $W^*[2]$ donc à $W[2]$. □

1.3.3 Application à la Domination impaire

Maintenant que les transitions aveugles ont été ajoutées à la machine de Turing, on peut désormais effectuer des transitions sur un nombre exponentiel de configurations dans le cas où leur reconnaissance n'est pas nécessaire. En revenant sur l'exemple de la domination impaire, nous avions vu qu'il est possible, comme pour le problème de domination classique, d'utiliser la première bande pour tirer R'. Ensuite d'associer une bande à chacun des sommets de B, d'encoder la parité du voisinage de chacun des sommets de B par la position de la tête de lecture sur des bandes remplies préalablement par une alternance de 0 et de 1. Il s'agit d'effectuer une lecture de R' et pour chacun de ses sommets v_i décaler la tête de lecture associée à ses voisins ($N(v_i)$). Le problème résidait dans le nombre exponentiel de configurations, or il est désormais possible de les passer sans les connaitre en utilisant des transitions aveugles et uniquement contrôler que la configuration terminale est bien 1 pour chacun des sommets.

Pour le problème Ensemble impair (voir 1.2.3) on a donc la description complète de la machine de Turing aveugle non-déterministe à $|B|$ bandes suivante : $M = (Q, \Gamma, \Delta, \Sigma, b, q_I, Q_A)$, avec $\Gamma = \{\square, 0, 1, v_1, \ldots, v_n\}$, $b = \square$, $\Sigma = \varnothing$, $Q = \{q_{r,s} \mid r \in [1, n+1], s \in [0, k]\} \cup \{q_s^{\text{ret}} \mid s \in [1, k+1]\} \cup \{q_{i,s}^{\text{sig}} \mid i \in [1, n], s \in [0, k]\} \cup \{q^{\text{sig}}, q^{\text{end}}, q^{\text{read}}, q_A\}$, $q_I = q_{1,0}$ et $Q_A = \{q_A\}$.

Le mot initial w est le mot vide, en conséquence, à l'état initial, toutes les cellules des $n+1$ bandes contiennent le symbole blanc $\square$.

Les transitions de la machine sont :

Étape 1 – Initialisation de R'

$\langle \square\square^n, q_{r,s}, v_i 1^n, q_{i+1,s+1}, (+1)(+1)^n \rangle$	$r \in [1, n], s \equiv 1 \ mod\ 2$
$\langle \square\square^n, q_{r,s}, v_i 0^n, q_{i+1,s+1}, (+1)(+1)^n \rangle$	$r \in [1, n], s \equiv 0 \ mod\ 2$
$\langle \square\square^n, q_{r,s}, \square 1^n, q_{r,s+1}, 0(+1)^n \rangle$	$r \in [1, n+1], s \equiv 1 \ mod\ 2$
$\langle \square\square^n, q_{r,s}, \square 0^n, q_{r,s+1}, 0(+1)^n \rangle$	$r \in [1, n+1], s \equiv 0 \ mod\ 2$
$\langle \square\square^n, q_{r,k}, \square 1^n, q^{\text{end}}, (-1)(-1)^n \rangle$	$r \in [1, n+1]$, si $s \equiv 1 \ mod\ 2$
$\langle \square\square^n, q_{r,k}, \square 0^n, q^{\text{end}}, (-1)(-1)^n \rangle$	$r \in [1, n+1]$, si $s \equiv 0 \ mod\ 2$
$\langle v_i \sqcup^n, q^{\text{end}}, v_i \sqcup^n, q^{\text{end}}, (-1)(-1)^n \rangle$	$i \in [1, n]$
$\langle \square 1^n, q^{\text{end}}, \square 1^n, q^{\text{end}}, 0(-1)^n \rangle$	
$\langle \square 0^n, q^{\text{end}}, \square 0^n, q^{\text{end}}, 0(-1)^n \rangle$	
$\langle \square\square^n, q^{\text{end}}, \square\square^n, q^{\text{read}}, (+1)(+1)^n \rangle$	

Atteindre l'état $q_{r,s}$ signifie que $s-1$ sommets parmi $v_1, \ldots, v_{r-1}$ ont déjà

été écrits sur la première bande, son utilisation nous permet de ne pas effectuer deux fois le même choix de sommet dans R' étant donné que, dans la table de transitions celles ayant $q_{r,s}$ pour état initial ne permettent pas l'écriture de sommets d'indices inférieur à r.

Atteindre l'état q^{end} signifie que l'initialisation de R' est terminée et que les têtes de lecture sont revenues aux cellules non-vides (contenant un autre symbole que le symbole blanc $\square$) les plus à gauche sur chaque bande.

Étape 2 : Exploration du voisinage

$\langle v_i \sqcup^n, q^{\text{read}}, v_i \sqcup^n, q^{\text{read}}, (+1)d_1 \dots d_n \rangle \qquad i \in [1,n]$, où $d_t = \begin{cases} +1 & \text{si } v_t \in N(v_i) \\ 0 & \text{sinon} \end{cases}$

$\langle \square 1^n, q^{\text{read}}, \square 1^n, q_A, 00^n \rangle$

L'exécution de la machine nécessitant seulement trois passages de R' un pour l'écrire, un pour revenir et un pour l'exploration du voisinage, on a bien la $W[2]$ complétude. Il est à noter que la deuxième étape ne peut s'effectuer qu'avec des transitions aveugles sinon on aurait un nombre exponentiel de parité possible sur l'ensemble des sommets de B (voir la figure 1.2).

1.4 Application à la (σ, ρ)-Domination

1.4.1 (σ, ρ)-Domination

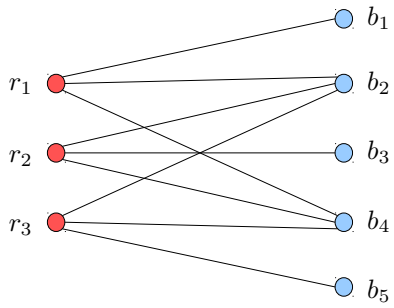
Définition

Les problèmes de domination sont centraux dans la théorie des graphes. Dans [62] Telle introduit la notion de domination généralisée qui, étant donnés deux ensembles d'entiers σ et ρ, pose le problème de l'existence (ou bien de la maximisation/minimisation) d'un ensemble D tel que tout sommet de D a un nombre appartenant à σ de voisins dans D et tout sommet de $V \setminus D$ a un nombre appartenant à ρ de voisins dans D ; un tel ensemble est dit (σ, ρ)-dominant. Ce qui nous donne la définition suivante pour la version existentielle :

Étant donnés σ et ρ deux ensembles non-vides d'entiers et un graphe $G = (V, E)$, le problème de domination généralisée ou (σ, ρ)-domination, est défini comme :

Ensemble (σ, ρ)-dominant
Entrée : un graphe $G = (V, E)$.
Question : Existe-t-il un sous-ensemble de sommets $D \subseteq V$ tel que :
- $\forall d \in D$, $|N(d) \cap D| \in \sigma$
- $\forall v \in V \setminus D$, $|N(v) \cap D| \in \rho$

Dans cette définition, on voit que σ et ρ ne sont pas des entrées mais sont fixés. En particulier, les problèmes Ensemble dominant, Ensemble stable et Code parfait peuvent être vus comme des instances de domina-



(a)

...	□	$\underline{r_1}$	r_2	r_3	□	...
...	□	$\underline{0}$	1	0	1	□	...
...	□	$\underline{0}$	1	0	1	□	...
...	□	$\underline{0}$	1	0	1	□	...
...	□	$\underline{0}$	1	0	1	□	...
...	□	$\underline{0}$	1	0	1	□	...

(b)

...	□	r_1	r_2	r_3	$\underline{□}$	...
...	□	0	$\underline{1}$	0	1	□	...
...	□	0	1	0	$\underline{1}$	□	...
...	□	0	$\underline{1}$	0	1	□	...
...	□	0	1	0	$\underline{1}$	□	...
...	□	0	$\underline{1}$	0	1	□	...

(c)

FIGURE 1.2 – Calcul de ENSEMBLE IMPAIR sur une machine de Turing multi-bandes aveugle avec $k = 3$. (a) Graphe d'entrée ; (b) État de la machine à la fin de la phase (1) : l'ensemble R' choisi est sur la première bande, les autres sont remplies selon la parité de la position de chaque case (0 pour pair, 1 pour impair) ; (c) Fin de la phase (2) : on a déplacé vers la droite la tête de lecture pour chaque bande associée à un sommet de B pour chacun de ses voisins dans R', toutes les têtes pointant sur 1, $\{r_1, r_2, r_3\}$ est un ensemble impair.

tion généralisée et deviennent respectivement Ensemble $(\mathbb{N}, \mathbb{N}^*)$-dominant, Ensemble $(\{0\}, \mathbb{N})$-dominant et Ensemble $(\{0\}, \{1\})$-dominant.

En complexité paramétrée

La plupart des problèmes de domination étant difficiles pour NP, dès l'introduction de la complexité paramétrée Downey et Fellows ont beaucoup étudié la version paramétré de ces problèmes [25, 33, 45, 51]. En reprenant les exemples précédents Ensemble dominant et Ensemble stable, il est intéressant de remarquer que, s'il s'agit de deux problèmes NP-complets, lorsque l'on étudie leur paramétrisation par la taille de l'ensemble dominant (la plus naturelle), le premier est complet pour $W[2]$ alors que le second est complet pour $W[1]$ [24]. La complexité paramétrée de problèmes de domination généralisées en faisant varier σ et ρ est étudié notamment dans [33, 45, 50].

Bien que d'autres paramétrisations soient possibles, en particulier par la largeur arborescente [17, 61], on ne s'intéresse ici qu'à la paramétrisation par la taille de l'ensemble dominant que l'on va nommer "standard" et par celle de l'ensemble dominé dite "duale" qui sont les paramétrisations plus étudiées [33].

Ensemble (σ, ρ)-dominant de taille k
Entrée : un graphe $G = (V, E)$, un entier k.
Paramètre : k.
Question : Existe-t-il un sous-ensemble de sommets $D \subseteq V$ de taille k tel que :
- $\forall d \in D$, $|N(d) \cap D| \in \sigma$
- $\forall v \in V \setminus D$, $|N(v) \cap D| \in \rho$

Ensemble (σ, ρ)-dominant de taille $n - k$
Entrée : un graphe $G = (V, E)$ d'ordre n, un entier k.
Paramètre : k.
Question : Existe-t-il un sous-ensemble de sommets $D \subseteq V$ de taille $n - k$ tel que :
- $\forall d \in D$, $|N(d) \cap D| \in \sigma$
- $\forall v \in V \setminus D$, $|N(v) \cap D| \in \rho$

Comme on le voit dans le tableau 1.4.1, les premiers résultats de complexité de (σ, ρ)-domination concernent les problèmes classiques de domination en théorie des graphes, comme Ensemble dominant [24] et Ensemble stable [25], directement par Downey et Fellows ou par la suite Code parfait [14] ou Ensemble totalement dominant [5].

Les premiers résultats généraux sur la complexité paramétrée de la (σ, ρ)-domination ont été montrés par Golovach *et al.* dans [33]. Nous rappellerons principalement les théorèmes suivants :

Théorème 2. *Pour tout σ et ρ ensembles non-vides finis d'entiers non-nuls* Ensemble (σ, ρ)-dominant de taille au plus k *et* Ensemble (σ, ρ)-dominant de taille exactement k *sont complets pour* $W[1]$.

Théorème 3. *Pour tout σ et ρ ensembles finis d'entiers non-nuls tels que σ ou $\overline{\sigma}$ sont finis, et ρ ou $\overline{\rho}$ sont finis,* Ensemble (σ, ρ)-dominant de taille au plus $n-k$ *et* Ensemble (σ, ρ)-dominant de taille exactement $n-k$ *sont FPT.*

Le premier théorème est intéressant car il donne la complétude pour $W[1]$ d'un grand nombre de problèmes de domination classique comme Code parfait. De plus, pour $\sigma = \rho = \mathbb{N}$ le problème de (σ, ρ)-domination est trivialement FPT (aucunes conditions), on ne peut donc pas obtenir un résultat de difficulté pour tous σ et tous ρ.

Le second théorème concernant la paramétrisation duale des problèmes (que l'on utilisera dans le second chapitre) et la domination impaire faible est intéressant car il regroupe la plupart des problèmes classiques de domination. L'exemple de la domination impaire, aussi montrée dans [33] en utilisant les résultats de [26] qui est $W[1]$-difficile, montre que le problème général de la (σ, ρ)-domination pour tous σ et ρ n'est pas FPT en paramétrisation duale.

1.4.2 Méthode par machine de Turing Aveugle

Théorème 4. *Pour tous ensembles récursifs d'entiers σ et ρ,* Ensemble (σ, ρ)-dominant de taille exactement k *et* Ensemble (σ, ρ)-dominant de taille au plus k *appartiennent à* $W[2]$.

Dans cette section, nous allons montrer l'appartenance à $W[2]$. De plus, on ne verra que la preuve de l'appartenance à $W[2]$ de Ensemble (σ, ρ)-dominant de taille au plus k, la preuve pour Ensemble (σ, ρ)-dominant de taille exactement k étant similaire.

1.4.3 Principe

Étant donnés deux ensembles récursifs (c-à-d. dont l'appartenance est calculable) $\sigma, \rho \subseteq \mathbb{N}$, un entier k, et un graphe $G = (\{v_1, \ldots, v_n\}, E)$, la machine de Turing à $(n+1)$ bandes M atteint l'état accepteur si et seulement si G a un ensemble (σ, ρ)-dominant de taille au plus k. M procède en trois étapes (voir l'exemple d'exécution 1.2) :

1. D, un sous-ensemble de V de taille au plus k, est construit de façon non-déterministe (toutes les possibilités sont dans la table des transitions) et est inscrit sur la première bande. De plus, pendant ce tirage, les $k+1$ premières cellules des n bandes suivantes (une bande pour chaque sommet

1. Quand la paramétrisation s'effectue par la taille de l'ensemble dominant, la complexité paramétrée de Ensemble (σ, IMPAIR)-dominant (resp. Ensemble (σ, PAIR)-dominant) pour $\sigma \in \{\text{IMPAIR}, \text{PAIR}\}$ peut être déduite de celle de Ensemble impair (respectivement Ensemble pair) montrée dans [33].

Domination généralisée			
Nom	Formulation (σ, ρ)	Standard	Duale
Ensemble dominant	$(\mathbb{N}, \mathbb{N}^*)$	W[2]-complet [24]	FPT [33]
Ensemble stable	$(\{0\}, \mathbb{N})$	W[1]-complet [25]	FPT [33]
Code parfait	$(\{0\}, \{1\})$	W[1]-complet [14, 25]	FPT [33]
Ensemble fortement stable	$(\{0\}, \{0, 1\})$	**W[1]-complet** (W[1] [33])	FPT [33]
Ensemble totalement dominant	$(\mathbb{N}^*, \mathbb{N}^*)$	**W[2]-complet** (W[2]-difficile [5])	FPT [33]
Ensemble (σ,IMPAIR)-dominant, $\sigma \in \{$IMPAIR,PAIR$\}$		W[1]-difficile W[2] [1]	W[1]-difficile [33], **W[2]**
Ensemble (σ,PAIR)-dominant, $\sigma \in \{$IMPAIR, PAIR$\}$		W[2] [1]	W[1]-difficile [33], **W[2]**
Ensemble (σ, ρ)-dominant, avec σ, ρ récursifs		**W[2]**	**W[2]**
Autres problèmes de domination			
Ensemble dominant connexe (Dual de Arbre couvrant de feuilles maximum)		**W[2]-complet** (W[2]-difficile [29])	FPT [32]
Noyau de digraphe		**W[2]-complet** (W[2]-difficile [37])	Inconnu
Problèmes de théorie des codes			
Distribution de poids		W[1]-difficile W[2] [26]	W[1]-difficile [33], **W[2]**
Distance minimale		W[2] [26]	W[1]-difficile [33], **W[2]**
Distribution de poids sur $\mathbb{F}_q$, (q puissance de premier)		W[1]-difficile W[2]	**W[1]-difficile**, **W[2]**
Distance minimale sur $\mathbb{F}_q$, (q puissance de premier)		**W[2]**	**W[1]-difficile**, **W[2]**

Figure 1.3 – Aperçu de la complexité paramétrée de problèmes de domination et de quelques problèmes de théorie des codes. La paramétrisation "standard" correspond à la taille de l'ensemble **dominant** (ou le poids de Hamming dans les problèmes de théorie des codes). Dans cette colonne, on considère des ensembles de taille k et au plus k sauf pour Ensemble fortement stable et Ensemble stable que l'on ne considère que pour l'égalité. La paramétrisation "duale" correspond à la taille de l'ensemble **dominé**. Les nouveaux résultats obtenus sont indiqués en gras, les anciens entre parenthèses

du graphe) sont remplies avec des 1 et des 0 de telle façon que la $i^{ème}$ cellule de chaque bande soit à 1 si et seulement si $i \in \rho$.

2. Le contenu de chacune des bandes de M associées à un sommet de D est remplacé par des 1 et des 0 de telle façon que la $i^{ème}$ cellule de chaque bande soit à 1 si et seulement si $i \in \sigma$. À la fin de cette seconde étape, toutes les têtes de lecture sont sur les symboles non-blancs les plus à gauche, la première bande contient D et les bandes suivantes contiennent les vecteurs caractéristiques de σ ou ρ selon qu'elles sont associées à un sommet de D ou de $V \setminus D$.
3. Pour chaque sommet v de D (lu sur la première bande), la tête de lecture de chacune des bandes associées à un sommet dans le voisinage extérieur de v ($N(v)$) est déplacé à gauche. Cette étape est réalisée à l'aide de transitions aveugles, en effet, on n'a pas besoin de connaitre le symbole sur chaque bande (hormis la première) et on ne pourrait pas inscrire toutes les configurations possibles dans la table de transition. À la fin de cette troisième étape, pour tout $v \in D$ (resp. $v \in \overline{D}$), la tête de lecture de la bande associée à v a été décalée à droite $|N(v) \cap D|$ fois, la tête de lecture lit 1 si et seulement si $|N(v) \cap D| \in \sigma$ (resp. $|N(v) \cap D| \in \rho$), donc D est un ensemble (σ, ρ)-dominant si et seulement si toutes les têtes de lecture (sauf la première) lisent un 1.

1.4.4 $W[2]$-complétude

Cette section est entièrement consacrée à la preuve de l'appartenance du problème de (σ, ρ)-domination à $W[2]$.

Démonstration. La description complète de la machine de Turing aveugle non-déterministe à $n+1$ bandes est la suivante : $M = (Q, \Gamma, \Delta, \Sigma, b, q_I, Q_A)$, avec $\Gamma = \{\square, 0, 1, v_1, \ldots, v_n\}$, $b = \square$, $\Sigma = \varnothing$, $Q = \{q_{r,s} \mid r \in [1, n+1], s \in [0, k]\} \cup \{q_s^{\text{ret}} \mid s \in [1, k+1]\} \cup \{q_{i,s}^{\text{sig}} \mid i \in [1, n], s \in [0, k]\} \cup \{q^{\text{sig}}, q_\rho^{\text{end}}, q_\sigma^{\text{end}}, q^{\text{read}}, q_A\}$, $q_I = q_{1,0}$ et $Q_A = \{q_A\}$.

Le mot initial w est le mot vide, en conséquence à l'état initial toutes les cellules des $n+1$ bandes contiennent le symbole blanc $\square$.

Les transitions de la machine sont :

Étape 1 – Initialisation de D et ρ :

$\langle \square\square^n, q_{r,s}, v_i 1^n, q_{i+1,s+1}, (+1)(+1)^n \rangle$	$r \in [1, n], s \in \rho \cap [0, k-1], i \in [r, n]$
$\langle \square\square^n, q_{r,s}, v_i 0^n, q_{i+1,s+1}, (+1)(+1)^n \rangle$	$r \in [1, n], s \in \overline{\rho} \cap [0, k-1], i \in [r, n]$
$\langle \square\square^n, q_{r,s}, \square 1^n, q_{r,s+1}, 0(+1)^n \rangle$	$r \in [1, n+1], s \in \rho \cap [0, k-1]$
$\langle \square\square^n, q_{r,s}, \square 0^n, q_{r,s+1}, 0(+1)^n \rangle$	$r \in [1, n+1], s \in \overline{\rho} \cap [0, k-1]$
$\langle \square\square^n, q_{r,k}, \square 1^n, q_\rho^{\text{end}}, (-1)(-1)^n \rangle$	$r \in [1, n+1]$, si $k \in \rho$
$\langle \square\square^n, q_{r,k}, \square 0^n, q_\rho^{\text{end}}, (-1)(-1)^n \rangle$	$r \in [1, n+1]$, si $k \in \overline{\rho}$
$\langle v_i \text{␣}^n, q_\rho^{\text{end}}, v_i \text{␣}^n, q_\rho^{\text{end}}, (-1)(-1)^n \rangle$	$i \in [1, n]$
$\langle \square 1^n, q_\rho^{\text{end}}, \square 1^n, q_\rho^{\text{end}}, 0(-1)^n \rangle$	
$\langle \square 0^n, q_\rho^{\text{end}}, \square 0^n, q_\rho^{\text{end}}, 0(-1)^n \rangle$	
$\langle \square\square^n, q_\rho^{\text{end}}, \square\square^n, q^{\text{sig}}, (+1)(+1)^n \rangle$	

Atteindre l'état $q_{r,s}$ signifie que $s-1$ sommets parmi $v_1, \ldots, v_{r-1}$ ont déjà été écrits sur la première bande, son utilisation nous permet de ne pas effectuer deux fois le même choix de sommet dans D étant donné que, dans la table de transitions celles ayant $q_{r,s}$ pour état initial ne permettent pas l'écriture de sommets d'indices inférieur à r. On remarque que l'on écrit le vecteur caractéristique de ρ sur chaque bande (excepté la première) en même temps que l'on choisit l'ensemble dominant D.

Atteindre l'état q_ρ^{end} signifie que les initialisations de D et ρ sont terminées et que les têtes de lecture sont revenues aux cellules non-vides (contenant un autre symbole que le symbole blanc $\square$) les plus à gauche sur chaque bande.

Étape 2 – Initialisation de σ :

$\langle v_i \sqcup^n, q^{\text{sig}}, v_i \sqcup^n, q_{i,0}^{\text{sig}}, 00^n \rangle$ $\quad i \in [1,n]$

$\langle v_i \sqcup^n, q_{i,s}^{\text{sig}}, v_i \sqcup^{i-1} 1 \sqcup^{n-i}, q_{i,s+1}^{\text{sig}}, 0(+1)^n \rangle$ $\quad i \in [1,n], s \in \sigma \cap [0,k-1]$

$\langle v_i \sqcup^n, q_{i,s}^{\text{sig}}, v_i \sqcup^{i-1} 0 \sqcup^{n-i}, q_{i,s+1}^{\text{sig}}, 0(+1)^n \rangle$ $\quad i \in [1,n], s \in \overline{\sigma} \cap [0,k-1]$

$\langle v_i \sqcup^n, q_{i,k}^{\text{sig}}, v_i \sqcup^{i-1} 1 \sqcup^{n-i}, q_1^{\text{ret}}, (+1)0^n \rangle$ $\quad i \in [1,n]$, si $k \in \sigma$

$\langle v_i \sqcup^n, q_{i,k}^{\text{sig}}, v_i \sqcup^{i-1} 0 \sqcup^{n-i}, q_1^{\text{ret}}, (+1)0^n \rangle$ $\quad i \in [1,n]$, if $k \in \overline{\sigma}$

$\langle v_i \sqcup^n, q_s^{\text{ret}}, v_i \sqcup^n, q_{s+1}^{\text{ret}}, 0(-1)^n \rangle$ $\quad i \in [1,n], s \in [1,k]$

$\langle v_i \sqcup^n, q_{k+1}^{\text{ret}}, v_i \sqcup^n, q_{i,0}^{\text{sig}}, 00^n \rangle$ $\quad i \in [1,n]$

$\langle \square \sqcup^n, q_1^{\text{ret}}, \square \sqcup^n, q_\sigma^{\text{end}}, (-1)0^n \rangle$

$\langle v_i \sqcup^n, q_\sigma^{\text{end}}, v_i \sqcup^n, q_\sigma^{\text{end}}, (-1)0^n \rangle$ $\quad i \in [1,n]$

$\langle \square \sqcup^n, q_\sigma^{\text{end}}, \square \sqcup^n, q^{\text{read}}, (+1)0^n \rangle$

Atteindre l'état $q_{s,i}^{\text{sig}}$ signifie que le premier symbole s du vecteur caractéristique de σ a été inscrit sur la bande associée au sommet v_i.

Étape 3 : Exploration du voisinage

$\langle v_i \sqcup^n, q^{\text{read}}, v_i \sqcup^n, q^{\text{read}}, (+1)d_1 \ldots d_n \rangle$ $\quad i \in [1,n]$, où $d_t = \begin{cases} +1 & \text{si } v_t \in N(v_i) \\ 0 & \text{sinon} \end{cases}$

$\langle \square 1^n, q^{\text{read}}, \square 1^n, q_A, 00^n \rangle$

σ et ρ étant des ensembles récursifs, leurs vecteurs caractéristiques de longueur k peuvent être déterminés et écrits sur toutes les bandes en temps $f(k)$, f étant une fonction quelconque. Durant la première étape, D ainsi que le vecteur caractéristique de ρ de longueur k sont écrits respectivement sur la première bande et sur toutes les autres bandes, et ensuite les têtes reviennent au symbole non-blanc le plus à gauche, on a donc $2(k+1)$ pas pour la première étape.

Durant la seconde étape, le vecteur caractéristique de σ de longueur k est écrit de manière successive sur les bandes correspondants aux sommets de D, comme pour chaque sommet on doit revenir au symbole non-blanc le plus à gauche, on a $k(2k)$ étapes.

Enfin, la dernière étape consiste à lire successivement tous les éléments v_i de D et pour chacun effectuer un décalage à droite des têtes de lecture des bandes correspondants aux sommets de son voisinage extérieur $N(v_i)$. Cette étape ne

nécessite donc que k étapes.

La machine a donc un nombre de transitions polynomial en $|G|$, ainsi qu'une séquence d'exécution acceptante d'au plus $2(k+1)+k(2k+2)$ étapes si et seulement si un ensemble (σ,ρ)-dominant de taille au plus k existe. En conséquence, il existe une réduction paramétrée de Ensemble (σ,ρ)-dominant de taille au plus k à Exécution courte d'une machine de Turing aveugle non-déterministe multi-bandes et donc, Ensemble (σ,ρ)-dominant de taille au plus k appartient à W[2]. □

Il est important de noter que l'utilisation des transitions aveugles est déterminante dans la troisième étape. En effet, une simulation naïve de ces transitions utiliserait 2^n transitions non-aveugles car la transition est applicable aux 2^n possibles configurations pouvant être lues sur les n bandes.

1.4.5 Paramétrisation duale

Une autre paramétrisation de la (σ,ρ)-domination intéressante est sa paramétrisation duale. Il s'agit d'utiliser comme paramètre non plus la taille du dominant que l'on cherche mais celle de l'ensemble dominé. On cherche donc un ensemble (σ,ρ)-dominé de taille k ce qui revient à chercher un ensemble (σ,ρ)-dominant de taille $n-k$. Dans [33], il est montré que pour σ et ρ finis ou co-finis ce problème est FPT mais que pour σ et ρ dans $\{PAIR, IMPAIR\}$ le problème est difficile pour $W[1]$ et dans $W[2]$. On va montrer ici à l'aide de la machine de Turing aveugle que pour tous σ et ρ récursifs le problème est dans $W[2]$.

Théorème 5. *Pour tout ensembles récursifs d'entiers σ et ρ,* Ensemble (σ,ρ)-dominant de taille au plus k *et* Ensemble (σ,ρ)-dominant de taille exactement $n-k$ *appartiennent à $W[2]$.*

Démonstration. La preuve de l'appartenance à $W[2]$ se fait de manière très similaire à celle de la paramétrisation standard 4, en effet au lieu de choisir l'ensemble dominant sur la première bande on va choisir le dominé. Au lieu d'initialiser les bandes restantes avec le vecteur caractéristique de ρ, on va initialiser chacune des bandes restantes comme suit : soit v le sommet, pour tout i dans $[0,d(v)]$ si $d(v)-i \in \sigma$ alors on met 1 sinon 0 dans la case d'indice i. Ensuite pour chaque sommet de l'ensemble dominé, on va faire de même mais avec $d(v)-i \in \rho$. Et enfin, on effectue le parcours de l'ensemble dominé, pour chaque élément on déplace à droite la tête de lecture de la bande associée à chacun de des voisins. On atteint l'état accepteur si toutes les têtes pointent sur un 1 à la fin du parcours.

L'initialisation des bandes se fait en fonction de l'appartenance de $d(v)-i$ à σ et ρ, i étant la position de la case et v le sommet associé à la bande car si un sommet à i voisins dans le dominé alors il a $d(v)-i$ voisins dans le dominant.

Ceci nous donne donc la machine de Turing aveugle suivante ayant la même taille et le même temps d'exécution : $M = (Q,\Gamma,\Delta,\Sigma,b,q_I,Q_A)$, avec $\Gamma = \{\square,0,1,v_1,\ldots,v_n\}$, $b = \square$, $\Sigma = \varnothing$, $Q = \{q_{r,s} \mid r \in [1,n+1], s \in [0,k]\} \cup$

$\{q_s^{\text{ret}} \mid s \in [1, k+1]\} \cup \{q_{i,s}^{\text{sig}} \mid i \in [1,n], s \in [0,k]\} \cup \{q^{\text{sig}}, q_\rho^{\text{end}}, q_\sigma^{\text{end}}, q^{\text{read}}, q_A\}$, $q_I = q_{1,0}$ et $Q_A = \{q_A\}$.

Le mot initial w est le mot vide, en conséquence à l'état initial toutes les cellules des $n+1$ bandes contiennent le symbole blanc $\square$.

Les transitions de la machine sont :

Étape 1 – Initialisation de D et "$d(v) - \sigma$" :

$\langle \square\square^n, q_{r,s}, v_i s_1 \dots s_n, q_{i+1,s+1}, (+1)(+1)^n \rangle$

$$r \in [1,n], s \in \rho \cap [0, k-1], i \in [r,n] \text{ où } s_t = \begin{cases} +1 & \text{si } d(v_t) - s \in \sigma \\ 0 & \text{sinon} \end{cases}$$

$\langle \square\square^n, q_{r,s}, \square s_1 \dots s_n, q_{r,s+1}, (+1)(+1)^n \rangle$

$$r \in [1,n], s \in \rho \cap [0, k-1], i \in [r,n] \text{ où } s_t = \begin{cases} +1 & \text{si } d(v_t) - s \in \sigma \\ 0 & \text{sinon} \end{cases}$$

$\langle \square\square^n, q_{r,k}, \square s_1 \dots s_n, q_\rho^{\text{end}}, (-1)(-1)^n \rangle$

$$r \in [1,n] \text{ où } s_t = \begin{cases} +1 & \text{si } d(v_t) - k \in \sigma \\ 0 & \text{sinon} \end{cases}$$

$\langle v_i \sqcup^n, q_\rho^{\text{end}}, v_i \sqcup^n, q_\rho^{\text{end}}, (-1)(-1)^n \rangle \qquad i \in [1,n]$

$\langle \square \sqcup^n, q_\rho^{\text{end}}, \square \sqcup^n, q_\rho^{\text{end}}, 0(-1)^n \rangle$

$\langle \square\square^n, q_\rho^{\text{end}}, \square\square^n, q^{\text{sig}}, (+1)(+1)^n \rangle$

Étape 2 – Initialisation de "$d(v) - \rho$" :

$\langle v_i \sqcup^n, q^{\text{sig}}, v_i \sqcup^n, q_{i,0}^{\text{sig}}, 00^n \rangle \qquad i \in [1,n]$

$\langle v_i \sqcup^n, q_{i,s}^{\text{sig}}, v_i \sqcup^{i-1} t \sqcup^{n-i}, q_{i,s+1}^{\text{sig}}, 0(+1)^n \rangle$

$$i \in [1,n], \text{ où } t = \begin{cases} +1 & \text{si } d(v_i) - s \in \rho \\ 0 & \text{sinon} \end{cases}$$

$\langle v_i \sqcup^n, q_{i,k}^{\text{sig}}, v_i \sqcup^{i-1} t \sqcup^{n-i}, q_1^{\text{ret}}, (+1)0^n \rangle$

$$i \in [1,n], \text{ où } t = \begin{cases} +1 & \text{si } d(v_i) - k \in \rho \\ 0 & \text{sinon} \end{cases}$$

$\langle v_i \sqcup^n, q_s^{\text{ret}}, v_i \sqcup^n, q_{s+1}^{\text{ret}}, 0(-1)^n \rangle \qquad i \in [1,n], s \in [1,k]$

$\langle v_i \sqcup^n, q_{k+1}^{\text{ret}}, v_i \sqcup^n, q_{i,0}^{\text{sig}}, 00^n \rangle \qquad i \in [1,n]$

$\langle \square \sqcup^n, q_1^{\text{ret}}, \square \sqcup^n, q_\sigma^{\text{end}}, (-1)0^n \rangle$

$\langle v_i \sqcup^n, q_\sigma^{\text{end}}, v_i \sqcup^n, q_\sigma^{\text{end}}, (-1)0^n \rangle \qquad i \in [1,n]$

$\langle \square \sqcup^n, q_\sigma^{\text{end}}, \square \sqcup^n, q^{\text{read}}, (+1)0^n \rangle$

Étape 3 : Exploration du voisinage

$\langle v_i \sqcup^n, q^{\text{read}}, v_i \sqcup^n, q^{\text{read}}, (+1)d_1 \dots d_n \rangle$ $\quad i \in [1,n]$, où $d_t = \begin{cases} +1 & \text{si } v_t \in N(v_i) \\ 0 & \text{sinon} \end{cases}$

$\langle \square 1^n, q^{\text{read}}, \square 1^n, q_A, 00^n \rangle$ □

1.5 Généralisations et application aux problèmes de théorie des codes

1.5.1 Quelques généralisations

Certains problèmes naturels de domination ne sont pas capturés par la (σ, ρ)-domination comme Ensemble dominant connexe. Dans cette section, on montre que la preuve de l'appartenance à $W[2]$ de la (σ, ρ)-domination (théorème 4) peut être généralisée à la (P, ρ)-domination, où P n'est plus seulement une contrainte de domination mais n'importe quelle propriété calculable s'appliquant au sous-graphe induit par l'ensemble dominant. Cela implique que Ensemble dominant connexe, difficile pour $W[2]$, est en fait complet pour $W[2]$. On montre aussi que la technique s'applique facilement aux digraphes avec l'exemple de Noyau de digraphe.

Ensemble (P, ρ)-dominant de taille au plus k :
Entrées : un graphe $G = (V, E)$, un entier k.
Paramètre : k.
Question : Existe-t-il un sous-ensemble $D \subseteq V$ tel que $|D| \leq k$ et :
– le sous-graphe de G induit par D satisfait la propriété P ;
– $\forall v \in V \setminus D, |N(v) \cap D| \in \rho$?

Théorème 6. *Si ρ est un ensemble récursif d'entiers et P une propriété récursive, alors* Ensemble (P, ρ)-dominant de taille au plus k *appartient à $W[2]$.*

Démonstration. On utilise la machine de Turing aveugle multi-bande de la (σ, ρ)-domination (théorème 4) avec $\sigma = \mathbb{N}$. On vérifie donc si un ensemble $(\mathbb{N}, \rho)$-dominant D existe, ensuite on compose cette machine avec une machine multi-bande classique qui calcule la propriété P sur le sous-graphe induit par D. Une telle machine existe car P est calculable. Comme le sous-graphe induit est de taille $O(k^2)$ et que P est calculable, l'exécution de la seconde machine se fait en temps $f(k)$ pour une fonction quelconque f. □

Noyau de digraphe :
Entrées : Un graphe orienté $G = (V, A)$, un entier k.
Paramètre : k.
Question : Existe-t-il un noyau D de G de taille au plus k ? Un *noyau* est un ensemble stable S (il n'existe aucun $u, v \in S$ tels que uv ou vu sont dans A) tel que pour tout sommet $x \in V \setminus S$, il existe au moins un $y \in S$ tel que $xy \in A$.

Théorème 7. *Noyau de digraphe est complet pour $W[2]$.*

Démonstration. La difficulté pour $W[2]$ est prouvée dans [37]. La preuve de l'appartenance à $W[2]$ est similaire à celle de ENSEMBLE (σ, ρ)-DOMINANT (théorème 4). La machine et son initialisation sont les mêmes jusqu'à la troisième étape, avec $\sigma = \{0\}$ et $\rho = \mathbb{N}^*$. Durant la troisième étape, seules les têtes associées à des *voisins entrants* sont décalées à droite. □

1.5.2 Application aux problèmes de théorie des codes

La complexité paramétrée de problèmes venant de la théorie des codes, en particuliers DISTANCE MINIMALE et DISTRIBUTION DES POIDS, a été étudiée dans [26] où leur appartenance à $W[2]$ est montrée ainsi que la difficulté pour $W[1]$ du second problème. Dans cette section, on utilise la méthode par machine de Turing aveugle pour prouver l'appartenance à $W[2]$ de la généralisation des ces problèmes aux codes linéaires sur $\mathbb{F}_q$, le corps à q éléments pour tout q puissance de premier, ainsi que l'appartenance à $W[2]$ des duaux de ces problèmes.

DISTANCE MINIMALE SUR $\mathbb{F}_q$:
Entrées : q une puissance de premier, k un entier, H une matrice $m \times n$ sur $\mathbb{F}_q$.
Paramètres : k, q.
Question : Existe-t-il une combinaison linéaire sur $\mathbb{F}_q$ d'au plus k colonnes de H qui donne le vecteur nul ?

DISTRIBUTION DE POIDS SUR $\mathbb{F}_q$:
Entrées : q une puissance de premier, k un entier, H une matrice $m \times n$ sur $\mathbb{F}_q$.
Paramètres : k, q.
Question : Existe-t-il une combinaison linéaire sur $\mathbb{F}_q$ de exactement k colonnes de H qui donne le vecteur nul ?

Théorème 8. DISTRIBUTION DE POIDS SUR $\mathbb{F}_q$ *est difficile pour* $W[1]$ *et appartient à* $W[2]$*, et* DISTANCE MINIMALE SUR $\mathbb{F}_q$ *appartient à* $W[2]$.

Démonstration. Comme DISTRIBUTION DE POIDS est un cas particulier de DISTRIBUTION DE POIDS SUR $\mathbb{F}_q$, avec $q = 2$, et que DISTRIBUTION DE POIDS est difficile pour $W[1]$ [33], DISTRIBUTION DE POIDS SUR $\mathbb{F}_q$ pour tout q puissance de premier est difficile pour $W[1]$.

Pour l'appartenance à $W[2]$, soit $\psi : [0, q) \to \mathbb{F}_q$ une fonction d'indexage sur $\mathbb{F}_q$ tel que $\psi(0) = 0$. q étant une puissance de premier, il existe un premier p et un entier c tels que $q = p^c$, et il existe un isomorphisme $\varphi : \mathbb{F}_q \to \mathbb{F}_p[X]/P(X)$, où $F_p[X]/P(X)$ est l'ensemble des polynômes dans X à coefficients dans $\mathbb{F}_p$ modulo $P(X)$. Soit H', une matrice $mc \times (n(q-1))$ à coefficients dans $\mathbb{F}_p$ telle que $\forall i, j, \ell \in [0, m) \times [0, n) \times [1, q)$, $\sum_{u=0}^{c-1} H'_{it,j\ell} X^t = \varphi(\psi(\ell) \cdot H_{i,j})$. A noter que chacune des $n(q-1)$ colonnes de H' correspond à une des colonnes de H multipliée par un élément non nul de $\mathbb{F}_q$. De plus, chacun des éléments $a \in \mathbb{F}_q$ est encodé dans $c \times 1$ blocs $\begin{pmatrix} r_0 \\ \vdots \\ r_{c-1} \end{pmatrix}$ tels que $\varphi(a) = \sum_{t=0}^{c-1} r_t X^t$. La matrice

H' de taille $mc \times (n(q-1))$ peut donc être calculée en temps $m.n.f(q)$ pour une fonction f quelconque.

On peut remarquer qu'il existe une combinaison linéaire de k colonnes de H égale à 0 si et seulement si il existe $0 \leq i_1 < i_2 < \ldots < i_k < m(q-1)$ telle que les colonnes correspondantes de H' se somment à 0 (i.e. $\forall j \in [0, mc), \sum_{r=1}^{k} H'_{j,i_r} = 0$) et $\forall r \in [1, k)$, $\left\lfloor \frac{i_r}{m} \right\rfloor \neq \left\lfloor \frac{i_{r+1}}{m} \right\rfloor$. La dernière condition garantit que les k colonnes de H' choisies correspondent à k colonnes distinctes de H.

Pour décider si de tels indices $i_1, \ldots, i_k$ existent, on utilise la machine de Turing à $(mc+1)$ bandes suivante : $M = (Q, \Gamma, \Delta, \Sigma, b, q_I, Q_A)$. La première bande est utilisée pour le choix des colonnes de H' et chacune des bandes suivantes est associée à une ligne de H'. L'alphabet est $\Gamma = \{\square, 0, 1\} \cup \{h_i | i \in [1, n]\}$ et les états sont $Q = \{q_{i,s} \mid i \in [1, n(q-1)+1], s \in [0, k \cdot p]\} \cup \{q_s^{\text{ret}} \mid s \in [1, k \cdot p + 1]\} \cup \{q_{i,s}^{\text{av}} \mid i \in [1, n], s \in [0, p-1]\} \cup \{q^{\text{read}}, q_A\}$, avec $q_I = q_{1,0}$, $b = \square$, $\Sigma = \varnothing$ et $Q_A = \{q_A\}$. Les transitions sont séparées en deux étapes :

Étape 1 - Initialisation : Tout d'abord, k colonnes de H' sont choisies de façon non-déterministe sur la première bande, pendant que les autres bandes sont remplies par k fois le motif 10^{p-1} (i.e. 1 suivi par $p-1$ fois 0), de telle façon que la $i^{\text{ème}}$ cellule soit à 1 si et seulement si $i \equiv 0 \mod p$. Pour ne pas choisir deux colonnes de H' correspondant à la même colonne de H mais avec un facteur différent, on passe au bloc de colonnes suivant, i.e. quand la colonne j est choisie, la suivante est prise parmi celles indicées de ℓ à $n(q-1)$ avec $\ell > j$ et $\ell \equiv 0 \mod (q-1)$:

$\langle \square\square^{m \cdot c}, q_{i,s}, h_j 1^{m \cdot c}, q_{\ell,s+1}, (+1)(+1)^{m \cdot c} \rangle$
$i \in [1, n(q-1)], s \in [0, k-1], j \in [i, n(q-1)]$, si $s \equiv 0 (mod\ p)$
ℓ est le plus petit entier tel que $\ell > j$ et $\ell \equiv 0 (mod\ q-1)$

$\langle \square\square^{m \cdot c}, q_{i,s}, h_j 0^{m \cdot c}, q_{\ell,s+1}, (+1)(+1)^{m \cdot c} \rangle$
$i \in [1, n(q-1)], s \in [0, k-1], j \in [i, n]$, if $s \not\equiv 0 (mod\ p)$
ℓ est le plus petit entier tel que $\ell > j$ et $\ell \equiv 0 (mod\ q-1)$

$\langle \square\square^{m \cdot c}, q_{i,s}, \square 1^{m \cdot c}, q_{i,s+1}, 0(+1)^{m \cdot c} \rangle$
$i \in [1, n(q-1)+1], s \in [k, kp)$, si $s \equiv 0 (mod\ p)$

$\langle \square\square^{m \cdot c}, q_{i,s}, \square 0^{m \cdot c}, q_{i,s+1}, 0(+1)^{m \cdot c} \rangle$
$i \in [1, n+1], s \in [k, kp)$, si $s \not\equiv 0 (mod\ p)$

$\langle \square\square^{m \cdot c}, q_{i,k \cdot p}, \square 1^{m \cdot c}, q_1^{\text{ret}}, (-1)(-1)^{m \cdot c} \rangle$ $\quad i \in [1, n(q-1)+1]$

$\langle \text{␣}\,\text{␣}^{m \cdot c}, q_s^{\text{ret}}, \text{␣}\,\text{␣}^{m \cdot c}, q_{s+1}^{\text{ret}}, (-1)(-1)^{m \cdot c} \rangle$ $\quad s \in [1, k]$

$\langle \text{␣}\,\text{␣}^{m \cdot c}, q_s^{\text{ret}}, \text{␣}\,\text{␣}^{m \cdot c}, q_{s+1}^{\text{ret}}, 0(-1)^{m \cdot c} \rangle$ $\quad s \in [k+1, kp+1]$

$\langle \text{␣}\,\text{␣}^{m \cdot c}, q_{k \cdot p+1}^{\text{ret}}, \text{␣}\,\text{␣}^{m \cdot c}, q^{\text{read}}, 00^{m \cdot c} \rangle$

Étape 2 - Reconnaissance : Pour pouvoir vérifier que la somme des vecteurs choisis est bien le vecteur nul sur $\mathbb{F}_p$, pour toute colonne h_i de l'ensemble choisi, la tête de lecture de chaque bande j se déplace sur la droite un nombre de fois égal à $H'_{i,j}$ en utilisant des transitions aveugles pour passer toutes les configurations possibles.

$$\langle h_i \sqcup^{mc}, q^{\text{read}}, h_i \sqcup^{mc}, q^{\text{av}}_{i,1}, (+1)0^{mc} \rangle \qquad i \in [1,n]$$

$$\langle \sqcup \sqcup^{mc}, q^{\text{av}}_{i,s}, \sqcup \sqcup^{mc}, q^{\text{av}}_{i,s+1}, 0d_1 \dots d_{mc} \rangle \qquad i \in [1,n], s \in [0,p-2]$$
$$\text{avec } \forall j \in [1,mc], d_j = \begin{cases} 1 & \text{si } H'_{i,j} > s \\ 0 & \text{sinon} \end{cases}$$

$$\langle \sqcup \sqcup^{m}, q^{\text{av}}_{i,p-1}, \sqcup \sqcup^{mc}, q^{\text{read}}, 00^{mc} \rangle \qquad i \in [1,n]$$

$$\langle \square 1^{mc}, q^{\text{read}}, \square 1^{mc}, q_A, 00^{mc} \rangle$$

Durant la première étape, un ensemble de colonnes D est choisi de façon non déterministe sur la première bande et sur chaque bande restante, kp sont remplis de 0 ou de 1 selon le reste modulo p de leur position (1 pour 0 et 0 sinon). Ensuite, toutes les têtes de lecture retournent au symbole non-blanc le plus à gauche. On remarque que toutes les colonnes de D sont choisies en garantissant que $\forall i \neq i' \in D$, $\lfloor \frac{i}{m} \rfloor \neq \left\lfloor \frac{i'}{m} \right\rfloor$. Durant la seconde étape, la somme des colonnes de D est calculée en déplaçant les têtes de lecture sur la droite. On atteint l'état accepteur si et seulement si à la fin de l'exécution toutes les têtes de lectures (sauf la première) sont sur le symbole 0, i.e. la somme de toutes les colonnes de D dans H' donne le vecteur nul. En ce qui concerne le nombre de transitions, on effectue $2kp$ transitions durant la première étape, puis au plus kp durant la seconde. De plus, la taille de la machine est polynomiale en n,m,q et k. Distribution de poids sur $\mathbb{F}_q$ appartient donc bien à $W[2]$.

La preuve de l'appartenance à $W[2]$ de Distance minimal sur $\mathbb{F}_q$ est semblable, la seule différence se situant sur D choisi de taille au plus k (au lieu de exactement k). □

Distance minimale duale sur $\mathbb{F}_q$:
Entrées : q une puissance de premier, k un entier, H une matrice $m \times n$ sur $\mathbb{F}_q$.
Paramètres : k, q.
Question : Existe-t-il une combinaison linéaire sur $\mathbb{F}_q$ d'au moins $n-k$ colonnes de H qui donne le vecteur nul ?

Distribution de poids duale sur $\mathbb{F}_q$:
Entrées : q une puissance de premier, k un entier, H une matrice $m \times n$ sur $\mathbb{F}_q$.
Paramètres : k, q.
Question : Existe-t-il une combinaison linéaire sur $\mathbb{F}_q$ de exactement $n-k$ colonnes de H qui donne le vecteur nul ?

Théorème 9. DISTANCE MINIMALE DUALE SUR $\mathbb{F}_q$ *et* DISTRIBUTION DE POIDS DUALE SUR $\mathbb{F}_q$ *sont dans* $W[2]$.

Démonstration. Tout d'abord, on effectue le même processus FPT que dans la paramétrisation standard (Théorème 8) pour obtenir la matrice H' sur $\mathbb{F}_p$ où p est la caractéristique de $\mathbb{F}_q$. Soit v le vecteur somme de toutes les colonnes de H', il est à noter qu'il existe un ensemble D d'au plus $n-k$ colonnes de H' dont la somme est le vecteur nul si et seulement si la somme de toutes les autres colonnes est v. Pour ce faire, on considère la matrice $\tilde{H} = (-v|H')$ et l'on modifie légèrement la machine de la paramétrisation standard (voir théorème 8) pour décider s'il existe un ensemble d'au plus $k+1$ colonnes qui inclue la première colonne dont la somme est le vecteur nul. On modifie donc la première étape de la machine pour forcer l'inclusion de la première colonne de $\tilde{H}$ dans D. La preuve de l'appartenance de DISTRIBUTION DE POIDS DUALE SUR $\mathbb{F}_q$ à $W[2]$ est la même à l'exception de la première étape où D est choisi de taille exactement k. □

Le théorème 8 montre que DISTANCE MINIMAL SUR $\mathbb{F}_q$ avec q puissance de premier, qui consiste à décider si il existe une combinaison linéaire d'au plus k colonnes de la matrice H avec entrées sur $\mathbb{F}_q$ qui donne le vecteur nul est dans $W[2]$. On peut aussi prouver de façon similaire l'appartenance à $W[2]$ du problème qui consiste à décider si la combinaison linéaire d'au plus k colonnes de H donne un vecteur donné. En revanche, on ne sait pas si le problème consistant à décider si une combinaison linéaire d'au plus k colonnes de H donne un vecteur sans entrées à zéro, *i.e.* un vecteur de poids de Hamming maximum. Pour être plus précis, quand q est premier on peut utiliser la même machine que pour DISTANCE MINIMAL DUALE SUR $\mathbb{F}_q$ (théorème 9) et changer la dernière transition pour vérifier que toutes les entrées sont différentes de 0, mais cette technique ne fonctionne plus si q est une puissance de premier (disons $q = p^2$), car les colonnes associées à certaines puissances peuvent être à zéro sans que l'entrée soit à zéro. Pour ce faire, il faudrait vérifier que les têtes de lecture d'un sous-ensemble de bandes ne pointent pas toutes sur 0.

1.6 Conclusion et perspectives

L'ensemble de ce travail a permis d'aboutir à la preuve de l'appartenance à $W[2]$ du cas général de la (σ, ρ)-domination avec σ et ρ récursifs, aussi bien pour la paramétrisation standard (théorème 4) que pour la paramétrisation duale (théorème 5). De plus, ce résultat a été étendu à d'autres problèmes de domination (voir la section 1.5.1) ainsi qu'à des problèmes issus de la théorie des codes (voir la section 1.5.2).

Tous ces résultats ont pu être obtenus grâce à une machine de Turing aveugle, dont le problème d'exécution courte a été montré complet pour $W[2]$ (théorème 1). L'utilisation de transitions aveugles (ne dépendants pas de la configuration) permet de passer outre une explosion du nombre de transitions, dans le cas

où la différentiation des configurations n'est pas nécessaire. Montrer l'appartenance d'un problème à $W[2]$ revient donc à représenter ce problème comme une exécution courte de la machine.

1.6.1 (σ, ρ)-domination

Tout d'abord, il est important de noter qu'un résultat de complétude pour la (σ, ρ)-domination en général est impossible à obtenir, étant donné que Ensemble stable de taille k est $W[1]$-complet [24] et correspond à de la $(\{0\}, \mathbb{N})$-domination, alors que Ensemble dominant est lui complet pour $W[2]$ [25]. De même, un résultat de difficulté générale pour $W[1]$ est impossible, étant donné que la $(\mathbb{N}, \mathbb{N})$-domination est trivialement FPT (la réponse étant toujours oui).

En revanche, ce travail a montré que tout problème de (σ, ρ)-domination est dans $W[2]$. Il reste donc à savoir si l'on peut trouver un théorème de séparation qui caractériserait les couples (σ, ρ) et donnerait une complétude pour chacune des classes. L'une des principales difficultés à envisager est due à l'analogue du théorème de Ladner [48], qui affirme l'existence de classes de complexité intermédiaires entre P et NP sous l'hypothèse $P \neq NP$. En version paramétrée, cela correspond à l'existence de classes intermédiaires entre les classes $W[i]$ sous l'hypothèse que celles-ci ne soient pas identiques [24]. La question se pose en effet pour la version impaire de la (σ, ρ)-domination qui appartient à $W[2]$ mais n'est difficile que pour $W[1]$.

De même, dans le cas de la paramétrisation duale, Golovach *et al.* ont montré dans [33] l'existence de couples σ, ρ pour lesquels le problème est FPT et d'autres pour lesquels le problème est difficile pour $W[1]$ en appartenant à $W[2]$. Nous avons montré l'appartenance à $W[2]$ du cas général mais un théorème de séparation reste possible. La différence principale est que, contrairement à la paramétrisation standard, on ne connait pas de cas où le problème est difficile pour $W[2]$. Une appartenance à $W[1]$ du cas général reste dès lors ouverte.

1.6.2 Machine de Turing Aveugle

En ce qui concerne la machine de Turing aveugle, de nombreuses perspectives restent ouvertes quant à son utilisation pour montrer l'appartenance à $W[2]$ de différents problèmes. En effet, sa structure permet de résoudre des cas généraux comme pour la (σ, ρ)-domination, et n'est limitée ni aux problèmes de domination ni même à la théorie des graphes.

L'exécution courte de la version simple de la machine de Turing est complète pour $W[1]$ [25], la version multi-bandes aveugle l'est pour $W[2]$ et il existe une version de l'exécution courte de machine de Turing pour $W[P]$ [15]. Il pourrait ainsi être intéressant d'étudier si différentes machines ne pourraient être complètes pour d'autres $W[i]$, la difficulté étant de trouver des problèmes naturels appartenant à ces classes. Une autre possibilité est de chercher une version paritaire du modèle qui pourrait correspondre aux problèmes de domination

avec parité, ceux-ci apparaissant situés entre $W[1]$ et $W[2]$ (étant difficile pour le premier mais n'appartenant qu'au second) en l'état.

Chapitre 2

Domination impaire faible

Dans ce chapitre, on s'intéresse à la domination impaire faible intervenant dans les problèmes de partage de secret quantique à l'aide d'état-graphe. Ce type de domination est défini comme :

Étant donné un graphe $G = (V, E)$, un ensemble de sommets $B \subseteq V$ est dominé de façon impaire faible (Weak Odd Dominated) s'il existe $D \subseteq V \setminus B$ tel que $\forall b \in B, |N(b) \cap D| = 1 \bmod 2$. On note $\kappa(G)$ la taille du plus grand ensemble WOD de G, $\kappa'(G)$ celle du plus petit ensemble non WOD et enfin $\kappa_Q(G)$ est le maximum de κ et de $|V| - \kappa'(G)$. Ces différentes valeurs ont été étudiées principalement dans [43], où il a été montré que les problèmes de décision associés à ces valeurs sont NP-complets.

La valeur $\kappa_Q(G)$ est d'un intérêt particulier car il correspond au seuil d'acceptation dans les protocoles de partage de secret quantique à l'aide d'état-graphe [34].

Dans la section 2.2 nous commencerons par améliorer les bornes existantes de κ et κ' en utilisant une méthode probabiliste. En particulier, nous montrerons que dans un graphe d'ordre n sans sommets isolés, $\kappa(G) \geq \frac{n}{4}$ et que dans un graphe d'ordre n sans sommets universels, $\kappa'(G) \leq \frac{7n}{8}$.

Ensuite, dans la section 2.3, nous montrerons la difficulté pour $W[1]$ et l'appartenance à $W[2]$ des problèmes paramétriques associés à κ, κ' et κ_q via un cycle de réduction à partir du problème classique de Ensemble Impaire [33].

Enfin, dans la section 2.4, nous montrerons l'existence d'un facteur constant d'approximation pour ces différentes valeurs ainsi que la non-existence d'un algorithme d'approximation polynomial pour κ et κ'. Ce chapitre regroupe les résultats publiés lors de la conférence FCT de 2013 [11].

2.1 Définition

2.1.1 Partage de secrets

Le partage de secret est un protocole de cryptographie dont le but est de partager un secret entre plusieurs personnes, ceci de façon à ce qu'un certain

nombre partageant leurs connaissances puissent retrouver ce secret. Dans un cas concret, on veut connaitre la combinaison d'un coffre de banque sans qu'un seul employé puisse l'ouvrir. Plus formellement, le partage de secret consiste à distribuer à un nombre n de dépositaires une partie d'une information (le secret) pour que k ou plus dépositaires puissent le reconstituer alors qu'un nombre inférieur n'en soit pas capable. On parle alors de protocoles de seuil (n, k).

Dans le cas classique il existe deux principaux protocoles :

- **Le protocole de Blakley [4] :** celui-ci repose sur le fait que k hyperplans non-parallèles de dimensions $k-1$ s'intersectent en un seul point, le secret consistera en une des coordonnés de ce plan. On va distribuer à chacun des n dépositaires les coordonnées d'un hyperplan auquel appartient le secret mais qui ne le fixe pas, en se réunissant k dépositaires auront donc accès au secret en résolvant le système linéaire tandis que pour un nombre inférieur k' on ne peut retrouver cette coordonnée.

- **Le protocole de Shamir [59] :** celui-ci repose sur le fait que k sommets suffisent à déterminer les coordonnés d'un polynôme p de degré $k-1$ sur un corps fini $\mathbb{F}_q$ avec $q > n$ dont le terme constant constituera le secret. On va distribuer à chacun des n dépositaires les coordonnées d'un sommet $(x, p(x))$ appartenant au polynôme avec $x \neq 0$, en se réunissant k dépositaires auront donc accès au secret en utilisant les polynômes de Lagrange, l'utilisation du polynôme sur un corps fini permettant de garantir de ne pas pouvoir approximer la solution.

Ces deux protocoles remplissent les conditions d'un protocole d'un seuil (n, k), en effet il faut bien que k dépositaires mettent en commun leur information pour retrouver le secret.

2.1.2 Partage de secrets à l'aide d'états graphes

Pour une bonne compréhension des états quantiques et de leur utilisation en théorie de l'information on pourra se référer à [53].

On s'intéresse maintenant aux protocoles de partage de secrets à l'aide d'états-graphe. Les états graphes sont un sous-ensemble particulier d'états quantiques [38] qui sont en bijections avec les graphes. Ils sont définis de la façon suivante :

Définition 9. *Étant donné un graphe $G = (V, E)$ de sommets $v_1, \ldots, v_n$, on défini l'état graphe associé de la façon suivante :*

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

avec $q(x)$ le nombre d'arêtes dans le sous-graphe induit $G[x] = (\{v_i \in V | x_i = 1\}, \{(x_i, x_j) \in E | x_i = x_j = 1\})$.

Les états graphes ont la propriété de point fixe suivante :

Propriété 1. *Étant donné un graphe $G = (V, E)$, pour tout sommet $u \in V$:*

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

avec $X = |x\rangle \to |\overline{x}\rangle$, $Z = |x\rangle \to (-1)^x |x\rangle$ et $Z_A = \bigotimes_{u \in A} Z_u$

Avec les états-graphes on peut partager des secrets classiques sous forme d'un bit $s \in \{0, 1\}$ ou des secrets quantiques sous forme d'un qubit $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$. On étudie un protocole de partage de secret classique à l'aide d'état graphe car bien qu'il soit possible de partager un secret classique avec protocole non-quantique et donc que leur mis en œuvre soit peu intéressante il permet de définir les structures d'accès au secret qui sont similaire dans le cas quantique.

Partage de secrets classiques à l'aide d'états graphes

Ici sont présentés les différents protocoles de partages de secrets à l'aide d'états-graphes de Markham et Sanders [49]. La structure d'accessibilité au secret classique est définie dans [35] par :

Définition 10. *Étant donné un graphe $G = (V, E)$, un ensemble de sommets $B \subseteq V$ est c-accessible si et seulement si $\exists D \subseteq B$ tel que $|D| \equiv 1 \ mod \ 2$ et $Odd(D) \subseteq B$.*

Étant donné un graphe $G = (V, E)$ d'ordre n, le protocole de partage d'un secret classique $s \in \{0, 1\}$ à n joueurs à l'aide d'état graphe est défini comme :

1. **Chiffrement : Le dealer prépare l'état graphe $|G\rangle$. Si $s = 1$ le dealer applique Z_V sur les qubits de l'état graphe. L'état résultant est donc :**
$$|G_s\rangle := Z_V^s |G\rangle$$
2. **Distribution : Chaque joueur j reçoit le qubit j de $|G_s\rangle$.**
3. **Reconstruction : Soit B un ensemble c-accessible de joueurs, par définition $\exists D \subseteq B$ tel que $|D| \equiv 1 \ mod \ 2$ et $Odd(D) \subseteq B$.**
   - **Les joueurs dans $Odd(D)$ appliquent $S = |x\rangle \to i^x |x\rangle$ sur leurs qubits.**
   - **Les joueurs dans D appliquent $H = |x\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle)$ sur leurs qubits.**
   - **Chaque joueur j dans $D \cup Odd(D)$ mesure son qubit dans la base $\{|0\rangle, |1\rangle\}$ et diffuse son résultat $s_j \in \{0, 1\}$ aux autres joueurs de B.**
   - **Le secret reconstruit est :**
$$|G_D| + \sum_{j \in D \cup Odd(D)} s_j \ mod \ 2$$
   avec $|G_D|$ le nombre d'arêtes dans le sous-graphe induit par D.

Propriété 2. *Étant donné un graphe $G = (V, E)$ et un ensemble de sommets $B \subseteq V$, B n'est pas c-accessible si et seulement si $\exists D \in V \setminus B$ tel que $B \subseteq Odd(D)$.*

On a donc qu'un ensemble de sommets est soit c-accessible soit WOD (Weak Odd Dominated : dominé faiblement de façon impaire), et on considérera qu'un ensemble est soit c-accessible soit non-WOD.

On remarque que si un ensemble est WOD alors toute partie de celui-ci l'est aussi et inversement en ajoutant des sommets à un ensemble non-WOD celui-ci reste non-WOD. Les valeurs à étudier dans un graphe sont donc la taille du plus grand ensemble WOD et du plus petit non-WOD.

Définition 11. *Étant donné un graphe $G = (V, E)$ soit :*

$$\kappa(G) = \max_{B \subseteq V, B\ WOD} |B| \quad \kappa'(G) = \min_{B \subseteq V, B\ c-accessible} |B|$$

Partage de secrets quantiques à l'aide d'état graphes

Étant donné un graphe $G = (V, E)$ d'ordre n, le protocole de partage d'un secret quantique $|\phi\rangle = \alpha |0\rangle + \beta 1$ à n joueurs à l'aide d'état graphe est défini comme :

1. **Chiffrement : Le dealer prépare l'état quantique $\alpha |G_0\rangle + \beta |G_1\rangle$ avec $|G_0\rangle := |G\rangle$ et $|G_1\rangle := Z_V |G\rangle$**
2. **Distribution : Chaque joueur j recoit le qubit j de $\alpha |G_0\rangle + \beta |G_1\rangle$.**
3. **Reconstruction : Soit B un ensemble non-WOD de joueurs tel que $V \setminus B$ est WOD. Par définition $\exists C, D \subseteq B$ tel que $V \setminus B \subseteq Odd(C)$, $|D| \equiv 1\ mod\ 2$ et $Odd(D) \subseteq B$.**
   - **Les joueurs dans B choisissent $u \in B$ qui va reconstruire le secret. Chaque joueur de $B \setminus \{u\}$ envoie son qubit à u.**
   - **u applique l'opérateur unitaire $\frac{1}{\sqrt{2}} \left(\begin{array}{c|c} I & U \\ \hline -U & I \end{array}\right)$ avec $U = (-1)^{|G_D|} X_D Z_{Odd(D}$ sur les $(|B|+1)$ qubits d'un système composé d'un qubit auxiliaire $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ et des qubits de B. Le résultat est l'état suivant sur $(n+1)$ qubits :**

$$\alpha |0\rangle \otimes |G_0\rangle + \beta |1\rangle \otimes |G_1\rangle$$

   - **u applique l'opérateur unitaire $\left(\begin{array}{c|c} I & 0 \\ \hline 0 & U' \end{array}\right)$ avec $U' = (-1)^{|G_C|} X_C Z_{V \setminus Odd(C)}$. Le résultat est l'état sur $(n+1)$ qubits suivant :**

$$(\alpha |0\rangle + \beta |1\rangle) \otimes |G\rangle$$

   Le secret est donc reconstruit sur le premier qubit.

On remarque ici que pour qu'un ensemble soit accessible il faut non-seulement que celui-ci soit non-WOD mais aussi que son complémentaire soit WOD. On a

donc une propriété intéressante appelé seuil quantique qui correspond à la taille à partir de laquelle tout ensemble accède au secret quantique. Le seuil quantique est défini par :

Définition 12. *Étant donné un graphe G d'ordre n soit :*

$$\kappa_Q(G) = \max(\kappa(G), n - \kappa'(G))$$

En effet, soit $B \subseteq V$ un ensemble de sommets si $|B| > \kappa_Q(G)$ alors $|B| > \kappa(G]$ donc B est par définition non-WOD (plus grand que le plus grand ensemble non-WOD) et $|B| > n - \kappa'(G)$ donc $n - |B| < \kappa'(G)$ donc par définition le complémentaire de B est WOD (plus petit que le plus petit non-WOD) donc B est accessible.

Protocole de seuil

Ici l'ajout d'un protocole de seuil de deux secrets classiques qui chiffrent le secret quantique permet d'obtenir l'effet de seuil sur le secret quantique *i.e.* étant donné $B \subseteq V$ un groupe de joueur soit $|B| \geq \kappa_Q(G)$ et B est accessible soit $|B| < \kappa_Q(G)$ et B n'a aucune information sur le secret.

Étant donné un graphe $G = (V, E)$ d'ordre n et un entier $k > \kappa_Q(G)$, le protocole de seuil de partage d'un secret quantique $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ à n joueurs à l'aide d'état graphe est défini comme :

1. **Chiffrement : Le dealer tire uniformément deux entiers aléatoires $p, q \in \{0, 1\}$ et applique $X^p Z^q$ au secret. Le résultat est l'état suivant $\alpha|p\rangle + (-1)^q \beta|1 - p\rangle$. Ensuite dealer prépare l'état quantique $\alpha|G_p\rangle + (-1)^q \beta|G_1 - p\rangle$ avec $|G_0\rangle := |G\rangle$ et $|G_1\rangle := Z_V|G\rangle$**
2. **Distribution : Chaque joueur j reçoit le qubit j de $\alpha|G_p\rangle + (-1)^q \beta|G_{1-p}\rangle$. De plus p et q sont distribués aux joueurs selon un protocole de seuil classique avec un seuil de k.**
3. **Reconstruction : Soit B un ensemble de taille $|B| \geq k$ donc comme $|B| \geq \kappa_Q(G)$, on a par définition $\exists C, D \subseteq B$ tel que $V \setminus B \subseteq Odd(C)$, $|D| \equiv 1 \ mod \ 2$ et $Odd(D) \subseteq B$.**
   - **Les joueurs dans B choisissent $u \in B$ qui va reconstruire le secret. Chaque joueur de $B \setminus \{u\}$ envoie son qubit à u.**
   - **u applique l'opérateur unitaire $\frac{1}{\sqrt{2}} \left(\begin{array}{c|c} I & U \\ \hline -U & I \end{array}\right)$ avec $U = (-1)^{|G_D|} X_D Z_{Odd(D}$ sur les $(|B|+1)$ qubits d'un système composé d'un qubit auxiliaire $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ et des qubits de B puis l'opérateur unitaire $\left(\begin{array}{c|c} I & 0 \\ \hline 0 & U' \end{array}\right)$ avec $U' = (-1)^{|G_C|} X_C Z_{V \setminus Odd(C)}$. Le résultat est l'état sur $(n+1)$ qubits suivant :**

$$(\alpha|p\rangle + \beta(-1)^q|1 - p\rangle) \otimes |G\rangle$$

   - **En utilisant le protocole classique les joueurs de B reconstruisent p et q.**
   - **u applique $Z^q X^p$ au qubit auxiliaire, l'état résultant est :**

$$\alpha|0\rangle + \beta|1\rangle$$

Ce dernier protocole de partage de secret quantique constitue la raison principale de l'étude des quantités de plus grand ensemble WOD, plus petit ensemble non-WOD et seuil quantique.

2.2 Bornes

2.2.1 État de l'art

Bornes générales

Les propriétés de κ, κ' et κ_Q ont été étudiées intensivement dans [43], et dans cette section on rappelle les résultats montrés dans cet article.

Théorème 10. *Pour tout graphe G d'ordre n,*

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

Lemme 1. *Pour tout graphe G d'ordre n et de degré Δ,*

$$\kappa(G) \leq \frac{n \cdot \Delta}{Delta + 1}$$

Lemme 2. *Pour tout graphe G d'ordre n et de degré minimum δ,*

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

Lemme 3. *Pour tout graphe G d'ordre $n > 5$,*

$$\kappa_Q(G) > 0.506n$$

Cette borne inférieur est un raffinement de $\kappa_Q(G) > \frac{1}{2}n$ venant du fait que deux ensemble de joueurs ne peuvent obtenir le secret quantique ce qui serait une violation du théorème "non-cloning" (*i.e.* il est impossible de dupliquer un état quantique).

Graphes à faible κ_Q

Ici on s'intéresse aux graphes à faible κ_Q, ces graphes sont intéressants non-seulement pour l'implémentation du partage de secret mais surtout pour leur propriétés combinatoires. En effet comme $\kappa_Q(G) = max(\kappa(G), n - \kappa'(G)$ et que $\kappa(G) > \Delta$ et $\kappa'(G) < \delta$ la plupart des constructions sont dites "quasi-unanime" avec κ_G en $n - \mathcal{O}(1)$.

Théorème 11. *Pour tout $i > 0$,*

$$\kappa_Q(Pal_{29}^{\bullet^i}) \leq n - n^{\frac{log(11)}{log(29)}} \approx n - n^{0.71}$$

avec Pal_{29} le graphe de Paley à 29 sommets, $Pal_{29}^{\bullet^1} = Pal_{29}$, $Pal_{29}^{\bullet^i} = Pal_{29}^{\bullet^{i-1}} \bullet Pal_{29}^{\bullet^{i-1}}$, $\bullet$ le produit lexicographique de graphe et $n = 29^{2^i}$ l'ordre du graphe.

Pour rappel le produit lexicographique de deux graphes $G_1 = (V_1, E_1)$ et $G_2 = (V_2, E_2)$ est définit par $G_1 \bullet G_2 = (V', E')$ avec $V' = V_1 \times V_2$ et $E' = \{((u_1, u_2), (v_1, v_2)) \,|(u_1, v_1) \in E_1$ ou $(u_1 = v_1$ et $(u_2, v_2) \in E_2)\}$. Ces graphes représentent la meilleure construction connue en ce qui concerne les graphes ayant un faible κ_Q. En revanche un résultat non-constructif montre l'existence d'une famille de graphe ayant un κ_Q linéaire.

Théorème 12. *Il existe une famille infinie de graphes $\{G_i\}$ telle que $\kappa_Q(G_i) \leq 0.811n_i$ avec n_i l'ordre de G_i*

Ce résultat est obtenu par application du lemme local asymétrique de Lovász. Un autre résultat non constructif montre aussi que les graphes aléatoires $G(n, \frac{1}{2})$ ont une bonne probabilité d'avoir un κ_Q linéaire. Un graphe aléatoire $G(n, k)$ est un graphe d'ordre n où chaque paire de sommets distincts a une probabilité k d'avoir une arête.

Théorème 13. *Il existe n_0 un entier positif tel que pour $n > n_0$, un graphe aléatoire $G(n, \frac{1}{2})$ a un κ_Q plus petit que $0.811n$ avec probabilité :*

$$Pr\left(\kappa_Q(G(n,\frac{1}{2})) < 0.811n\right) \geq 1 - \frac{1}{n}$$

2.2.2 Nouveaux résultats

Dans cette section on améliore les bornes connues concernant les plus grand ensembles WOD et plus petits ensembles non-WOD dans un graphe. Ces bornes améliorés seront essentielles dans la section suivante concernant le choix de la paramétrisation. Le plus grand ensemble WOD d'un graphe G d'ordre n et de degré Δ satisfait $\Delta \leq \kappa(G) \leq \frac{n\Delta}{\Delta+1}$ [43]. La borne $\kappa(G) \geq \Delta$ vient du fait que chaque sommet domine de façon impaire son propre voisinage. On améliore ici cette borne en utilisant une méthode probabiliste.

Lemme 4. *Pour tout graphe G d'ordre n et de degré minimum $\delta > 0$,*

$$\kappa(G) \geq \left(\frac{1}{2} - \frac{1+\log(2\delta)}{4\delta}\right) n$$

De plus, $\kappa(G) \geq \frac{n}{4}$ quand $\delta \geq 1$, et $\kappa(G) \geq \frac{8}{27}n$ quand $\delta \geq 2$.

Démonstration. La preuve de ce lemme est l'évaluation de la taille du voisinage impaire d'un ensemble de sommets choisis de façon aléatoire. Étant donné $q \in [0.5, 1]$, soit D un sous-ensemble de sommets créé en choisissant chacun des sommets $v \in V(G)$ avec probabilité $1-q$. L'espérance de la taille de D est $(1-q)n$. Pour tout v, la probabilité de l'évènement $v \in Even(D) := \{u \in V \setminus D, |N(u) \cap D] = 0 \bmod 2\}$, est $P_0(v) = q.\sum_{k=0}^{\delta(v)/2} \binom{\delta(v)}{2k}(1-q)^{2k}q^{\delta(v)-2k}$, et la probabilité de l'évènement $v \in Odd(D)$ est $P_1(v) = q.\sum_{k=0}^{\delta(v)/2} \binom{\delta(v)}{2k+1}(1-q)^{2k+1}q^{\delta(v)-2k-1}$. Or v n'est pas dans D avec probabilité $P_0(v)+P_1(v) = q$ (car si il n'est pas dans D il appartient soit à son voisinage pair soit à son voisinage impair), de plus $P_0(v)-P_1(v) = q\sum_{k=0}^{\delta(v)} \binom{\delta(v)}{k}(q-1)^k q^{\delta(v)-k} = q(2q-1)^{\delta(v)}$. En conséquence, $P_1(v) = \frac{1}{2}(q-q(2q-1)^{\delta(v)})$, et l'espérance de la taille de $Odd(D)$ est $E[|Odd(D)|] = \sum_{v\in V(G)} \frac{1}{2}(q-q(2q-1)^{\delta(v)})$. Soit $x = 2q-1$ et δ le degré minimum de G, $E[|Odd(D)|] \geq \frac{n}{4}(x+1)(1-x^\delta)$, est maximal pour $x = 0$ quand $\delta = 1$, donc $E[|Odd(D)|] \geq \frac{n}{4}$. Donc il existe $D \subseteq V(G)$ tel que $|Odd(D)| \geq \frac{n}{4}$ ainsi $\kappa(G) \geq \frac{n}{4}$. Quand $\delta = 2$, $\frac{n}{4}(x+1)(1-x^2)$ est maximal pour $x = \frac{1}{3}$, donc $E[|Odd(D)|] \geq \frac{8n}{27}$. Dans le cas général, $E[|Odd(D)|] \geq \frac{n}{4}(1+x-2x^\delta)$, ce qui est minimal pour $x = (2\delta)^{-\frac{1}{\delta-1}}$. Donc $E[|Odd(D)|] \geq \frac{n}{4}(1+(2\delta)^{-\frac{1}{\delta-1}}-2(2\delta)^{-\frac{\delta}{\delta-1}}) = \frac{n}{4}(1+\frac{\delta-1}{\delta}e^{-\frac{\log(2\delta)}{\delta-1}}) \geq \frac{n}{4}(1+\frac{\delta-1}{\delta}(1-\frac{\log(2\delta)}{\delta-1})) = n(\frac{1}{2}-\frac{1+\log(2\delta)}{4\delta})$. □

La borne du lemme 4 n'est pas serrée, en effet, pour les graphes C_5^k d'ordre $n = 5k$ composés de l'union disjointe de k C_5 (le cycle de taille 5), $\kappa(C_5^k) = 2n/5$. Concernant les graphes connexes, le plus grand ensemble WOD d'un peigne d'ordre $2k$ (un chemin de taille k P_k avec un sommet pendant sur chaque sommet

du chemin) est de taille k. On conjecture que pour tout graphe connexe G d'ordre n, $\kappa(G) \geq \lfloor n/2 \rfloor$.

La plupart des graphes d'ordre n n'ont pas d'ensemble WOD plus grand que $0.811n$. En effet, le théorème 8 de [43] implique que pour un graphe aléatoire $G(n, 1/2)$ (graph d'ordre n où chaque paire de sommets a une arrête avec probabilité $\frac{1}{2}$), $Pr(\kappa(G(n, 1/2)) \leq 0.811n) \geq 1 - \frac{1}{n}$.

Comme pour le plus grand ensemble WOD, le plus petit ensemble non-WOD d'un graphe G d'ordre n et de degré minimum δ satisfait la condition $\frac{n}{\delta+1} \leq \kappa'(G) \leq \delta+1$ [43]. La borne $\kappa'(G) \leq \delta + 1$ viens du fait qu'un sommet avec son voisinage constitue un ensemble non-WOD. Notez que une utilisation similaire de méthode probabiliste comme pour le lemme 4 n'améliore pas la borne, en effet, l'espérance de la taille de $D \cup Odd(D)$ pour un sous-ensemble choisi aléatoirement D ne donne pas de borne supérieure pour les ensembles non-WOD car on a comme contrainte que D doit être de taille impaire. À la place, on améliore la borne des ensembles non-WOD en renforçant la propriété de dualité $\kappa'(G)+\kappa(\overline{G})\geq n$ de [43] de la façon suivante :

Lemme 5. *Pour tout graphe G d'ordre n,*

$$n - \kappa(\overline{G}) \leq \kappa'(G) \leq n - \frac{\kappa(\overline{G})}{2}$$

Démonstration. La preuve de ce lemme consiste à prouver que pour tout graphe G, $\kappa'(\overline{G})\leq n-\frac{\kappa(G)}{2}$. À cette fin, on commence par prouver que $\exists D\subseteq V(G)$ tel que $|D|=1 \bmod 2$ and $|Odd(D)|\geq\frac{\kappa(G)}{2}$. En effet soit $D\subseteq V(G)$ un ensemble de sommet non-vide tel que $|Odd(D)|=\kappa(G)$. Si $|D|=1 \bmod 2$ alors on a $|Odd(D)|\geq\frac{\kappa(G)}{2}$. Autrement, si D est de taille paire alors $\forall v\in D$, $|N(v)|+|Odd(D\backslash\{v\})|\geq|Odd(D)|=\kappa(G)$. Donc soit $\{v\}$ soit $D\backslash\{v\}$, qui sont tous les deux de taille impaire, a un voisinage impaire de taille plus grande que $\frac{\kappa(G)}{2}$. Ainsi, $\exists C\subseteq V(G)$ tel que $|C|=1 \bmod 2$ et $|Odd(C)|\geq\frac{\kappa(G)}{2}$. Comme $|C|=1 \bmod 2$ implique que $\forall v \notin C$, $v\in Odd(C) \Leftrightarrow v\notin Odd_{\overline{G}}(C)$ (où $Odd_{\overline{G}}(C)$ est le voisinage impaire de C dans $\overline{G}$), $|C\cup Odd_{\overline{G}}(C)|\leq n-\frac{\kappa(G)}{2}$. Ainsi $\kappa'(\overline{G})\leq|C\cup Odd_{\overline{G}}(C)|\leq n-\frac{\kappa(G)}{2}$. □

Corollaire 1. *Pour tout graphe G d'ordre n et de degré $\Delta < n - 1$,*

$$\kappa'(G) \leq \frac{7n}{8} \qquad \textit{and} \qquad \kappa'(G) \leq \left(\frac{3}{4} + \frac{1 + \log(2(n - \Delta - 1)}{8(n - \Delta - 1)}\right) n$$

La condition $\Delta < n - 1$ du corolaire 1 est nécessaire car pour tout entier n, $\kappa'(K_n) = n$, où K_n est le graphe complet d'ordre n. De la même façon, la condition $\delta > 0$ du lemme 4 est aussi nécessaire car $\kappa(\overline{K_n}) = 0$ ($\overline{K_n}$ étant un stable de taille n). Considérant la classe des graphes remplissant ces conditions, i.e. les graphes n'ayant ni sommets universels ni sommets isolés, on montre une version plus forte de la propriété de dualité :

Lemme 6. *Pour tout graphe G d'ordre n avec un sommet universel ou un sommet isolé,*

$$\kappa'(G) + \kappa(\overline{G}) = n$$

Démonstration. Si G a un sommet isolé v son voisinage impair est vide donc $\kappa'(G)$=1, et comme dans $\overline{G}$ v est universel $\kappa(\overline{G})$=n−1. Sinon, soit u un sommet universel de G et soit $D \subseteq V(G)$ tel que $|Odd_{\overline{G}}(D)|=\kappa(\overline{G})$. Dans $\overline{G}$ u étant un sommet isolé, $|Odd_{\overline{G}}(D \oplus \{u\})|=|Odd_{\overline{G}}(D)|=\kappa(\overline{G})$, où $\oplus$ dénote la différence symétrique. Comme soit D ou $D \oplus \{u\}$ est de taille impaire, $\exists C \in \{D, D \oplus \{u\}\}$ tel que $|C|=1 \bmod 2$ et $|Odd_{\overline{G}}(C)|=\kappa(\overline{G})$. De plus $|Odd_G(C)|=n-\kappa(\overline{G})$, donc $\kappa'(G) \leq n-\kappa(\overline{G})$, ce qui implique $\kappa'(G)=n-\kappa(\overline{G})$ comme $\kappa'(G) \geq n-\kappa(\overline{G})$ pour tout graphe [43]. □

La propriété de dualité forte permet de se débarrasser des sommets isolés et des sommets universels dans les calculs de $\kappa(G)$ et $\kappa(\overline{G})$. Par exemple, si G a un sommet universel u, $\kappa'(G) = n - \kappa(\overline{G}) = n - \kappa(\overline{G} \setminus u)$, comme u est isolé dans $\overline{G}$.

2.3 Complexité Paramétrée

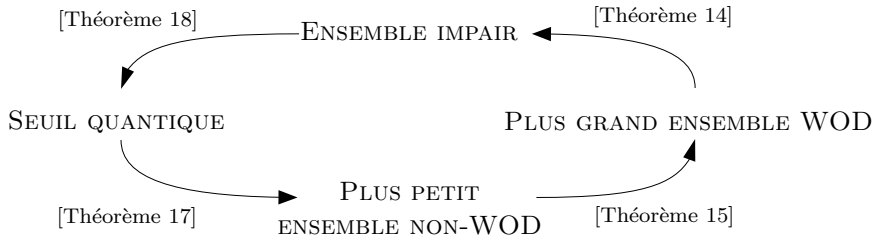


Figure 2.1 – Cycle de réduction entre Ensemble Impair et les différents problèmes de domination impaire faible

2.3.1 Choix du paramètre

Dans la section précédente on montre une borne linéaire sur la taille de $\kappa(G)$ or ce résultat implique que si on paramétrise le problème d'existence d'un ensemble WOD par la taille de celui-ci alors il sera FPT. Plus précisément, étant donné un graphe G et un paramètre k, décider si $\kappa(G) \geq k$ est FPT en utilisant

l'algorithme suivant :

`Kappa`(G, k) :
• Supprimer tous les sommets isolés. Soit n l'ordre du graphe résultant G'.
• Si $k \leq \frac{n}{4}$ alors 'vrai'
• Sinon $\forall D \subseteq V(G')$, si $|Odd(D)| < k$ alors 'faux' sinon 'vrai'.

La première étape de l'algorithme ne change pas le résultat car pour tout sommet isolé u, $\kappa(G) = \kappa(G \setminus \{u\})$. La complexité de cet algorithme est de $O^*(2^n)$ car il parcours tous les sous-ensembles possibles de n sommets, et comme on a montré dans le lemme 4 que $k = \frac{n}{4}$ alors la complexité en fonction de k est $O^*(2^{4k})$, donc le problème de l'existence d'un ensemble WOD de taille au moins k est FPT.

En ce qui concerne le plus petit ensemble non-WOD, étant donné un graphe G d'ordre n et de paramètre k, décider si $\kappa'(G) \leq n-k$ est FPT par l'algorithme suivant :

`Kappa'`(G, k) :
• Si G a un sommet universel u alors `Kappa`$(\overline{G} \setminus u, k)$
• Sinon si $k \leq n/8$ alors 'vrai'
• Sinon $\forall D$ de taille impaire si $|D \cup Odd(D)| > n-k$ alors 'faux' sinon 'vrai'.

La première étape correspond à l'application du lemme 6 : si G a un sommet universel u, $\kappa'(G) = n - \kappa(\overline{G}) = n - \kappa(\overline{G} \setminus u)$. Comme pour l'algorithme précédant, la complexité est de $O^*(2^n)$ avec l'exploration de tous les sous-ensembles possibles ce qui donne grâce à la borne du corollaire 1 une complexité de $O^*(2^{\frac{16}{7}k})$ et assure l'appartenance à FPT.

Le fait que les problèmes d'existence d'un ensemble WOD de taille k et d'ensemble non-WOD de taille $n-k$ soient FPT ne dépend que de l'existence des bornes du lemme 4 et du corolaire 1 et nous donne une relation linéaire entre le paramètre k et la taille de l'entrée n. On a donc un algorithme FPT mais celui-ci est en fait un algorithme exponentiel, ce choix de paramètre parait donc non-pertinent.

On va donc s'intéresser à la paramétrisation duale du problème qui se retrouve dans la littérature [33], on va donc utiliser comme paramètre non plus la taille du dominant recherché mais celle celle de l'ensemble dominé, on recherche donc un ensemble dominant de taille $n - k$ ce qui nous donne :

PLUS GRAND ENSEMBLE WOD DE TAILLE AU MOINS $n - k$
Entrée : Un graphe G d'ordre n, un entier k
Paramètre : k.
Question : $\kappa(G) \geq n - k$?

PLUS PETIT ENSEMBLE NON-WOD DE TAILLE AU PLUS k
Entrée : Un graphe G d'ordre n
Paramètre : Un entier k

Question :$\kappa'(G) \leq k$?

En ce qui concerne le problème de seuil quantique, étant donné un graphe G d'ordre n et un paramètre k décider si $\kappa_Q(G)=\max(\kappa(G), n-\kappa'(G))\geq k$ est FPT car $\kappa_Q(G)\geq 0.506n$ [43]. On va donc comme pour les problèmes précédents étudier la paramétrisation duale :

Seuil quantique au moins $n-k$
Entrée : Un graphe G d'ordre n
Paramètre : Un entier k
Question :$\kappa_Q(G) \geq n-k$?

Le reste de cette section consistera en la démonstration de la FPT-équivalence de ces différents problèmes avec Ensemble Impair de taille au plus k défini dans [25] comme :
Ensemble Impair de taille au moins k
Entrée : Un graphe biparti $G = (R \bigcup B, E)$ d'ordre n
Paramètre : Un entier k
Question : Existe-t-il un ensemble $D \subseteq R$ tel que $|D| \leq k$ et $B = Odd(D)$

2.3.2 Plus grand ensemble WOD

Théorème 14. Ensemble WOD de taille au moins $n-k$ *est plus difficile que* Ensemble impair *par FPT-réduction.*

Démonstration. Étant donné (G, k) où $G=(R\cup B, E)$ une instance de Ensemble impair soit (G', k') (voir figure 2.2) une instance de Ensemble WOD de taille au moins $n'-k'$ tel que $G'=(A\cup D\cup F\cup c, E_1\cup E_2\cup E_3)$, $n'=|R|+(k+2)|B|+(k+2)+1$ et $k'=k+1$ où :

$A=\{a_u, u\in R\}$

$D=\{d_{u,i}, u\in B, 1 \leq i \leq k+2\}$

$F=\{f_i, 1 \leq i \leq k+2\}$

$E_1=\{cf_i, 1 \leq i \leq k+2\}$

$E_2=\{ca_u, u\in R\}$

$E_3=\{a_u d_{v,i}, uv\in E, 1 \leq i \leq k+2\}$

• Si (G', k') est une instance positive de Ensemble WOD de taille au moins $n'-k'$, soit $C\subseteq V(G')$ le plus petit ensemble tel que $|Odd(C)|\geq n'-k'$. F est un ensemble stable de taille $k+2>k'$ donc il existe au moins un $f\in F\cap Odd(C)$ sinon l'ensemble dominé serait de taille inférieure à $n'-k'$. Comme c est l'unique voisin d'un tel f, c appartient à C. Pour tout $u\in B$, le sous-ensemble $D_u=\{d_{u,i}, 1\leq i\leq k+2\}$

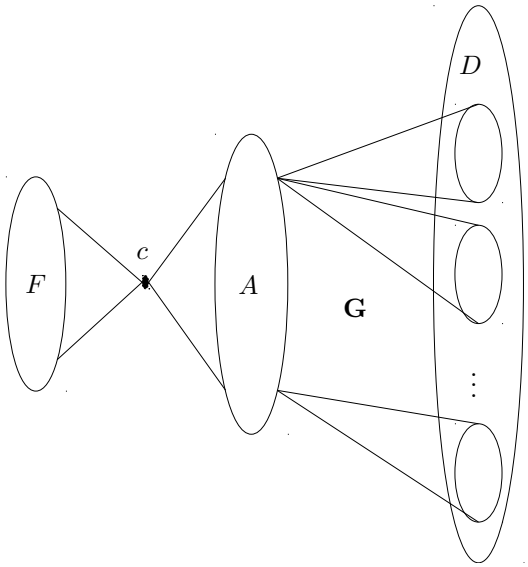


FIGURE 2.2 – Réduction de ENSEMBLE WOD DE TAILLE AU MOINS $n-k$ à ENSEMBLE IMPAIR

est un ensemble stable de taille $k+2 > k'$ dont le voisinage est strictement inclue dans A, donc $\forall u \in B, D_u \subseteq Odd(C \cap A)$ (sinon on aurait encore un ensemble dominé de taille inférieur à $n'-k'$) donc $D \subseteq Odd(C \cap A)$. Comme $c \in C$ et $A \subseteq Odd(\{c\})$, par minimalité de C, $D \cap C = \emptyset$. Soit $R' = \{u \in R, a_u \in C\}$, de taille $|R'| = |C \cap A| = |C| - 1 \leq k$. Comme $\forall u \in B, u \in Odd(R') \Leftrightarrow D_u \subseteq Odd(C)$, $B \subseteq Odd(R')$ donc (G, k) est une instance positive de ENSEMBLE IMPAIR.

• Si (G, k) est une instance positive de ENSEMBLE IMPAIR, il existe $R' \subseteq R$, tel que $|R'| \leq k$ et $B = Odd(R')$. Soit $A' = \{a_u, u \in R'\}$, comme $\forall u \in B, u \in Odd(R') \Leftrightarrow D_u \subseteq Odd(A')$, $D \subseteq Odd(A')$ donc $D \subseteq Odd(A' \cup \{c\})$. Comme $A \cup F$ est un ensemble stable dominé par c, $(F \cup A \cup D) \setminus A' = V(G') \setminus (A' \cup \{c\}) \subseteq Odd(A' \cup \{c\})$. De plus $|Odd(A' \cup \{c\}) \geq n' - (k+1) = n' - k'$, donc (G', k') est une instance positive de ENSEMBLE WOD DE TAILLE AU MOINS $n'-k'$. □

Comme ENSEMBLE IMPAIR est difficile pour $W[1]$ [33], ENSEMBLE WOD DE TAILLE AU MOINS $n'-k'$ l'est aussi. De plus, le graphe utilisé dans la preuve du théorème 14 est biparti(voir figure 2.2), on a donc :

Corollaire 2. ENSEMBLE WOD DE TAILLE AU MOINS $n-k$ *est difficile pour* $W[1]$ *même restreint aux graphes bipartis.*

2.3.3 Plus petit ensemble non-WOD

Cas général

Théorème 15. Ensemble Non-WOD de taille au plus k *est plus difficile que* Ensemble WOD de taille au moins $n-k$ *par FPT-réduction.*

Démonstration. Étant donné (G, k) où $G = (V, E)$ et $n = |V|$ une instance de Ensemble WOD de taille au moins $n-k$, soit (G', k') (voir figure 2.3) une instance de Ensemble Non-WOD de taille au plus k' tel que $G' = (A \cup B \cup \{c\}, E_1 \cup E_2 \cup E_3)$ et $k' = k + 2$ où :

$A = \{a_i, 1 \leq i \leq k + 3\}$

$B = \{b_u, u \in V\}$

$E_1 = \{b_u b_v, uv \in E\}$

$E_2 = \{a_i c, 1 \leq i \leq k + 3\}$

$E_3 = \{b_u a_i, u \in V, 1 \leq i \leq k + 3\}$

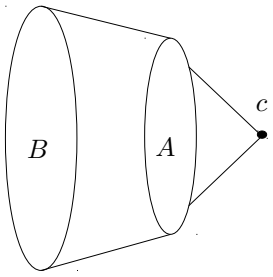


Figure 2.3 – Réduction de Ensemble Non-WOD de taille au plus k à Ensemble WOD de taille au moins $n-k$

• Si (G, k) est une instance positive de textscEnsemble WOD de taille au moins $n-k$, il existe $C \subseteq V$ tel que $|Odd(C)| \geq n-k$. Il y a deux cas possible selon la parité de la taille de C :

– Si $|C| = 0 \bmod 2$, soit $C' = \{b_u, u \in C\} \cup \{a\}$, où a est un sommet quelconque de A. Comme A est connecté par un graphe biparti complet à B, $A \subseteq Even(C')$ et $c \in Odd(C')$. Comme $a \in C'$ est connecté à tous les sommets de B, pour tout $u \in Odd(C)$ dans G, $b_u \notin Odd(C')$ dans G', donc $|C' \cup Odd(C')| \leq k + 2 = k'$.

– Si $|C| = 1 \bmod 2$, soit $C' = \{b_u, u \in C\} \cup \{a, c\}$, où a est un sommet quelconque de A. Comme A est connecté par un graphe biparti complet à B, que chaque sommet de A est voisin de c et que $|B \cap C'| = 1 \bmod 2$, on a $A \subseteq Even(C')$. De la même façon $|Odd(C') \cup C'| \leq k + 2 = k'$.

Ainsi dans les deux cas (G', k') est une instance positive de Ensemble Non-WOD de taille au plus k.

• Si (G', k') est une instance positive de Ensemble Non-WOD de taille au plus k, il existe $C' \subseteq V(G')$ tel que $|C' \cup Odd(C')| \leq k$ et $|C'| = 1 \bmod 2$. A est un ensemble stable de taille $k + 3 > k'$, donc il existe $a \in A$ tel que $a \in Even(C')$. Comme A est connecté à $V(G') \setminus A$ par un graphe biparti complet $|C'| = 1 \bmod 2$, $|C' \cap A| = 1 \bmod 2$ donc par minimalité $|C' \cap A| = 1$, soit a ce sommet. Let $C = \{u, b_u \in C'\}$, comme a est connecté à tous les sommets de B, $\forall u \in V, b_u \in Odd(C') \Leftrightarrow u \in Even(C)$ donc $|Even(C)| < k$ on obtient donc que (G, k) est une instance positive de textscEnsemble WOD de taille au moins $n-k$. □

Corollaire 3. Ensemble Non-WOD de taille au plus k *est difficile pour* $W[1]$.

Cas biparti

La preuve de la difficulté pour $W[1]$ de Ensemble Non-WOD de taille au plus k ne respecte pas la bipartition du graphe. On va montrer dans cette section que la difficulté pour $W[1]$ est conservé même en restreignant à cette classe de graphes.

Théorème 16. Ensemble Non-WOD de taille au plus k *pour les graphes bipartis est plus difficile que* Ensemble Non-WOD de taille au plus k *par* FPT*-réduction.*

Démonstration. Étant donné (G, k) une instance de Ensemble Non-WOD de taille au plus k soit (G', k') (voir figure 2.4) une instance biparti de Ensemble Non-WOD de taille au plus k avec :

$G' = (A \cup B_1 \cup B_2 \cup D \cup F \cup H, E_1 \cup E_2 \cup E_3 \cup E_4 \cup E_5)$, $k' = 2k$

$A = \{a_u, u \in V\}$

$E_1 = \{a_u b_{i,v}, i \in \{1, 2\}, uv \in E\}$

$B_1 = \{b_{1,u}, u \in V\}$

$E_2= \{a_u b_{2,u}, u \in V\}$

$B_2 = \{b_{2,u}, u \in V\}$

$E_3 = \{b_{i,u} d_{i,u,j}, i \in \{1, 2\}, u \in V, 1 \leq j \leq 2k + 1\}$

$D = \{d_{i,u,j}, i \in \{1, 2\}, u \in V, 1 \leq j \leq 2k + 1$

$E_4 = \{d_{i,u,j} f_{i,u,j,l}, i \in \{1, 2\}, \} u \in V, 1 \leq j, l \leq 2k + 1\}$

$F = \{f_{i,u,j,l}, i \in \{1, 2\}, u \in V, 1 \leq j, l \leq 2k + 1\}$

$E_5 = \{f_{i,u,j,l} h_p, i \in \{1, 2\}, u \in V, 1 \leq j, l, p \leq 2k + 1\}$

$H = \{h_i, 1 \leq i \leq 2k + 1\}$

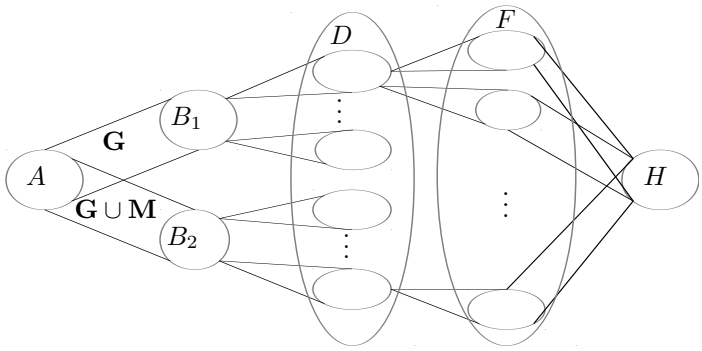


FIGURE 2.4 – Réduction du cas biparti au cas général de ENSEMBLE NON-WOD DE TAILLE AU PLUS k

• Si (G, k) est une instance positive de ENSEMBLE NON-WOD DE TAILLE AU PLUS k, il existe $C \subseteq V$ tel que $|C \cup Odd(C)| \leq k$. Soit $C' = \{a_u, u \in C\}$, notez que $|Odd(C') \cap B_1| = |Odd(C)|$ comme $\forall u, v \in V, a_u b_{1,v} \in E_1 \Leftrightarrow uv \in E$. De plus, $|Odd(C') \cap B_2| = |Odd(C) \oplus C|$, comme $\forall u, v \in V,\ a_u b_{2,v} \in E_1 \Leftrightarrow uv \in E$ et $\forall u \in V, a_u b_{2,u} \in E_2$. Donc $|C' \cup Odd(C')| = |C| + |Odd(C)| + |Odd(C) \oplus C| = 2|C \cup Odd(C)| \leq 2k = k'$ ainsi (G', k') est une instance bipartie positive de ENSEMBLE NON-WOD DE TAILLE AU PLUS k.

• Si (G', k') est une instance bipartie de ENSEMBLE NON-WOD DE TAILLE AU PLUS k, il existe $C' \subseteq V'$ tel que $|C' \cup Odd(C')| \leq 2k$ et $|C'| = 1 \bmod 2$. H étant un ensemble stable de taille $2k+1 > k'$, il existe un sommet $h \in H$ tel que $h \in Even(C')$, et comme H est connecter par un graphe biparti complet à F alors $|F \cap C'| = 0 \bmod 2$. F est composé de $(2k+1)2|V| > k'$ ensembles stables F_i de taille $2k+1 > k'$ donc $\forall i \in [1, (2k+1)2|V|] \exists f_i \in F_i$ tel que $f_i \in Even(C')$. Comme chaque F_i est connecté à un sommet $d \in D$ et connecté à H par un graphe biparti complet, $|F \cap C'| = 0 \bmod 2$ et $D \cap C' = \emptyset$. Par minimalité de C' on a que $|F \cap C'| = 0 \bmod 2$ implique $C' \cap F = \emptyset$. D étant composé de $2|V| > k'$ ensembles stables D_i de taille $2k + 1 > k'$, alors il existe $i \in [1, 2|V|]$ tel que $D_i \subseteq Even(C')$, comme D_i est connecté à un sommet $b \in B_1 \cup B_2$, on a $C' \cap (B_1 \cup B_2) = \emptyset$. Donc $C' \subseteq A$ et $Odd(C') \subseteq B_1 \cup B_2$, soit $C = \{u \in V, a_u \in C'\}$, alors $|C' \cup Odd(C')| = |C| + |Odd(C)| + |Odd(C) \oplus C| = 2|C \cup Odd(C)|$. Comme $|C' \cup Odd(C')| \leq k'$, on a $|C \cup Odd(C)| \leq k$ ce qui vérifie que (G, k) est une instance positive de ENSEMBLE NON-WOD DE TAILLE AU PLUS k. □ □

Corollaire 4. ENSEMBLE NON-WOD DE TAILLE AU PLUS k *est difficile pour* $W[1]$ *même restreint aux graphes bipartis.*

2.3.4 Seuil quantique

Difficulté du seuil quantique

Dans cette section on considère le problème de seuil quantique, le seuil quantique noté $\kappa_Q(G)$ d'un graphe G d'ordre n est défini comme étant $\kappa_Q(G) = \max(\kappa(G), \kappa(\overline{G})) = \max(\kappa(G), n-\kappa'(G))$.

Théorème 17. Seuil quantique supérieur à $n-k$ *est plus difficile que* Ensemble Non-WOD de taille au plus k *par une FPT-réduction.*

Démonstration. Étant donné (G, k) une instance de Ensemble Non-WOD de taille au plus k soit (G^{k+1}, k) une instance de Seuil quantique supérieur à $n-k$ où G^p est le graphe obtenu en prenant p copies disjointes de G. Comme $\kappa_Q(G) = \max(\kappa(G), n - \kappa'(G))$ [43], il y a deux possibilités pour $\kappa_Q(G^{k+1}) \geq (k+1)n-k$, soit $\kappa(G^{k+1})$ ou bien $n(k+1) - \kappa'(G^{k+1})$ est maximal :

- Si $\kappa(G^{k+1}) \geq (k+1)n-k$, comme les $k+1$ copies de G sont disjointes le plus grand ensemble WOD de G^{k+1} est constitué de $k+1$ copies du plus grand ensemble WOD de G (un dans chaque copie de G), donc $(k+1)\kappa(G) \geq (k+1)n - k \Leftrightarrow \kappa(G) \geq n - \frac{k}{(k+1)}$, or $\frac{k}{k+1} < 1$ donc $\kappa(G) \geq n$. Comme pour tout graphe G d'ordre n on a $\kappa(G) < n$ (en effet il faut un sommet pour pouvoir dominer de façon impair) il y a une contradiction.
- Si $(k+1)n - \kappa'(G^{k+1}) \geq (k+1)n-k$. Comme les $k+1$ copies de G sont disjointes le plus petit ensemble non-WOD de G^{k+1} est le plus petit ensemble non-WOD de G, donc $\kappa'(G^{k+1}) \leq k \Leftrightarrow \kappa'(G) \leq k$ ce qui est équivalent à (G, k) est une instance positive de Ensemble Non-WOD de taille au plus k.

□

Cette preuve respectant la bipartition du graphe, Seuil quantique supérieur à $n-k$ est donc difficile pour $W[1]$ même restreint aux graphes bipartis.

Corollaire 5. Seuil quantique supérieur à $n-k$ *est difficile pour $W[1]$ même restreint aux graphes bipartis.*

Équivalence des problèmes

Jusqu'ici on a prouvé la difficulté pour $W[1]$ de tous les problèmes de partage de secrets quantiques, par des FPT-réductions successive en partant de Ensemble impair. ces problèmes sont non-seulement difficile pour $W[1]$ mais équivalent à Ensemble impair et appartiennent à $W[2]$. En effet, Ensemble impair est plus difficile que Seuil quantique supérieur à $n-k$ par une FPT-réduction ce qui complète la boucle :

Théorème 18. Ensemble impair *est plus difficile que* Seuil quantique supérieur à $n-k$ *par une FPT-réduction.*

Démonstration. Étant donné (G, k) une instance de Seuil quantique supérieur à $n-k$, soit (G', k') (voir figure 2.5) une instance de Ensemble impair avec :

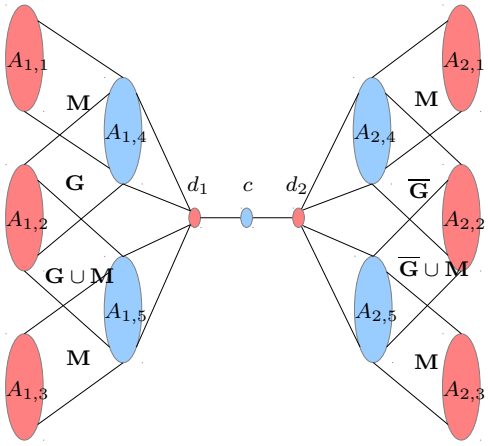


FIGURE 2.5 – Réduction de ENSEMBLE IMPAIR à SEUIL QUANTIQUE SUPÉRIEUR À $n-k$

$G' = (A \cup \{d_1\} \cup \{d_2\} \cup \{c\}, E_1 \cup E_2 \cup E_3 \cup E_4 \cup E_5 \cup \{d_1c\} \cup \{d_2c\})$

$$A = \bigcup_{1 \leq i \leq 2, 1 \leq j \leq 5} A_{i,j} \qquad E_1 = \{a_{1,2,u}a_{1,j,v}, j \in \{4,5\}, uv \in E\}$$

$$A_{i,j} = \{a_{i,j,u}, u \in V\} \qquad E_2 = \{a_{2,2,u}a_{2,j,v}, j \in \{4,5\}, uv \notin E\}$$

$$E_3 = \{a_{i,j,u}a_{i,l,u}, i \in \{1,2\}, j \in \{1,3\}, l \in \{4,5\}, u \in V\}$$

$$E_4 = \{d_i a_{i,j,u}, i \in \{1,2\}, j \in \{4,5\}, uv \in E\}$$

$$E_5 = \{a_{i,2,u}a_{i,5,u}, i \in \{1,2\}, u \in V\}$$

Et avec $B = A_{i,4} \cup A_{i,5} \cup \{c\}$, $R = A_{i,1} \cup A_{i,2} \cup A_{i,3}$ et $k' = 2k + 1$.

• Si (G, k) est une instance positive de SEUIL QUANTIQUE SUPÉRIEUR À $n-k$, comme $\kappa_Q(G) = \max(\kappa(G), \kappa(\overline{G}))$ et comme $n \geq \kappa(G) + \kappa'(G)$ [43], soit $\kappa(G)$, soit $\kappa(\overline{G})$ est plus grand que $n-k$:

– Si $\kappa(G) \geq n-k$, il existe $C \subseteq V$ tel que $|Odd(C)| \geq n-k$. Soit $C' \subseteq R$ définit par $C' = \{a_{1,2,u}, u \in C\} \cup \{a_{1,1,u}, u \in Even(C)\} \cup \{a_{i,3,u}, u \in C \oplus Even(C)\} \cup \{d_2\}$ où $\oplus$ est la différence symétrique. Comme $d_2 \in C'$, alors c, $A_{2,4}$ et $A_{2,5}$ sont dans $Odd(C')$. Comme $a_{1,2,u}a_{1,4,v} \in E_1 \Leftrightarrow uv \in E$ et $\{a_{1,2,u}, u \in C\} \subseteq C'$, alors $\{a_{1,4,u}, u \in Odd(C)\} \subseteq Odd(C')$.

$A_{1,1}$ est connecté à $A_{1,4}$ par un couplage et $\{a_{1,1,u}, u \in Even(C)\} \subseteq C'$ donc $\{a_{1,4,u}, u \in Even(C)\} \subseteq Odd(C')$ et ainsi $A_{1,4} \subseteq Odd(C')$. Comme $A_{1,5}$ est connecté à $A_{1,2}$ comme $A_{1,4}$ plus un couplage, $\{a_{1,5,u}, u \in Odd(C) \oplus C\} \subseteq Odd(C' \cap A_{1,2})$ and $\{a_{1,5,u}, u \in Even(c) \oplus C\} \subseteq Odd(C' \cap A_{1,3})$, donc $A_{1,5} \subseteq Odd(C')$. On a ainsi $B \subseteq Odd(C')$, et $|C'| = |C| + |Even(C)| + |Even(C) \oplus C| + 1 = 2|Even(C) \cup C| + 1 \leq 2k + 1 = k'$, donc (G', k') est une instance positive de Ensemble impair.

– Si $\kappa(\overline{G}) \geq n-k$ alors $d_1 \in C'$ au lieu de d_2 et en utilisant les même relations de voisinage dans $\overline{G}$ au lieu de G on obtient que (G', k') est une instance positive de Ensemble impair.

• Si (G', k') est une instance positive de Ensemble impair, il existe $C' \subseteq R$ tel que $B \subseteq Odd(C')$. c est dominé par d_1 ou d_2 (pas les deux sinon il est dominé de façon paire). Si $d_2 \in C'$, alors $A_{2,4}$ et $A_{2,5}$ sont dans $Odd(C')$. Comme $A_{1,4}$ est connecté à $A_{1,1}$ par un couplage $A_{1,2} \cap C' \neq \emptyset$ car $|A_{1,2}| \geq k$ (et qu'avec un couplage il faudrait autant de sommets dans le dominant). Soit $C = \{u | a_{1,2,u} \in C'\}$ un ensemble de sommet dans V, on a alors comme précédemment $|C'| = 2|Even(C) \cup C| + 1$ ce qui implique que $|C'| = 2|Odd(C)| + 1$, donc que $\kappa(G) \geq n-k$ ce qui est équivalent à (G, k) est une instance positive de Seuil quantique supérieur à $n-k$. Si $d_1 \in C'$, de la même façon $\kappa(\overline{G}) \geq n-k$, donc (G, k) est une instance positive de Seuil quantique supérieur à $n-k$ d'après [43]. □

Corollaire 6. *Tous les problèmes suivants :* Ensemble WOD de taille au moins $n-k$, Ensemble Non-WOD de taille au plus k *et* Seuil quantique supérieur à $n-k$ *même restreint aux graphes bipartis sont FPT-équivalents à* Ensemble impair *et donc sont difficiles pour* $W[1]$ *et appartiennent à* $W[2]$.

2.4 Complexité Approximation

2.4.1 Approche

Dans la section précédente, nous avons vu que l'approche par paramétrisation en utilisant une paramétrisation classique, par la taille de l'ensemble recherché, ne permet pas de résoudre les problèmes de domination impaire en temps polynomial en fixant un paramètre. Dans cette section, on va donc prendre une approche différente par approximation, *i.e.* si l'on peut pas résoudre ces problèmes en temps polynomial, on peut en revanche peut être avoir une approximation de la solution convenable en temps polynomial.

Définitions des classes et des réductions

Tout d'abord pour l'approche par approximation, il faut considérer la version d'optimisation des problèmes et non plus existence. En effet, il s'agit ici d'essayer de trouver une solution la plus proche possible de la solution optimale. De

façon formel, les problèmes d'optimisation combinatoires sont définis de la façon suivante :

Définition 13. *Un problème d'optimisation combinatoire A est un quintuplet (I, S, f, m, g) avec :*

- *I l'ensemble des instances du problème ;*
- *$S = \bigcup_{x \in I} S_x$ l'ensemble des solutions réalisables du problème pour chaque instance $x \in I$;*
- *$f : I \to S$ tel que étant donné $x \in I$ une instance du problème, $f(x) \in S_x$ est une solution réalisable de x ;*
- *$m : I \times S \to \mathbb{R}^+$ étant donnés $x \in I$ et $y = f(x) \in S_x$, $m(x, y)$ est la mesure de y ;*
- *g est le but du problème : **min** ou **max**.*

Étant une donnée instance $x \in I$ de A, une solution réalisable optimale de x notée opt_x respecte la propriété suivante :

$$m(x, opt_x) = g\{m(x, t) | t \in S_x\}$$

Définition 14. *Étant donné $A = (I, S, f, m, g)$ un problème d'optimisation, $\epsilon > 0$ un réel et soit $\rho = 1 + \epsilon$, un algorithme Alg est appelé algorithme de ρ-approximation du problème A si pour toute instance $x \in I$ il renvoie une solution réalisable $y = Alg(x) \in S$ avec pour mesure $m(x, y)$ tel que :*

$$|m(x, y) - m(x, opt_x)| \leq \epsilon \cdot m(x, opt_x)$$

Définition 15. *Étant donné $\rho \in \mathbb{R}$, $\rho > 1$, $APX(\rho)$ est sous-classe de NPO (pendant de NP pour les problèmes d'optimisations) contenant les problèmes admettant un algorithme ρ-approximation.*
APX est l'union des $APX(\rho)$ pour tout $\rho \in \mathbb{R}, \rho > 1$

On défini maintenant les réductions à l'intérieur de cette classe de la façon suivante :

Définition 16. *Étant donnés $A = (I_A, S_A, f_A, m_A, g_A)$ et $B = (I_B, S_B, f_B, m_B, g_B)$ deux problèmes d'optimisations. Une paire de fonctions $h : I_A \to I_B$ et $k : S_B \to S_A$ si et seulement si :*

- *h et k sont calculables en temps polynomiale*
- *$\forall x \in I_A$, $h(x) \in I_B$*

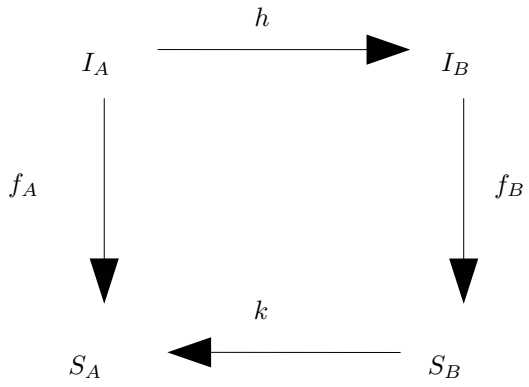


FIGURE 2.6 – Schéma d'une L-réduction

– $\forall x \in I_A$, $f_A(x)$ *est une solution de* x *implique* $k(f_B(h(x)))$ *est une solution de* x *(voir figure 2.6)*

– *il existe une constante positive* α *tel que* $\forall x \in I_A$ *:*

$$opt_{h(x)} \leq \alpha \cdot opt_x$$

– *il existe une constante positive* β *tel que* $\forall x \in I_A$ *et* $y' \in S_B$ *solution de* $h(x)$ *:*

$$|m_A(x, opt_x) - m_A(x, k(y'))| \leq \beta |m_B(h(x), opt_{h(x)}) - m_B(y')|$$

Propriété 3. *APX est clos par L-réduction.*

La principale conséquence de cette propriété qui nous intéressera concerne les démonstrations de complétude pour APX. En effet, comme APX est clos par L-réduction alors étant deux problèmes A et B de APX, A étant complet pour APX alors montrer une L-réduction de B à A revient à montrer la complétude de B pour APX.

On peut encore raffiner la complexité d'approximation en cherchant non plus à avoir une approximation de ratio fixe mais à définir un schéma qui pour un ratio ϵ donné donne une $(1+\epsilon)$-approximation. Si un tel schéma s'exécute en temps polynomial en la taille de l'entrée pour $\epsilon \in]0,1[$ on parle alors de $PTAS$ et même si l'on n'a pas la solution exacte on peut s'en rapprocher tout en permettant une exécution réelle.

Définition 17. *Un schéma d'approximation pour le problème A est une famille de $(1+\epsilon)$-approximations notée Alg_ϵ pour tout $\epsilon \in]0,1[$.*

Si ce schéma d'approximation pour le problème A s'exécute en temps polynomial en $|x|$ pour tout $\epsilon \in]0,1[$ il est dit $PTAS$ (Polynomial-Time Approximation Scheme).

Par extension $PTAS$ est la classe de problème admettant un $PTAS$.

De façon similaire à la complexité classique ou pour la complexité paramétrée la question $PTAS = APX$ reste ouverte.

Propriété 4. *Étant donné A un problème d'optimisation tel que A est complet pour APX alors A n'admet pas de $PTAS$ sous l'hypothèse $P \neq NP$.*

Il s'agit donc pour un problème A donné :
- soit d'exhiber un $PTAS$ pour montrer son appartenance à la classe $PTAS$.
- soit de monter qu'il existe une L-réduction de A à un problème complet pour APX donc qu'il n'existe pas de $PTAS$ pour A sous l'hypothèse $P \neq NP$.

Définitions des problèmes de domination impaire

Dans le cadre de la complexité d'approximation, le problème de trouver le plus grand ensemble WOD devient donc un problème de maximisation dont les solutions admissibles sont les ensembles WOD et dont la mesure est la taille de ces ensembles. Comme dans le cas des stables il n'existe aucun ensemble WOD on doit ajouter cette possibilité, ce qui nous donne la définition suivante :
Ensemble Max WOD
Entrée : un graphe $G = (V, E)$
Solution admissible : un ensemble de sommets $D \in V$ tel qu'il existe un ensemble $X \in V \setminus D$ avec $Odd(X) = D$, $D = \emptyset$ si il n'en existe aucun
Mesure : $|D|$
Objectif : maximisation

On a donc par définition $\kappa(G)$ comme mesure de la solution réalisable optimale. Pour le cas où il n'y a pas de solutions admissibles et donc $\kappa(G) = 0$, le ratio n'est pas défini, on le considèrera à 1.

De la même façon on a pour les ensembles non-WOD le problème de minimisation suivant :
Ensemble Min non-WOD
Entrée : un graphe $G = (V, E)$
Solution admissible : Ensemble de sommets $D \in V$ tel qu'il n'existe pas d'ensemble $X \in V \setminus D$ avec $Odd(X) = D$
Mesure : $|D|$
Objectif : minimisation

On remarque que de façon similaire aux ensembles WOD, $\kappa'(G)$ est la mesure de la solution réalisable optimale, mais qu'en revanche dans ce cas il existe toujours une solution réalisable.

Pour le problème de l'accessibilité quantique on a par le théorème du non-clonage que soit un état est non-accessible soit son complémentaire est non-accessible dans le cas contraire on accèderait à deux copies d'un état quantique. On considèrera donc ici tout ensemble de sommets comme solution réalisable mais la mesure dépendra de l'accessibilité de l'ensemble : si il n'est pas accessible (i.e. il est WOD) alors ce sera sa taille, sinon (il est non-WOD) ce sera la taille de son complémentaire. Ce qui nous donne la définition suivante :
Max non-Accessible Set
Entrée : un graphe $G = (V, E)$
Solution admissible : un ensemble de sommets $D \in V$
Mesure : soit $Dom = \{X \in V | Odd(X) = D\}$ $\begin{cases} |D| \text{ si } Dom \text{ est non-vide} \\ |V| - |D| \text{ si } Dom \text{ est l'ensemble vide} \end{cases}$
Objectif : maximisation

Comme pour les précédents problèmes on a $\kappa_Q(G)$ comme mesure de la réalisation de la solution réalisable optimale.

2.4.2 Plus grand ensemble WOD

Ici on s'intéressera à la complexité d'approximation du problème Ensemble Max WOD et on démontrera qu'il est complet pour APX et donc n'admet pas de $PTAS$ si $P \neq NP$.

Théorème 19. *Le problème* Ensemble Max WOD *est complet pour* APX.

La preuve de la difficulté consiste en une réduction depuis Max 3-Sat B dont la difficulté pour APX est prouvée dans [55], pour tout $B \in \mathbb{N}^*$,

Max 3-Sat B
Entrée : une formule 3-CNF ψ où chaque littéral apparait au plus B fois.
Solution admissible : une affectation des variables de ψ.
Mesure : le nombre de clauses satisfaites.
Objectif : maximisation

Lemme 7. *Pour tout* $B \geq 0$ Ensemble Max WOD *est plus difficile que* Max 3-Sat B *par L-réduction.*

Démonstration. Soit ψ une instance de Max 3-Sat B avec n clauses, soit f tel que $f(\psi) = G'$ (voire figure 2.7) soit une instance de Ensemble Max WOD tel que $G' = (C \cup D \cup F, E_1 \cup E_2)$ où :

$C = \{a, \overline{a} | a \text{ est une variable de } \psi\}$

$F = \{f_{a,j} | a \text{ est une variable de } \psi, j \in [1, 4B+1]\}$

$D_i = \{d_{i,a}, d_{i,b}, d_{i,c}, d_{i,ab}, d_{i,ac}, d_{i,bc}, d_{i,abc} | a, b, c \text{ sont les littéraux de la } i^{ème} \text{ clause de } \psi\}$

$D = \bigcup_{i \in [1,n]} D_i$

$E_1 = \{ad_{i,a}, ad_{i,ab}, ad_{i,ac}, ad_{i,abc} | i \in [1,n]\} \cup$
$\{bd_{i,b}, bd_{i,ab}, bd_{i,bc}, bd_{i,abc} | i \in [1,n]\} \cup$
$\{cd_{i,c}, cd_{i,ac}, cd_{i,bc}, cd_{i,abc} | i \in [1,n]\}$

$E_2 = \{af_{a,j}, \overline{a}f_{a,j} | j \in [1, 4B+1], F_{i,j} \subseteq F\}$

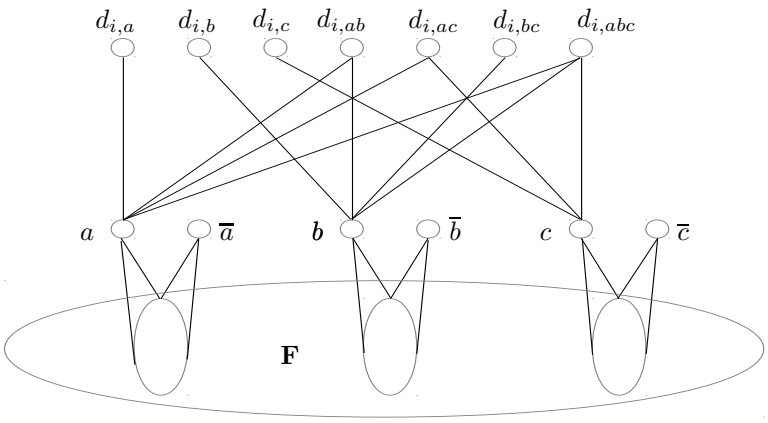


FIGURE 2.7 – Partie du graphe de la réduction de MAX 3-SAT B à ENSEMBLE MAX WOD correspondant à la clause $a \vee b \vee c$

• Soit g une fonction telle que, étant donné $D \subseteq V(G')$ un ensemble de sommets de G', $g(D)$ est une affectation de ψ tel que la variable a si le sommet $a \in D$ (même si $\overline{a} \in D$) et est faux autrement. La fonction g est calculable en temps polynomial et comme G' est polynomial en $|\psi|$, f est calculable en temps polynomial.

Dans G', $|C| \leq 6n$ et $|D| = 7n$, et comme chaque variable de ψ est dans au

plus B clauses, alors $|F| \leq 3n \times 4B + 1$, donc la taille de G' est linéaire dans la taille de ψ. Soit $MaxSAT(\psi)$ la valeur maximum du nombre de clauses vrai dans la solution optimale de Max 3-Sat B sur ψ, comme $|G'| = \alpha|\psi|$ et que $MaxSAT(\psi) \geq \frac{|\psi|}{2}$, on a $\kappa(G') \leq 2\alpha MaxSAT(\psi)$.

Étant donné $C' \subseteq C$, et $(a \vee b \vee c)$ la $i^{ème}$ clause de ψ, $C' \cap \{a, b, c\} \neq \emptyset$ si et seulement si $|Odd(C') \cap D_i| = 4$ comme (voir figure 2.8) :

- si $|C'| = 1$, soit $a \in C'$ alors $d_{i,a}, d_{i,ab}, d_{i,ac}, d_{i,abc} \in Odd(C')$ et $d_{i,b}, d_{i,c}, d_{i,bc} \in Even(C')$ et symétriquement pour b et c.
- si $|C'| = 2$, soit $a, b \in C'$ alors $d_{i,a}, d_{i,b}, d_{i,ac}, d_{i,bc} \in Odd(C')$ et $d_{i,c}, d_{i,ab}, d_{i,abc} \in Even(C')$ et symétriquement pour b, c et a, c.
- si $|C'| = 3$, soit $a, b, c \in C'$ alors $d_{i,a}, d_{i,b}, d_{i,c}, d_{i,abc} \in Odd(C')$ et $d_{i,ab}, d_{i,ac}, d_{i,bc} \in Even(C')$.

Ceci correspond au fait que chaque élément d'un ensemble apparait dans la moitié des parties de celui-ci (ici il n'y pas pas l'ensemble vide).

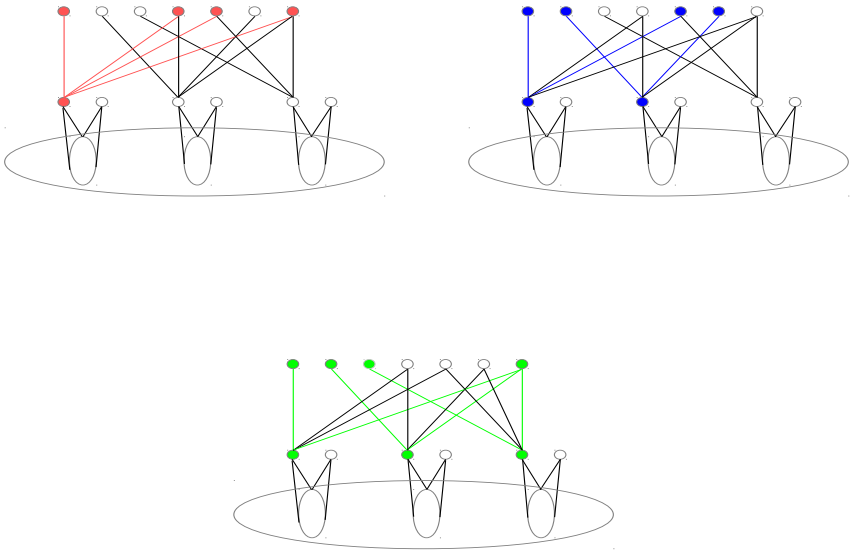


Figure 2.8 – 4 d_i dont toujours dominer quelque soit le nombre de sommets dans le dominant

Pour toute variable a de ψ, il existe $F_a = \{f_{a,j} | j \in [1, 4B+1]\}$ un ensemble stable de taille $4B + 1$ connecté uniquement à a et $\overline{a}$. Soit $C' \subseteq C$, comme $|Odd(C') \cap D_i| \leq 4$ et que la variable a apparait dans au plus B clauses de ψ, si $a, \overline{a} \in C'$, $|Odd(C' \setminus \overline{a})| > |Odd(C')|$ il n'y a donc aucune paire $a, \overline{a}$ dans la solution optimale de Max WOD Set.

• Soit X_{opt} la solution optimale de Max WOD Set, comme il n'y a pas

de paire $a, \overline{a}$ dans X_{opt}, alors $F \subseteq Odd(X_{opt})$ et le nombre de D_i dominés par X_{opt} est $MaxSAT(\psi)$. Soit l le nombre de clauses satisfaites par $g(X)$, $MaxSAT(\psi) - l = k$ implique que $g(X)$ satisfait k clauses de moins que $g(X_{opt})$. Donc X domine de façon impaire k D_i de moins que X_{opt} ou contient une paire $a, \overline{a}$, donc X domine de façon impaire $4k$ sommets de moins que X_{opt}. On a donc $MaxSAT(\psi) - l \leq \beta(\kappa(G') - |Odd(X)|)$. □

Preuve du théorème 19. Pour tout $B \geq 3$ Max 3-Sat B est difficile pour APX et il existe une L-réduction de Max 3-Sat B à Max WOD Set, donc Max WOD Set est au difficile pour APX. La complétude est obtenue la méthode des probabilités conditionnelles [57] sur la borne linéaire de $\kappa(G)$ donné par le lemme 4 qui donne une $(1 + \frac{1}{4})$-approximation polynomiale de κ.

Corollaire 7. *Il existe un $\epsilon > 0$ tel qu'il n'existe pas de $(1+\epsilon)$-approximation de* Max WOD Set *en temps polynomial sous condition $P \neq NP$ i.e. il n'existe pas de $PTAS$ pour* Max WOD Set *sous condition $P \neq NP$.*

2.4.3 Plus petit ensemble non-WOD

Ici on s'intéressera à la complexité d'approximation du problème Ensemble Min non-WOD et on démontrera qu'il est complet pour APX et donc n'admet pas de $PTAS$ si $P \neq NP$.

Théorème 20. *Le problème* Ensemble Min non-WOD *est complet pour APX.*

La preuve de la difficulté réside dans une réduction depuis Ensemble Max WOD prouvé difficile pour APX dans le théorème 19.

Lemme 8. Ensemble Min non-WOD *est plus difficile que* Ensemble Max WOD *par L-réduction.*

Démonstration. Étant donné un graphe $G = (V, E)$ instance de Ensemble Max WOD de taille n, soit f tel que $f(G) = G'$ est une instance de Ensemble Min non-WOD tel que $G' = (V \cup d, E_1 \cup E_2)$ (voir figure 2.9) où :

$$E_1 = \{uv | u \in V, v \in V, uv \notin E\}$$

$$E_2 = \{ud | u \in V\}$$

Soit une fonction g telle que, étant donné $X \subseteq V(G')$ un ensemble non-WOD de G', $g(X)$ est un ensemble WOD de G définie par $g(X) = \{u | u \notin X, u \neq d\}$. Comme X est un ensemble non-WOD il existe $D \subseteq X$ tel que $|D| = 1 \bmod 2$ et $Odd(D) \subseteq X$, donc $\overline{X} \subseteq Even(D)$, et ainsi on a $\overline{X} \subseteq Odd(D)$ dans $\overline{G'}$. Comme d est isolé dans $\overline{G'}$, $\overline{X} \subseteq Odd(D)$ dans G donc $g(X)$ est un ensemble WOD dans G et $|g(X)| = n - |X|$. g est calculable en temps polynomial et comme G' est de taille polynomial en n (de taille $n + 1$), f est calculable en temps polynomial.

Avec le lemme 6, $\kappa'(G') + \kappa(\overline{G'}) = n+1$, donc $\overline{G'}$ est G auquel on ajoute un sommet isolé et qu'un sommet isolé ne change pas la valeur de κ il ne domine ni n'est dominé par personne), donc $\kappa'(G') = n + 1 - \kappa(G)$. Avec le lemme 4, $\kappa(G) \geq \frac{n}{4}$, donc $\kappa(G') \leq \alpha\kappa(G)$.

En ajoutant $|g(X)| = n - |X|$ à $\kappa'(G') = n + 1 - \kappa(G)$ on obtient que pour toute solution X de Ensemble Min non-WOD, $|\kappa(G) - |g(X)|| \leq \alpha|\kappa'(G') - |X||$.

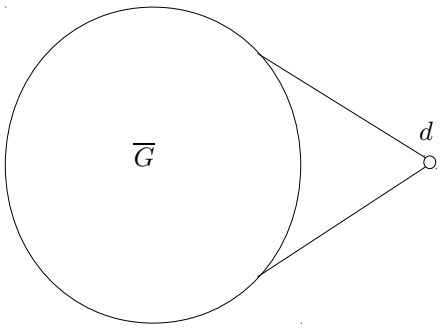


Figure 2.9 – Réduction de Ensemble Min non-WOD à Ensemble Max WOD

□

Preuve du théorème 20. Ensemble Max WOD est difficile pour APX et il existe une L-réduction de Ensemble Max WOD vers Ensemble Min non-WOD, donc Ensemble Min non-WOD est aussi difficile pour APX. Pour la complétude on utilise comme pour Ensemble Max WOD la méthode des probabilités conditionnelles [57] sur le corollaire 1 ce qui donne une $(1 + \frac{1}{8})$-approximation polynomiale de κ'.

Corollaire 8. *Il existe un $\epsilon > 0$ tel qu'il n'existe pas de $(1+\epsilon)$-approximation polynomiale de* Ensemble Min non-WOD *sous condition $P \neq NP$ i.e. il n'existe pas de $PTAS$ pour* Ensemble Min non-WOD *sous condition $P \neq NP$.*

2.4.4 Plus grand ensemble non-accessible

En ce qui concerne le problème Ensemble Max non-Accessible, l'utilisation de la méthode des probabilités conditionnelles [57] sur la borne $\kappa_Q > \frac{1}{2}$ de [34] nous donne une $(\frac{1}{2})$-approximation polynomiale de κ_Q. En revanche bien que l'on ait la propriété suivante de κ_Q : pour tout graphe G d'ordre n $\kappa_Q(G) = max(\kappa(G), n - \kappa'(G))$ et $\kappa_Q(G) = max(\kappa(G), \kappa(\overline{G}))$ [34], on n'a pas pu montrer de réduction de Ensemble Max WOD ni de Ensemble Min non-WOD à Ensemble Max non-Accessible. Comme nous n'avons pu non plus

exhiber de $PTAS$ pour ce problème son positionnement dans APX reste ouvert soit complet, soit $PTAS$ soit intermédiaire.

2.5 Conclusion et perspectives

L'utilisation dans la première partie du chapitre d'une méthode non-déterministe a permis une amélioration des bornes inférieures et supérieures de respectivement κ et κ'. On a donc obtenue de façon non-déterministe $\kappa(G) \geq \frac{n}{4}$ (lemme 4) pour tous les graphes sans sommets isolés et $\kappa'(G) \leq \frac{7n}{8}$ (corollaire 1) pour tous les graphes sans sommets universels. En revanche, l'utilisation de cette méthode n'a pas permis de raffiner la borne inférieure sur le seuil quantique $\kappa_Q(G) \leq 0.506n$ obtenue par *Perdrix et al.* dans [43].

Ces bornes permettent de démontrer que la paramétrisation "naturelle" du problème par la taille de la solution pour trouver le plus grand ensemble WOD et le plus petit ensemble non-WOD conduit à des algorithmes FPT, mais avec un noyau linéaire dans la taille de l'entrée. Nous nous sommes donc penchés sur la paramétrisation "duale" Ensemble WOD de taille au moins $n-k$, Ensemble Non-WOD de taille au plus k et Seuil quantique supérieur à $n-k$, et avons montré leur appartenance à $W[2]$ ainsi que leur difficulté pour $W[1]$ par l'équivalence avec le problème classique Ensemble impair via une série circulaire de réductions. Ces derniers résultats montrent qu'il n'y a pas d'algorithme FPT pour ces problèmes à moins que la hiérarchie W ne s'effondre.

Enfin, nous nous sommes penchés sur la complexité en approximation de la version optimisation de ces différents problèmes. L'application de la méthode des probabilités conditionnelles [57] sur les bornes linéaires montrées précédemment donne une appartenance à APX de ces problèmes. Ensuite, nous avons montré la complétude pour APX de Ensemble Max WOD et Ensemble Min Non-WOD via une réduction à Max 3-Sat B. En revanche, le même résultat n'as pas pu être montré pour Ensemble Max non-Accessible et un algorithme $PTAS$ n'a pas pu être exhibé. Le problème de sa complexité en approximation reste donc ouvert.

2.5.1 Bornes

Tout d'abord, concernant la borne sur le plus grand sommet WOD dans le graphes sans sommets isolés de $\kappa(G) \geq \frac{n}{4}$ (lemme 4), on peut remarquer que celle-ci est proche de la meilleure construction connue. Cette dernière consiste en l'union disjointe de cycles de taille 5, C_5^i, dont le plus grand ensemble WOD est de taille $\kappa(C_5^i) = 2i$. En revanche, en ce qui concerne le seuil quantique, aucune construction dont κ_Q soit linéaire dans la taille de l'entrée n'est connue, alors que l'on sait par des méthodes non-constructives que de telles constructions existent [43].

2.5.2 Complexité paramétrée

En ce qui concerne la complexité paramétrée, il faut souligner que la paramétrisation standard donne des algorithmes FPT pour les différents problèmes de domination impaires faibles mais avec un noyau de taille linéaire dans la taille de l'entrée 2.3.1. La paramétrisation duale pour calculer κ, κ' et κ_Q étant difficile pour $W[1]$ (corollaire 6), elle ne donne donc pas d'algorithmes efficaces.

On a également montré que ces problèmes sont difficiles pour $W[1]$ et appartiennent à $W[2]$, ceci en montrant leur FPT-équivalence avec ENSEMBLE IMPAIR, ce dernier étant un problème classique dont la complexité reste un problème ouvert. De plus, ces problèmes sont de bons candidats à l'appartenance à une classe W-intermédiaire, équivalente paramétrée aux classes NP-intermédiaires de Ladner [48].

Enfin, d'autres pistes restent ouvertes quant au choix du paramètre. En effet, pour les problèmes de graphes, et en particulier pour les problèmes de domination, la largeur d'arborescence et la largeur de coupe ont été utilisées comme paramètres [17, 61]. L'étude de la complexité selon ces paramètres pourrait ainsi être intéressante.

2.5.3 Complexité en approximation

Pour la complexité en approximation, la principale piste de réflexion consiste à montrer, soit la complétude pour APX de ENSEMBLE MAX ACCESSIBLE dont on n'a pas pu faire la preuve contrairement à ENSEMBLE MAX WOD et ENSEMBLE MIN NON-WOD (théorèmes 19 et 20), alors qu'il existe les relations directes entre κ_Q et les valeurs κ et κ', soit à exhiber un algorithme $PTAS$.

Chapitre 3

Degré minimum par complémentation locale

Dans ce chapitre, on s'intéresse au degré minimum par complémentation locale. Cette propriété très importante en théorie de l'information quantique intervient dans les ratios de codes quantiques [1], dans la complexité de préparation d'états-graphes [41] qui sont utilisés comme ressources pour le calcul quantique par mesures [58], ou dans les seuils de partage de secrets quantiques [49, 34].

Cette propriété vient de la complémentation locale, une opération classique de théorie des graphes introduite par Kotzig [46], qui consiste à complémenter le voisinage d'un sommet d'un graphe : deux graphes sont LC-équivalents si et seulement si une série de complémentations locales permet de passer de l'un à l'autre. On défini le *degré minimum par complémentation locale* d'un graphe G comme étant le plus petit degré minimum sur tous les graphes LC-équivalents à G.

Dans [43], il a été montré que le problème de décision du degré minimum par complémentation locale est NP-difficile et APX-complet.

Tout d'abord dans la section 3.2, on prouve que pour tout graphe d'ordre n, le degré minimum par complémentation locale est au plus $\frac{3}{8}n + o(n)$, et $\frac{n}{4} + o(n)$ dans le cas des graphes bipartis. On prouve aussi que le degré minimum par complémentation locale est inférieur à la moitié du nombre de couverture par sommet (à un terme logarithmique près).

Ensuite dans la section 3.3, on étudie la complexité paramétrée du problème du degré minimum par complémentation locale ainsi que sa restriction aux graphes bipartis. On prouve que ces deux problèmes sont FPT-équivalents au problème classique Ensemble pair, ce qui implique leur appartenance à $W[2]$. Cependant, cela n'implique pas de résultat de difficulté étant donné que la difficulté pour $W[1]$ de Ensemble pair reste un problème ouvert depuis sa définition [33].

Pour finir dans la section 3.4, on introduit un algorithme exponentiel pour calculer le degré minimum par complémentation locale, principalement basé sur

les bornes supérieures. On prouve que le degré minimum par complémentation locale d'un graphe d'ordre n peut être calculé en temps $\mathcal{O}^*(1.938^n)$. On montre aussi que cet algorithme peut grandement être amélioré pour les graphes bipartis et donc que le degré minimum par complémentation locale d'un graphe biparti d'ordre n peut être obtenu en temps $\mathcal{O}^*(1.466^n)$.

3.1 Introduction

Complémentation locale

La complémentaion locale d'un graphe G par rapport à un sommet u notée $G \star u$ consiste à complémenter le voisinage de ce sommet (voir figure 3.1), donc pour tous sommets v et w voisins de u, il a une arête entre v et w dans $G \star u$ si et seulement si il n'y a pas d'arête entre v et w dans G. Soit en utilisant la notation $v \sim_G w$ pour noter que v et w sont voisins :

Définition 18. *La complémentation locale d'un graphe $G = (V, E)$ par rapport à un de ses sommets $u \in V$ est l'application $G \mapsto G \star u$ telle que $v, w \in V$, $v \sim_{G \star u} w$ si et seulement si $(v \sim_G w)$ xor $(u \sim_G v \wedge u \sim_G w)$.*

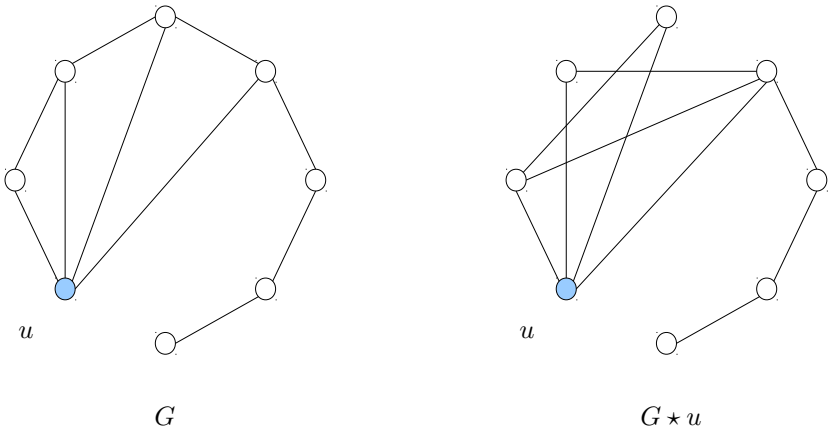


FIGURE 3.1 – Exemple de complémentation locale

La complémentation locale est une involution : $G \star u \star u = G$. Deux graphes G et H sont dit LC-équivalents (pour *Local Complementation*) si et seulement si il existe une séquence de complémentations locales de G vers H :
$G \equiv_{LC} H \Leftrightarrow \exists u_0, \ldots u_k, G \star u_0 \ldots \star u_k = H$. La complémentation locale n'est pas commutative. En effet $G \star u \star v$ est différent de $G \star v \star u$ si u est voisin de v.

En revanche $G \star u \star v \star u$ est égale à $G \star v \star u \star v$: cette opération est appelée *pivoting*.

La complémentation locale a été introduite par Kotzig [46]. L'étude de cette quantité a de nombreuses applications en théorie des graphes : Bouchet [8, 9] et de Fraysseix [22] ont utilisé la complémentation locale pour définir les graphes circulaires, et Oum [54] fait le lien entre la notion de mineur et la complémentation locale. Une propriété importante de la complémentation locale montrée par Bouchet [6] est que la LC-équivalence peut être décidée en temps polynomial en l'ordre des graphes.

Rang de coupe

La complémentation locale est liée au rang de coupe [1] [6, 54] : étant donné un graphe $G = (V, E)$, un ensemble de sommets $A \subseteq V$ formant une bipartition $(A, V \backslash A)$ de V, $\text{cutrk}_G(A)$ est le rang de l'application linéaire $L_A : 2^A \to 2^{V \backslash A} = X \mapsto Odd_G(X) \cap (V \backslash A)$, i.e. L_A associe à un sous-ensemble de A son voisinage impair dans $V \setminus A$. L_A est linéaire par rapport à la différence symétrique : $L_A(X \Delta Y) = L_A(X) \Delta L_A(Y)$. Le rang de coupe peut également être défini comme le rang de la matrice de coupe, une sous-matrice de la matrice d'adjacence ayant comme lignes les sommets de A et comme colonnes les sommets de $V \setminus A$. On a aussi pour tout $A \subseteq V$, $\text{cutrk}_G(A) = \text{cutrk}_G(V \backslash A)$.

Deux graphes LC-équivalents ont le même rang de coupe [7] :

Propriété 5. *Étant donné deux graphes G et H tels que $G \equiv_{LC} H$, $\forall A \subseteq V(G)$* $\text{cutrk}_G(A) = \text{cutrk}_H(A)$

Cependant l'inverse (deux graphes ayant le même rang de coupe sont LC-équivalents) conjecturé dans [6], a été infirmé par Fon deer Flaass [31] : le contre exemple consiste en deux graphes de Petersen isomorphes qui ont le même rang de coupe mais qui ne sont pas LC-équivalents (voir figure 3.2).

LU-équivalence

Plus récemment, la complémentation locale a émergé en tant qu'opération cruciale en théorie de l'information quantique. Le formalisme des états-graphes consiste à représenter des états quantiques à l'aide de graphes (voir [39] pour les détails). Ce formalisme puissant permet de représenter de façon graphique l'intrication quantique : chaque sommet représente un bit quantique (qubit) et chaque arête représente de façon intuitive l'intrication entre deux qubits.

Comme l'intrication est une propriété *non locale*, la puissance de l'intrication ne peut que diminuer en appliquant des opérations *locales* sur un état quantique. Par conséquent l'intrication est invariante par des opérations *localement réversibles*. Dans le domaine de la théorie de l'information quantique,

1. Elle a été utilisée par Bouchet [6] et d'autres sous le nom de *fonction de connectivité*, et formulée par Oum en temps que rang de coupe [54].

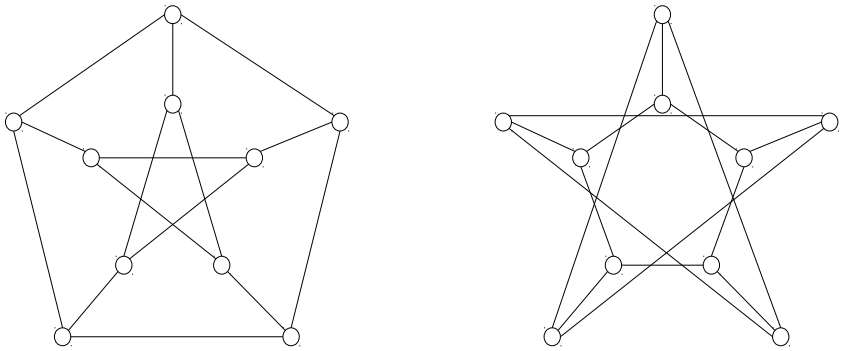


FIGURE 3.2 – Exemple de deux graphes de Petersen ayant le même rang de coupe mais n'étant pas LC-équivalents

deux états quantiques ont la même intrication si et seulement si ils sont LU-équivalents *i.e.*, s'il existe une série de transformations locales qui transforment un état en l'autre.

La LU-équivalence des états quantiques peut être définie pour les graphes de la façon suivante : deux graphes sont LU-équivalents si et seulement si leurs états correspondants sont LU-équivalents. Van den Nest [64] a prouvé que deux graphes LC-équivalents sont LU-équivalents. De plus Hein *et al.* [39] ont montré que deux graphes LU-équivalents ont le même rang de coupe. Ainsi la LU-équivalence est plus faible que la LC-équivalence mais plus forte que l'équivalence de rang de coupe (voir figure 3.3).

En utilisant le contre-exemple de Fon der Flaass's basé sur les graphes de Peteresen (voir 3.2), on peut trouver deux graphes avant le même rang de coupe mais n'étant pas LU-équivalents [31].

Il a été conjecturé que la LC- et la LU-équivalence coïncidaient [47]. En effet, LC- et LU-équivalence coïncident pour de nombreuses familles de graphes [63], cependant un contre-exemple de deux graphes d'ordre 27 LU-équivalents mais non LC-équivalents a été trouvé à l'aide d'une méthode assistée par ordinateurs [65].

Degré minimum par complémentation locale

Il s'agit ici de la notion clef de ce chapitre, le degré minimum par complémentation locale dont on va donner de nouvelles bornes et étudier la complexité paramétrée est défini de la façon suivante :

Définition 19. *Étant donné un graphe G, le* degré minimum par complémentation

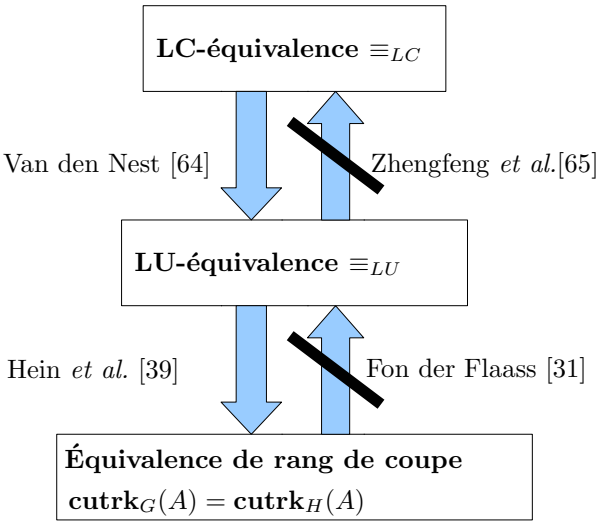


FIGURE 3.3 – Liens entre les différentes relations d'équivalence

locale *de* G *est*

$$\delta_{loc}(G) = \min_{H \equiv_{LC} G} \delta(H)$$

Le degré minimum par complémentation locale a été utilisé pour borner le ratio de certains codes quantiques obtenus par concaténation de graphes [2]. Cette quantité a aussi été utilisée pour caractériser la complexité de la préparation d'états-graphes [41] qui sont utilisés notamment dans le calcul quantique par mesure [58] (un modèle de calcul quantique très prometteur en terme d'implémentation physique), aussi bien qu'en calcul quantique aveugle [10] par exemple. Le degré minimum par complémentation locale est aussi utilisé pour borner le seuil qui peut être atteint par des protocoles de partage de secret quantique à base d'états-graphes [49, 34].

Le degré minimum par complémentation locale est relié à la fonction de rang de coupe ainsi qu'au plus petit ensemble de la forme $D \cup Odd_G(D)$:

Propriété 6. *(de [43]) Étant donné un graphe* $G = (V, E)$*,*

$$\delta_{loc}(G) + 1 = \min_{\emptyset \subset D \subseteq V} |D \cup Odd_G(D)| = \min\{|A| : A \subseteq V \wedge \mathrm{cutrk}_G(A) < |A|\}$$

La seconde équation donne une caractérisation du degré minimum par complémentation locale par la fonction de rang de coupe qui implique que deux graphes ayant la même fonction de rang de coupe ont le même degré minimum par complémentation

locale. Comme deux graphes LU-équivalents ont la même fonction de rang de coupe, ils ont aussi le même degré minimum par complémentation locale. Ainsi, le degré minimum par complémentation locale est invariant dans les trois classes d'équivalence basées sur la complémentation locale, les opérations unitaires locales et la fonction de rang de coupe.

Bornes supérieures sur le degré minimum par complémentation locale

Le degré minimum par complémentation locale a été étudié pour plusieurs familles de graphes : le degré minimum par complémentation locale de l'hypercube est au moins logarithmique dans l'ordre de l'hypercube [42] ; le degré minimum par complémentation locale d'un graphe de Paley $\mathcal{P}_n$ d'ordre n est au moins $\sqrt{n}$. Il n'y a pas de borne supérieure au degré minimum par complémentation locale des graphes de Paley, néanmoins on sait que tous les graphes de Paley n'ont pas un degré minimum par complémentation locale linéaire (i.e., $\delta_{loc}(\mathcal{P}_n) = \Theta(n)$) [43, 42].

Il n'existe pas de construction explicite donnant un degré minimum par complémentation locale supérieur à la racine carrée de l'ordre, cependant il a été prouvé *via* des méthodes probabilistes qu'il existe des graphes d'ordre n dont le degré minimum par complémentation locale est supérieur à $0.189n$ [43]. Il y a même des graphes bipartis dont le degré minimum par complémentation locale est linéaire : pour tout entier n il existe un graphe biparti d'ordre n et de degré minimum par complémentation locale au moins $0.110n$ [43].

Concernant les bornes supérieures, la propriété 6 implique que le degré minimum par complémentation locale est au plus la moitié de l'ordre du graphe, car aucun ensemble supérieur à la moitié des sommets ne peut avoir un rang de coupe complet.

Complexité du degré minimum par complémentation locale

Une motivation dans l'étude de la complexité du calcul du degré minimum par complémentation locale vient de la difficulté à trouver des graphes ayant un "grand" degré minimum par complémentation locale. En effet, on ne connait pas de construction explicite de graphes ayant un degré minimum par complémentation locale linéaire dans leur ordre, bien que des graphes aléatoires aient de "grands" degrés minimums par complémentation locale avec une forte probabilité. Donc pour produire des graphes avec un "grand" degré minimum par complémentation locale, on peut tirer un graphe aléatoire puis vérifier si son degré minimum par complémentation locale est suffisamment "grand". Cependant, calculer le degré minimum par complémentation local est difficile, même pour les graphes bipartis : le problème de décision associé est NP-complet et difficile à approximer (APX-complet) [43].

3.2 Bornes supérieures pour le degré minimum par complémentation locale

Pour améliorer les bornes existantes pour le degré minimum par complémentation locale, on utilisera la propriété suivante : dans tout graphe biparti $G = (V_1, V_2, E)$, il existe un sous-ensemble non-vide de sommets de V_1 qui domine de façon impaire au plus $\frac{|V_2|}{2(1-2^{-|V_1|})}$ sommets (dans V_2), donc de manière intuitive tant que V_1 n'est pas trop petit par rapport à V_2 il existe un sous-ensemble non-vide de V_1 qui domine au plus la moitié des sommets de V_2. Cette propriété est une conséquence directe de la borne appelée borne de Plotkin [56] sur les codes linéaires :

Lemme 9. *Pour tout graphe biparti $G = (V_1, V_2, E)$, il existe un sous-ensemble non-vide $D \subseteq V_1$ tel que*

$$|Odd_G(D)| \leq \frac{|V_2|}{2(1-2^{-|V_1|})}$$

Démonstration. $C := \{Odd_G(D) : D \subseteq V_1\}$ est un code linéaire de taille $n = |V_2|$ et de rang $k = |V_1|$, où $Odd_G(D)$ est identifié par son vecteur indicateur dans V_2. Selon la borne de Plotkin [56], la distance minimale d de C est au plus $n/(2(1-2^{-k}))$, donc il existe un sous-ensemble non-vide $D \subseteq V_1$ tel que $|Odd_G(D)| \leq |V_2|/(2(1-2^{-|V_1|}))$. □

On peut définir une borne supérieure pour le degré minimum par complémentation locale avec le transversal minimum (plus petit nombre de sommets tel que chaque arête en contienne au moins un) de la façon suivante :

Lemme 10. *Étant donné un graphe G d'ordre n et de nombre de couverture par sommets $\tau(G) > 0$,*

$$2\delta_{loc}(G) \leq \tau(G) + \log_2(\tau(G)) + 1$$

Démonstration. Soit $G = (V, E)$ un graphe d'ordre n, et soit S un ensemble stable de taille $\alpha = n - \tau(G)$, et $R \subseteq S$ un sous-ensemble de taille k que l'on fixera plus tard. Soit $G' = (R, (V \backslash S) \cup R, E')$ un graphe biparti tel que pour tout $u \in R$, $N_{G'}(u) = \{u\} \cup N_G(u)$. Il y a deux copies de R dans G', une de chaque part du graphe biparti : il y a un couplage entre chacune des deux copies de R, les autres arêtes de G' sont celles de G entre R et $V \setminus S$. D'après le lemme 9 il existe $D \subseteq R$ tel que :

$$|Odd_{G'}(D)| \leq \frac{|V| - |S| + |R|}{2(1-2^{-|R|})} = \frac{\tau(G) + k}{2(1-2^{-k})}$$

Le voisinage impair de D dans G' dépend de celui de D dans G de la façon suivante : $Odd_{G'}(D) = \Delta_{u \in D} N_{G'}(u) = \Delta_{u \in D}(\{u\} \cup N_G(u)) = D \Delta Odd_G(D)$, or comme $D \subseteq S$ et S est un stable, D est un stable dans G on a donc $D \Delta Odd_G(D) = D \cup Odd_G(D)$. Ainsi $|Odd_{G'}(D)| = |D \cup Odd_G(D)|$. On a donc, $\delta_{loc}(G) + 1 \leq \frac{\tau(G)+k}{2(1-2^{-k})}$.

– Si $\lceil \log_2(\tau(G)+1) \rceil \leq n - \tau(G)$, alors on pose $k = \lceil \log_2(\tau(G)+1) \rceil$:

$$\delta_{loc}(G)+1 \leq \frac{\tau(G) + \lceil \log_2(\tau(G)+1) \rceil}{2(1-2^{-\lceil \log_2(\tau(G)+1) \rceil})} < \frac{1}{2}(\tau(G)+\log_2(\tau(G)))+1 \quad (3.1)$$

Pour prouver la seconde partie de l'équation 3.1, soit $\tau(G) = 2^r + y$ avec $y < 2^r$. On a alors $\lceil \log_2(\tau(G)+1) \rceil = r+1$, ainsi

$$\delta_{loc}(G)+1 \quad \leq \quad \frac{2^r + y + r + 1}{2(1-2^{-r-1})}$$

De plus, on a par calcul standard que $\frac{2^r+y+r+1}{1-2^{-r-1}} < 2^r + y + \log_2(2^r+y) + 2$ quand $r > 0$. Ainsi $2\delta_{loc}(G) + 2 < \tau(G) + \log_2(\tau(G)) + 2$. Quand $r = 0$, $\tau(G) = 1$, G est une étoile (et potentiellement des sommets isolés), donc $2\delta_{loc}(G) \leq 2 = \tau(G) + \log_2(\tau(G)) + 1$.

– Si $\lceil \log_2(\tau(G)+1) \rceil > n - \tau(G)$, alors il est suffisant de prouver que $2\delta_{loc}(G) \leq n$ comme $\tau(G)+\log_2(\tau(G))+1 \geq \tau(G)+\lceil \log_2(\tau(G)+1) \rceil > n$. Pour tout ensemble $S \subseteq V$ de taille $\lfloor \frac{n}{2} \rfloor + 1$, $\text{cutrk}_G(S) < |S|$ car $|V \setminus S| < |S|$, ainsi selon la propriété 6,

$$\delta_{loc}(G) < \lfloor \frac{n}{2} \rfloor + 1 \leq n/2$$

□

Dans le lemme 10, la condition $\tau(G) > 0$ n'est utilisée que pour exclure le graphe stable et pour s'assurer de la bonne définition du logarithme. La borne est atteinte par les graphes étoiles : $\delta_{loc}(S_n) = 1$ et $\tau(S_n) = 1$. C'est l'unique cas où la borne est atteinte pour $\tau(G) > 1$, la preuve peut être modifiée pour pouvoir retirer le facteur constant : si $\tau(G) > 1$, $2\delta_{loc}(G) \leq \tau(G) + \log_2(\tau(G))$.

La borne sur le degré minimum par complémentation locale par le nombre de couverture par sommets amène une amélioration de la borne du degré minimum par complémentation locale pour le cas biparti :

Théorème 21. *Pour tout graphe biparti G d'ordre $n > 0$,*

$$\delta_{loc}(G) < \frac{n}{4} + \log_2 n$$

Démonstration. Si $n \leq 2$, la propriété est satisfaite. Sinon, comme G est biparti $\tau(G) \leq \lfloor \frac{n}{2} \rfloor$, donc d'après le lemme 9,

$$\delta_{loc}(G) \leq \frac{1}{2}(\tau(G)+\log_2(\tau(G))+1) \leq \frac{n}{4}+\frac{1}{2}\log_2(n/2)+\frac{1}{2} \leq \frac{n}{4}+\frac{1}{2}\log_2 n < \frac{n}{4}+\log_2 n$$

□

Contrairement au cas biparti, la borne utilisant le nombre de couverture par sommets n'implique pas d'amélioration pour la borne du degré minimum par complémentation locale dans le cas général. Cependant, on prouve que le degré minimum par complémentation locale d'un graphe d'ordre n est au plus $\frac{3}{8}n + o(n)$ en exploitant la structure des noyaux des applications linéaires associées aux coupes du graphe :

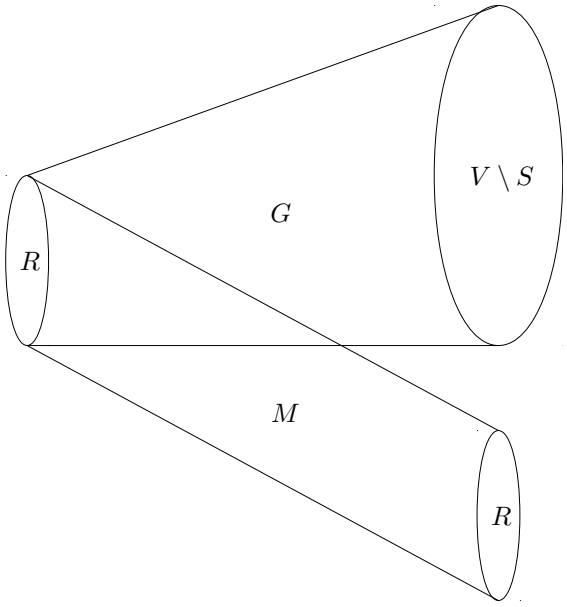


FIGURE 3.4 – Construction de la preuve du lemme 10

Théorème 22. *Pour tout graphe G d'ordre $n > 0$,*

$$\delta_{loc}(G) < \frac{3}{8}n + \log_2 n$$

Démonstration. Pour tout entier $0 < k < n/2$, soit S un sous-ensemble de $\lfloor n/2 \rfloor + k$ sommets de G. Soit $L : S \to V \setminus S$ l' application $D \mapsto Odd_G(D) \setminus S$ qui est linéaire pour la différence symétrique, i.e. $L(D_1 \Delta D_2) = L(D_1)\Delta L(D_2)$. On a pour tout $D \in Ker(L)$, $D \cup Odd(D) \subseteq S$. D'après le théorème du rang, $dim(Ker(L)) \geq 2k - 1$. Soit $R \subseteq S$ une base de $Ker(L)$. Soit $G' = (R, S \times \{1, 2, 3\}, E')$ (voir figure 3.5) un graphe biparti tel que pour tout $D \in R, N_{G'}(D) = D \times \{1\} \cup Odd_G(D) \times \{2\} \cup (Odd_G(D)\Delta D) \times \{3\}$: le voisinage de D dans G' est l'union disjointe de D, $Odd_G(D)$ et $D\Delta Odd_G(D)$. On a alors $|R| \geq 2k-1$ et $|S \times \{1, 2, 3\}| = 3(\lfloor n/2 \rfloor + k)$, donc d'après le lemme 3.2, il existe un sous-ensemble $R_0 \subseteq R$ tel que $|Odd_{G'}(R_0)| \leq \left\lfloor \frac{3}{2} . \frac{\lfloor n/2 \rfloor + k}{1 - 2^{-2k+1}} \right\rfloor$.

Soit $F := \Delta_{D \in R_0} D$. Comme R est une base de $R_0 \neq \emptyset$, $F \neq \emptyset$. De plus $Odd_{G'}(R_0) = \Delta_{D \in R_0} N_{G'}(D) = \Delta_{D \in R_0}(D \times \{1\} \cup Odd_G(D) \times \{2\} \cup (Odd_G(D)\Delta D) \times \{3\}) = F \times \{1\} \cup Odd_G(F) \times \{2\} \cup (F\Delta Odd_G(F)) \times \{3\}$. Ainsi $|Odd_{G'}(R_0)| = |F| + |Odd_G(F)| + |F\Delta Odd_(F)| = 2|F \cup Odd_G(F)|$. On a

donc,

$$|F \cup Odd_G(F)| \quad \leq \quad \left\lfloor \frac{1}{2} \left\lfloor \frac{3}{2} . \frac{\lfloor n/2 \rfloor + k}{1 - 2^{1-2k}} \right\rfloor \right\rfloor$$

On choisi $k{=}\lfloor 4 \log_2(n)/3 \rfloor$ pour garantir $|F \cup Odd_G(F)| \leq \frac{3}{8}n + \log_2(n) + O(1)$. Plus précisément, on a

$$|F \cup Odd_G(F)| \leq \frac{3}{8} . \frac{n + 2\lfloor 4 \log_2(n)/3 \rfloor}{1 - 2 \times 2^{-2\lfloor 4 \log_2(n)/3 \rfloor}} \leq \frac{3}{8} . \frac{n + 8 \log_2(n)/3}{1 - 8.n^{-8/3}}$$

qui est strictement plus petit que $\frac{3}{8}n + \log_2 n + 1$ quand $n > 60$. Pour $2 < n \leq 61$, on peut vérifier que la borne de l'équation 3.2 est en fait strictement plus petite que $\frac{3}{8}n + \log_2(n) + 1$. Ainsi pour tout $n > 2$, $\min_{D \neq \emptyset} |D \cup Odd_G(D)| < \frac{3}{8}n + \log_2 n + 1$, donc $\delta_{loc}(G) < \frac{3}{8}n + \log_2 n$. Finalement on peut vérifier aisément que $\delta_{loc}(G) < \frac{3}{8}n + \log_2 n$ est aussi vrai pour $n \leq 2$. □

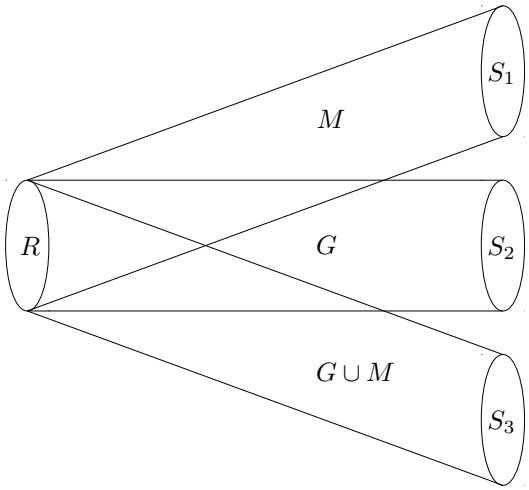


FIGURE 3.5 – Construction de la preuve du théorème 22

Choisir $k = \lfloor \log_2(n)/2 \rfloor$ dans la preuve du théorème 22 donne une borne asymptotiquement meilleure :

$$\delta_{loc}(G) \leq 3/8n + 3/4 \log_2(n) + O(1)$$

.

3.3 Complexité paramétrée

Le problème de décision associé au degré minimum par complémentation locale est NP-complet et dur à approximer : il n'existe pas d'algorithme de k-approximation en temps polynomial pour ce problème pour toute constante k sous l'hypothèse $P \neq NP$ [43]. Dans cette section on va donc considérer la complexité paramétrée de ce problème ainsi que sa restriction aux graphes bipartis. La définition du problème paramétré est la suivante :

Degré minimum par complémentation locale
Entrée : un graphe G, un entier k.
paramètre : k.
question : $\delta_{loc}(G) \leq k$?

Degré minimum par complémentation locale biparti
Entrée : un graphe biparti G, un entier k.
paramètre : k.
question : $\delta_{loc}(G) \leq k$?

Ici on va monter l'équivalence de ce problème même restreint au cas biparti avec le problème classique Ensemble pair dont l'appartenance à $W[2]$ à été montrée dans [33] mais qui n'est difficile ni pour $W[1]$ ni pour $W[2]$.
Ensemble pair
Entrée : un graphe biparti $G = (R, B, E)$, un entier k.
paramètre : k.
question : Existe-t-il un sous-ensemble de sommets $D \subseteq R$ non vide, tel que $|D| \leq k$ et $Even_G(D) = B$, *i.e.* chaque sommet de B a un nombre pair de voisins dans D ?

La démonstration de cette équivalence se fait en deux temps, d'abord on prouve que Ensemble pair est plus difficile que Degré minimum par complémentation locale, et ensuite que Degré minimum par complémentation locale biparti est plus difficile que Ensemble pair, Degré minimum par complémentation locale biparti étant la restriction aux graphes bipartis de Degré minimum par complémentation locale ce dernier est plus difficile on obtient donc bien une boucle d'équivalence.

Théorème 23. Ensemble pair *est plus difficile que* Degré minimum par complémentation locale *par* FPT*-réduction.*

Démonstration. Étant donné (G, k) une instance de Degré minimum par complémentation locale, soit (G', k') une instance de Ensemble pair (voir figure 3.6) avec :

$G' = (A_1 \cup A_2, \cup A_3, A_4 \cup A_5, E_1 \cup E_2 \cup E_3)$, $k' = 2k+2$

$\forall i \in [1, 5], A_i = \{a_{i,u}, \forall u \in V(G)\}$

$E_1 = \{(a_{1,u}, a_{4,u}), \forall u \in V(G)\}$,

$E_2 = \{(a_{i,u}, a_{5,u}), \forall i \in \{2,3\}, \forall u \in V(G)\}$

$E_3 = \{(a_{2,u}, a_{i,v}), \forall i \in \{4,5\}, \forall \{u,v\} \in E(G)\}$

G' est donc constitué de cinq copies A_is de $V(G)$ et il y a un couplage entre A_1 et A_4, et entre A_3 et A_5. De plus, le sous-graphe induit par $A_2 \cup A_4$ est le double biparti de G (i.e. un graphe biparti constitué de deux copies de G dont les arêtes correspondent à celles de G), tandis que $A_2 \cup A_5$ est le double biparti de G augmenté d'un couplage. On a bien G' biparti chacun des A_i étant un stable.

- Si (G,k) est une instance positive de Degré minimum par complémentation locale il existe un sous ensemble de sommets $D \subseteq V(G)$ tel que $D \neq \emptyset$ et $|D \cup Odd_G(D)| \leq k+1$. Soit $D' = \{a_{1,u} \mid u \in Odd_G(D)\} \cup \{a_{2,u} \mid u \in D\} \cup \{a_{3,u} \mid u \in Odd_G(D)\Delta D\}$, D' est donc composé de la copie de D dans A_2, de la copie de $Odd_G(D)$ dans A_1 et de celle de $D\Delta Odd_G(D)$ dans A_3. Rappelons que $Odd_{G'}(D') = \emptyset$, et $D' \neq \emptyset$ comme $D \neq \emptyset$. De plus $|D'| = |Odd_G(D)| + |D| + |D\Delta Odd_G(D)| = 2|D \cup Odd_G(D)| \leq 2k+2 = k'$. Donc D' fait de (G', k') une instance positive de Ensemble pair.

- Si (G', k') est une instance positive de Ensemble pair il existe $D \subseteq A_1 \cup A_2 \cup A_3$ tel que $|D| \leq k'$ et $Odd_{G'}(D) = \emptyset$. Pour $i \in [1,3]$, soit $D_i = \{u \in V(G) \mid a_{i,u} \in D\}$. Rappelons que $D_1 = Odd_G(D_2)$ et $D_3 = Odd_G(D_2)\Delta D_2$. $D \neq \emptyset$ implique que $D_2 \neq \emptyset$, de plus $|D_2 \cup Odd_G(D_2)| = \frac{1}{2}(|D_2| + |Odd_G(D_2)| + |Odd_G(D_2)\Delta D_2|) = \frac{1}{2}|D| \leq \frac{1}{2}k' = k+1$, donc D_2 fait de (G,k) une instance positive de Degré minimum par complémentation locale.

□

Corollaire 9. Degré minimum par complémentation locale *appartient à* $W[2]$.

L'appartenance à $W[2]$ de Degré minimum par complémentation locale car non seulement Ensemble pair mais aussi tous les problèmes de domination avec des notions de parité appartiennent à $W[2]$ [11]. On affine cette appartenance à $W[2]$ en prouvant l'équivalence de Degré minimum par complémentation locale et Degré minimum par complémentation locale biparti à Ensemble pair. Ces problèmes constituent une sous-classe de $W[2]$ particulière car l'absence de résultat de difficulté pour Ensemble pair est un problème qui reste ouvert depuis longtemps en complexité paramétré [26]. Cet état de fait contraste avec la classe des problèmes équivalents à Ensemble impair qui appartiennent aussi à $W[2]$ mais qui en plus sont difficiles pour $W[1]$ [11], cette classe contenant d'autres problèmes liés aux états-graphes comme Plus grand ensemble WOD et Seuil quantique[11].

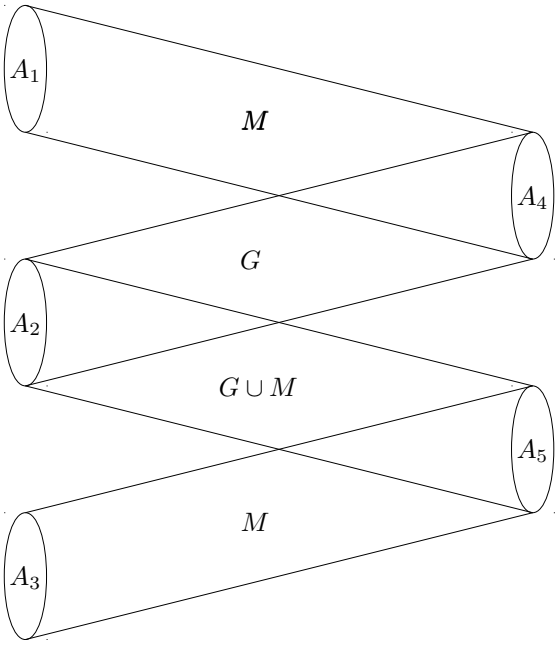


FIGURE 3.6 – Réduction de ENSEMBLE PAIR à DEGRÉ MINIMUM PAR COMPLÉMENTATION LOCALE

Théorème 24. DEGRÉ MINIMUM PAR COMPLÉMENTATION LOCALE BIPARTI *est plus difficile que* ENSEMBLE PAIR *par une FPT-réduction.*

Démonstration. Si $(G = (R, B, E), k)$ est une instance positive de ENSEMBLE PAIR, alors il existe $D \subseteq R$ tel que $0 < |D| \leq k$ et $Odd_G(D) = \varnothing$, donc $0 < |D \cup Odd_G(D)| \leq k$ ce qui implique que (G, k) est aussi une instance positive de DEGRÉ MINIMUM PAR COMPLÉMENTATION LOCALE BIPARTI.

Si (G, k) est une instance positive de DEGRÉ MINIMUM PAR COMPLÉMENTATION LOCALE BIPARTI, en revanche il peut y avoir deux raisons pour lesquelles (G, k) ne soit pas une instance positive de ENSEMBLE PAIR :

- L'ensemble D tel que $0 < |D \cup Odd_G(D)| \leq k$ peut ne pas être inclus dans R.
- Pour résoudre ENSEMBLE PAIR, on veut $Odd_G(D) = \emptyset$.

Concernant le premier point, un gadget biparti ayant un degré minimum par complémentation locale de $k+1$ est attaché à chaque sommet de B pour garantir qu'aucun sommet de B ne peut apparaitre dans D en respectant $|D \cup Odd(D)| \leq k$. Ce gadget est un graphe de Paley P_q dont les sommets sont $\{0, \ldots, q-1\}$ pour $q = 1 \bmod 4$ une puissance de premier, et (i, j) est une arête si et seulement

si $\exists x, i - j = x^2 \bmod q$. Le degré minimum par complémentation locale d'un graphe de Paley est au moins la racine carrée de son ordre. Cependant pour conserver la bipartition du graphe on va utiliser son double biparti. En effet, il est prouvé dans [42] que le degré minimum par complémentation locale d'un double biparti est le même que celui du graphe original ($\delta_{loc}(G^{\oplus 2}) \geq \delta_{loc}(G)$).

Pour le deuxième point, chaque sommet de B est dupliqué k fois de telle façon à ce que pour tout $D \subseteq R$ si un sommet $v \in B$ est dans le voisinage impaire de D alors ses k copies sont aussi dans le voisinage impair ce qui contredit la condition $|D \cup Odd(D)| \leq k$.

Ceci nous donne la construction suivante, soit q un nombre premier tel que $q \geq k^2 + 1$ et $q = 1 \bmod 4$ d'après la version modulaire du postulat de Bertrand [21] un tel q est inférieur à $2k^2+1$, soit (G', k) une instance de Degré minimum par complémentation locale biparti (voir figure 3.7) tel que :

$G' = (R \cup P', P, E_G \cup E_{\text{Paley}})$, avec

$P = \cup_{b \in B, i \in [0,k]} P_{b,i}$

$P' = \cup_{b \in B, i \in [0,k]} P'_{b,i}$

$P_{b,i} = \{p_{b,i,r}, \forall r \in [0, q-1]\}$

$P'_{b,i} = \{p'_{b,i,r}, \forall r \in [0, q-1]\}$

$E_{\text{Paley}} = \cup_{b \in B, i \in [0,k]} E^{(b,i)}_{\text{Paley}}$

$E^{(b,i)}_{\text{Paley}} = \{(p_{b,i,r}, p'_{b,i,r'}), \forall r, r' \in [0,q-1] \ s.t. \ \exists \ell \in [0, q-1], \ell^2 = r - r' \bmod q\}$

- Si (G, k) est une instance positive de Ensemble pair avec $D \subseteq E$ tel que $Odd_G(D) = \emptyset$, alors $Odd_{G'}(D) = \emptyset$ donc (G', k) est une instance positive de Degré minimum par complémentation locale biparti.
- Si (G', k) est une instance positive de Degré minimum par complémentation locale biparti avec D tel que $|D \cup Odd_{G'}(D)| \leq k$. pour tout $b \in B, i \in [0, k]$, soit $D'_{b,i} = D \cap (P_{b,i} \cup P'_{b,i})$, dans le sous-graphe induit par $P_{b,i} \cup P'_{b,i}$, $|D' \cup Odd_{G'[P_{b,i} \cup P'_{b,i}]}(D)| \leq k$, ainsi $D'_{n,i} = \emptyset$ comme $\delta_{loc}(\text{Paley}_{k^2+1}) > k$. Donc $D \subseteq R$. de plus s'il existe $p_{b,i,0} \in Odd_{G'}(D)$ alors $\forall j \in [0, k], p_{b,j,0} \in Odd_{G'}(D)$, alors $|D \cup Odd_{G'}(D)| > k+1$, donc par contradiction $Odd_{G'}(D) = \emptyset$. Ainsi (G, k) est une instance positive de Ensemble pair.

□

Corollaire 10. Degré minimum par complémentation locale *et* Degré minimum par complémentation locale biparti *sont FPT-équivalent à* Ensemble pair.

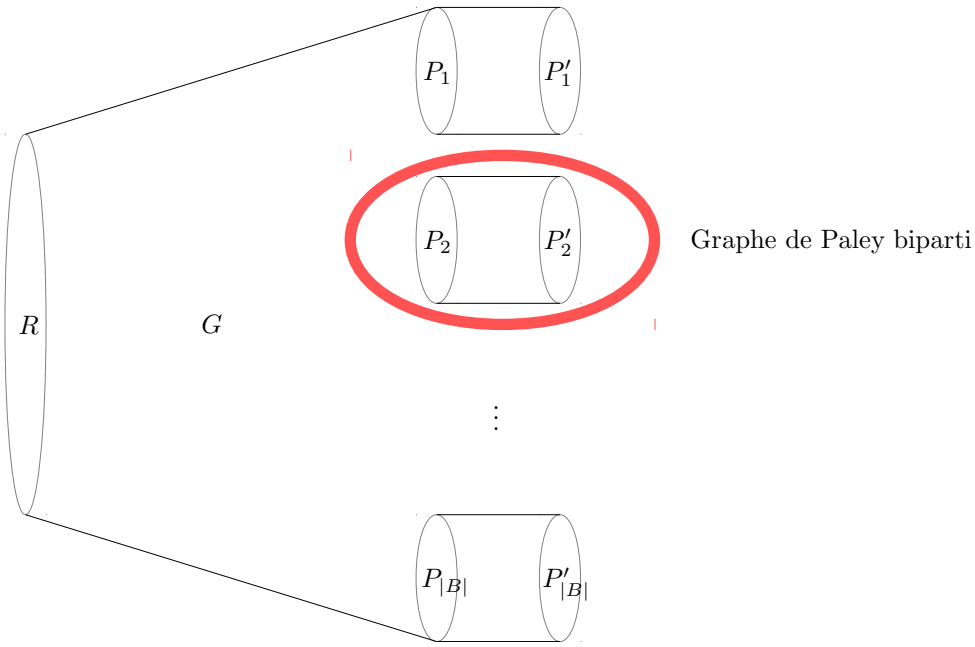


FIGURE 3.7 – Réduction de DEGRÉ MINIMUM PAR COMPLÉMENTATION LOCALE BIPARTI à ENSEMBLE PAIR

La difficulté pour $W[1]$ de ENSEMBLE PAIR reste un problème ouvert depuis longtemps en complexité paramétrée, la FPT-équivalence avec DEGRÉ MINIMUM PAR COMPLÉMENTATION LOCALE peut donner de nouvelles perspectives concernant la complexité paramétré de ce problème.

3.4 Algorithmes Exponentiels

Dans cette section, on présente un algorithme exact en temps exponentiel pour le calcul du degré minimum par complémentation locale en utilisant les bornes obtenues dans la section 3.2, et ensuite on raffine cet algorithme dans le cas des graphes bipartis.

Propriété 7. *Le degré minimum par complémentation locale d'un graphe d'ordre n peut être calculé en temps $\mathcal{O}^*(1.938^n)$.*

Démonstration. Avec la propriété 6 et le théorème 22 on obtient, $\delta_{loc}(G)+1 = \min\{|A| : |A| \leq \frac{3}{8}n + \log_2(n) \wedge \text{cutrk}_G(A) < |A|\}$. L'algorithme consiste à énumérer tous les sous-ensemble de sommets de taille au plus $\frac{3}{8}n+\log_2(n)$ et calculer leur rang de coupe. Le rang de coupe pouvant être calculé en temps

polynomial, la complexité de cet algorithme est donc $\mathcal{O}^*(2^{H(\frac{3}{8})n})$ où $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ est la fonction binaire d'entropie. □

Pour le cas biparti, énumérer tous les sous-ensembles de taille $\frac{n}{4} + \log_2(n)$ amène à un algorithme de complexité $\mathcal{O}^*(1.755^n)$. Cet algorithme naïf peut amélioré en :

Théorème 25. *Le degré minimum par complémentation locale d'un graphe biparti d'ordre n peut être calculé en temps* $\mathcal{O}^*(1.466^n)$.

Démonstration. On utilise la propriété suivante des graphes bipartis : étant donné un graphe biparti $G = (V_1, V_2, E)$, $\delta_{loc}(G)+1 = \min_{\emptyset \subset D \subseteq V_1 \text{ or } \emptyset \subset D \subseteq V_2} |D \cup Odd_G(D)|$. En effet, pour tout $D \subseteq V_1 \cup V_2$, $(D \cap V_1) \cup Odd_G(D \cap V_1)$ et $(D \cap V_2) \cup Odd_G(D \cap V_2)$ sont des sous-ensembles de $D \cup Odd_G(D)$. Soit $|V_1| = \alpha n$ et $|V_2| = (1-\alpha)n$. On pose sans perte de généralité $\alpha \leq 1/2$. Comme V_1 est un ensemble de couverture par sommets, le lemme 10 nous donne $\delta_{loc}(G) \leq \frac{\alpha}{2}n + \frac{\log_2(\alpha n)}{2}$. Ainsi pour calculer le degré minimum par complémentation locale, il suffit d'énumérer tous les sous-ensembles D de taille au plus $\frac{\alpha}{2}n + \frac{\log_2(\alpha n)}{2}$ dans V_1 et V_2 et de calculer leur voisinage impair, qui se fait en temps polynomial en n. Il y a $\binom{\alpha n}{\frac{\alpha}{2}n + \frac{\log_2(\alpha n)}{2}} + \binom{(1-\alpha)n}{\frac{\alpha}{2}n + \frac{\log_2(\alpha n)}{2}} = \mathcal{O}^*(2^{(1-\alpha)nH(\frac{\alpha}{2(1-\alpha)})})$ sous-ensembles à énumérer. La fonction $\alpha \mapsto (1-\alpha)H(\frac{\alpha}{2(1-\alpha)})$ est maximale pour $\alpha_0 = 0.3885$, et $2^{(1-\alpha_0)H(\frac{\alpha_0}{2(1-\alpha_0)})} = 1.46557$. □

3.5 Conclusion et perspectives

Le travail sur la borne supérieure avec pour base la borne de Plotkin [56], a permis de montrer une majoration du degré minimum par complémentation locale par une fonction du nombre de couverture par sommets (lemme 10). Partant de ce résultat, la borne $\delta_{loc}(G) < \frac{n}{4} + \log_2 n$ (théorème 21) a pu être établi pour les graphes bipartis et étendu à $\delta_{loc}(G) < \frac{3}{8}n + \log_2 n$ (théorème 22) dans le cas général.

En ce qui concerne le travail sur la complexité paramétrée, on a pu établir que le problème de détermination du degré minimum par complémentation locale paramétré par la taille du résultat appartenait à $W[2]$ mais aussi sa FPT-équivalence avec Ensemble pair par deux $FPT-$réductions de l'un à l'autre. En revanche, ce dernier problème n'étant pas montré difficile pour une classe $W[i]$, un résultat de difficulté pour le degré minimum par complémentation locale n'a pu être établi.

Le problème de détermination du degré minimum par complémentation locale étant NP-complet, les bornes établies précédemment ont permis l'élaboration d'algorithmes exacts en temps exponentiels : en temps $\mathcal{O}^*(1.938^n)$ dans le cas général et raffiné à $\mathcal{O}^*(1.466^n)$ dans le cas biparti.

3.5.1 Bornes

Il n'existe pas de construction explicite donnant un degré minimum par complémentation locale supérieur à la racine carrée de l'ordre, cependant il a été prouvé *via* des méthodes probabilistes qu'il existe des graphes d'ordre n dont le degré minimum par complémentation locale est supérieur à $0.189n$ [43]. Il reste donc un écart assez important avec la borne $\delta_{loc}(G) < \frac{3}{8}n + \log_2 n$ du théorème 22.

De plus, la construction de graphes ayant un grand degré minimum par complémentation locale est difficile. Instinctivement on se heurte au problème suivant : construire un graphe à grand degré minimum (linéaire) tels que les voisinages communs de chaque paire de sommets ne soient pas trop grands.

3.5.2 Complexité paramétrée

En ce qui concerne la complexité paramétrée, il est important de noter que si un résultat de difficulté pour une classe $W[i]$ n'a pu être obtenue pour Degré minimum par complémentation locale son appartenance à $W[2]$ et plus particulièrement sa FPT-équivalence à Ensemble pair restent très intéressantes. En effet, ce dernier est un problème classique de complexité paramétré resté ouvert et est un bon candidat à l'appartenance d'une possible classe intermédiaire dans la hiérarchie W équivalentes de la classe NP-intermédiaire de Ladner [48].

De plus, on peut noter que cette FPT-équivalence constitue un pont entre la domination paire (Ensemble pair) et la domination impaire (Degré minimum par complémentation locale) et peut donc servir de piste pour la réflexion sur les liens existants entre les deux, sachant que leur FPT-équivalence ou leur différence reste un problème ouvert.

3.5.3 Algorithmes exponentiels

Pour les algorithmes exponentiels, bien que ceux-ci soient des applications des nouvelles bornes montrés dans la section 3.2, ils permettent néanmoins d'étendre le calcul du degré minimum par complémentation locale à des graphes de taille plus importante, sachant que les principales applications quantiques de celui-ci s'effectuent pour l'instant sur des systèmes de tailles limités.

Remerciments

Je remercie mes maîtres de thèse Pablo Arrighi et Simon Perdrix ainsi que Mehdi Mhalla pour m'avoir guidé tout au long de ma thèse. Je remercie aussi les rapporteurs Mathieu Liedloff et Paul Dorbec pour leurs conseils sur le manuscrit. Je tiens aussi à remercier Laurent Besacier, Christian Boitet et Rachid Echahed qui m'ont apporté aide et soutien durant ma thèse. Enfin je remercie Spin et Anne-So pour avoir relu ma thèse ainsi que mes parents pour leur soutien. Sans oublier Diane pour tout le soutien et le réconfort qu'elle m'a apporté toutes ces années.

Bibliographie

[1] Salman Beigi, Isaac Chuang, Markus Grassl, Peter Shor, and Bei Zeng. Graph concatenation for quantum codes. *Journal of Mathematical Physics*, 52(2), 2011.

[2] Salman Beigi, Isaac Chuang, Markus Grassl, Peter Shor, and Bei Zeng. Graph concatenation for quantum codes. *Journal of Mathematical Physics*, 52(2) :022201, 2011.

[3] Charles H. Bennett. Quantum cryptography : Public key distribution and coin tossing. In *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984.

[4] George Robert Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference1979*, 48 :313–317, 1979.

[5] Hans L. Bodlaender and Dieter Kratsch. A note on fixed parameter intractability of some domination-related problems. Unpublished.

[6] André Bouchet. Graphic presentations of isotropic systems. *Journal of Combinatorial Theory, Series B*, 45(1) :58–76, 1988.

[7] André Bouchet. Connectivity of isotropic systems. *Annals of the New York Academy of Sciences*, 555(1) :81–93, 1989.

[8] André Bouchet. κ-transformations, local complementations and switching. In *Cycles and Rays*, pages 41–50. Springer, 1990.

[9] André Bouchet. Circle graph obstructions. *Journal of Combinatorial Theory, Series B*, 60(1) :107–144, 1994.

[10] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

[11] David Cattanéo and Simon Perdrix. Parameterized complexity of weak odd domination problems. In *International Symposium on Fundamentals of Computation Theory*, pages 107–120. Springer, 2013.

[12] David Cattanéo and Simon Perdrix. The parameterized complexity of domination-type problems and application to linear codes. In *Theory and Applications of Models of Computation - 11th Annual Conference, TAMC 2014, Chennai, India, April 11-13, 2014. Proceedings*, pages 86–103, 2014.

[13] David Cattanéo and Simon Perdrix. Minimum degree up to local complementation : Bounds, parameterized complexity, and exact algorithms. In *International Symposium on Algorithms and Computation*, pages 259–270. Springer, 2015.

[14] M. Cesati. Perfect Code is W[1]-complete. *Inf. Proc. Let.*, 81 :163–168, 2002.

[15] M. Cesati. The Turing way to parameterized complexity. *Journal of Computer and System Sciences*, 67 :654–685, 2003.

[16] Marco Cesati. Compendium of parameterized problems. *Department of Computer Science, Systems, and Industrial Engineering, University of Rome Tor Vergata*, 22, 2006.

[17] M. Chapelle. Parameterized Complexity of Generalized Domination Problems on Bounded Tree-Width Graphs. *Computing Research Repository*, abs/1004.2, 2010.

[18] James Cheetham, Frank Dehne, Andrew Rau-Chaplin, Ulrike Stege, and Peter J Taillon. Solving large fpt problems on coarse-grained parallel machines. *Journal of Computer and System Sciences*, 67(4) :691–706, 2003.

[19] Jianer Chen, Iyad A Kanj, and Weijia Jia. Vertex cover : further observations and further improvements. *Journal of Algorithms*, 41(2) :280–301, 2001.

[20] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Physical Review Letters*, 83(3) :648, 1999.

[21] John Cullinan and Farshid Hajir. Primes of prescribed congruence class in short intervals. *Integers*, 12 :A56, 2012.

[22] Hubert De Fraysseix. Local complementation and interlacement graphs. *Discrete Mathematics*, 33(1) :29–35, 1981.

[23] Rod G Downey and Michael R Fellows. *Fixed-parameter tractability and completeness III : Some structural aspects of the W hierarchy*, pages 191–225. Cambridge University Press, 1993.

[24] Rod G. Downey and Michael R. Fellows. Fixed-Parameter Tractability and Completeness I : Basic Results. *SIAM Journal on Computing*, 24 :873–921, 1995.

[25] Rod G Downey and Michael R Fellows. Fixed-parameter tractability and completeness ii : On completeness for w [1]. *Theoretical Computer Science*, 141(1) :109–131, 1995.

[26] Rod G Downey, Michael R Fellows, Alexander Vardy, and Geoff Whittle. The parametrized complexity of some fundamental problems in coding theory. *SIAM Journal on Computing*, 29(2) :545–570, 1999.

[27] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6) :661, 1991.

[28] Michael R. Fellows. *Parameterized Complexity : The Main Ideas and Some Research Frontiers*, pages 291–307. Springer Berlin Heidelberg, Berlin, Heidelberg, 2001.

[29] Michael R Fellows. Blow-ups, win/win's, and crown rules : Some new directions in fpt. In *International Workshop on Graph-Theoretic Concepts in Computer Science*, pages 1–12. Springer, 2003.

[30] Michael R. Fellows and Michael A. Langston. Nonconstructive advances in polynomial-time complexity. *Information Processing Letters*, 26(3) :157 – 162, 1987.

[31] DG Fon-Der-Flaass. Local complementations of simple and directed graphs. In *Discrete analysis and operations research*, pages 15–34. Springer, 1996.

[32] Giulia Galbiati, Francesco Maffioli, and Angelo Morzenti. A short note on the approximability of the maximum leaves spanning tree problem. *Information Processing Letters*, 52(1) :45–49, 1994.

[33] Petr A. Golovach, Jan Kratochvìl, and Ondrej Suchỳ. Parameterized complexity of generalized domination problems. *Discrete Applied Mathematics*, 160(6) :780–792, 2009.

[34] Sylvain Gravier, Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. Quantum secret sharing with graph states. In *International Doctoral Workshop on Mathematical and Engineering Methods in Computer Science*, pages 15–31. Springer, 2012.

[35] Sylvain Gravier, Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. On weak odd domination and graph-based quantum secret sharing. *Theoretical Computer Science*, 598 :129–137, 2015.

[36] Lov K Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical review letters*, 79(2) :325, 1997.

[37] Gregory Gutin, Ton Kloks, Chuan Min Lee, and Anders Yeo. Kernels in planar digraphs. *Journal of Computer and System Sciences*, 71(2) :174–184, 2005.

[38] M. Hein, J. Eisert, and H. J. Briegel. Multiparty entanglement in graph states. *Phys. Rev. A*, 69 :062311, Jun 2004.

[39] Marc Hein, Jens Eisert, and Hans J Briegel. Multiparty entanglement in graph states. *Physical Review A*, 69(6) :062311, 2004.

[40] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Physical Review A*, 59(3) :1829, 1999.

[41] Peter Høyer, Mehdi Mhalla, and Simon Perdrix. Resources required for preparing graph states. In *International Symposium on Algorithms and Computation*, pages 638–649. Springer, 2006.

[42] Jérôme Javelle. *Cryptographie Quantique : Protocoles et Graphes*. PhD thesis, Université Grenoble Alpes, 2014.

[43] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. *On the Minimum Degree Up to Local Complementation : Bounds and Complexity*, pages 138–147. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[44] Zhengfeng Ji, Jianxin Chen, Zhaohui Wei, and Mingsheng Ying. The lu-lc conjecture is false. *arXiv preprint arXiv :0709.1266*, 2007.

[45] T. Kloks and L. Cai. Parameterized tractability of some (efficient) y-domination variants for planar graphs and t-degenerate graphs. *International Computer Symposium (ICS)*, 2000.

[46] Anton Kotzig. Eulerian lines in finite 4-valent graphs and their transformations. *Journal of the ACM (JACM)*, pages 219–230, 1968.

[47] O Krueger and RF Werner. Some open problems in quantum information theory. *arXiv preprint quant-ph/0504166*, 2005.

[48] Richard E Ladner. On the structure of polynomial time reducibility. *Journal of the ACM (JACM)*, 22(1) :155–171, 1975.

[49] Damian Markham and Barry C Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78(4) :042309, 2008.

[50] H. Moser and D. M. Thilikos. Parameterized complexity of finding regular induced subgraphs. *Journal of Discrete Algorithms*, 7 :181–190, 2009.

[51] Hannes Moser and Dimitrios M. Thilikos. Parameterized complexity of finding regular induced subgraphs. *Journal of Discrete Algorithms*, 7(2) :181 – 190, 2009. Selected papers from the 2nd Algorithms and Complexity in Durham Workshop {ACiD} 2006.

[52] Rolf Niedermeier. Invitation to fixed-parameter algorithms, 2006.

[53] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[54] Sang-Il Oum. Approximating rank-width and clique-width quickly. *ACM Transactions on Algorithms (TALG)*, 5(1) :10, 2008.

[55] Christos Papadimitriou and Mihalis Yannakakis. Optimization, approximation, and complexity classes. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 229–234. ACM, 1988.

[56] Morris Plotkin. Binary codes with specified minimum distance. *IRE Transactions on Information Theory*, 6(4) :445–450, 1960.

[57] Prabhakar Raghavan. Probabilistic construction of deterministic algorithms : approximating packing integer programs. *Journal of Computer and System Sciences*, 37(2) :130–143, 1988.

[58] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22) :5188, 2001.

[59] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11) :612–613, 1979.

[60] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2) :303–332, 1999.

[61] J. A. Telle and A. Proskurowski. Algorithms for Vertex Partitioning Problems on Partial k-Trees. *SIAM Journal on Discrete Mathematics*, 10 :529–550, 1997.

[62] Jan Arne Telle. Complexity of domination-type problems in graphs. *Nordic J. of Computing*, 1(1) :157–171, March 1994.

[63] Maarten Van den Nest. Local equivalence of stabilizer states and codes. *PhD thesis*, 2005.

[64] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. Graphical description of the action of local clifford transformations on graph states. *Physical Review A*, 69(2) :022316, 2004.

[65] Bei Zeng, Hyeyoun Chung, Andrew W Cross, and Isaac L Chuang. Local unitary versus local clifford equivalence of stabilizer and graph states. *Physical Review A*, 75(3) :032325, 2007.