Rapport de stage de M2: algorithmes holographiques

Yann Strozecki

Maître de stage : Arnaud Durand

19 mars 2008

Table des matières

Introduction

Dans ce mémoire j'étudie les algorithmes holographiques ou accidentels de L.Valiant. Ils tirent leur nom du fait que l'on peut réduire une somme exponentielle à un calcul polynômial grâce à des interférences entre les termes de cette somme. Cette nouvelle technique permet de construire des algorithmes polynômiaux pour des problèmes ressemblant fortement à des problèmes $\sharp P$-complets tels que $\sharp$ SAT ou $\sharp$ Couplage. Pour cela on utilise un cadre algébrique élégant et une réduction vers le problème de comptage des couplages parfaits dans un graphe planaire, qu'on sait être dans FP depuis Kasteleyn [4].

Dans une première partie je décris les problèmes cibles de la réduction, c'est à dire les polynômes de graphe PerfMatch et Pfaff et j'étudie la complexité de leur évaluation. Je présente ensuite la théorie générale et plusieurs exemples significatifs en simplifiant certaines démonstrations et en utilisant un cadre unifié. Ces exemples mettent en évidence de nouvelles frontières entre facilement et difficilement calculable, par exemple le problème $\sharp$Pl-Rtw-Mon-3CNF est dur modulo 2 et facile modulo 7.

Cette technique peut ensuite être adaptée à la réduction vers d'autres problèmes cibles comme la parité du nombre de couplages parfaits d'un graphe biparti. J'expose à la fin du rapport pourquoi cette démarche a échoué jusqu'à maintenant et les pistes pour élargir la classe des problèmes traitables par algorithme holographique.

Je tiens à remercier Arnaud Durand pour son aide, la qualité de ses conseils et de ses corrections au présent rapport.

Chapitre 1

Préliminaires algébriques : les polynômes de graphe

Dans cette partie on décrit un certain nombre de polynôme de graphes qui sous certaines conditions, notamment la planarité du graphe, s'évaluent facilement. Ils sont tous en lien avec le nombre de couplages dans un graphe. Les démonstrations proviennent pour le Permanent du premier chapitre du livre de Jerrum [3] et pour le Pfaffien sont inspirés du livre de théorie des matrices de Brualdi et Ryser [5] et de mes propres réflexions.

1.1 Définitions

Définition 1 (Matrice antisymétrique d'adjacence)**.** Soit un graphe pondéré G ayant des sommets numérotés de 1 à n, on définit la matrice antisymétrique d'adjacence $A_S(\overrightarrow{G}) = (a_{i,j})_{1 \leq i,j \leq n}$ par

$$a_{ij} = \begin{cases} w(i,j), \text{ si (i,j)} \in E(\overrightarrow{G}) \text{ et i<j} \\ -w(i,j), \text{ si (i,j)} \in E(\overrightarrow{G}) \text{ et i>j} \\ 0 \text{ sinon} \end{cases}$$

Cela va être pour nous la manière canonique de représenter un graphe non orienté. On peut aussi représenter un graphe par une matrice triangulaire en posant $w(i,j) = 0$ quand i est plus grand que j. C'est alors la matrice d'adjacence du graphe.

Enfin un graphe biparti est représenté par une matrice dont le coefficient $a_{i,j}$ est le poids de l'arête qui relie le $i^{\text{ème}}$ sommet du premier ensemble de sommet au $j^{\text{ème}}$ du second ensemble.

On supposera dans toute la suite que les poids du graphe sont à valeur dans un corps $\mathbb{K}$ qui sera éventuellement fini à p éléments, on le notera alors $\mathbb{F}_p$. Quand le graphe n'est pas pondéré, on affecte par convention le poids 1 aux arêtes présentes et 0 aux autres.

Définition 2 (Permanent)**.** Le Permanent d'une matrice M est défini de la manière

suivante :

$$\mathsf{Per(M)} = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} m_{i,\sigma(i)}$$

Le Permanent est un déterminant au signe des monômes près. Si la matrice est une matrice d'adjacence d'un graphe non pondéré, son permanent est le nombre de recouvrement par cycle du graphe. Si la matrice représente un graphe biparti non pondéré, son Permanent est égal au nombre de couplages parfaits dans le graphe. Ce problème est $\sharp P$-complet pour les réductions Turing (voir [6]) alors que le calcul du déterminant est NC^2-complet.

Remarque 1. Dans $\mathbb{F}_2$ le déterminant et le permanent sont égaux car la fonction signe notée sg, qui intervient dans le déterminant et pas dans le permanent, est la fonction constante qui donne 1. L'évaluation du Permanent est alors dans NC^2. On en déduit que trouver la parité du nombre de couplages d'un graphe biparti est dans NC^2 donc dans P.

Définition 3 (PerfMatch)**.** Soient G un graphe pondéré par $w_{i,j}$ poids de l'arête (i,j) et $\mathcal{C}$ l'ensemble de ses couplages parfaits.

$$\mathsf{PerfMatch}(G) = \sum_{C \in \mathcal{C}} \prod_{(i,j) \in C} w_{i,j}$$

Le PerfMatch est une généralisation du problème de compter le nombre des couplages parfaits dans un graphe, on tient compte aussi du poids des couplages.

Définition 4 (Pfaffien)**.** Le Pfaffien d'une matrice antisymétrique d'adjacence d'un graphe G vaut 1 si la dimension de la matrice est 0, 0 si la dimension est impaire (il n'y a alors pas de couplage parfait) et si la dimension est paire :

$$\mathsf{Pfaf}(M) = \sum_{\pi} \mathrm{sg}(\pi) w(i_1, i_2) w(i_3, i_4) \dots w(i_{2n-1}, i_{2n})$$

où

1. π est la permutation $j \to i_j \, , \forall j \leq 2n$
2. la somme est sur toutes les permutations représentant un couplage parfait. Les couplages parfaits sont des listes d'arêtes notées $\{(i_1, i_2), \dots, (i_{2n-1}, i_{2n})\}$. Pour les décrire de manière unique, on supposeras $i_{2k-1} < i_{2k}$ et $i_{2k-1} < i_{2k+1}$ pour $k = 1, \dots, n$, c'est à dire que chaque arête est représentée par un couple avec le plus petit sommet en premier et que les arêtes sont ordonnées de manière croissante suivant leur première coordonnée.
3. $w(i,j)$ représente le poids de l'arête (i,j), c'est aussi le coefficient $a_{i,j}$ de la matrice antisymétrique d'adjacence.

Remarque 2. Ni le signe, ni la valeur absolue d'un monôme associé à un couplage parfait ne dépend de la façon dont on représente le couplage parfait, c'est à dire l'ordre dans lequel est donné les arêtes et l'ordre dans chaque couple.

1. En effet si on change dans la liste le couple (i, j) par (j, i), on obtient la nouvelle permutation π en composant l'ancienne avec la transposition (i, j) ce qui change son signe. Mais par ailleurs on change $w(i, j)$ en $w(j, i) = -w(i, j)$ car la matrice est antisymétrique, donc on ne change pas le signe du monôme.
2. Si on change l'ordre dans lequel on donne la liste d'arête par exemple en échangeant (i_{2j-1}, i_{2j}) et (i_{2k-1}, i_{2k}), c'est comme si on composait π par la permutation $(i_{2j-1}, i_{2k-1}) \circ (i_{2j}, i_{2k})$, ce qui ne change pas son signe, et on ne change pas non plus les poids dans le monôme (la multiplication commute !).

Donc le choix d'un représentant pour un couplage ne change pas le monôme dans le Pfaffien. On voit donc ce polynôme comme une somme sur tous les couplages parfaits, qu'on représentera par la liste de ses arêtes ordonnées comme on le désire.

Définition 5 (PfafSum)**.** Soit M une matrice de taille n, et A un sous-ensemble de $[1, \ldots, n]$, on note $M[A]$ la matrice obtenue en rayant lignes et colonnes d'indice dans A. La somme Pfaffienne, notée PfafSum, est le polynôme en les λ_i suivant :

$$\mathsf{PfafSum}(M) = \sum_A \left(\prod_{i \in A} \lambda_i \right) Pf(M[A])$$

On peut généraliser exactement de la même manière le PerfMatch en MatchSum.

Remarque 3. On applique généralement ce polynôme à un graphe doublement pondéré (arêtes et sommets). Les λ_i prenant pour valeur le poids du sommet i, on calcule alors la somme de tous les Pfaffiens du graphe initial auquel on a retiré un ensemble arbitraire de point.

On va utiliser cela dans la suite avec les poids des sommets tous égaux à 0 ou 1. On dit qu'un sommet de poids 1 est superflu (*ommitable node* en anglais) car un couplage qui ne le sature pas contribue quand même à la PfafSum. De la même manière on dit qu'on ne peut pas omettre les sommets de poids 0 car les couplages les omettant contribuent pour 0 à la PfafSum.

1.2 Complexité en général de ces polynômes

On peut se demander à quelles classes de comptage ou de fonctions appartiennent les polynômes précédemment définis. Leur complexité dépend du corps dans lequel ces polynômes sont évalués et des poids qu'on permet sur les arêtes et sommets des graphes.

Théorème 1. *Le Permanent et le PerfMatch avec des poids entiers positifs sur les arêtes sont des problèmes $\sharp P$-complet.*

Démonstration. C'est à partir de ces problèmes que Valiant à inventé les classes de comptage et on peut trouver les preuves de complétude de ces problèmes dans son article fondateur [6].

La démonstration originale ne permet pas de poids sur les arêtes ce qui revient à avoir uniquement 1 et 0 comme poids. On peut simuler une arête de poids n entier reliant les

sommets a et b. Pour cela on relie a à n nouveaux sommets et b à n autres nouveaux sommets qu'on relie entre eux deux à deux, toutes les arêtes étant de poids 1. Cette opération ne modifiant pas la valeur du PerfMatch, on peut le calculer avec uniquement des arêtes de poids 1.

D'autre part, avec le Théorème 10, je montre par des techniques holographiques qu'on peut réduire à MatchSum avec des poids dans un sous-ensemble de $\mathbb{Q}$ un problème $\sharp P$-complet. On peut montrer que MatchSum se réduit au calcul du Permanent et du PerfMatch, ce qui prouve le théorème sans utiliser le résultat de Valiant. □

Trouver des classes de complexité pour les problèmes du calcul du PerfMatch ou du Pfaffien avec des poids dans un corps quelconque est plus difficile. Une solution est d'utiliser la notion de machine de Turing algébrique introduite dans un article de Damm [1] qui généralise la classe $\sharp P$ à tous les corps. Je redonne ici rapidement les définitions nécessaires mais on peut se reporter à l'article pour plus de détails.

Définition 6. Une machine de Turing algébrique est une machine dont les transitions sont pondérées par les éléments d'un anneau $\mathcal{S}$.

Le poids d'un chemin de calcul est le produit des poids des transitions de l'état initial à l'état final.

Une fonction f est dans $\mathcal{S} - \sharp P$ si il existe une machine de Turing algébrique non déterministe s'arrêtant en temps polynômial telle que la somme des poids des chemins de calcul sur un élément x est égal à $f(x)$.

Théorème 2. *Les problèmes PerfMatch, Pfaffien, MatchSum et PfafSum sur un corps* $\mathbb{K}$ *sont dans* $\mathbb{K} - \sharp P$.

Démonstration. La preuve de ces affirmations est simple et se fait par construction d'une machine appropriée. Par exemple, pour calculer MatchSum d'un graphe, il faut énumérer de manière non déterministe tous les sous-ensembles de sommets, le poids de la transition étant le poids du sommet si il n'est pas dans le sous-ensemble, 1 si il y est. Dans chaque branche de l'arbre de calcul on énumère ensuite tous les sous-ensemble d'arêtes, le poids de chaque transition étant celui de l'arête si on la retient.

Enfin dans chaque branche on vérifie que l'ensemble d'arête engendré donne bien un couplage de l'ensemble de sommet engendré. Si ça n'est pas le cas on fait une transition finale de poids 0. Les poids des transitions de vérification sont fixés à 1 pour ne pas modifier le poids du chemin de calcul. On a un arbre de calcul de profondeur polynômial en la taille du graphe.

Donc quand on a ensemble A qui décrit un couplage parfait d'un graphe induit par un sous-ensemble de sommets B, le poids du chemin de calcul est le produit des poids des arêtes de A multiplié par le produit des poids des sommets qui ne sont pas dans B. Quand on additionne ces valeurs pour tous les couplages possible on obtient le MatchSum du graphe donc $\mathcal{C} - \mathsf{MatchSum} \in \mathcal{C} - \sharp P$ et on peut faire la même chose pour les autres polynômes. □

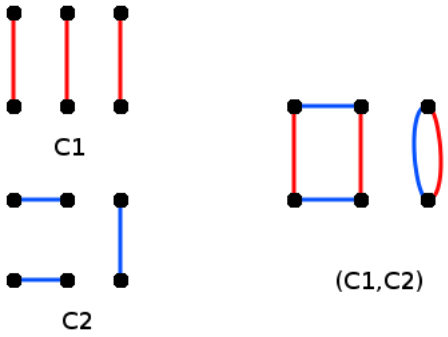

FIG. 1.1 – Les couplages C_1 et C_2 donnent naissance à un recouvrement par cycle pair noté (C_1, C_2).

1.3 Calcul effectif du Pfaffien

Lemme 1. *Le nombre de pairs de couplages parfaits donnant naissance à un même recouvrement par cycles pairs est égal au nombre d'orientations des cycles de ce recouvrement.*

Démonstration. Il est facile de voir, comme dans l'exemple de la Figure 1.1, que si on fait l'union de la liste des arêtes de deux couplages parfaits on obtient un recouvrement par cycle pair du graphe. Si on considère les couplages donnant naissance à un recouvrement, on remarque que restreint à un cycle, il n'y a que deux possibilités : prendre une arête sur deux en commençant soit par la première soit par la deuxième. Donc si il y a t cycles (de longueur strictement supérieur à 2, dans le cas de longueur 2 les deux couplages partage une même arête), on a 2^t couples donnant naissance au recouvrement, par ailleurs il y a aussi 2^t possibilités d'orientation de ces cycles. □

Lemme 2. *Le terme* $t = \mathrm{sg}(\pi_1) w_1(i_1, i_2) \dots w_1(i_{2n-1}, i_{2n}) \mathrm{sg}(\pi_2) w_2(i_1, i_2) \dots w_2(i_{2n-1}, i_{2n})$, *produit de la contribution des couplages* C_1 *et* C_2 *au Pfaffien dépends uniquement du recouvrement par cycle engendré par* C_1 *et* C_2.

Démonstration. Remarquons que si on a deux pairs différentes mais donnant le même recouvrement par cycle, la valeur absolue de t est la même, car on se contente de faire commuter des poids w dans le produit.

On fixe un recouvrement par cycle pair et un cycle $A = (a_1, \dots, a_{2k})$ de ce recouvrement qu'on peut supposer constitué des $2k$ premiers sommets. On note R l'ensemble des autres cycles. Nécessairement la restriction à A d'un couple de couplage engendrant le recouvrement est soit (A_1, A_2), soit (A_2, A_1) avec $A_1 = \{(a_1, a_2), \dots, (a_{2k-1}, a_{2k})\}$ et $A_2 = \{(a_2, a_3), \dots, (a_{2k}, a_1)\}$.

Il faut montrer que le terme t associé à ces deux pairs est le même c'est à dire que le signe est le même. On suppose que (C_1, C_2) restreint à A vaut (A_1, A_2), il suffit de montrer que si on échange A_1 par A_2 dans C_1 et A_2 par A_1 dans C_2 t ne change pas.

Si dans la liste d'arête qui représente C_1, on met d'abord celles qui apparaissent dans A_1 alors π_1 peut s'écrire $(\pi_1)_{|A} \circ (\pi_1)_{|R}$. On a le même résultat pour C_2, donc si C_1' et C_2' sont les couplages modifiés en A, on a $\pi_1' = (\pi_2)_{|A} \circ (\pi_1)_{|R}$ et $\pi_2' = (\pi_1)_{|A} \circ (\pi_2)_{|R}$. Donc $\mathrm{sg}(\pi_1)\,\mathrm{sg}(\pi_2) = \mathrm{sg}(\pi_1')\,\mathrm{sg}(\pi_2')$. Comme seules les permutations différaient dans t, on a bien le même terme pour les deux pairs.

On a montré qu'on peut échanger la restriction à un cycle dans deux couplages de la pair, donc par récurrence on montre qu'on peut en échanger autant que l'on veut ce qui démontre le lemme. □

Théorème 3. *Calculer le Pfaffien d'une matrice antisymétrique d'un graphe G est dans P. En fait $\mathsf{Pfaf}(M)^2 = \det(M)$.*

Démonstration. Le déterminant s'écrit :

$$\det M(G) := \sum_{\pi \in \mathfrak{S}_n} \mathrm{sg}\,\pi \prod_{i=0}^{n-1} a_{i,\pi(i)}$$

Si on considère l'ensemble A des permutations dont la décomposition en cycle de support disjoint contient un cycle impair, on remarque que sa contribution au déterminant est nulle. En effet on peut réaliser une involution de A dans A, en remplaçant dans chaque permutation le cycle de longueur impair contenant le plus petit élément par son inverse. Cette transformation ne modifie pas la valeur absolue de la contribution de la permutation dans le déterminant mais change son signe donc globalement la contribution des éléments de A est nulle.

Par le Lemme 1 on sait déjà que le nombre d'orientations d'un recouvrement par cycle, c'est à dire le nombre de permutations donnant naissance à de tels recouvrement est en bijection avec le nombre de pairs de couplage donnant naissance au même recouvrement. Dans $\mathsf{Pfaf}(M)^2$ on a une somme sur toutes les pairs de couplages parfaits, du produit des termes correspondant au deux couplages dans le Pfaffien. On sait par le Lemme 2 que quand les couples donnent naissance au même recouvrement, la valeur du produit (le terme t) est la même, de plus la valeur d'un monôme du déterminant correspondant au recouvrement ne varie pas en fonction de l'orientation des cycles.

Il suffit donc de montrer qu'on a égalité entre un terme du déterminant correspondant à une permutation π et un terme de $\mathsf{Pfaf}(M)^2$ correspondant à (C_1, C_2) si π et (C_1, C_2) donnent naissance au même recouvrement par cycle du graphe.

Pour cela il suffit de remarquer que les poids en jeu sont les mêmes dans les deux termes, à condition de prendre une représentation par liste d'arêtes de (C_1, C_2) qui respecte l'orientation de π, c'est à dire en orientant les arêtes comme dans π. On va montrer de plus que $\pi_1\pi_2^{-1} = \pi$ et que donc $\mathrm{sg}(\pi_1)\,\mathrm{sg}(\pi_2)) = \mathrm{sg}(\pi)$. Soit $\sigma = (a_1, \ldots, a_{2k})$ un des cycles de π, alors on en prends dans le début de la liste de C_1 $(a_1, a_2), \ldots, (a_{2k-1}, a_{2k})$ et dans le début de C_2 $(a_2, a_3), \ldots, (a_{2k}, a_1)$. On a alors que $(\pi_1\pi_2^{-1})_{[|1,\ldots,2k|]} = \sigma$ par un calcul évident, on en déduit que l'égalité est vraie en mettant à la suite tous les cycles de cette manière dans C_1 et C_2. □

Corollaire 1. *On peut également calculer le $\mathsf{PfafSum}$ en temps polynômial.*

Démonstration. Soit G le graphe doublement pondéré dont on veut calculer le PfafSum. On ajoute k sommets au graphe G et on relie chaque sommet à tous les nouveaux sommets par une arête du poids associé au sommet. Si on calcule le Pfaffien de G' on obtient exactement le PfafSum de G dont on a oublié k sommets multiplié par un coefficient. Il suffit de faire ce calcul pour tous les k possibles, à chaque fois en temps polynômial par le Théorème 3, et d'en déduire le PfafSum en temps polynômial également. □

1.4 Calcul effectif du PerfMatch

On a vu que le PerfMatch comme le Permanent sont des archétypes de problème $\sharp P$ complet. Le but de cette section est de montrer que le calcul du nombre de couplages parfaits est un problème facile dans le cas ou le graphe est planaire. On se servira de ce résultat par la suite pour construire des réductions particulières vers les couplages parfaits d'un graphe planaire et montrer ainsi que certains problèmes sont dans FP.

Dans cette section tout les graphes seront non pondérés et non orientés sauf précision contraire.

Définition 7 (Orientation impaire d'un cycle)**.** Soit G un graphe, C un cycle de longueur paire et $\overrightarrow{G}$ une orientation, on dit que C est orienté de manière impaire par rapport à $\overrightarrow{G}$ si le nombre de ses arêtes orientées dans le même sens est impair.

Définition 8 (Orientation Pfaffienne)**.** Soit un graphe G et $\overrightarrow{G}$ une orientation, on dit qu'elle est Pfaffienne si pour tous couplages parfaits C_1 et C_2, tout cycle de $C_1 \cup C_2$ est d'orientation impaire dans $\overrightarrow{G}$.

Lemme 3. *Il y a une bijection entre les pairs (ordonnées) de couplages parfaits dans un graphe G et les recouvrements par cycles de longueur paire de ce graphe.*

Démonstration. A un couple de couplage on associe le recouvrement par cycle pair constitué de l'union des arêtes des couplages. On doit encore orienter ce recouvrement, il suffit d'en orienter chaque cycle. Dans un cycle on trouve l'arête qui joint le sommet de plus petit indice du cycle au plus petit des ses voisins. Si cette arête est dans le premier couplage on oriente le cycle du plus petit sommet vers le plus grand ce qui force l'orientation de tout le cycle. Si l'arête est dans le deuxième couplage, on oriente le cycle dans l'autre sens. Il est facile de voir que la fonction ainsi définie est une bijection. □

On note $\tilde{G}$ le multigraphe orienté obtenu à partir du graphe non orienté G, en remplaçant chaque arête non orientée par deux arêtes de sens opposé.

Lemme 4. $\det A_S(\overrightarrow{G})$ *est le nombre de recouvrement par cycles pairs de $\tilde{G}$.*

Démonstration. On peut voir toutes les permutations comme un produit de cycle, si ces cycles ne correspondent pas à des arêtes du graphe, le terme associé à la permutation dans le déterminant est nul. On a déjà vu dans le Théorème 3 que les termes du déterminants associés à une permutation comptant au moins un cycle de longueur impair s'annulent.

Donc on a exactement un terme non nul du déterminant par recouvrement par cycle pair.

Comme l'orientation est Pfaffienne, dans chaque cycle on a un nombre impair d'arête apparaissant avec un poids -1. Mais comme le cycle est pair, sa signature est -1, donc dans le produit chaque cycle contribue pour 1. On en déduit que chaque recouvrement par cycle pair contribue pour 1 dans la somme du déterminant, ce qui démonte le lemme. □

Théorème 4 (Kasteleyn). *Pour toute orientation Pfaffienne $\overrightarrow{G}$ de G,*

$$\mathit{PerfMatch}(G) = \sqrt{\det A_S(\overrightarrow{G})}$$

Démonstration. Les Lemmes 3 et 4 permettent de montrer le théorème immédiatement. □

Pour le lemme suivant on a besoin de connaître la formule suivante sur un graphe planaire,

Formule d'Euler : faces + arêtes − sommets = 2

Lemme 5. *Soit un graphe planaire connexe $\overrightarrow{G}$ dont toutes les faces ont un nombre impair d'arêtes orientées dans le sens des aiguilles d'une montre. Alors, dans tous ses cycles non orientés, le nombre d'arêtes dans le sens des aiguilles d'une montre est de parité opposée au nombre des sommets à l'intérieur du cycle.*

Démonstration. Soit un cycle C, et f le nombre de face à l'intérieur de ce cycle. On note c_i le nombre d'arêtes orienté dans le sens des aiguilles d'une montre dans la face i. Par hypothèse $c_i = 1 \pmod 2$, donc $f = \sum_{i=1}^{f} c_i \pmod 2$. Chaque arête à l'intérieur de C fait partie de exactement deux faces, une de chaque côté de l'arête. Elle est orientée dans le sens des aiguilles d'une montre pour exactement une des deux faces. Donc si on note c le nombre d'arêtes orientées dans le sens des aiguilles d'une montre sur C et e le nombre d'arêtes dans c, on a par la remarque précédente $\sum_{i=1}^{f} c_i = c + e$.

On utilise la formule d'Euler pour faire apparaître v le nombre de sommets à l'intérieur de C : $e = v + f - 1$. On combine les deux dernières égalités pour obtenir

$$f = c + e \pmod 2$$
$$f = c + v + f - 1 \pmod 2$$
$$c + v = 1 \pmod 2$$

et donc $c+v$ est impair, c'est à dire que les parités du nombre de sommets à l'intérieur de C et du nombre d'arêtes orientées dans le sens des aiguille d'une montre sont opposées. □

Corollaire 2. *Dans les conditions du lemme précédent, $\overrightarrow{G}$ est une orientation Pfaffienne.*

Démonstration. Considérons un cycle C du recouvrement par cycles pairs obtenu par l'union d'une pair de couplage parfait. Si on considère les sommets à l'intérieur de C, il n'y a pas d'arête entre eux et des éléments hors de C par planarité. Donc le recouvrement par cycles pairs restreint à ces sommets est aussi un recouvrement par cycle pair. On en déduit qu'il y a un nombre pair de sommets à l'intérieur de C. Par le Lemme 5, C a un nombre impair d'arêtes orientées dans le sens des aiguilles d'une montre donc il est orienté de manière impaire. □

Théorème 5. *Tout graphe planaire admet une orientation Pfaffienne.*

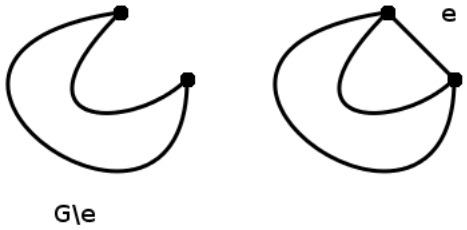

FIG. 1.2 – Ajouter une arête sur la face extérieure rajoute une face

Démonstration. Il suffit de vérifier qu'on peut construire une orientation d'un graphe planaire H vérifiant les conditions du Lemme 5. On suppose que le graphe est connexe, sinon il suffit de le séparer en composante connexe et de faire l'opération suivante sur chaque composante.

On raisonne par induction sur le nombre d'arêtes en partant d'un graphe qui est un arbre. Remarquons d'abord que toute orientation d'un arbre vérifie les conditions du Lemme 5 car il n'y a alors pas de cycle. Supposons qu'on a un graphe H vérifiant les conditions du Lemme 5 et qu'on rajoute à ce graphe une arête e sur la face extérieure. Cela créé une seule face comme dans la Figure 1.4 et on choisit de l'orienter pour qu'un nombre impair d'arêtes soient dans le sens des aiguilles d'une montre sur cette face. On obtient un graphe avec une arête de plus vérifiant les conditions du Lemme 5 ce qui prouve l'étape d'induction.

On reconstruit le graphe H par cette méthode avec une orientation qui vérifie les conditions du Lemme 5 ce qui nous assure qu'elle est Pfafienne. □

On remarque que la démonstration précédente est constructive, en effet il suffit par exemple de trouver une suite de sommet qui fasse passer du graphe G à un arbre. Pour cela il suffit de trouver la face extérieure à chaque étape ce qui est réalisable en temps

polynômial. Nécessairement cette face contient au moins un cycle, on en retire la première arête ce qui ne romps pas la connexité on recommence jusqu'à avoir un arbre. On peut alors construire une orientation Pfaffienne comme expliqué dans le théorème précédent en temps polynômial.

Corollaire 3. *On déduit des deux théorèmes précédents que calculer le nombre de couplages parfaits d'un graphe planaire est dans FP.*

Corollaire 4. *On pourait démontrer exactement de la même manière avec des graphes pondérés que le* PerfMatch *d'un graphe planaire se calcule en temps polynômial.*

Chapitre 2

Algorithmes holographiques

On va construire des graphes dans le but que certains de leurs polynômes caractéristiques, ici le PerfMatch, représentent un problème combinatoire donné. Pour facilement arriver à nos fins on construit ces graphes à partir d'éléments de bases dont on connaît bien les propriétés. Les définitions suivantes sont tirés des travaux de Valiant, principalement [9] et de ceux de Cai [11].

2.1 Rappel sur les produits tensoriels

Quelques notations :

On va travailler par la suite avec un espace vectoriel ambiant E et un corps $\mathbb{K}$. L'anneau des matrices de taille n sur k, à coefficient dans le corps $\mathbb{K}$, sera noté $\mathcal{M}_{n,k}(\mathbb{K})$ ou $\mathcal{M}_{n,k}$ quand le corps n'importe pas.

La loi de groupe d'un espace vectoriel est notée $+$ comme la loi de groupe du corps. La loi externe d'un espace vectoriel ainsi que la multiplication du corps sont notées "." mais on omettra le plus souvent ce symbole. Enfin le produit scalaire entre deux vecteurs u et v sera noté $< u, v >$.

Définition 9. Le produit tensoriel de deux espaces vectoriels E_1 et E_2 sur le corps $\mathbb{K}$, noté $E_1 \otimes E_2$, est l'espace vectoriel constitué des combinaisons linéaires des éléments de la forme (x_1, x_2) avec $x_i \in E_i$, aussi notés $x_1 \otimes x_2$. Ils vérifient les propriétés suivantes :

1. $(x_1, x_2) + (x_1', x_2) = (x_1 + x_1', x_2)$
2. $(x_1, x_2) + (x_1, x_2') = (x_1, x_2 + x_2')$
3. $(ax_1, x_2) = a(x_1, x_2) = (x_1, ax_2)$

On peut montrer que l'objet ainsi défini est unique. On peut bien sur prolonger cette définition à n produits tensoriels d'espaces en remarquant qu'ils sont associatifs.

Remarque 4. Si $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_m)$ sont respectivement des bases des espaces vectoriels A et B alors l'ensemble des $a_i \otimes b_j$, $(i, j) \in [1, \ldots, n] \times [1, \ldots, m]$ est une base de $A \otimes B$.

Supposons que les espaces vectoriels, ce qui sera le cas par la suite, sont de la forme $\mathcal{M}_{n,k}$. On a alors un isomorphisme naturel de $\mathcal{M}_{n,k} \otimes \mathcal{M}_{n',k'}$ vers $\mathcal{M}_{n.n',k.k'} : M \otimes N \to R$ où R est la matrice de coefficient $R_{i.n'+p,j.k'+t} = M_{i,j}.N_{p,t}$. Par la suite on va confondre $M \otimes N$ et son image par l'isomorphisme.

Remarque 5. Supposons qu'on ait une base $\mathbf{b}$ de vecteurs $b_1, \ldots, b_k$ de taille n. Alors on peut voir $e_1 \otimes \cdots \otimes e_l$, $e_i \in \mathbf{b}$ comme un vecteur de dimension n^l par le morphisme précédent. Pour alléger la notation on écrira souvent e^i pour signifier le i-ème coefficient du vecteur e. Pour tout $i \leq n^l$ dont la décomposition n-aire s'écrit $i = i_1 \ldots i_l$ on a par définition l'égalité :

$$(e_1 \otimes \cdots \otimes e_l)^i = e_1^{i_1} \ldots e_l^{i_l}$$

Lemme 6. *Soient deux vecteurs $u = u_1 \otimes \cdots \otimes u_k$ et $v = v_1 \otimes \cdots \otimes v_k$ avec pour tout i des vecteurs u_i et v_i de même dimension. Alors* $< u, v >= \prod_{1 \leq i \leq k} < u_i, v_i >$.

Démonstration. Supposons qu'on veut calculer $< a \otimes b, c \otimes d >$ avec a et c de longueur k. Par définition du produit tensoriel on a $a \otimes b = (a_1 b, a_2 b, \ldots, a_k b)$ et $c \otimes d = (c_1 d, c_2 d, \ldots, c_k d)$.

Donc si on calcule le produit scalaire on obtient $\sum_{1 \leq i \leq k} a_i c_i < b, d >=< a, c >< b, d >$.
Le lemme se démontre alors par une récurrence évidente. □

Remarque 6 (Matrice de changement de base)**.** Soient $\mathbf{b_1}$ et $\mathbf{b_2}$ deux bases qu'on peut représenter par des matrices dont les vecteurs lignes sont les éléments de la base. Soit T la matrice de passage entre les bases $\mathbf{b_1}$ et $\mathbf{b_2}$, c'est à dire $\mathbf{b_1} = T\mathbf{b_2}$.

Alors $T^{\otimes k}$ est la matrice de passage entre les bases ${\mathbf{b_1}}^{\otimes k}$ et ${\mathbf{b_2}}^{\otimes k}$, c'est à dire ${\mathbf{b_1}}^{\otimes k} = T^{\otimes k}{\mathbf{b_2}}^{\otimes k}$.

Cette remarque nous servira par la suite dans le cas particulier où la base a deux vecteurs de dimension 2.

2.2 Portes de couplage et signature

Définition 10 (Porte de couplage)**.** Une porte de couplage est un triplet (G, I, O), où G est un graphe (V, E) et I, O sont des sous-ensembles disjoints de sommets de V représentant ses *entrées* et ses *sorties*. Les autres sommets seront appelés sommets internes.

Une porte de couplage est donc un graphe avec certains sommets considérés comme des entrées et d'autres comme des sorties. On voit le graphe comme un circuit qui émet et reçoit des informations, cette manière de voir vient de l'informatique quantique dont on peut simuler certains circuits [7] avec les constructions suivantes.

Définition 11 (Sous-graphe induit)**.** Soient $G = (V, E)$ un graphe et $V' \subseteq V$ un sous-ensemble des sommets. Le sous-graphe de G induit par V' a pour ensemble de sommets V' et pour ensemble d'arêtes $E' = \{(u, v) \in E | u, v \in V'\}$.

A chaque porte de couplage on veut associer une matrice qui contient tous les nombres de couplages parfaits du graphe auquel on a enlevé un sous-ensemble quelconque de ses entrées et sorties. Si on a p entrées et n sorties on a donc une matrice $M \in \mathcal{M}_{2^n,2^p}(\mathbb{K})$.

On a une bijection naturelle entre les nombres de $\{0, \ldots, 2^n - 1\}$ et les sous-ensembles de $\{1, \ldots, n\}$. On note cette bijection f, elle est définie par $x \in f(i)$ ssi le $x^{\text{ème}}$ bit de i en binaire est 1 (le premier bit est le bit de poids fort). On suppose les entrées et sorties numérotées de 1 à n et 1 à p respectivement, qu'on met en bijection avec $\{0, \ldots, 2^n - 1\}$ et $\{0, \ldots, 2^p - 1\}$ par f et f' grâce à la remarque précédente.

Définition 12 (Matrice d'une porte de couplage)**.** Soit (G, I, O) une porte de couplage à n sorties et p entrées, on note $M = (m_{i,j})$ la matrice de couplage de cette porte. L'entrée $m_{i,j}$ de la matrice de couplage est le PerfMatch du sous-graphe induit par $V \backslash (f(i) \cup f'(j))$.

Remarque 7. On appelle *porte génératrice*, une porte qui n'a pas d'entrées, et *porte de reconnaissance* une porte qui n'a pas de sorties.

Elles ont donc pour matrice de couplage, des vecteurs colonne et ligne respectivement qu'on appellera la *signature standard* de ces portes.

Définition 13 (Base)**.** Une *base* de taille n est un ensemble de vecteurs non nuls de dimension 2^n.

Remarque 8. On se limitera dans la suite, sauf mention contraire, à $n = 1$ et deux vecteurs indépendants, c'est alors une base au sens algébrique. En fait Cai et Lu démontrent dans un article [12] que tous les algorithmes holographiques intéressants peuvent être obtenus avec des bases de taille 1.

Exemple 1. Les deux bases les plus fréquemment utilisées seront la base standard $\mathbf{b_0} = \{(1, 0), (0, 1)\}$ et la base $\mathbf{b_1} = \{(-1, 1), (1, 0)\}$ sur un corps $\mathbb{K}$ quelconque qui contient alors toujours 0,1 et -1.

On considère l'ensemble X des vecteurs obtenus par k produits tensoriels des vecteurs de la base $\mathbf{b} = \{n, p\}$,

$$X = \{x_1 \otimes \cdots \otimes x_k | \, x_i \in \mathbf{b}, i \leq k\} .$$

Comme $\mathbf{b}$ est une base au sens algébrique de $\mathbb{K}^2$, X engendre $\left(\mathbb{K}^2\right)^{\otimes k}$ qu'on confond avec $\mathbb{K}^{2^k}$. On peut donc exprimer tout vecteur de l'espace comme une combinaison linéaire des vecteurs de X.

Définition 14 (Signature selon une base)**.** Soit $\mathbf{b}$ une base, la définition de *signature* est légèrement différente selon que la porte considérée est génératrice ou de reconnaissance :

1. On considère une porte génératrice A de signature standard u de taille 2^k, u s'écrit de manière unique comme une somme de vecteurs de X. On nomme $valG(A, x)$ pour $x \in X$ le coefficient devant x dans la décomposition de u par rapport à X.

2. On considère une porte de reconnaissance B de signature standard u de taille 2^k. On note $valR(B, x)$ pour $x \in X$ le produit scalaire de u et de x.

On peut représenter la signature par un vecteur de taille 2^k contenant tous les $valG(A, x)$ (ou $valR(B, x)$) pour $x \in X$. On voit les $x \in X$ comme des mots de $\{n, p\}^k$ qu'on ordonne de manière lexicographique en posant par convention $n < p$. Cela nous donne une manière unique de représenter la signature selon une base par un vecteur.

Remarque 9. On peut voir la signature de manière plus algébrique. Si u est la signature standard, vue comme un vecteur ligne, d'une porte génératrice alors sa signature dans la base $\mathbf{b}$ est le vecteur $u.\left(\mathbf{b}^{\otimes k}\right)^{-1}$.

Si u est la signature standard, vue comme un vecteur colonne, d'une porte de reconnaissance alors sa signature dans la base $\mathbf{b}$ est le vecteur $\mathbf{b}^{\otimes k}.u$.

Remarque 10. Si la base est orthonormée, $valG(A, x)$ est aussi le produit scalaire de x et u. De plus le vecteur représentant la signature d'une porte génératrice ou de reconnaissance selon la base standard est sa signature standard. En effet un vecteur $x = x_1 \otimes \cdots \otimes x_k$ avec $\forall j \leq k$, $x_j \in \mathbf{b_0}$ est représenté par un vecteur de taille 2^k qui a exactement un 1 en position $i = i_1 \dots i_l$ avec $i_j = 1$ si $x_j = (1, 0)$, 0 sinon. Or ce vecteur est le $i^{\text{ème}}$ dans l'ordre qui permet de représenter une signature et quand on calcule $< u, x >$ on sélectionne en fait la $i^{\text{ème}}$ coordonnée de u.

On aurait pu donner toutes les définitions précédentes dans le cas de graphes avec des sommets superflus, en remplaçant PerfMatch par MatchSum.

Définition 15 (Poids de Hamming)**.** Pour α un entier dont la décomposition binaire est $\alpha_1 \dots \alpha_n$, on appelle poids de Hamming de α, noté $wt(\alpha)$, l'entier $\sum_{i=1}^{n} \alpha_i$.

Cette fonction est juste une notation formelle pour dire qu'on compte le nombre de 1 dans la décomposition binaire.

Définition 16 (Signature symétrique)**.** Si $valG(A, x = x_1 \otimes \cdots \otimes x_k)$, $x_i \in \{n, p\}$ ne dépend que du nombre de n et p et pas de leur positions dans x, on dit que la signature de E selon la base $\{n, p\}$ est symétrique.

On peut reformuler cela en disant qu'une signature v est symétrique si v_α ne dépend que de $wt(\alpha)$. On note ces signatures $[S_0, \dots, S_k]$, avec S_i la valeur d'un v_α tel que $wt(\alpha) = i$.

On a bien sûr $t = 2^k$, t étant la longueur de la signature sous sa forme classique. Cette notation est beaucoup plus concise et la plupart des signatures rencontrées seront de ce type.

2.3 Exemples

Je donne ici quatre exemples de portes de couplage qui permettent d'illustrer les définitions précédentes de signature standard et selon une base. De plus l'existence de ces portes qui ont des signatures particulières va servir dans les démonstration ultérieures

Porte génératrice

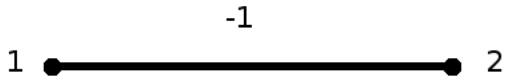

FIG. 2.1 – Une porte génératrice minimale avec deux sorties

La signature standard de la porte génératrice de la Figure 2.1 est $u = (-1, 0, 0, 1)$. Il est normal que les coefficient du milieu soient nuls, ils correspondent aux nombres de couplages parfaits dans un graphe avec un nombre de sommet impair qui est toujours nul. Le premier coefficient correspond au poids des couplages sans noeud enlevé, c'est à dire ici juste l'arête de poids -1 qui relie 1 à 2. Le dernier coefficient correspond au poids des couplages ou tout les sommets d'entrées sont enlevés, il n'y a pas de sommet, par convention le poids du couplage est 1 car c'est un produit vide.

Si on veut la signature selon la base $\mathbf{b_1} = \{n, p\}$ avec $n = (-1, 1)$ et $p = (1, 0)$, on commence par remarquer que :

$$\begin{cases} n \otimes n = (1, -1, -1, 1) \\ n \otimes p = (-1, 0, 1, 0) \\ p \otimes n = (-1, 1, 0, 0) \\ p \otimes p = (1, 0, 0, 0) \end{cases}$$

Comme $\mathbf{b_1}$ est une base de $\mathbb{K}^2$, les 4 vecteurs précédents sont une base de $(\mathbb{K}^2)^{\otimes 2} \simeq \mathbb{K}^4$. On vérifie facilement que $u = n \otimes n + n \otimes p + p \otimes n$. La signature par rapport à $\mathbf{b_1}$ vaut alors $(1, 1, 1, 0)$ en se rappelant que l'ordre lexicographique donne $n \otimes n < n \otimes p < p \otimes n < p \otimes p$.

On peut se demander quelle serait la signature d'une telle porte si on considère les sommets comme des sommets d'entrée et non de sortie. Sa signature standard est la transposée de $u = (-1, 0, 0, 1)$. Sa signature selon la base $\mathbf{b_1}$ qu'on obtient en calculant les produits scalaires de ${}^t u$ et des vecteurs de la base est $(0, 1, 1, -1)$.

Porte génératrice avec un noeud superflu

L'exemple de la Figure 2.2 est une porte génératrice avec un noeud superflu. Sa signature est donc donnée par les valeurs de MatchSum selon que la seule sortie soit prise en compte ou non, elle est égale à (v, w). Dans ce cadre là, on voit que l'on peut obtenir n'importe quelle signature standard de taille 2 ce qui n'est pas le cas si on ne se permet pas de sommets superflus. En effet PerfMatch est toujours nul sur un graphe avec un nombre impair de sommets donc les signatures standards sont toujours composées pour moitié de zéro.

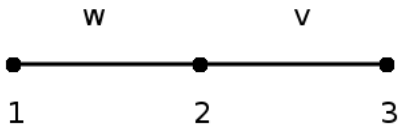

FIG. 2.2 – Une porte génératrice avec le noeud 1 superflu et le noeud 3 qui est le noeud de sortie

Porte en étoile

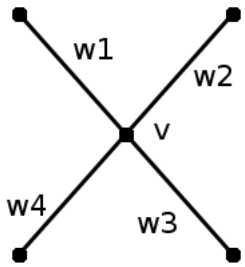

FIG. 2.3 – Une porte de reconnaissance dont tous les sommets sauf le sommet central v sont des entrées

Proposition 1. *Pour tout k et tout ensemble de poids $w_1, \ldots, w_k$ il existe une porte de reconnaissance à k entrées B telle que sur l'entrée $x = x_1 \otimes \cdots \otimes x_k \in \mathbf{b_1}^{\otimes k}$, la valeur de $valR(B, x)$ est :*

1. $-(w_1 + \cdots + w_k)$ *si* $x_1 = \cdots = x_k = n$
2. w_i *si* $x_i = p$ *et pour tout* $j \neq i$ $x_j = n$
3. 0 *pour le reste des cas*

Démonstration. Le graphe de la Figure 2.3 avec un noeud central et k noeuds d'entrée reliés à celui-ci par des poids w_i vérifie ces conditions. En effet les seuls couplages parfaits sont réalisés quand on oublie $k-1$ portes d'entrée, on a alors un couplage de poids w_i constitué de la $i^{\text{ème}}$ arête. Les coefficients non nuls de la signature standard u de cette porte de couplage sont donc à des positions s'écrivant avec un seul 0 dans leur décomposition binaire (on ne prend qu'un seul sommet d'entrée). Les coefficients non nuls valent w_j si le 0 est le $j^{\text{ème}}$ chiffre de la décomposition binaire de i. Par exemple si $k = 3$ on obtient la signature standard suivante : $(0, 0, 0, w_1, 0, w_2, w_3, 0)$.

Il faut remarquer que si $x = x_1 \otimes \cdots \otimes x_k \in \mathbf{b_1}^{\otimes k}$ alors le i-ème coefficient de x avec $i = a_1 \dots a_k$ décomposition binaire de i vaut comme dans la Remarque 5

$$\prod_{j=1}^{k} x_j^{a_j} \tag{2.1}$$

Supposons qu'il y ait deux ou plus occurrences de $p = (1, 0)$ dans x et que i a au plus un 0 dans sa décomposition binaire. Alors en position i de x, on a 0 car dans le produit 2.1 il y a alors un j tel $x_j^{a_j} = p_1 = 0$. On en déduit que $u.x = 0$, car u_i est non nul seulement en de tels i.

De la même façon, si il y a un seul p dans x à la position j dans la décomposition $x_1 \otimes \cdots \otimes x_k \in \mathbf{b_1}^{\otimes k}$, les $i^{\text{ème}}$ coefficients de x avec un seul 0 dans la décomposition binaire de i en position différente de j sont nuls. Seul le coefficient correspondant au couplage constitué de l'arête de poids w_j vaut 1 dans x donc $valR(B, x) = u.x = w_j$.

Enfin si $x_1 = \cdots = x_k = n$, les coefficients de x en position i, dont l'écriture binaire contient exactement un 0, valent $(-1) \cdot 1^{k-1} = -1$. On en déduit que $valR(B, x) = u.x = -(w_1 + \cdots + w_k)$. □

Porte en triangle

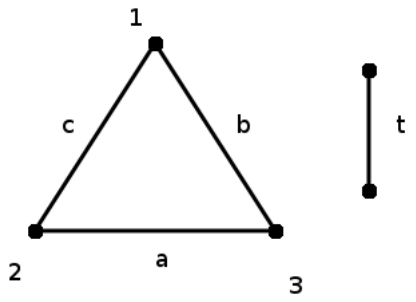

FIG. 2.4 – Une porte d'arité 3 avec les composantes impaires non nulles

Lemme 7. *On peut réaliser la signature standard* $(0, ta, tb, 0, tc, 0, 0, t)$ *pour toute valeur de* a, b, c, t.

Démonstration. Il suffit de calculer la signature standard de la Figure 2.4, les sommets 1,2 et 3 étant considérés comme des sorties si c'est une porte génératrice, des entrées si c'est une porte de reconnaissance. □

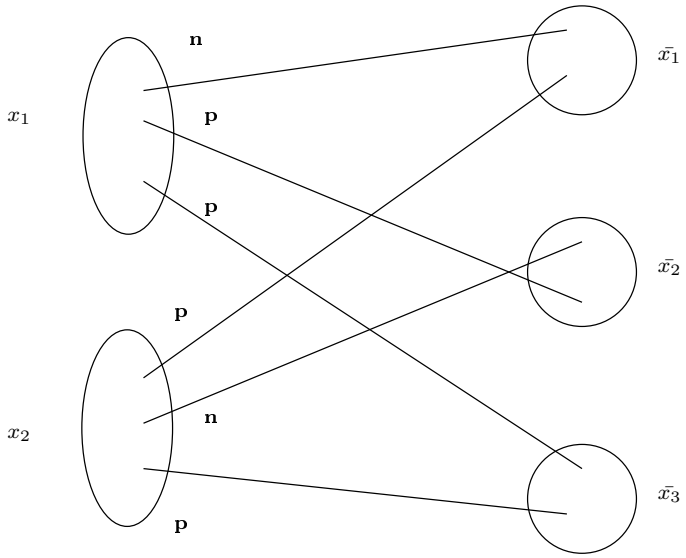

FIG. 2.5 – Un circuit de couplage qui donne la bijection entre x et $\bar{x}$

2.4 Concept et théorème fondamental

Définition 17 (Circuit de couplage)**.** Un circuit de couplage est constitué d'un ensemble de portes génératrices $\{A_1, \ldots, A_g\}$, d'un ensemble de portes de reconnaissance $\{B_1, \ldots, B_l\}$ et d'un ensemble d'arêtes $\{C_1, \ldots, C_f\}$ qui joignent chacune exactement une sortie d'une porte génératrice et une entrée d'une porte de reconnaissance. Toutes les entrées et les sorties doivent être reliées, on a donc le même nombre d'entrées et de sorties.

Remarque 11. Le circuit de couplage n'est jamais qu'un graphe pondéré avec une certaine structure. Si ce graphe est planaire on peut en particulier calculer son PerfMatch en temps polynômial. Les circuits de couplage seront souvent construit à partir d'un graphe bipartite planaire en remplaçant les sommets par des portes de couplage ce qui assure la planarité du graphe si les portes sont planaires.

Soient $\Omega = (A, B, C)$ un circuit de couplage qui a f sommets de sortie et $\mathbf{b} = \{n, p\}$ une base, on pose $X = \mathbf{b}^f$. On a $A = (A_1, \ldots, A_k)$ portes génératrices, on peut décomposer X en $X_1 \otimes \cdots \otimes X_k$ avec, quand A_i a p sommets de sortie, $X_i = \mathbf{b}^p$. Un élément $x = x_1 \otimes \cdots \otimes x_k \in X$ est donc un vecteur ligne de dimension 2^f comme expliqué dans le paragraphe sur le produit tensoriel.

Les arêtes entre les porte génératrices et les portes de reconnaissance réalise une bijection entre les f entrées et les f sorties. À x on associe $\bar{x}$ qui est l'image par cette bijection de x (on permute les éléments de la base), on peut considérer que les arêtes transmettent les éléments de la base des portes génératrices vers les portes de reconnaissance. Comme à $B = (B_1, \ldots, B_l)$ on peut associer une décomposition en $X_1 \otimes \cdots \otimes X_l$, on note souvent $\bar{x} = \bar{x_1} \otimes \cdots \otimes \bar{x_l}$.

Exemple 2. Dans la Figure 2.5 on voit comment les arêtes de C réalisent la bijection entre x et $\bar{x}$. On a par exemple $x_1 = n \otimes p \otimes p$ et $\bar{x_1} = n \otimes p$.

Définition 18 (Holant). Soit un circuit de couplage $\Omega = (A, B, C)$ alors le Holant de ce circuit est :

$$\mathsf{Holant}(\Omega) = \sum_{x \in \mathbf{b}^f} \left[\prod_{1 \leq j \leq k} valG(A_j, x_j) \right] \left[\prod_{1 \leq i \leq l} valR(B_i, \bar{x_i}) \right]$$

Le théorème suivant montre en particulier que le Holant ne dépend pas de la base choisie.

Théorème 6. *Pour tout circuit de couplage Ω correspondant à un graphe G, et toute base* $\mathbf{b}$*,*

$$\mathit{Holant}(\Omega) = \mathit{PerfMatch}(G).$$

Si on prend pour $\mathbf{b}$ la base standard, le théorème est trivialement vrai. En effet $valG(A_j, x_j)$ et $valR(B_i, \bar{x_i})$ sont juste les valeurs des couplages parfaits de A_j et B_i moins les sommets correspondant à x_j et $\bar{x_i}$. En effet si $x_j = b_1 \otimes \cdots \otimes b_k$ tel que pour tout t inférieur à k, $b_t \in \mathbf{b}$, $valG(A_j, x_j)$ est par définition de la signature standard le PerfMatch de A_j moins les sorties numérotées $t \in [1, \ldots k]$ telles que $b_t = p$.

Le terme $\left[\prod_{1 \leq j \leq k} valG(A_j, x_j) \right] \left[\prod_{1 \leq i \leq l} valR(B_i, \bar{x_i}) \right]$ représente alors la somme des poids des couplages parfaits du graphe en fixant les arêtes de C reliant les éléments de x à ceux de $\bar{x}$. Comme on somme sur tout les x, donc sur tous les sous-ensembles de C possibles, on obtient le $\mathsf{PerfMatch}(G)$ car tout couplage parfait de G est composé d'un sous-ensemble d'arêtes de C et d'un couplage partiel parfait de A et de B.

Démonstration. On commence par fixer $x \in \mathbf{b}^f$ et on construit un graphe $G(x)$ en remplaçant toutes les portes génératrices A_j par un gadget qu'on appellera A'_j. À une porte A_j d'arité k "générant" x_j on associe k portes d'arité 1 du type de la Figure 2.2, de manière à ce que leur signature corresponde à x_j. On réalise cela en remarquant que $x_j = e_1 \otimes \cdots \otimes e_k$ où $e_i \in \mathbf{b}$ et en prenant les poids de la $i^{\text{ème}}$ porte de façon à ce que sa signature soit e_i.

Si on calcule la signature standard des k générateurs on obtient exactement x_j, donc selon $\mathbf{b}$, $valG(A'_j, x_j) = 1$. On multiplie dans chaque A'_j les poids de la première porte par $valG(A_j, x_j)$, les A'_j engendrent alors x_j avec un coefficient $valG(A_j, x_j)$. Par conséquent $\left(\prod_{1 \leq j \leq k} valG(A_j, x_j) \right) x$ est la signature standard des portes génératrices. On nomme u la signature standard des portes de reconnaissance, le nombre de couplages parfaits dans le graphe $G(x)$ est le produit scalaire $< \left(\prod_{1 \leq j \leq k} valG(A_j, x_j) \right) \bar{x}, u >$. Or par définition

$< u, \bar{x} >= \prod_{1 \leq i \leq l} valR(B_i, \bar{x}_i)$ donc

$$\mathsf{MatchSum}(G(x)) = \prod_{1 \leq j \leq k} valG(A_j, x_j) \prod_{1 \leq i \leq l} valR(B_i, \bar{x}_i).$$

Considérons maintenant le graphe $G(x_2, \ldots, x_k)$ qui est le graphe $G(x)$ dans lequel on a remplacé les portes génératrices engendrant x_1 par A_1 (on se rapproche du graphe de départ). Soit v_1 la signature standard de A_1, par définition de la signature selon une base $v_1 = \sum_{x_1 \in X_1} valG(A_1, x_1)x_1$.

On obtient le polynôme MatchSum du graphe comme la somme sur tout les $x_1 \in X_1$ des couplages parfaits de $G(x)$. On en déduit que

$$\mathsf{MatchSum}(G(x_2, \ldots, x_k)) = \sum_{x_1 \in X_1} valG(A_1, x_1) \prod_{2 \leq j \leq k} valG(A_j, x_j) \prod_{1 \leq i \leq l} valR(B_i, \bar{x}_i)$$

Il ne reste plus qu'a finir la preuve par induction, le graphe obtenu à la fin est exactement G pour lequel PerfMatch et MatchSum sont les mêmes car il n'y a plus de sommets superflus. □

Je vais donner une deuxième preuve plus algébrique et beaucoup plus simple, on peut aussi en trouver une autre du même type dans un article de Cai [16].

Démonstration. Il faut d'abord remarquer que si on a deux portes génératrices A_1 et A_2 de signatures respectives u_1 et u_2, la signature de la porte de sortie $A_1 \cup A_2$ en ordonnant les sorties de manière à ce que celles de A_1 soient avant celles de A_2 est $u_1 \otimes u_2$.

En utilisant cette remarque, on obtient $u = u_1 \otimes \cdots \otimes u_k$ avec u_i signature standard de A_i. De plus par définition de la signature selon une base, $u_i = \sum_{x_i \in X_i} valG(A_i, x_i)x_i$. Donc par linéarité du produit tensoriel

$$u = \sum_{x_1 \otimes \cdots \otimes x_k \in \mathbf{b}^f} \left(\prod_{1 \leq j \leq k} valG(A_j, x_j) x_1 \otimes \cdots \otimes x_k \right)$$

On écrit $\overline{x_1 \otimes \cdots \otimes x_k}$ sous la forme $\bar{x_1} \otimes \cdots \otimes \bar{x_l}$ et de la même manière $v = v_1 \otimes \cdots \otimes v_l$. Par le Lemme 6 on a l'égalité $< \bar{x_1} \otimes \cdots \otimes \bar{x_l}, v_1 \otimes \cdots \otimes v_l >= \prod_{1 \leq i \leq l} < \bar{x_i}, v_i >$. Puis par définition de la signature d'une porte de reconnaissance $< \bar{x}, v >= \prod_{1 \leq i \leq l} valR(B_i, \bar{x_i})$.

On peut donc conclure par linéarité du produit scalaire que

$$< \bar{u}, v >= \sum_{x_1 \otimes \cdots \otimes x_k \in \mathbf{b}^f} \left[\prod_{1 \leq j \leq k} valG(A_j, x_j) \right] \left[\prod_{1 \leq i \leq l} valR(B_i, \bar{x_i}) \right]$$

Or on a observé que si u est la signature standard de toutes les portes génératrices et v celle de toutes les portes de reconnaissance, $< \bar{u}, v >$ est le PerfMatch du graphe ce qui démontre le théorème. □

Corollaire 5. *On a en fait montré le théorème plus général* $\mathsf{Holant}(\Omega) = \mathsf{MatchSum}(G)$, *en prenant la définition de signature correspondante.*

Remarque 12. Le Holant est une manière de reformuler le PerfMatch ou le MatchSum, en rendant plus évidente certaines contraintes combinatoires imposées par les portes. Cela va nous servir à construire des graphes dont le PerfMatch sera la solution de problèmes qu'on peut exprimer avec un Holant.

Définition 19. On dit qu'un problème de comptage ♯F a une réduction holographique simple si il existe une fonction en temps polynômial qui transforme une instance de ♯F en un graphe planaire dont les arêtes ont un poids "facilement calculable" (entier ou rationnel par exemple) et tel que le Holant de ce graphe donne ♯F.

Cette définition nous donne plus une marche à suivre pour prouver que certains problèmes sont dans FP qu'un nouveau type de réduction.

Chapitre 3

Application de la méthode

3.1 Liste des problèmes

Je donne ici la définition des problèmes dont on va déterminer la complexité grâce à des algorithmes holographiques.

1. X-MATCHING
   Entrée : Un graphe pondéré biparti $G = (V, E, W)$ en entrée, V étant partitionné en V_1 et V_2, tel que tous les sommets de V_1 soient de degré au plus 2.
   Sortie : La somme des poids des couplages de toutes tailles, où le poids d'un couplage est le produit des poids des arêtes du couplage et de, pour tout sommet non saturé de V_2, $-(w_1 + \cdots + w_k)$ somme des poids des arêtes arrivant en ce sommet.
2. PL-X-MATCHING
   Même problème que le précédent mais on demande au graphe d'être planaire.
3. ♯ PL-RTW-MON-3CNF
   Entrée : Une formule dans une forme très particulière : elle est planaire (**Pl**), sous forme normale conjonctive, avec 3 littéraux par clause au plus, sans négation (**Mon**otone) et chaque variable apparaît au plus 2 fois (**R**ead **tw**ice).
   Sortie : Le nombre de valuation satisfaisant la formule.
4. PL-NODE-BIPARTITION
   Entrée : Un graphe planaire de degré au plus 3.
   Sortie : Le cardinal du plus petit ensemble de sommet tel que si on le retire, le graphe induit est biparti.
5. ♯ EXACT3COVER
   Entrée : Un ensemble d'élément E et un ensemble T de triplet de E.
   Sortie : Le nombre de sous-ensemble $S \subset T$ recouvrant E sans doublon, c'est à dire que tout élément de E est contenu dans un unique triplet de S.

3.2 Complexité de problèmes proches

Définition 20 (Formule planaire)**.** On représente une formule sous forme normale conjonctive par un graphe biparti dont les sommets sont les variables et les clauses et dont les arêtes relient les variables aux clauses où elles (ou leurs négations) apparaissent. La formule est dite planaire si le graphe l'est.

Proposition 2. $\oplus$ Pl-Mon-3CNF *est* $\oplus P$*-complet.*

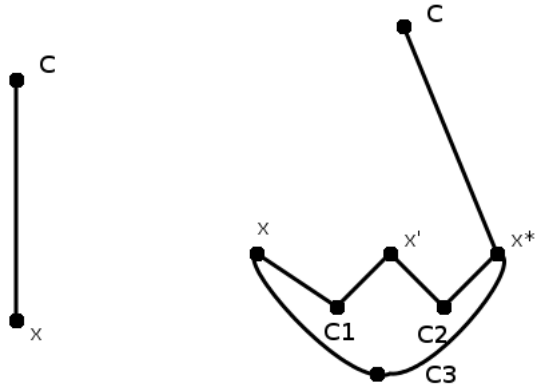

Fig. 3.1 – Transformation de la formule où x apparaît négativement dans C en une formule planaire sans négation de x dans C

Démonstration. L'appartenance à $\oplus P$ est évidente car vérifier si une valuation rends la formule vraie se fait en temps polynômial en la longueur de la formule.

La démonstration de la complétude se fait par réduction de $\oplus$Pl-3CNF à $\oplus$Pl-Mon-3CNF. En effet on sait que $\sharp$Pl-3CNF est $\sharp P$-complet par réduction parcimonieuse, voir [2]. Il suffit de retirer les variables niées en conservant la parité du nombre de solutions sans perdre la planarité.

Soit une formule $3CNF$ et x une variable, on remplace les occurrences négatives de x par x^*. On ajoute une nouvelle variable x' et les clauses $x \vee x^*$, $x \vee x'$ et $x' \vee x^*$ à F. Donc si x et x^* sont de valeurs opposées, alors x' est forcément vraie. x et x^* ne peuvent être toutes les deux fausses mais elles peuvent être toutes les deux vraies, alors x' prend n'importe quelle valeur. Donc on a une bijection entre les valuations satisfaisant la formule de départ et celles satisfaisant la formule modifiée quand x et x^* sont distinctes et les autres solutions qui sont en nombre pair ne modifient pas la parité.

On veut que la formule ainsi construite soit planaire, il faut faire uniquement des changements "locaux" pour en être sur. Il suffit pour cela d'introduire une nouvelle variable pour chaque occurrence d'une négation d'une variable. On peut alors dans le graphe planaire de départ ajouter les deux nouvelles variables et les trois nouvelles clauses au voisinage du sommet représentant la variable comme sur la Figure 3.1. □

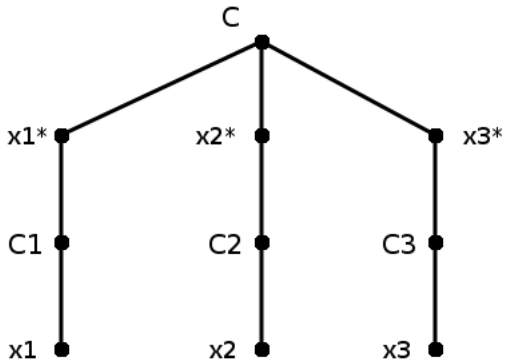

FIG. 3.2 – Le gadget pour la réduction de $\oplus Pl - Mon - 3CNF$ à $\oplus Pl - Rtw - Mon - 3CNF$

Proposition 3. $\oplus$PL-RTW-MON-3CNF *est* $\oplus P$*-complet.*

Démonstration. On procède par réduction de $\oplus$PL-MON-3CNF à $\oplus$PL-RTW-MON-3CNF. Soit ϕ une instance de $\oplus$PL-MON-3CNF et x une variable de ϕ intervenant dans $k > 2$ clauses. On va introduire les variables x_1, x_1^*, x_2, x_2^*, x_3 et x_3^*. Chacune de ces variables interviendra dans au plus $\lceil k/3 \rceil + 1$ clauses.

On divise les clauses dans lesquelles apparaissent x en trois parties et on le remplace par x_1, x_2 ou x_3 selon la partie. On ajoute les clauses $C_i = x_i \vee x_i^*$ pour $i = 1, 2, 3$ et $C = x_1^* \vee x_2^* \vee x_3^*$ en conservant la planarité comme montré dans la Figure 3.2. On va montrer que la parité du nombre de solutions n'est pas modifiée par cette transformation.

1. Si tous les x_i sont vrais à la fois, les x_i^* peuvent prendre toutes les valeurs sauf faux,faux,faux à cause de la clause C. On a donc 7 fois plus de solutions que quand x est vrai, ce qui ne modifie pas la parité de ce nombre de solutions.
2. Si tous les x_i sont faux alors tous les x_i^* sont vrais à cause des clauses C_i. On a donc le même nombre de solutions que quand x est faux.
3. Si on a au moins un x_i, supposons x_1, vrai et un x_j, supposons x_2, faux alors la valeur de x_1^* n'influe pas sur la satisfaction de la formule. On a dans ce cas un nombre de solutions pair ce qui n'influe pas sur la parité du nombre total de solutions.

La transformation décrite ne modifie ni la planarité, ni la monotonie, ni la parité du nombre de solution de la formule. En appliquant environ k fois pour chaque variable x apparaissant dans k clauses cette transformation on obtient une formule Read twice. On ne rajoute qu'un nombre linéaire de variables et de clauses donc on a bien une réduction en temps polynômial, ce qui montre la complétude du problème. □

On peut trouver une démonstration différente de ce théorème dans un article de Valiant [10] par réduction à un problème de couplage ou une démonstration proche pour un problème similaire [8].

3.3 Réductions holographiques

X-MATCHING

Théorème 7. PL-X-MATCHING *a une réduction holographique à* PerfMatch*, c'est à dire* Pl-X-matching $\in FP$.

Démonstration. Soit G le graphe planaire représentant une instance de X-MATCHING, ses sommets sont divisés en une bipartition (V_1, V_2). On va remplacer chaque sommet de V_1 par une porte génératrice comme celle de la Figure 2.1 de signature $(1, 1, 1, 0)$ selon la base $\mathbf{b_1}$. Comme il y a au plus deux arêtes vers un sommet de V_1, on peut les faire arriver sur les deux sorties de la porte génératrice qui remplacent le sommet.

On remplace chaque sommet de V_2 recevant k arêtes par une porte de reconnaissance à k entrées du type de la Figure 2.3 dont les poids w_i sont ceux des k arêtes reliées au sommet remplacé.

On va associer à chaque $x = x_1 \otimes \cdots \otimes x_k \in {\mathbf{b_1}}^k$ un ensemble d'arête et on va montrer que le terme associé à x dans le Holant est le poids du couplage (au sens de X-MATCHING) si cet ensemble est un couplage, 0 sinon. L'élément p de la base représente le fait de sélectionner une arête pour le couplage, et n de ne pas la sélectionner, c'est bien une bijection car on a exactement une sortie de porte génératrice par arête du graphe de départ.

Pour que cela soit un couplage il faut que chaque sommet soit saturé par au plus une arête. Or dès qu'une porte génératrice émet $p \otimes p$ le terme du Holant est nul. De plus, dès qu'une porte de reconnaissance B_i reçoit plus d'un p, $valR(B_i, \bar{x})$ est nul par la Proposition 1 donc le terme est nul. Toujours par la Proposition 1, si la porte B_i reçoit exactement un p de l'émetteur A_t, $valR(B_i, \bar{x}) = w$ où w est le poids de l'arête entre les sommets correspondant à B_i et A_t par construction du circuit de couplage. Enfin si la porte de reconnaissance ne reçoit aucun p, $valR(B_i, \bar{x}) = -(w_1 + \cdots + w_k)$ donc si un terme représente bien un couplage, sa valeur est celle du poids couplage au sens de X-MATCHING.

Le circuit de couplage est planaire donc par le Théorème 6, on peut calculer en temps polynômial son Holant et donc le X-MATCHING de G. □

Ce théorème serait vraiment intéressant si on pouvait remplacer le poids d'un couplage au sens de X-MATCHING, par le poids au sens classique c'est à dire remplacer $-(w_1 + \cdots + w_k)$ par 1. On calculerait alors le nombre de couplages d'un graphe planaire, un problème qui paraît plutôt être $\sharp P$-complet. On peut se demander si c'est possible au prix de contraintes plus fortes sur le graphe et/où dans un corps fini, on trouverait alors la valeur modulo la cardinalité du corps.

PL-RTW-MON-3CNF

Lemme 8. *On peut réaliser les signatures symétriques* $[1, 0, 1]$ *et* $[0, 1, 1, 1]$ *dans* $\mathbb{F}_7$.

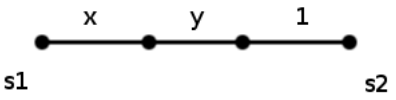

FIG. 3.3 – Une porte génératrice à deux sorties

Démonstration. La base qui sert à réaliser ces deux signatures simultanément est $\mathbf{b_2} = \{n = (1,6), p = (3,5)\}$. On trouve la preuve de ce lemme dans un article de Cai [15] mais il avait été précédemment prouvé par Valiant [10] avec des bases de taille 2. On peut réaliser la signature standard $(3,0,0,5)$ avec la porte génératrice de la Figure 3.3 dont les sommets s_1 et s_2 sont des sorties, en posant $x = 3$ et $y = 5$. Si on calcule $n \otimes n + p \otimes p$ on obtient modulo 7 $(3,0,0,5)$ donc on réalise bien la signature $[1,0,1]$ selon la base $\mathbf{b_2}$ dans $\mathbb{F}_7$.

On peut réaliser la signature standard $u = [0,3,0,5]$ avec la Figure 2.4 à 3 entrées. Il faut prendre pour cela $a = b = c = \frac{3}{5}$ et $t = 5$. On considère cette porte comme une porte de reconnaissance, pour calculer sa signature selon $\mathbf{b_2}$ il faut calculer les produits scalaires de la signature standard avec les éléments de $\mathbf{b_2}^{\otimes 3}$. On obtient par exemple $< u, n \otimes n \otimes n >= 3.3.n_0.(n_1)^2 + 5.(n_1)^3 = 0 \pmod 7$. En effectuant tout les calculs on trouve la signature symétrique $[0,1,1,1]$ selon la base $\mathbf{b_2}$ dans $\mathbb{F}_7$. □

Cai montre [15] que ces signatures peuvent être réalisées simultanément uniquement dans $\mathbb{F}_7$.

Théorème 8. $\sharp_7$PL-RTW-MON-3CNF *a une réduction holographique à* PerfMatch*, c'est à dire* $\sharp_7$PL-RTW-MON-3CNF $\in FP$.

Démonstration. Soit G le graphe planaire qui représente une formule PL-RTW-MON-3CNF, on a d'un coté les variables et de l'autre les clauses qui sont reliées par une arête si et seulement si la variable apparaît dans la clause. Les sommets représentant les variables sont saturés par exactement deux arêtes, alors que ceux représentant des clauses le sont par trois arêtes à cause des propriétés des formules considérées. Une clause est vrai ssi toutes ses variables ne prennent pas la valeur faux car toutes les variables apparaissent sous forme positive. Une variable doit être considérée comme simultanément vraie (ou fausse) dans les deux clauses ou elle apparaît.

On remplace donc les sommets de variables par une porte de couplage génératrice ayant deux sorties de signature symétrique $[1,0,1]$. On remplace les portes représentant les clauses par des portes de reconnaissance avec 3 entrées de signature symétrique $[0,1,1,1]$. On conserve les arêtes entre clauses et variables et on leur affecte un poids 1, on a alors bien un circuit de couplage planaire car le graphe G était planaire.

On va montrer que le Holant de ce circuit est égal au nombre d'assignation de variables satisfaisant la formule. Un élément $x = x_1 \otimes \cdots \otimes x_k \in (\mathbf{b}^2)^{\otimes k}$ représente une distribution de valeur de vérité : la variable représentée par la $i^{\text{ème}}$ porte génératrice est vraie ssi $x_i = p \otimes p$ et fausse si $x_i = n \otimes p$. Les x ne correspondant pas à une distribution

de valeur de vérité, c'est à dire contenant des $n \otimes p$ ou $p \otimes n$, ne contribuent pas au Holant. Le terme est non nul et vaut 1 si chaque porte de reconnaissance est reliée à au moins une porte génératrice représentant une variable vraie ($p \otimes p$). Or cela correspond à la satisfaction de toutes les clauses c'est à dire que la distribution de valeur de vérité correspondant à x satisfait la formule. Le Holant compte donc le nombre distributions satisfaisant la formule.

Ces signatures sont réalisées dans $\mathbb{F}_7$, donc on obtient seulement le nombre des solutions modulo 7 quand on calcule le Holant. Enfin en appliquant le Théorème 6, on peut calculer en temps polynômial le Holant du circuit de couplage planaire construit. □

Le problème ♯Pl-Rtw-Mon-3CNF est $\sharp P$-complet pour réduction Turing. Si il l'était pour réduction parcimonieuse, ce résultat impliquerait que $\sharp_7 P = FP$!

Pl-Node-Bipartition

Pour ce problème on va travailler dans la base $\mathbf{b_3} = \{(1,1),(-1,1)\}$. On veut réaliser la signature $[0,1,0]$ pour une porte génératrice et les signatures $[x,y,x]$ et $[x,y,y,x]$ pour des portes de reconnaissances. On peut trouver la preuve de la réalisabilité de ces signatures dans un article de Cai [11] ainsi qu'une caractérisation complète des signatures réalisables dans $\mathbf{b_2}$.

Ce problème est intéressant à deux titres :

1. il n'est pas ad hoc et peut être utilisé en pratique dans sa forme générale pour optimiser l'assignation de tâche par exemple
2. on utilise la réduction holographique de manière indirecte avec une interpolation ce qui peut ouvrir la voie à de nouvelles réductions

Théorème 9. Pl-Node-Bipartition *a une réduction holographique à PerfMatch, c'est à dire* Pl-Node-Bipartition *est dans* FP.

Démonstration. Soit un graphe G instance de Pl-Node-Bipartition. Ses sommets de degré 1 ne joue pas de rôle dans le fait de trouver une bipartition donc on suppose que le graphe n'en a pas. On va remplacer chaque arête du graphe par une porte génératrice de signature $[0,1,0]$. De même on remplace chaque sommet du graphe par une porte de reconnaissance de signature $[y,1,y]$ si il est de degré 2 et $[y,1,1,y]$ si il est de degré 3. On relie ensuite les sorties des gadgets des arêtes aux entrées des gadgets des sommets qu'elle rejoignent dans G et on obtient un circuit de couplage planaire car G était planaire.

Un élément $\bar{x} = \bar{x_1} \otimes \cdots \otimes \bar{x_k}$ image d'un élément x de la base va être associé à une partition en trois de l'ensemble des sommets. Les sommets dont les portes associées ont un $x_i = n \otimes n$ ou $n \otimes n \otimes n$ constituent l'ensemble A_1, Les sommets dont les portes associées ont un $x_i = p \otimes p$ ou $p \otimes p \otimes p$ constituent l'ensemble A_2 et le reste constitue l'ensemble A_3.

Les seuls x qui contribuent au Holant sont ceux tels que le graphe induit en retirant les sommets de A_3 est biparti d'ensemble indépendant A_1 et A_2. En effet pour qu'un terme du Holant soit non nul il faut que chaque porte génératrice émette $n \otimes p$ ou $p \otimes n$, or ces porte représentent les arêtes qui doivent donc toujours aller d'un sommet de A_1 à

un sommet de A_2. Le terme associé à un graphe biparti qui a l sommets contribue de y^l au Holant.

Il faut remarquer qu'un même graphe biparti peut être représenté par plusieurs x différents, qui contribueront néanmoins chaque fois pour y^l au Holant. Si la représentation n'est pas injective comme on vient de le remarquer, elle est surjective, c'est à dire que tout graphe biparti induit par l'oubli d'un certain nombre de sommet peut être décrit par un x dont la contribution au Holant est non nulle. Le calcul du Holant nous donne ici un polynôme en y et le degré de ce polynôme est la taille maximale d'un graphe induit biparti.

On peut calculer les coefficients du polynômes par interpolation c'est à dire en calculant ses valeurs sur n points où n est le nombre de sommets du graphe de départ et donc le degré maximal du polynôme. L'évaluation en un point est le calcul du Holant pour un certain y, donc du PerfMatch d'un graphe planaire ce qui se fait en temps polynômial. Le calcul des coefficients à partir des valeurs en les points est lui aussi en temps polynômial donc on a montré Pl-Node-Bipartition est dans FP. □

♯ Exact3Cover

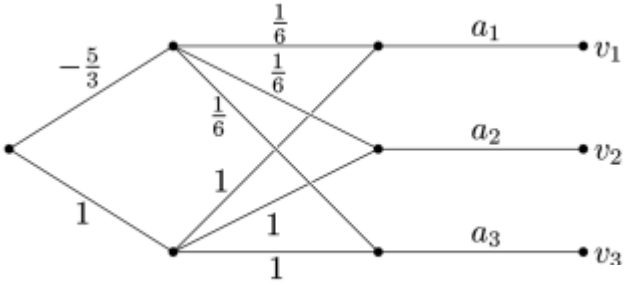

Fig. 3.4 – Une porte génératrice bien compliquée

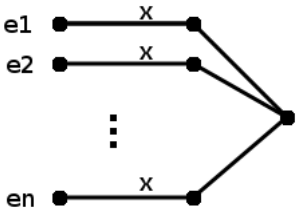

Fig. 3.5 – Une porte très simple

Ici je revisite la preuve de Jerrum [3] de complétude du Permanent pour $\sharp P$. Sa première étape consiste à réduire ♯ Exact3Cover au problème de calculer les couplages avec certains poids rationnels sur les arêtes. On va voir que cela revient à faire une réduction holographique vers MatchSum.

Lemme 9. *On peut réaliser les signatures standards* $[0, x, 0 \ldots, 0]$ *(avec* n *entrées) et* $\left[\frac{1}{3}, 0, 0, \frac{1}{3}\right]$ *avec des portes à noeuds superflus.*

Démonstration. La porte de la Figure 3.4 (directement prise dans le livre de Jerrum) doit être comprise comme ayant ses sommets de sortie à gauche des arêtes a_i, les arêtes a_i étant les arêtes de liaison entre reconnaisseur et générateur. Par ailleurs tous les sommets qui ne sont pas de sortie sont superflus. Si on calcule alors la signature standard de cette porte on trouve bien $\left[\frac{1}{3}, 0, 0, \frac{1}{3}\right]$.

La signature standard $[0, x, 0 \ldots, 0]$ est réalisée par la porte de reconnaissance 3.5, les sommets e_i étant les entrées. □

Si on arrivait à faire cette réduction grâce à des gadgets sans sommets superflus, on aurait directement une preuve du caractère $\sharp P$-complet du problème PerfMatch par une réduction parcimonieuse. On peut montrer qu'il n'y a pas de porte plus simple, c'est à dire avec moins de sommets, pour la signature standard $\left[\frac{1}{3}, 0, 0, \frac{1}{3}\right]$. On peut par contre se demander si on peut la réaliser avec des poids plus simples, ou si on peut trouver une base dans laquelle la signature se réalise plus économiquement. Enfin on peut vouloir utiliser des gadgets planaires, les deux proposés le sont mais le premier ne peut pas avoir ses sommets de sortie sur la face extérieure ce qui pose un problème si on veut réaliser un circuit planaire.

Théorème 10. *Il existe une réduction holographique de* ♯ Exact3Cover *à MatchSum.*

Démonstration. Soit une instance de ♯ Exact3Cover avec E l'ensemble d'élément et T celui des triplets de E. On créé un circuit de couplage en associant à chaque triplet une porte de signature $\left[\frac{1}{3}, 0, 0, \frac{1}{3}\right]$ et à chaque élément une porte de signature $\left[0, 3^k, 0 \ldots, 0\right]$ avec j entrées si l'élément apparaît dans j triplets et que k est le cardinal de E. On relie les gadgets des triplets aux gadget des éléments qu'ils contiennent et on décide que les portes de triplets sont des portes génératrices et les portes d'éléments sont des portes de reconnaissance ce qui ne change rien.

On va montrer que le Holant de ce circuit évalué dans la base standard $\mathbf{b_0} = \{n, p\}$ est la valeur de ♯ Exact3Cover. On considère un élément $x = x_1 \otimes \cdots \otimes x_{3l} \in {\mathbf{b_0}}^{3l}$ avec l le cardinal de l'ensemble T. Les x qui contribuent au Holant sont ceux tels que $x_{3i} \otimes x_{3i+1} \otimes x_{3i+2} = n \otimes n \otimes n$ ou $p \otimes p \otimes p$, on peut considérer que la porte de sortie génère tous les éléments du triplet ou aucun. Pour que le terme ne soit pas nul il faut que chaque porte de reconnaissance reçoive un unique n, c'est à dire qu'on ne choisisse pas un élément deux fois ou aucune fois. Donc un élément x qui donne naissance à un terme non nul du Holant décrit un sous-ensemble de T qui recouvre E sans doublon. Enfin la valeur de chacun de ces termes non nuls est $3^k.\frac{1}{3^k} = 1$ donc on a bien montré le théorème. □

Corollaire 6. *MatchSum est $\sharp P$-dur car* ♯ Exact3Cover *est $\sharp P$-complet pour les réductions parcimonieuses (on le montre en y réduisant $\sharp 3SAT$).*

3.4 Les bases de taille 1 suffisent

On énonce ici le résultat de l'article de Cai, The Power of Dimensionality Resolved [14] qui montre qu'on a besoin de base de taille 1 uniquement pour les algorithmes holographiques. Il introduit pour cela le concept de base et de signature dégénérée qui sont les seuls obstacles au théorème principal de l'article que je cite ci-dessous.

Théorème 11. *Soient $G_1, \ldots, G_s$ des signatures de générateurs et $R_1, \ldots, R_t$ des signatures de reconnaisseurs simultanément réalisables dans la même base $\mathbf{b}$ de taille quelconque. Si toutes les signatures des générateurs ne sont pas dégénérées alors il existe une base $\hat{\mathbf{b}}$ de taille 1 facilement calculable à partir de $\mathbf{b}$ dans laquelle toutes ces signatures sont simultanément réalisables.*

Comme les algorithmes holographiques utilisant uniquement des générateurs dégénérés sont triviaux, on peut toujours se ramener au cas de base de taille 1.

3.5 Caractérisation des signatures réalisables

On considère uniquement les bases de taille 1 grâce au résultat du paragraphe précédent ce qui simplifie le problème. Il existe une caractérisation des signatures symétriques réalisables en une base quelconque par des portes planaires. Néanmoins cette caractérisation utilise celle des *matchgate*, des portes dont la signature est construite à partir du Pfaffien et non du PerfMatch. On représente leur signature par une matrice appelée *naked character matrix*. Ces portes ont l'avantage de ne pas être planaire ce qui rends leur caractérisation algébrique plus facile. Les identités qui caractérisent entièrement leur *naked character matrix* sont appelées les identités utiles de Grassmann-Plücker ou identités de porte de couplage. Grâce au lemme suivant on transfère la caractérisation des *matchgate* aux portes de couplage.

Lemme 10. *Étant donné une matchgate de naked character matrix B, il existe une porte de couplage planaire de signature B.*

La preuve marche grâce à un gadget qui est capable de simuler le croisement de deux arêtes. La réciproque est aussi vrai et se prouve par simple changement de poids du graphe.

On peut alors caractériser les signatures symétriques réalisables par des équations polynômiales qui dépendent de la base dans laquelle on veut les réaliser. Donc l'ensemble des bases dans lesquelles on peut réaliser une signature est une variété. Si on veut savoir si plusieurs signatures sont réalisables simultanément il suffit de calculer si l'intersection de ces variétés est non vide, ce qui se fait en temps polynômial. Le problème de trouver une base dans laquelle sont réalisées plusieurs signatures simultanément s'appelle le Simultaneous Realizability Problem (SRP).

Théorème 12. *Il y a un algorithme polynômial pour* SRP.

Ces théorèmes et remarques sont tirés de l'article Holographic Algorithms : From Art to Science de Cai [13]. L'intérêt de ce résultat est de pouvoir construire des algorithmes holographiques en ne s'intéressant qu'a modéliser le problème combinatoire avec des signatures symétriques, l'existence de porte de couplage réalisant ces signatures simultanément est ensuite automatiquement décidée.

3.6 Calcul de parité

Dans cette section j'essaie d'adapter la méthode de Valiant à d'autres problèmes en choisissant un problème cible différent mais en utilisant toujours le Holant et le Théorème 6.

On a déjà vu qu'on sait calculer facilement le Permanent d'un graphe modulo 2. Or on sait aussi que le PerfMatch d'un graphe biparti peut s'exprimer par un Permanent. Donc en utilisant le Théorème 6 on obtient que le Holant d'un graphe biparti est calculable modulo 2 en temps polynômial.

A partir de maintenant une porte génératrice (respectivement de reconnaissance) bipartie signifiera qu'on peut découper le graphe en deux partitions indépendantes (pas nécessairement de tailles égales) dont toutes les sorties (respectivement les entrées) sont dans la même partition. On pourrais assouplir cette définition de porte bipartie en oubliant la condition sur les entrées et sorties, mais alors pour avoir un circuit biparti il faudrait ajouter des contraintes dans la manière de relier les portes.

Lemme 11. *Un circuit de couplage dont toutes les portes génératrices et de reconnaissances sont biparties est biparti.*

Démonstration. Soient $\{E_1, \ldots, E_g\}$ les portes génératrices et $\{R_1, \ldots, R_l\}$ les portes de reconnaissances. On note $E_i = E_i^1 \cup E_i^2$ (respectivement $R_i = R_i^1 \cup R_i^2$) la décomposition en deux partitions des sommets de E_i (respectivement de R_i) et on suppose que les sorties sont dans E_i^1 (respectivement les entrées dans R_i^1).

Alors on peut partitionner le circuit de couplage en $A_1 = \left(\bigcup_{i=1}^{g} E_i^1\right) \cup \left(\bigcup_{i=1}^{l} R_i^2\right)$ et $A_2 = \left(\bigcup_{i=1}^{g} E_i^2\right) \cup \left(\bigcup_{i=1}^{l} R_i^1\right)$. Par définition les arêtes du graphe sont dans $E_i^1 \times E_i^2$, $R_j^1 \times R_j^2$ et $E_i^1 \times R_j^2$ donc A_1 et A_2 sont bien indépendants et le graphe est donc biparti. □

Remarque 13. La porte présentée dans l'exemple 2.3 est bipartie.

Remarque 14. On peut réaliser la signature standard $(0, x, y, 0)$ pour tout x et y grâce à la porte génératrice bipartie de la Figure 3.6. Sa signature par rapport à la base $\mathbf{b_1}$ est $(0, x, y, x + y)$.

L'idée au départ était de trouver une manière mécanique de transformer une porte non bipartie en une porte ayant la même signature et bipartie, en sacrifiant si il le faut la planarité. Cela n'est pas possible pour la raison suivante :

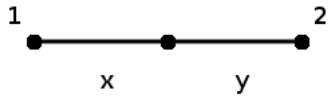

FIG. 3.6 – Une porte bipartie avec deux sorties numérotées 1 et 2

Théorème 13 (Expressivité des portes biparties)**.** *La signature standard d'une porte bipartie vérifie qu'il existe un entier k tel que les seuls coefficients non nuls de la signature sont ceux en $i^{ème}$ position avec $wt(i) = k$.*

Démonstration. Soit une porte bipartie, qu'on supposera génératrice, partitionnée en V_1 et V_2. Tout couplage parfait de cette porte sera un sous-ensemble des arêtes entre V_1 et V_2 puisque ces ensembles sont indépendants. Donc le PerfMatch d'un tel graphe est non nul uniquement si les deux ensembles V_1 et V_2 sont de même cardinal. Si la partition qui contient les sorties, supposons V_1 est de cardinal inférieur à celle qui ne les contient pas alors la signature est nulle. Si $|V_1| - |V2| = k \geq 0$, alors si on retire un nombre différent de k sorties au graphe, le graphe induit aura un Perfmatch nul, toujours pour des raisons de cardinalité des partitions, ce qui montre le théorème. □

Donc on ne peut pas automatiquement trouver une porte bipartie qui réalise une signature quand une porte générale la réalise. Pire, dans le cas de X-MATCHING, la porte de reconnaissance est bipartie mais on ne peut pas réaliser $(-1, 0, 0, 1)$ la signature standard de la porte génératrice.

Remarque 15. On pourrait espérer améliorer la situation en se permettant des noeuds superflus, ce qui permet d'obtenir des signatures intéressantes, mais malheureusement le polynôme MatchSum n'est lui à priori pas plus facile à calculer dans $\mathbb{F}_2$.

On peut par exemple construire un graphe biparti dont le MatchSum est la valeur de X-MATCHING. Mais bien qu'on puisse calculer facilement le MatchSum à partir du Perfmatch, on ne peut pas calculer la parité de MatchSum à partir de la parité de Perfmatch.

3.7 Quelques idées pour la suite

Pour finir une petite liste de questions ouvertes et de pistes pour tirer le maximum de la théorie des algorithmes holographiques.

1. Généraliser la caractérisation des signatures symétriques réalisables à toutes les signatures.
2. S'intéresser à l'expressivité du Holant, tout les problèmes peuvent-ils être exprimés par cet objet ? Cela parait difficile pour des problèmes non locaux comme ♯HAMILTONIANPATH. Si c'était pourtant le cas ♯PERFECTMATCHING serait ♯P-complet pour réduction parcimonieuse.

3. Trouver de nouveaux exemples de réduction holographique.
4. Utiliser le théorème du Holant pour montrer la dureté du problème cible plutôt que la facilité du problème qu'on réduit.
5. Pour calculer facilement les couplages parfaits dans un graphe il suffit qu'il admette une orientation Pfaffienne, les graphes planaires étant un cas particulier. Peut on réduire de nouveaux problèmes à des circuits de couplage non planaire mais ayant une orientation Pfaffienne ?
6. Identifier d'autres polynômes composés d'une somme exponentielle de terme mais calculable rapidement pour leur appliquer le même genre de démarche qu'au PerfMatch.
7. Se servir des réductions holographiques pour montrer que certains problèmes sont *Fixed Parameter tractable*.
8. Trouver une contrainte qui rend l'évaluation de MatchSum facile pour s'en servir comme cible d'une réduction holographique.
9. Trouver un problème de parité qu'on peut résoudre en temps polynômial grâce à une réduction vers le PerfMatch d'un graphe biparti.
10. Réduire des problèmes durs au MatchSum d'un graphe planaire.

Bibliographie

[1] Carsten Damm, Markus Holzer, and Pierre McKenzie. The complexity of tensor calculus. *Computational Complexity*, 11(1-2) :54–89, 2002.

[2] Harry B. Hunt III, Madhav V. Marathe, Venkatesh Radhakrishnan, and Richard Edwin Stearns. The complexity of planar counting problems. *SIAM J. Comput.*, 27(4) :1142–1167, 1998.

[3] M. Jerrum. *Sampling and Counting*. Birkhäuser, Basel, 2003.

[4] P.W. Kasteleyn. The statistics of dimers on a lattice. *Physica*, 27 :1209–1225, 1961.

[5] H.J.Ryser R.A.Brualdi. *Combinatorial Matrix Theory*. Cambridge University Press, Cambridge, 1991.

[6] Leslie G. Valiant. The complexity of computing the permanent. *Theor. Comput. Sci.*, 8 :189–201, 1979.

[7] Leslie G. Valiant. Quantum computers that can be simulated classically in polynomial time. In *STOC*, pages 114–123, 2001.

[8] Leslie G. Valiant. Completeness for parity problems. In *COCOON*, pages 1–8, 2005.

[9] Leslie G. Valiant. Holographic algorithms. *Electronic Colloquium on Computational Complexity (ECCC)*, (099), 2005.

[10] Leslie G. Valiant. Accidental algorthims. *focs*, 0 :509–517, 2006.

[11] Jin yi Cai and Vinay Choudhary. Some results on matchgates and holographic algorithms. In *ICALP (1)*, pages 703–714, 2006.

[12] Jin yi Cai and Pinyan Lu. Bases collapse in holographic algorithms. In *IEEE Conference on Computational Complexity*, pages 292–304, 2007.

[13] Jin yi Cai and Pinyan Lu. Holographic algorithms : from art to science. In *STOC*, pages 401–410, 2007.

[14] Jin yi Cai and Pinyan Lu. Holographic algorithms : The power of dimensionality resolved. In *ICALP*, pages 631–642, 2007.

[15] Jin yi Cai and Pinyan Lu. On symmetric signatures in holographic algorithms. In *STACS*, pages 429–440, 2007.

[16] Jin yi Cai and Hong Zhu. Progress in computational complexity theory. *J. Comput. Sci. Technol.*, 20(6) :735–750, 2005.