N° d'ordre : 101-2003

THÈSE

présentée devant

L'UNIVERSITÉ CLAUDE BERNARD LYON 1

pour l'obtention du

DIPLÔME DE DOCTORAT

(arrêté du 30 mars 1992)

présentée et soutenue publiquement le 7 juillet 2003 par

Guillaume Malod

spécialité : mathématiques

Polynômes et coefficients

Au vu des rapports de

M. Peter Bürgisser,
M. Felipe Cucker,
M. Christian Michaux.

Devant la commission d'examen formée de

M. Gregory Cherlin, président du jury,
M. Fokko Du Cloux,
M. Miki Hermann,
M. Pascal Koiran,
M. Christian Michaux,
M. Bruno Poizat, directeur de thèse.

Remerciements

Je remercie d'abord mon directeur de thèse Bruno Poizat pour ses conseils et sa patience. J'ai également apprécié les remarques précises et détaillées des rapporteurs Felipe Cucker, Pascal Koiran et Christian Michaux. Je remercie par ailleurs Gregory Cherlin, Fokko Du Cloux et Miki Hermann d'avoir accepté de participer au jury.

Ce travail a bénéficié de mes discussions avec Hervé Fournier et Natacha Portier. Il a été élaboré dans une ambiance détendue grâce aux occupants du bureau 219 de l'institut Girard Desargues : Sébastien Foulle, Olivier Frécon, Camille Laurent-Gengoux, Ammar Mahmood et Boris Thibert.

A ma famille et à mes amis.

Table des matières

Remerciements i

Introduction 1

Chapitre 1. Calculs et polynômes 3
- 1. Polynômes 4
- 2. Calculs 4
- 3. Constantes 6
- 4. Complexité 6

Chapitre 2. Théorie de Valiant 9
- 1. Définitions 10
- 2. Le permanent 12
- 3. Précisions sur les conventions de Valiant 14
- 4. Caractérisation de la classe VP 16
- 5. Circuits fortement multiplicativement disjoints 23
- 6. La classe VQP 31
- 7. Classes de complexité potentielles 35

Chapitre 3. Théorie de Valiant sans constantes 37
- 1. Définitions 38
- 2. Le polynôme HC_n 39
- 3. Comparaison avec les classes de Valiant 44

Chapitre 4. Coefficients d'un polynôme : cas du degré borné 47
- 1. Position du problème 48
- 2. Le corps $\{0, 1\}$ 49
- 3. Polynômes de degré polynomialement borné 50

Chapitre 5. Coefficients d'un polynôme : cas du degré non borné 53
- 1. Classes de degré non borné 54
- 2. Un polynôme complet 55
- 3. Corps de caractéristique positive 64
- 4. Conséquence pour l'hypothèse de Valiant non bornée 68
- 5. Corps de caractéristique nulle 68

Chapitre 6. Dérivation simultanée de polynômes 71
- 1. Dérivée partielle itérée par rapport à une variable 73
- 2. Dérivation partielle par rapport à plusieurs variables 76

Conclusion 79

Bibliographie 81

Introduction

Avec les opérations usuelles $(+, -, \times)$, on calcule des polynômes. Les polynômes et leur calcul via des modèles simples, comme les circuits, se retrouvent à la base des questions de complexité algébrique, lorsqu'on ne calcule plus sur les booléens mais directement sur les éléments d'un corps.

La représentation d'un polynôme par un circuit peut être bien plus compacte que la donnée de la liste des coefficients de ses monômes, ou même de celle des termes de son développement. Le déterminant d'une matrice de taille n, par exemple, est calculable par un circuit de taille polynomiale en n, mais comporte un nombre exponentiel de monômes. Les problèmes naturels qui se posent concernent l'effet d'opérations mathématiques sur la taille des circuits calculant des polynômes. Ainsi ont été étudiés le calcul du plus grand diviseur commun de deux polynômes et le test d'irréducibilité.

Nous nous intéressons au passage d'un polynôme à sa fonction coefficient et réciproquement, ainsi qu'au calcul de dérivées partielles itérées. Nous serons amenés à utiliser le cadre de la théorie de Valiant, qui définit un analogue algébrique de la classe P, la classe des suites de polynômes VP, considérées comme facilement calculables, parmi les suites de polynômes facilement descriptibles de la classe VNP.

Dans le premier chapitre nous détaillons le cadre de notre étude, en précisant les modèles de calcul employés et les notions de complexité mises en jeu.

Nous présentons brièvement au deuxième chapitre la théorie de Valiant classique. Nous introduisons alors la notion de circuit multiplicativement disjoint afin de donner une nouvelle caractérisation de la classe VP (proposition 1). Nous illustrons cette caractérisation en donnant une preuve simplifiée de l'égalité entre les classes VNP et $\mathrm{VNP_e}$ et nous étudions quelques-unes des perspectives que cette notion engendre. En particulier, la disjonction des multiplications s'applique aussi à la classe VQP des suites de polynômes de complexité quasi-polynomialement bornée. Nous en déduisons une preuve simple de la VQP-complétude du déterminant et répondons à une conjecture de Bürgisser en donnant d'autres polynômes VQP-complets (théorème 5 et corollaire 2).

Le troisième chapitre est consacré à l'exposé d'une version plus stricte de la théorie de Valiant, où l'on ne s'autorise pas de constantes arbitraires et que nous utiliserons afin de bien mettre en valeur les calculs nécessaires pour passer d'un polynôme à sa fonction coefficient. Nous démontrons les résultats essentiels dans ce cadre, en profitant du travail effectué au chapitre précédent, notamment la complétude du hamiltonien, que nous choisissons de préférence au permanent afin que les propriétés démontrées soient valables en toute caractéristique.

Le quatrième chapitre aborde enfin les questions qui nous préoccupent. Nous posons le problème et montrons que le cadre de la théorie de Valiant stricte et le travail effectué au troisième chapitre permettent d'obtenir rapidement des résultats pour les polynômes de degré polynomialement borné : d'une part que la classe VNP^0 est stable par passage à la fonction coefficient et réciproquement (proposition 2), d'autre part que supposer que ce résultat est vrai pour la classe VP^0 est équivalent à affirmer que $\mathrm{VP}^0 = \mathrm{VNP}^0$ (théorème 8).

Nous tentons au cinquième chapitre d'étendre ces résultats au cas des polynômes de degré non borné. Nous montrons, en adoptant une démarche similaire au cas borné, que le problème est essentiellement celui du calcul rapide de gros coefficients binomiaux. Deux cas se présentent alors : sur les corps de caractéristique positive nous parvenons à calculer rapidement et obtenons des résultats similaires à ceux du quatrième chapitre (proposition 5 et théorème 10), ainsi qu'un résultat intéressant sur les rapports entre classes de degré borné et non-borné (théorème 11) ; sur les corps de caractéristique nulle, nous constatons que le problème revient alors exactement à calculer rapidement ces gros coefficients binomiaux, et que cela aurait pour conséquence un calcul rapide de la factorielle.

Enfin dans le sixième chapitre nous étudions l'effet de la dérivation sur les circuits calculant des polynômes. Nous montrons d'abord que ce problème est lié aux questions soulevées auparavant (propositions 6 et 7). L'action de dérivées partielles itérées peut faire exploser la taille de la représentation de polynômes par des circuits. Nous retrouvons le résultat de Kaltofen qui montre que c'est le nombre de variables par rapport auxquelles on dérive qui a un effet néfaste, plus que l'ordre de dérivation, et nous montrons qu'il ne coûte pas beaucoup plus cher alors de calculer simultanément toutes les dérivées partielles jusqu'à un ordre donné (théorème 15).

CHAPITRE 1

Calculs et polynômes

Nous présentons dans ce court chapitre ce que nous voulons calculer, ainsi que les modèles de calcul et les mesures de complexité employées par la suite.

1. Polynômes

Nous nous intéressons aux polynômes à coefficients entiers en caractéristique fixée. Ces polynômes sont donc des polynômes abstraits, donnés par la suite des coefficients de leurs monômes. En caractéristique nulle, deux polynômes sont identiques si les deux suites sont égales. En caractéristique positive p, deux polynômes sont identiques si les deux suites sont égales modulo p. Il importe de distinguer cette notion de celle de fonction polynôme, qui correspond aux valeurs que prend un polynôme sur un corps. Deux polynômes identiques définissent la même fonction polynôme sur un corps quelconque, mais deux polynômes définissant la même fonction sur un corps ne sont pas forcément identiques. En caractéristique p, positive ou nulle, deux polynômes définissant la même fonction sur un sous-ensemble infini d'un corps de caractéristique p sont identiques.

2. Calculs

Pour définir la notion de calcul d'un polynôme, nous utilisons un modèle simple : le calcul par circuit ou de manière équivalente par *straight line program*, similaire au calcul par circuits pour les booléens et dont les définitions sont données ci-dessous. On pourra trouver des détails sur la définition d'un circuit booléen dans [**22**] et dans [**23**], et sur des circuits pour une structure arbitraire dans [**14**].

DÉFINITION 1. Un *circuit arithmétique* est la donnée d'un graphe orienté fini, sans cycle orienté, dont les noeuds sont de degré entrant 0 ou 2 et qui possède un unique noeud de degré sortant 0. Les noeuds de degré entrant 0 sont appelés *entrées* et étiquetés par une variable. Les autres noeuds, de degré entrant 2, sont étiquetés par $+$ ou $\times$. Le noeud de degré sortant 0 est appelé *sortie*. La taille d'un circuit est le nombre de noeuds qu'il contient, sa profondeur est la longueur maximale d'un chemin orienté allant d'une entrée à la sortie. Les noeuds d'un circuit sont souvent appelés *portes*.

DÉFINITION 2. Un *straight line program* (ou *SLP*) de taille t est la donnée ordonnée de t instructions, l'instruction i étant soit une variable, soit de la forme $(+, j, k)$ ou $(\times, j, k)$, où j et k sont des entiers strictement plus petits que i.

On définit inductivement le polynôme calculé par un circuit :

- pour une porte d'entrée, il s'agit de la variable qui l'étiquette.
- pour une porte étiquetée par $+$, recevant une flèche d'une porte calculant le polynôme f et une autre d'une porte calculant le polynôme g, c'est le polynôme $f+g$.
- pour une porte étiquetée par $\times$, recevant une flèche d'une porte calculant le polynôme f et une autre d'une porte calculant le polynôme g, c'est le polynôme $f \cdot g$.

La notion de polynôme calculé par un SLP se définit sans difficulté par induction sur la taille : on considère que les n variables occupent les n premières cases, une instruction suivante effectue une multiplication ou une addition en précisant l'adresse de ses arguments.

La *complexité de calcul* d'un polynôme est la plus petite taille d'un circuit (ou d'un SLP) le calculant. La taille définie ici, aussi bien pour les circuits que pour les SLP, est la taille totale : les variables d'entrée sont prises en compte dans le calcul de la taille. Si on ne les compte pas, on définit la *taille fine*, utilisée par exemple pour les SLP de [**5**], sans vraiment altérer les résultats que l'on démontre.

Une porte d'un circuit sera souvent notée par une lettre grecque minuscule et la définition du polynôme calculé est valable pour une porte interne du circuit. Le *sous-circuit* associé à la porte α d'un circuit C est le sous-graphe de C constitué des portes β telles qu'il existe un chemin orienté de β à α. Les instructions d'un SLP sont identifiées par l'entier donnant leur posistion dans l'ordre. On peut définir sans difficulté le polynôme calculé par une instruction donnée d'un SLP et le sous-programme associé à cette instruction.

Ces deux modèles sont équivalents dans la mesure où l'on peut passer d'un circuit à un SLP de même taille et réciproquement. Pour passer d'un SLP à un circuit il suffit de considérer le graphe ayant pour sommets les entiers $1, \ldots, t$, etiquetés par $+$, $\times$ ou une variable selon l'instruction, avec une arête de la porte i à la porte j si et seulement si l'instruction i est le numéro d'un des deux arguments de j. Notons qu'un circuit possède a priori une unique porte de sortie, ce qui n'est pas stipulé dans le cas d'un SLP. On peut facilement se ramener à ce cas en élagant les instructions qui ne jouent pas le rôle d'argument par la suite. Pour passer d'un circuit à un SLP, il faut numéroter les portes de 1 à t, de telle sorte que s'il y a une arête de la porte i à la porte j, i soit strictement inférieur à j. Il est toujours possible de trouver une telle numérotation, par exemple en numérotant d'abord les entrées, puis les portes qui ne reçoivent de flèches que des entrées, et ainsi de suite. Le SLP obtenu est la suite des instructions correspondant aux portes ainsi numérotées, dans l'ordre. Un circuit permet de définir la profondeur de manière plus naturelle, tandis qu'un SLP, dont les portes sont déjà ordonnées, se prête souvent mieux aux démonstrations par induction sur la taille. Nous utiliserons la notion la plus pratique selon le contexte.

Ces modèles représentent un calcul où l'on peut utiliser plusieurs fois un résultat intermédiaire. Il est parfois intéressant de s'imposer comme restriction que tout résultat intermédiaire ne peut être utilisé qu'une seule fois, c'est-à-dire que le degré sortant de chaque porte est inférieur ou égal à 1, ce qui se traduit par la définition suivante.

Définition 3. Un *terme arithmétique* est un circuit dont le graphe est un arbre.

3. Constantes

Pour l'instant nos circuits ne comportent pas de constantes et ne peuvent donc pas effectuer de soustractions. Un circuit calcule ainsi un polynôme en les variables d'entrée, dont les coefficients sont des entiers positifs. Un tel circuit est appelé *monotone.* Pour un circuit de taille t, chacun des coefficients du polynôme calculé est borné par 2^{2^t} et le degré total du polynôme est majoré par 2^t.

On peut ensuite considérer des circuits où une ou plusieurs variables sont remplacées par 0 ou 1. Un exemple simple est un circuit comportant une seule variable qui est remplacée par 1. Ce circuit *numérique* calcule alors un entier inférieur à 2^{2^t}, donc de taille (en bits) au plus 2^t. Le nombre de SLP de taille t étant borné par $2^{t+2t\log t}$, il n'est pas possible que chacun des 2^{2^t} entiers de taille 2^t soit calculable par un circuit de taille inférieure à t. Les problèmes liés au calcul de gros entiers joueront un rôle important par la suite.

On peut aussi autoriser les substitution de variables par les valeurs 0, 1 ou -1. On obtient alors des circuits capables d'effectuer des soustractions et de simuler les calculs booléens via les polynômes suivants :

$$\neg\epsilon \equiv (1-\epsilon), \quad \epsilon \vee \eta \equiv \epsilon + \eta - \epsilon \cdot \eta, \quad \epsilon \wedge \eta \equiv \epsilon \cdot \eta.$$

Un circuit de taille t calcule alors un polynôme dont les coefficients sont des entiers relatifs bornés en valeur absolue par 2^{2^t}.

On peut enfin choisir de permettre l'utilisation de n'importe quelle constante d'un corps de base donné. Un circuit calcule alors un polynôme a coefficients dans ce corps. C'est le choix qui est fait dans [**5**] et dans les travaux de Kaltofen. Les calculs peuvent alors parfois exploiter les propriétés algébriques de certains éléments, comme par exemple pour le calcul des coefficients du produit de deux polynômes avec une transformée de Fourier rapide.

4. Complexité

4.1. Complexité de calcul d'un polynôme.

Un circuit calcule un polynôme en un nombre fixé de variables. Comme nous l'avons dit, la taille d'un plus petit circuit calculant un polynôme donné est sa complexité. Evidemment cette complexité dépendra a priori des conventions adoptées pour les constantes. Nous n'introduisons pas dès à présent de notation particulière pour les différentes notions de complexité qui en découlent. Nous préciserons toujours les conventions adoptées lors de l'énoncé de chaque résultat.

4.2. Manipulation de circuits.

Certaines questions de complexité peuvent déjà se poser au niveau des polynômes et des circuits les calculant. La représentation des polynômes par circuits est compacte, au sens où un circuit représente souvent un calcul beaucoup plus rapide d'un polynôme que la somme de ses monômes. Par exemple, le déterminant d'une matrice carrée est un polynôme comportant un nombre factoriel de monômes, mais il peut être calculé par un circuit de taille polynomiale. Il est donc intéressant de pouvoir manipuler les polynômes sous la forme de circuits aussi bien que lorsqu'ils sont représentés comme somme de monômes. C'est le but de travaux comme ceux de Kaltofen (cf. [**10**]), qui cherchent à montrer que l'on peut obtenir des circuits de taille raisonnable dans certains cas (tester l'irréducibilité, calculer le plus grand diviseur commun ou la factorisation). Nous citons ici un résultat sur la dérivation qui illustre simplement notre propos.

LEMME 1. *Si un polynôme est calculable par un circuit de taille t, alors sa dérivée partielle par rapport à une variable est calculable par un circuit de taille $4t$.*

Ce résultat est facile à démontrer et il existe une forme plus forte et surprenante : on peut obtenir un circuit qui calcule *simultanément* les dérivées partielles par rapport à chacune des variables et qui est de taille inférieure à quatre fois la taille du circuit initial (cf. [**2, 12**]). L'effet de la dérivation en général et la question d'une dérivation simultanée à des ordres supérieurs seront étudiés plus en détails au chapitre 6.

4.3. Suites de polynômes.

Si l'on peut déjà se poser de nombreuses questions de complexité pour la manipulation des polynômes représentés par des circuits, d'autres problèmes intéressants se posent de manière plus naturelle pour les suites de polynômes. Considérons par exemple le calcul du déterminant de la matrice $(x_{i,j})$ de taille n. Le déterminant est un polynôme en les variables $x_{i,j}$. Ce que l'on considère en fait, lorsqu'on parle du calcul du déterminant d'une matrice et de sa complexité, c'est la croissance de la complexité de calcul du déterminant d'une matrice de taille n lorsque n augmente. Encore une fois, la notion de complexité utilisée, qui dépend des constantes autorisées, sera précisée dans les définitions.

DÉFINITION 4. Soit $f = (f_n)$ une suite de polynômes dont le nombre de variables est borné par un polynôme en n. La *complexité* de f est la suite (c_n), où c_n est la complexité de f_n.

4.4. Uniformité et non-uniformité.

Ce point de vue nous amène à parler de la notion d'uniformité. Les suites de polynômes apparaissent naturellement pour représenter un problème de calcul qui se pose pour des entrées dont la taille peut être arbitrairement grande. Dans des cas pratiques, les polynômes de la suite considérée appartiennent visiblement à une même famille : pour le déterminant, c'est la suite des polynômes calculant le déterminant d'une matrice de taille de plus en plus grande. Mais la définition du paragraphe précédent n'exclut pas que l'on puisse considérer des suites de polynômes (f_n) où f_n et f_m n'ont aucun rapport apparent pour n différent de m. En outre, cette définition n'exclut pas non plus que la suite de circuits qui calcule une suite de polynômes présente la même caractéristique : même si on considère une suite uniforme de polynômes comme celle associée au déterminant, la définition de la complexité ci-dessus accepte que le déterminant de matrices de tailles différentes soit calculé par des circuits sans aucune ressemblance.

Ces considérations ont entraîné la définition de suites *uniformes*, en imposant par exemple que la suite de circuits calculant une suite de polynômes soit engendrée par une machine de Turing. Les classes que nous considérons n'imposent pas cette contrainte. Nous acceptons la non-uniformité de la suite de circuits parce que l'uniformité n'apporte rien aux questions que nous nous posons : la considération de classes non-uniformes se rapproche des manipulations au niveau des circuits, puisque l'on s'intéresse à des opérations sur un circuit, sans se préoccuper des relations entre les circuits d'une suite. Par ailleurs nos résultats peuvent s'adapter facilement au contexte uniforme. Les suites que nous considérons sont en général uniformes ; par abus de langage, nous dirons souvent "le permanent" pour désigner la suite des polynômes calculant le permanent d'une matrice de taille croissante.

Les classes de Valiant, que nous définissons au chapitre 2, présentent un degré de non-uniformité supplémentaire, car elles permettent l'utilisation de constantes arbitraires pour chaque circuit de la suite. Notre point de vue, qui consiste à étudier les polynômes en caractéristique fixée mais indépendamment d'un corps de base, nous amènera à refuser la non-uniformité due aux constantes et à définir des classes plus strictes qui n'autorisent pas de constantes arbitraires dans les calculs (cf. chapitre 3).

CHAPITRE 2

Théorie de Valiant

Nous présentons ici les classes de complexité VP et VNP introduites par Valiant. Elles fournissent un cadre pour l'étude de la complexité de calcul des polynômes sur un corps. Après un rappel des définitions et résultats essentiels, nous donnons une nouvelle caractérisation de la classe VP qui fournit une preuve simple de l'égalité des classes VNP et VNP_e. Nous décrivons ensuite une caractérisation de la classe VQP qui permet de démontrer facilement la VQP-complétude du déterminant et d'autres familles de polynômes.

1. Définitions

La première classe veut intuitivement décrire les polynômes raisonnablement calculables, comme un parallèle à la classe P de calcul sur les booléens. C'est cependant une classe non-uniforme, où l'on peut en outre utiliser gratuitement des constantes arbitraires, ce qui la rend algorithmiquement peu réaliste, mais elle constitue une abstraction simple qui permet d'énoncer des résultats élégants.

Définition 5. Une suite de polynômes (f_n) appartient à la classe VP si le nombre de variables, le degré et la complexité de f_n sont bornés par un polynôme en n. Notons que chaque circuit de la suite calculant (f_n) peut utiliser des constantes du corps de base (indépendamment dans chaque circuit).

La classe suivante décrit des polynômes calculables par des circuits de taille exponentielle mais que l'on peut facilement décrire. Si la classe précédente se voulait le pendant de la classe P, celle-ci reflète la classe NP, d'où le nom un peu malheureux qui lui est donné. Nous appellerons *somme de Valiant* une somme sur des valeurs booléennes comme celle de la définition.

Définition 6. Une suite de polynômes (f_n) appartient à la classe VNP s'il existe une suite $(g_n(y_1, \dots, y_{v(n)}))$ appartenant à la classe VP telle que :

$$f_n(x_1, \dots, x_{u(n)}) = \sum_{\bar{\epsilon} \in \{0,1\}^{v(n)-u(n)}} g_n(x_1, \dots, x_{u(n)}, \bar{\epsilon}).$$

Comme en complexité classique, on introduit une notion de réduction entre deux suites de polynômes et donc une notion de complétude. La réduction est ici très stricte puisqu'elle correspond à une simple affectation de valeurs ou de variables aux variables du polynôme.

Définition 7. Un polynôme f est une *projection* d'un polynôme g si $f(\bar{x}) = g(a_1, \dots, a_m)$, où les a_i sont des éléments du corps de base ou des variables choisies parmi $x_1, \dots, x_n$.

Définition 8. Une suite (f_n) est une *p-projection* d'une suite (g_n) s'il existe une fonction $t(n)$ polynomialement bornée telle que pour tout n, f_n soit une projection de $g_{t(n)}$.

Définition 9. Une suite de polynômes (f_n) appartenant à VNP est VNP-complète si toute suite (g_n) appartenant à VNP est une p-projection de (f_n).

La question fondamentale, similaire à P $=$? NP pour les calculs booléens, est de savoir si les classes VP et VNP sont distinctes ou non. Comme on peut s'y attendre, les classes VP et VNP sont stables par p-projection, si bien que cette question revient à se demander si un problème VNP-complet donné (il en existe) appartient à VP.

Il est aussi utile ici de définir les classes $\mathrm{VP_e}$ et $\mathrm{VNP_e}$, analogues des classes précédentes lorsqu'on base la complexité sur les termes arithmétiques au lieu des circuits.

Définition 10. Une suite (f_n) de polynômes appartient à la classe $\mathrm{VP_e}$ s'il existe une suite (T_n) de termes arithmétiques telle que T_n calcule le polynôme f_n et la taille de T_n soit bornée par un polynôme en n. Notons que chaque terme T_n peut utiliser des constantes du corps de base.

Définition 11. Une suite (f_n) de polynômes appartient à la classe $\mathrm{VNP_e}$ s'il existe une suite $(g_n(y_1, \dots, y_{v(n)}))$ appartenant à la classe $\mathrm{VP_e}$ telle que :

$$f_n(x_1, \dots, x_{u(n)}) = \sum_{\bar{\epsilon} \in \{0,1\}^{v(n)-u(n)}} g_n(x_1, \dots, x_{u(n)}, \bar{\epsilon}).$$

La question de savoir si $\mathrm{VP_e} = \mathrm{VP}$ est ouverte, mais un des principaux théorèmes de Valiant, qui est un élément essentiel de la preuve de complétude du permanent, affirme que $\mathrm{VNP_e} = \mathrm{VNP}$. Ce résultat est curieusement similaire à l'équivalence des circuits et des termes sous un bloc de quantifications existentielles en complexité classique (cf. [**14**]). Nous en donnons une démonstration simplifiée à la section 4.

Nous introduisons ici une dernière classe, celle des suites de polynômes de complexité quasi-polynomialement bornée, ainsi qu'une notion de réduction associée, pour laquelle le déterminant est VQP-complet. Nous reparlerons de cette classe à la section 6.

DÉFINITION 12. Une fonction t de $\mathbb{N}$ dans $\mathbb{N}$ est *quasi-polynomialement bornée* s'il existe deux constantes a et b telle que $t(n)$ soit inférieure ou égale à $n^{a \cdot \log^b n}$ pour tout n supérieur ou égal à 2.

DÉFINITION 13. Une suite (f_n) de polynômes appartient à la classe VQP si le nombre de variables et le degré de f_n sont polynomialement bornés et si la complexité de f_n est quasi-polynomialement bornée. Notons que chaque circuit de la suite calculant (f_n) peut utiliser des constantes du corps de base.

DÉFINITION 14. Une suite (f_n) est une qp-*projection* d'une suite (g_n) s'il existe une fonction $t(n)$ quasi-polynomialement bornée telle que pour tout n, f_n soit une projection de $g_{t(n)}$.

2. Le permanent

La restriction sur le degré imposée par Valiant aux suites de polynômes qu'il considère est motivée a posteriori par la complétude d'un problème "naturel", à savoir le calcul du permanent :

$$\mathrm{per}_n(z_{i,j}) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} z_{i,\sigma(i)}$$

THÉORÈME 1. *La suite* (per_n) *est* VNP-*complète pour tout corps de caractéristique différente de* 2.

Notons qu'en caractéristique 2 le permanent et le déterminant se confondent et sont de complexité polynomiale. Le déterminant est en effet de complexité polynomiale en toute caractéristique, par exemple en utilisant les algorithmes sans divisions présentés dans [**13**] et dans [**20**]. Le théorème 1 revient à dire qu'on ne sait pas montrer que le permanent n'appartient pas à la classe VP. On a par contre des résultats si on restreint sévèrement le modèle de calcul.

THÉORÈME 2. *Le permanent n'est pas calculable par un circuit monotone de taille polynomiale.*

Ce résultat est démontré dans [**9**]. Cette propriété est renforcée par Sengupta et Venkateswaran ([**16**]), qui montrent que même un permanent dont les entrées valent 0 ou 1 nécessite un circuit monotone de taille au moins exponentielle.

Le permanent possède en outre certaines propriétés remarquables dont nous nous inspirerons pour nos démonstrations. Tout d'abord sa fonction coefficient par rapport à toutes ses variables, notion que nous définirons plus précisément au chapitre 4, est calculable par un circuit de taille et degré polynomialement bornés. Il s'agit du polynôme g, défini sur les variables $\epsilon_{i,j}$ pour i et j compris entre 1 et n inclus :

$$g(\bar{\epsilon}) = \left(\prod_{\substack{1 \leq i,j,k,l \leq n \\ i=k \text{ ssi } j \neq l}} (1 - \epsilon_{i,j}\epsilon_{k,l}) \right) \cdot \left(\prod_{i=1}^{n} \sum_{j=1}^{n} \epsilon_{i,j} \right)$$

Si on note $\bar{z}^{\bar{\epsilon}}$ le polynôme $\prod_{i,j} z_{i,j}^{\epsilon_{i,j}}$, c'est-à-dire le monôme où la variable $z_{i,j}$ apparaît si et seulement si $\epsilon_{i,j}$ vaut 1, le permanent s'écrit :

$$\operatorname{per}(z_{i,j}) = \sum_{\bar{\epsilon} \in \{0,1\}^{n^2}} g(\bar{\epsilon}) \ \bar{z}^{\bar{\epsilon}}.$$

Le polynôme $g(\bar{\epsilon})$ vaut ainsi 1 si la matrice $(\epsilon_{i,j})$ est une matrice de permutation et 0 sinon, car le premier facteur de g garantit qu'il y aura au plus un 1 par ligne et par colonne et le deuxième qu'il y aura au moins un 1 dans chaque ligne. $\bar{z}^{\bar{\epsilon}}$ calcule ensuite le monôme correspondant à la permutation définie par $\bar{\epsilon}$.

Par ailleurs, le permanent est le coefficient du monôme $y_1 \cdots y_n$ dans le développement du polynôme suivant (cf. [**8**]) :

$$f_n(\bar{y}, \bar{z}) = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} z_{i,j} y_j \right).$$

En effet, lorsqu'on développe ce produit, pour obtenir un terme en $y_1 \ldots y_n$, il faut choisir dans chaque facteur du produit un terme de la somme, donc associer à chaque i un j, de telle sorte que l'on obtienne en fin de compte tous les y_j, ce qui revient à choisir une permutation de $\{1, \ldots, n\}$. La suite (f_n) appartient clairement à la classe VP.

3. Précisions sur les conventions de Valiant

3.1. Degré formel.

La définition des classes de Valiant ci-dessus nécessite quelques précisions : on peut se demander quel est le degré que l'on borne. Il peut s'agir du degré du polynôme lui-même, du degré de la représentation canonique de la fonction polynôme associée, du degré du circuit calculant le polynôme, notion qui reste d'ailleurs à définir. Si on observe plus en détails les définitions de Valiant, on se rend compte que le degré qu'il borne est celui du polynôme calculé par le circuit. Ainsi, sur un corps fini, une suite de polynômes de degré croissant exponentiellement et calculable par une suite de circuits de taille polynomiale n'est pas dans VP bien que la suite de fonctions polynômes qu'elle définit soir représentable par une suite de polynômes de degré polynomialement borné. Par exemple, sur le corps à deux éléments $\{0, 1\}$, toute fonction en n variables se représente par un polynôme de degré n, mais il n'est pas clair qu'à toute suite (f_n) de P/poly corresponde une suite de polynômes (g_n) la représentant sur $\{0, 1\}$ et appartenant à VP.

La remarque suivante permet de rattacher la borne imposée sur le degré d'un polynôme au circuit le calculant.

Définition 15. Le *degré formel* d'un circuit est défini par induction : une constante est de degré 0, une variable de degré 1 ; pour une porte d'addition on prend le sup des degrés arrivant et pour une porte de multiplication on prend la somme.

Il est bien connu qu'on peut tronquer un polynôme à l'ordre d sans trop augmenter sa complexité (cf. [**5**]).

Lemme 2. *Soit C un circuit de taille t calculant le polynôme f ; il existe un circuit C' calculant le polynôme f tronqué à l'ordre d, de taille inférieure à $t(d+1)^2+d$ et de degré formel inférieur ou égal à d.*

Preuve. Soit donc C un circuit de taille t calculant f. On va représenter dans C' chacune des portes de C par un uple de $(d+1)$ portes correspondant aux composantes homogènes de degré 0 à d. La porte α est donc représentée par l'uple $(\alpha_0, \ldots, \alpha_d)$, où α_i est la composante homogène de degré i du polynôme calculé par la porte α. Une variable x est représentée par l'uple $(0, x, 0, \ldots, 0)$, une constante a par l'uple $(a, 0, \ldots, 0)$. Soit α une porte de C, recevant des flèches des portes β et γ. Le calcul de α_k se fait de la manière suivante :

- si α est une porte d'addition, $\alpha_k = \beta_k + \gamma_k$.
- si α est une porte de multiplication, $\alpha_k = \sum_{j=0}^{k} \beta_j \gamma_{k-j}$.

On montre facilement par induction que α_k calcule la composante homogène de degré k du polynôme calculé à la porte α de C. La taille est donc multipliée au pire par $(d+1)^2$, à cause des multiplications. Enfin il faut faire la somme des composantes homogènes à la fin du calcul, ce qui se fait en d opérations. ☐

Dire qu'un polynôme de degré réel polynomial est calculable par un circuit de taille polynomiale est alors équivalent à dire que ce polynôme est calculé par un circuit de taille polynomiale et de degré formel polynomial. On peut donc reprendre la définition de la classe VP et dire qu'une suite (f_n) de polynômes appartient à la classe VP si f_n est calculable par un circuit de taille et de degré formel polynomiaux.

3.2. Degré des constantes.

Il y a une inégalité de traitement dans la définition de Valiant entre les variables et les constantes. On ne considère que des polynômes de degré borné, par contre les calculs sur les constantes ne sont pas bridés. Cette asymétrie peu satisfaisante n'est qu'apparente, comme le montre le lemme suivant.

LEMME 3. *Soit $C(\bar{x}, \bar{a})$ un circuit de taille t et de degré formel d, il existe un circuit $C'(\bar{x}, \bar{y})$ et des constantes $\bar{b}$ tels que :*

- *$C(\bar{x}, \bar{a})$ et $C'(\bar{x}, \bar{b})$ calculent le même polynôme.*
- *$C'(\bar{x}, \bar{y})$ est de taille t et de degré formel inférieur ou égal à $d \cdot t$.*

Preuve. Considérons le circuit $C(\bar{x}, \bar{a})$ comme un SLP. Appelons instruction constante de C une instruction qui calcule un polynôme ne dépendant pas des variables $\bar{x}$. Définissons C' comme le SLP obtenu à partir de C en remplaçant les instructions constantes par de nouvelles variables z_i distinctes deux à deux.

Si l'instruction k de C n'est pas constante, nous allons montrer que le degré du polynôme calculé par l'instruction k de C' est de degré inférieur ou égal à k fois le degré du polynôme calculé par l'instruction k de C. Notons donc d_k le degré du noeud k de C et d'_k celui du noeud k de C' et montrons par récurrence que si d_k est différent de 0, alors d'_k est inférieur ou égal à $k \cdot d_k$.

Pour k égal à 1, la première instruction de C' est forcément une variable, donc de degré 1. La première instruction de C est la même variable et l'inégalité sur les degrés est vérifiée. Si la propriété est vraie pour toutes les instructions de position strictement inférieure à k, montrons qu'elle est vraie pour l'instruction k. Les cas suivants peuvent se présenter :

- cette instruction est une variable et l'inégalité est facilement vérifiable.
- cette instruction est une addition, dont les arguments ont pour position i et j respectivement :

  $$d'_k \;=\; \max(d'_i, d'_j) \;\leq\; \max(i \cdot d_i, j \cdot d_j) \;\leq\; \max(i, j) \cdot \max(d_i, d_j) \;\leq\; k \cdot d_k.$$

- cette instruction est une multiplication, dont les arguments ont pour position i et j respectivement, le polynôme calculé par l'une au moins des instructions i et j étant de degré non-nul (car si les deux sont de degré nul, le noeud k de C est aussi de degré nul). On a alors $d'_k = d'_i + d'_j$. Si les polynômes calculés en i et j sont tous deux de degré non-nul et en supposant que i est inférieur ou égal à j, cela donne :
$$d'_k \;\leq\; i \cdot d_i + j \cdot d_j \;\leq\; j \cdot (d_i + d_j) \;\leq\; k \cdot d_k.$$
Si le polynôme calculé en i est de degré nul, par exemple, alors l'instruction i a été remplacée par une variable dans C', ce qui donne :
$$d'_k \;\leq\; 1 + j \cdot d_j \;\leq\; (j+1) \cdot d_j \;\leq\; k \cdot d_k.$$

Il suffit enfin d'appliquer ce résultat au dernier noeud de C' pour voir qu'on obtient un SLP possédant les propriétés désirées, puis un circuit. ☐

On définit alors une nouvelle notion de degré pour un circuit.

Définition 16. Le *degré formel complet* d'un circuit est défini par induction : les constantes et les variables sont de degré 1 ; pour une porte d'addition on prend le sup des degrés arrivant et pour une porte de multiplication on prend la somme.

On peut donc définir la classe VP en ne considérant que les suites de polynômes calculables par une suite de circuits de taille polynomialement bornée, de degré formel complet polynomialement borné. Nous adopterons désormais ce point de vue. Les résultats énoncés dans les sections suivantes sont donc aussi valables pour des circuits sans constantes. Nous restons pour l'instant dans le cadre historique, mais nous utliserons le cadre sans constantes au chapitre3.

4. Caractérisation de la classe VP

Les réflexions précédentes ont permis de redéfinir la classe VP en ne mentionnant plus la borne sur le degré des polynômes, mais en exigeant juste que la suite de polynômes soit calculable par une suite de circuits dont la taille et le degré formel complet sont polynomialement bornés. Il serait encore plus satisfaisant d'avoir un modèle de calcul dont on borne juste la taille, c'est-à-dire qui capturerait bien la classe VP. Si les classes $\mathrm{VP_e}$ et VP étaient égales, le modèle des termes arithmétiques serait parfait car la classe $\mathrm{VP_e}$ est définie très simplement comme la classe des suites de polynômes calculables par une suite de termes de taille polynomialement bornée, le degré du polynôme calculé par un terme étant inférieur ou égal à sa taille. De plus le permanent est plus immédiatement complet pour la classe $\mathrm{VNP_e}$ que pour la classe VNP. La $\mathrm{VNP_e}$-complétude est d'ailleurs une étape de la preuve de VNP-complétude du permanent, l'autre étape étant l'égalité

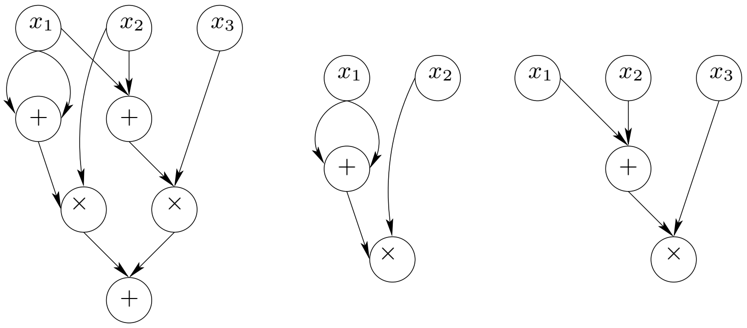


FIG. 1. Un circuit multiplicativement disjoint.

des classes $\mathrm{VNP_e}$ et VNP. Cependant il est peu probable que les classes $\mathrm{VP_e}$ et VP soient égales. Nous proposons ici de caractériser la classe VP via les circuits multiplicativement disjoints, dont la puissance de calcul est intermédiaire entre celle des termes arithmétiques et celle des circuits.

DÉFINITION 17. Soit α une porte d'addition ou de multiplication, β et γ les portes dont α reçoit une flèche, α est *disjointe* si les sous-circuits associés à β et γ sont disjoints.

DÉFINITION 18. Un circuit est *multiplicativement disjoint* si toutes ses portes de multiplication sont disjointes.

Un circuit est un terme arithmétique si et seulement si toutes ses portes sont disjointes. Un circuit multiplicativement disjoint peut être vu comme un terme pour les multiplications. C'est aussi un moyen de controler le degré du polynôme calculé par un circuit, un peu dans l'esprit des SLP à multiplications retardées utilisés dans [**1**] pour caractériser la classe $\sharp$P. Le circuit de la figure 1 est multiplicativement disjoint, comme le montre la représentation des deux portes de multiplication et de leurs sous-circuits disjoints. Nous allons montrer que cette notion permet de caractériser la classe VP.

PROPOSITION 1. Une suite de polynômes (f_n) appartient à la classe VP si et seulement si il existe une suite (C_n) de circuits multiplicativement disjoints, de taille polynomialement bornée, telle que C_n calcule le polynôme f_n.

Cette proposition est une conséquence immédiate des lemmes 4 et 5. La preuve du deuxième lemme est due à Natacha Portier.

LEMME 4. *Soit C un circuit multiplicativement disjoint de taille t, le degré formel complet de C est inférieur ou égal à t.*

Preuve. Ceci se montre par induction sur la taille. C'est évident pour un circuit de taille 1. Si c'est vrai pour tout circuit de taille strictement inférieure à t, montrons que c'est vrai pour un circuit de taille t. Soit γ la porte de sortie, qui reçoit des flèches des portes α et β. Si γ est une porte d'addition, le degré des polynômes calculé par α et β est inférieur ou égal à (t-1), donc le degré du polynôme calculé par γ est bien inférieur à t. Si γ est une porte de multiplication, les sous-circuits correspondant aux portes α et β sont disjoints, de taille t_α et t_β respectivement. Les degrés des polynômes que ces portes calculent sont par hypothèse d'induction inférieurs ou égaux à t_α et t_β respectivement. Le degré du polynôme calculé par γ est $t_\alpha + t_\beta$, ce qui est bien inférieur à la taille $t = t_\alpha + t_\beta + 1$ du circuit. □

Lemme 5. *Soit C un circuit de taille t et de degré formel complet d, il existe un circuit multiplicativement disjoint C', calculant le même polynôme que C et de taille inférieure ou égale à dt.*

Preuve. Pour cette démonstration, nous considérons des circuits qui peuvent éventuellement avoir plusieurs sorties, c'est-à-dire comportant plusieurs noeuds de degré sortant 0.

Nous construisons une suite de circuits mutliplicativement disjoints C_f, avec f compris entre 1 et d inclus, telle que, pour toute porte α de C de degré e inférieur ou égal à f :

- C_f contient des portes $\alpha_1, \dots, \alpha_{d+1-e}$ calculant dans C_f le même polynôme que α dans C ; la porte α_k est appelée clone de α d'indice k.
- les portes du sous-circuit de C_f associé au clone α_k sont des clones d'indice compris entre k et $k + e - 1$ inclus.

Le circuit C_1 est constitué de d copies du sous-circuit de C obtenu en ne gardant que les portes de degré formel complet 1. Il ne comporte donc pas de portes de multiplication et est bien multiplicativement disjoint. Chaque porte α de C de degré 1 est clonée d fois, et les portes du sous-circuit associé à une porte α_k sont des clones d'indice $k = k + 1 - 1$. Les hypothèses précédentes sont donc vérifiées.

Supposons qu'on ait construit le circuit C_{e-1}. Nous commençons par ajouter les portes de mutliplication. Soit α une porte de multiplication de C de degré e, recevant des flèches des portes β et γ de degré e_1 et e_2 respectivement (avec $e = e_1 + e_2$). On ajoute les clones $\alpha_1, \dots, \alpha_{d+1-e}$. Pour i compris entre 1 et $d + 1 - e$ inclus, α_i reçoit une flèche du clone β_i et une flèche du clone γ_{i+e_1} de C_{e-1} (ces clones existent car $1 \leq i \leq d + 1 - e$ et $e_1 + 1 \leq i + e_1 \leq d + 1 - e_2$). Comme chaque clone de β dans C_{e-1} calcule le même polynôme que β dans C, et de même pour γ, chaque clone de α dans C_{e-1} calcule le même polynôme que α dans C. Pour montrer que le circuit résultant est multiplicativement disjoint il suffit de vérifier que chaque porte α_i est disjointe. Or on sait que les portes du sous-circuit associé à β_i sont des clones d'indices compris entre i et $i + e_1 - 1$ et que les portes du sous-circuit associé à γ_{i+e_1-1} sont des clones d'indices compris entre $i + e_1$ et $i + e_1 + e_2 - 1$. Les deux sous-circuits envoyant une flèche vers α_i sont donc bien disjoints. On vérifie enfin la dernière propriété : les portes du sous-circuit associé à α_i sont la réunion

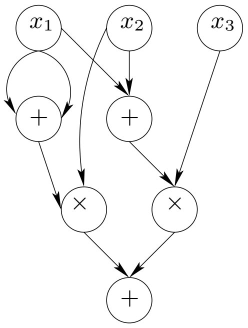


FIG. 2. Un circuit multiplicativement disjoint calculant le polynôme $2x_1x_2 + x_1x_3 + x_2x_3$

des portes du sous-circuit associé à β_i et des portes du sous-circuit associé à γ_{i+e_1-1}. Ce sont donc des clones d'indice compris entre i et $i + e_1 + e_2 - 1 = i + e - 1$ inclus.

On traite ensuite les portes d'addition en suivant un ordre tel que lorsqu'on clone une porte chaque porte dont elle reçoit une flèche a déjà été clonée. Soit α une porte d'addition de C de degré e, recevant des flèches des portes β et γ de degré e et e' respectivement (avec $e' \leq e$). On ajoute les clones $\alpha_1, \ldots, \alpha_{d+1-e}$. Pour i compris entre 1 et $d + 1 - e$ inclus, α_i reçoit une flèche du clone β_i et une flèche du clone γ_i. Comme on ajoute une porte d'addition le circuit reste multiplicativement disjoint. Chaque clone de α calcule le bon polynôme. Enfin les portes du sous-circuit associé à α_i sont des clones d'indice compris entre i et $i + e - 1$, car e' est inférieur ou égal à e.

Soit C' le sous-circuit associé à la sortie de C dans C_d. Par construction il est multiplicativement disjoint et calcule le même polynôme que C. Chaque porte de C a été clonée au plus d fois, donc la taille de C' est inférieure ou égale à dt. ☐

Remarquons qu'il est nécessaire d'avoir considéré un polynôme de degré formel complet d, et non simplement de degré d. Un circuit de degré d pourrait faire des suites de multiplications sur des constantes, suites qui ne pourraient être disjointes sans augmenter exponentiellement la taille.

Nous pouvons désormais montrer que circuits et termes sont équivalents sous une somme de Valiant. Nous montrons d'abord qu'un circuit multiplicativement disjoint peut s'exprimer comme une somme de Valiant devant un terme. Pour cela nous déterminons les monômes qui apparaissent dans le développement d'un polynôme calculé par un circuit multiplicativement disjoint. Cette démarche préfigure l'objet principal de notre travail, à savoir l'étude de la fonction coefficient d'un polynôme et de sa complexité. Nous déduirons de ce théorème un corollaire qui met bien en valeur ce lien.

THÉORÈME 3. $\mathrm{VNP} = \mathrm{VNP}_\mathrm{e}$.

Preuve. Il suffit de montrer que la classe VP est contenue dans la classe VNP_e.

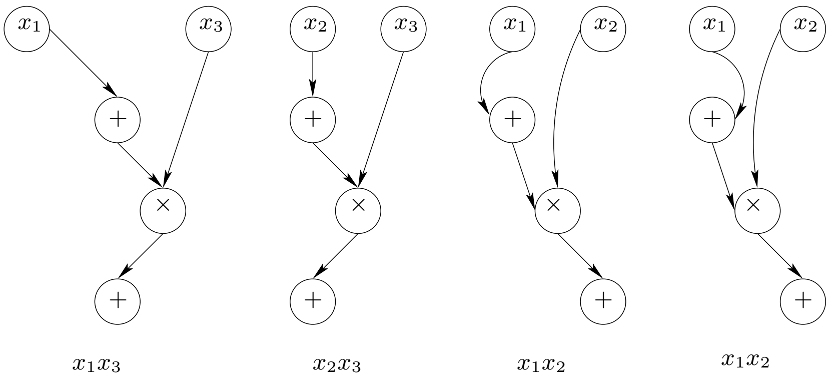


FIG. 3. Les développements du circuit de la figure 2 et les termes associés

Intuitivement, nous nous intéressons aux termes qui apparaissent dans le développement du polynôme calculé par un circuit multiplicativement disjoint sans constantes (on pourra substituer ensuite), si on ne regroupe pas les termes : pour un circuit réduit à une entrée, le seul terme est la variable ou la constante qui l'étiquette ; les termes qui apparaissent pour une porte de somme sont l'union disjointe des termes apparaissant dans les portes dont elle reçoit une flèche ; les termes qui apparaissent pour un produit sont les produits de deux termes, chacun apparaissant dans une porte dont la porte de multiplication reçoit une flèche. Nous formalisons ceci avec la notion de développement (cf. figures 2 et 3).

Soit C un circuit multiplicativement disjoint. Un graphe D est un *développement* de C si les conditions suivantes sont réunies :

(i) si α est une porte de multiplication appartenant à D et si β et γ sont les deux portes de C reliées d'une flèche vers α, alors les arêtes (β, α) et (γ, α) sont toutes deux dans D.

(ii) si α est une porte d'addition appartenant à D, il existe exactement une arête dans D allant vers α.

(iii) D est un sous-graphe de C contenant la sortie de C et tel que pour toute porte α de D distincte de la sortie, D contient au moins une arête partant de α.

On note $\mathrm{dev}(C)$ l'ensemble des développements de C et $d(D)$ le produit des variables étiquetant les entrées de D (si une variable apparaît plusieurs fois, elle est élevée à la puissance correspondante).

Nous allons montrer par récurrence sur la taille que si f est le polynôme calculé par un circuit C multiplicativement disjoint, on a :

$$f(\bar{x}) = \sum_{D \in \mathrm{dev}(C)} d(D).$$

Si C est de taille 1, C calcule le polynôme $f(x) = x$, il n'y a qu'un seul développement et la propriété est évidente.

Supposons que la propriété soit vraie pour tout circuit de taille inférieure ou égale à t, montrons qu'elle est vraie pour un circuit C de taille $t+1$.

Premier cas : la sortie de C est une porte de multiplication. C calcule alors le polynôme suivant :

$$f(\bar{x}) = f_1(\bar{x}) \cdot f_2(\bar{x}) = \left(\sum_{D_1 \in \mathrm{dev}(C_1)} d(D_1) \right) \left(\sum_{D_2 \in \mathrm{dev}(C_2)} d(D_2) \right),$$

où f_1 et f_2 sont les polynômes calculés par les deux sous-circuits C_1 et C_2 envoyant une flèche vers la porte de multiplication. C est multiplicativement disjoint, donc les deux sous-circuits C_1 et C_2 sont disjoints. Un développement de C contient la sortie de C et donc la sortie de C_1 et celle de C_2 (car toutes deux envoyaient une flèche vers la sortie de C). En notant qu'un développement de C se décompose ainsi en un développement de C_1 et un développement de C_2, on construit facilement une bijection entre $\mathrm{dev}(C_1) \times \mathrm{dev}(C_2)$ et $\mathrm{dev}(C)$, de telle sorte que si D est l'image de (D_1, D_2), $d(D) = d(D_1) \cdot d(D_2)$. Nous reprenons alors notre calcul :

$$f(\bar{x}) = \sum_{\substack{D_1 \in \mathrm{dev}(C_1) \\ D_2 \in \mathrm{dev}(C_2)}} d(D_1) \cdot d(D_2) = \sum_{D \in \mathrm{dev}(C)} d(D).$$

Deuxième cas : la sortie de C est une porte d'addition. C calcule alors le polynôme suivant :

$$f(\bar{x}) = f_1(\bar{x}) + f_2(\bar{x}) = \left(\sum_{D_1 \in \mathrm{dev}(C_1)} d(D_1) \right) + \left(\sum_{D_2 \in \mathrm{dev}(C_2)} d(D_2) \right),$$

où f_1 et f_2 sont les polynômes calculés par les deux sous-circuits C_1 et C_2 envoyant une flèche vers la porte d'addition (C_1 et C_2 peuvent être confondus). Un développement de C contient la sortie de C et donc la flèche provenant de C_1 ou celle provenant de C_2 mais pas les deux. Un développement de C correspond ainsi soit à un développement de C_1 soit à un développement de C_2, ce qui nous permet de construire une bijection entre l'union disjointe $\mathrm{dev}(C_1) \sqcup \mathrm{dev}(C_2)$ et $\mathrm{dev}(C)$, de telle sorte que si D est l'image d'un développement D_1 de C_1, alors $d(D) = d(D_1)$, et si D est l'image d'un développement D_2 de C_2, alors $d(D) = d(D_2)$. On en déduit que :

$$f(\bar{x}) = \sum_{D \in \mathrm{dev}(C_1) \sqcup \mathrm{dev}(C_2)} d(D) = \sum_{D \in \mathrm{dev}(C)} d(D).$$

Nous avons désormais une expression du polynôme calculé par C sous la forme d'une somme sur les développements. Pour montrer le théorème, il nous reste à coder les sous-graphes de C et à montrer que la fonction qui reconnaît les développements et la fonction d qui calcule le monôme correspondant sont calculables par un terme pour ce codage. Ce n'est pas difficile mais un peu fastidieux.

Numérotons de 1 à t les portes de C. Partitionnons l'ensemble $\{1, 2, \ldots, t\}$ en trois ensembles E, M, A contenant respectivement les numéros des portes d'entrée, de multiplication, d'addition et supposons que t est le numéro de la sortie. Pour i appartenant à E, notons V_i la variable étiquetant l'entrée numérotée i. Un développement D sera codé par des variables $a_{i,j}$ pour i et j compris entre 1 et t inclus et tels que l'arête (i, j) appartienne à C, cette variable valant 1 si l'arête (i, j) appartient à D et 0 sinon, et par les variables p_i pour i compris entre 1 et t inclus, cette variable valant 1 si la porte i appartient à D et 0 sinon.

Nous calculons le produit des polynômes suivants, qui correspondent aux conditions de la définition d'un développement de C. On commence par imposer que si une arête appartient à D, alors les sommets qu'elle relie appartiennent à D :

$$\prod_{(i,j)\in C} (a_{i,j} p_i p_j + 1 - a_{i,j}).$$

(i) Pour garantir que si D contient une porte de multiplication D contienne aussi les deux arêtes que celle-ci reçoit :

$$\prod_{\substack{i\in M \text{ et } j,k \text{ tels que} \\ (j,i)\in C \text{ et } (k,i)\in C}} (p_i a_{j,i} a_{k,i} + (1 - p_i)).$$

(ii) Pour garantir que si D contient une porte d'addition D contienne exactement une des deux arêtes que celle-ci reçoit :

$$\prod_{\substack{i\in A \text{ et } j,k \text{ tels que} \\ (j,i)\in C \text{ et } (k,i)\in C}} \left(\ p_i\ (a_{j,i}(1 - a_{k,i}) + a_{k,i}(1 - a_{j,i}))\ +\ 1 - p_i\ \right).$$

(iii) Pour garantir que D contienne la sortie t et que toute porte de D distincte de la sortie envoie au moins une arête vers une autre porte de D (notons que si un sous-graphe D d'un circuit multiplicativement disjoint satisfait les conditions (i) et (ii), toute porte envoie au plus une flèche vers une autre porte dans D, ce qui permet d'écrire une disjonction comme une somme) :

$$p_t \cdot \prod_{1\leq i<t} \left(p_i \cdot \left(\sum_{\substack{j \text{ tel que} \\ (i,j)\in C}} a_{i,j} \right) + 1 - p_i \right) .$$

Enfin, après avoir ainsi vérifié que $\bar{a}, \bar{p}$ code bien un développement de C, pour calculer le monôme correspondant :

$$\prod_{i\in E} \left(p_i \cdot V_i + 1 - p_i\right).$$

Ces calculs peuvent clairement être effectués par un terme de taille polynomiale en le nombre de portes du circuit multiplicativement disjoint C. On peut alors écrire le polynôme calculé par C comme la somme sur tous les codages (qui sont de taille polynomiale) du terme calculant d, d'où le théorème. □

Comme annoncé, nous pouvons en déduire le corollaire suivant. Les notations employées sont celles du chapitre 4 mais elles devraient être assez explicites.

COROLLAIRE 1. *Soit* $(f_n(x_1, \ldots, x_n))$ *appartenant à* VP*, chaque polynôme* $f_n(\bar{x})$ *peut s'écrire comme une somme à partir de sa fonction coefficient totale* g_n *:*

$$\sum_{\bar{\epsilon}_1,\ldots,\bar{\epsilon}_n} g_n(\bar{\epsilon}) \cdot x_1^{\bar{\epsilon}_1} \cdots x_n^{\bar{\epsilon}_n},$$

avec (g_n) *appartenant à* $\mathrm{VNP_e}$*.*

Preuve. Il suffit de reprendre la construction du théorème 3, sauf qu'à la fin on construit le terme $h_n(\bar{a}, \bar{p}, \bar{\epsilon})$, qui prend un uple $\bar{a}, \bar{p}$, vérifie s'il code un développement, calcule la représentation binaire $\bar{\gamma}_1, \ldots, \bar{\gamma}_n$ des puissances des variables dans le monôme associé à ce développement et teste si pour tout i, les uples $\bar{\gamma}_i$ et $\bar{\epsilon}_i$ sont égaux. $g_n(\bar{\epsilon})$ est la somme sur tous les $\bar{a}, \bar{p}$ de $h_n(\bar{a}, \bar{p}, \bar{\epsilon})$. □

5. Circuits fortement multiplicativement disjoints

L'idée de la section précédente était de se rapprocher des termes arithmétiques pour définir la classe VP, car les propriétés intéressantes comme la VNP-complétude du permanent se démontrent en passant par l'universalité du permanent pour un polynôme calculé par un terme. Il serait intéressant de pouvoir montrer directement l'universalité du permanent pour un polynôme calculé par un circuit multiplicativement disjoint, mais ceci semble difficile. Nous introduisons ici un modèle encore un peu plus strict, celui des circuits

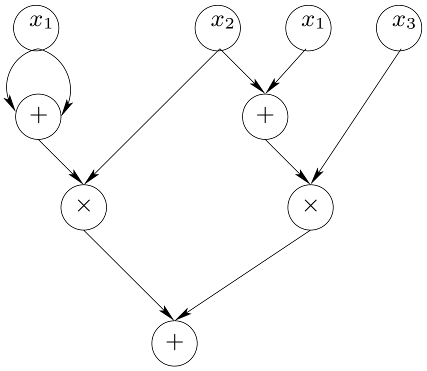


FIG. 4. Un circuit fortement multiplicativement disjoint

fortement multiplicativement disjoints, pour lesquels on peut montrer plusieurs propriétés d'universalité directement.

DÉFINITION 19. Un circuit est *fortement multiplicativement disjoint* si pour toute porte de multiplication α, recevant des flèches des portes β et γ, l'un des deux sous-circuits C_β et C_γ est disjoint du reste du circuit.

Comme on l'a déjà mentionné, dans un circuit l'argument d'une porte n'est pas spécifique à cette porte, il peut être réutilisé par une autre porte. Dans un terme arithmétique, chaque argument est spécifique à une porte de calcul. Dans un circuit fortement multiplicativement disjoint, c'est un phénomène intermédiaire pour les portes de multiplication : chaque porte de multiplication a au moins l'un de ses arguments qui a été calculé spécifiquement pour elle. C'est bien le cas dans l'exemple de la figure 4 ; l'autre argument de la porte de multiplication de gauche, l'entrée x_2, est par contre réutilisé par le circuit.

On commence par montrer que certains polynômes permettent de simuler efficacement les circuits fortement multiplicativement disjoints. Le premier lemme, qui sera utilisé plusieurs fois ensuite, est dans le même esprit que la construction montrant que le permanent simule efficacement les termes arithmétiques (cf. [**5**]).

Si G est un graphe orienté contenant les sommets s et t, un chemin de s à t est une suite $s, s_1, \ldots, s_k, t$ de sommets deux à deux distincts tels que les arêtes (s, s_1), (s_k, t) et (s_i, s_{i+1}), pour i compris entre 1 et $k-1$ inclus, appartiennent à G. Si les arêtes de G sont de plus munies d'un poids, on définit le poids d'un chemin orienté de s à t comme le produit des poids des arêtes. Le poids du couple (s, t) dans G est la somme des poids des chemins de s à t.

LEMME 6. *Soit C un circuit fortement multiplicativement disjoint de taille m, il existe un graphe orienté sans cycle G, avec deux sommets distingués s et t, tel que :*
- *G est de taille inférieure ou égale à $m + 1$.*
- *le poids de (s, t) dans G est le polynôme calculé par C.*

Preuve. La démonstration se fait encore une fois dans le cas plus général des circuits à plusieurs sorties. Dans un circuit fortement multiplicativement disjoint, chaque porte de multiplication a donc au moins un de ses sous-circuits qui est disjoint du reste du circuit. On appelle porte réutilisable toute porte du circuit qui n'est pas présente dans un tel sous-circuit disjoint d'une porte de multiplication. Dans le cas du circuit de la figure 4, toutes les portes sont réutilisables sauf l'entrée x_1 de gauche, la porte d'addition à laquelle elle envoie deux flèches et l'entrée x_3 de droite.

Montrons par induction sur la taille m du circuit que pour tout circuit fortement multiplicativement disjoint C à plusieurs sorties il existe un graphe G, avec un sommet distingué s, tel que :

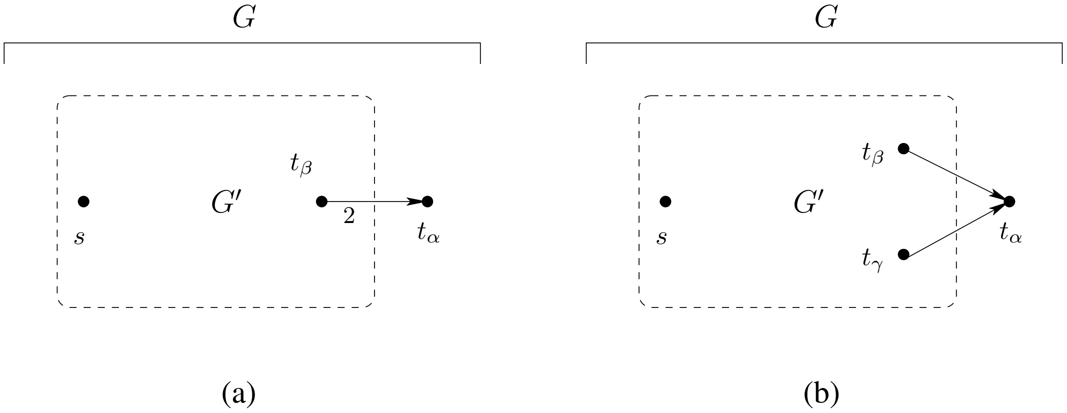
- G est de taille inférieure ou égale à $m+1$.
- pour toute porte réutilisable α du circuit C, il existe un sommet t_α de G tel que le poids de (s, t_α) dans G soit le polynôme calculé par la porte α de C.
- G est sans cycle orienté.

Un circuit de taille $m = 1$ se réduit à une entrée α, d'étiquette u (variable ou constante). On considère le graphe G à 2 sommets s_α et t_α, où le sommet s_α est relié au sommet t_α par une arête de poids u. Ce graphe est bien de taille inférieure ou égale à $m+1$ et il vérifie les conditions demandées.

Supposons que l'hypothèse d'induction soit vraie pour tout entier strictement inférieur à m, avec m supérieur ou égal à 2. Soit C un circuit fortement multiplicativement disjoint à plusieurs sorties de taille m. Soit α une sortie de C (il en existe au moins une).

Si α est une entrée d'étiquette u, il suffit d'appliquer l'hypothèse d'induction au circuit C' obtenu en enlevant α et d'ajouter au graphe G' résultant un sommet t_α recevant une flèche de s à laquelle on attribue le poids u. Une porte réutilisable β de C distincte de α est une porte réutilisable de C', donc il existe un sommmet t_β de G', et donc de G, satisfaisant les propriétés attendues. De même pour la porte α. La taille de G est inférieure ou égale à $(m-1)+1+1$, donc à $m+1$. Le graphe G est bien sans cycle.

Si α est une porte d'addition, on applique l'hypothèse d'induction au circuit C' obtenu en enlevant α. Le graphe G' ainsi obtenu est sans cycle et de taille inférieure ou égale à $(m-1)+1$. Si α reçoit ses flèches de la même porte β, cette porte est forcément réutilisable, donc il existe un sommet t_β tel que le poids de (s, t_β) soit le polynôme calculé par la porte β. Le polynôme calculé par la porte α vaut deux fois ce polynôme. Il suffit d'ajouter un sommet t_α au graphe G' recevant une flèche de poids 2 du sommet t_β (cf. figure 5 (a)). Si α reçoit ses flèches de deux portes β et γ distinctes, ces portes sont nécessairement réutilisables, donc il existe des sommets t_β et t_γ dans G' tels que le poids de (s, t_β) soit le polynôme calculé par β et le poids de (s, t_γ) soit le polynôme calculé par γ. On construit le graphe G en ajoutant un sommet t_α, ainsi que les arêtes de poids 1 (t_β, t_α) et (t_γ, t_α) (cf.figure 5 (b)). Ceci ne change pas le poids entre deux sommets de G'. Dans tous les cas, une porte réutilisable de C distincte de α est une porte réutilisable de C', et il



(a) (b)

FIG. 5. Cas d'une somme

existe un sommet adéquat dans G' donc dans G. La taille de G est inférieure ou égale à $(m-1)+1+1$, donc à $m+1$. Le graphe G est bien sans cycle.

Si α est une porte de multiplication, en appelant encore β et γ les portes nécessairement distinctes dont α reçoit une flèche et en supposant que le sous-circuit associé à la porte γ est disjoint du reste du circuit, le circuit obtenu en ôtant la porte α est constitué de deux circuits disjoints C_β et C_γ, de tailles respectives m_β et m_γ avec $m = m_\beta + m_\gamma + 1$. On applique l'hypothèse d'induction au circuit C_β, ce qui produit un graphe G_β sans cycle, de taille inférieure ou égale à $m_\beta + 1$, avec deux sommets s et t_β tels que le poids de (s, t_β) dans G_β soit le polynôme calculé par la porte β dans C_β. On applique l'hypothèse d'induction au circuit C_γ, ce qui produit un graphe G_γ sans cycle, de taille inférieure ou égale à $m_\gamma + 1$, avec deux sommets s_γ et t_γ tels que le poids de (s_γ, t_γ) dans G_γ soit le polynôme calculé par la porte γ dans C_γ. Le graphe G s'obtient en identifiant le sommet t_β de G_β avec le sommet s_γ de G_γ (cf. figure 6). Le poids de (s, t_γ) dans G est clairement le produit du poids de (s_β, t_β) dans G_β et du poids de (s_γ, t_γ) dans G_γ, c'est donc le polynôme calculé par la porte α dans C. Une porte réutilisable de C distincte de α est donc une porte réutilisable de C_β. On en déduit l'existence d'un sommet adéquat dans G_β. Cette construction ne change pas le poids des sommets de G_β dans le graphe G. Le poids des sommets de G_γ change, mais ils correspondent à des portes de C qui ne sont pas réutilisables. La taille de G est inférieure ou égale à $m_\beta + 1 + m_\gamma + 1 - 1$, donc à $m+1$. Le graphe G est bien sans cycle. $\square$

Le résultat suivant est donc un petit peu plus fort que l'universalité du permanent pour les termes. Il se montre à partir du lemme précédent exactement comme dans [**5**]. Il pourrait servir de première étape dans la démonstration de la complétude du permanent pour la classe VNP.

LEMME 7. *Soit f un polynôme calculable par un circuit fortement multiplicativement disjoint de taille m, f est projection de* per_m.

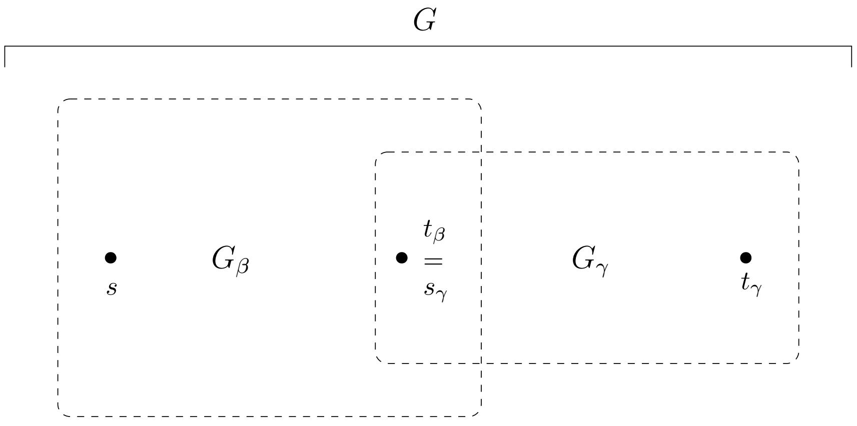


FIG. 6. Cas d'un produit

Preuve. Soit G un graphe orienté à n sommets (numérotés de 1 à n) dont les arêtes sont munies de poids. On associe à G la matrice $A = (a_{i,j})$ de taille n en posant $a_{i,j} = 0$ s'il n'y a pas d'arête du sommet i au sommet j et $a_{i,j} = u$ si l'arête existe et son poids vaut u. Une permutation σ de $\{1, \ldots, n\}$ se décompose en cycles. Pour le graphe G cela correspond à une *couverture par cycles*, c'est-à-dire un ensemble de cycles orientés de G dont les ensembles de sommets constituent une partition des sommets de G. Si on définit le poids d'une couverture par cycles comme le produit des poids des arêtes qu'elle contient, le permanent de la matrice A est la somme des poids des couvertures par cycles de G, indépendamment de la façon de numéroter les sommets de G.

Soit f un polynôme calculable par un circuit fortement multiplicativement disjoint de taille m. On prend le graphe orienté sans cycle G de taille $m+1$ du lemme 6, qui contient deux sommets s et t tels que le poids de (s,t) dans G soit le polynôme f. Appelons G' le graphe de taille m obtenu en identifiant les sommets s et t et en ajoutant une boucle de poids 1 à tous les sommets sauf au sommet s. Le permanent de la matrice correspondante est le poids des couvertures par cycles du graphe G'. Il y a une bijection évidente entre une couverture par cycle de G' et un chemin de s à t de G, de telle sorte que le poids de la couverture soit égal au poids du chemin : toute couverture par cycles de G' est constituée d'un cycle passant s et des boucles sur les autres sommets, car le graphe G était acyclique. Le permanent de la matrice est donc le polynôme f. ☐

Nous pouvons montrer un résultat similaire pour le hamiltonien. Nous l'utiliserons pour démontrer la complétude de cette suite de polynômes dans un cadre un peu plus strict que celui de Valiant au chapitre 3. Il est défini de la manière suivante :

$$\mathrm{HC}_n(\bar{x}) = \sum_{\sigma} \prod_{i=1}^{n} x_{i,\sigma(i)},$$

où la somme est prise pour tous les cycles σ de S_n de longueur n.

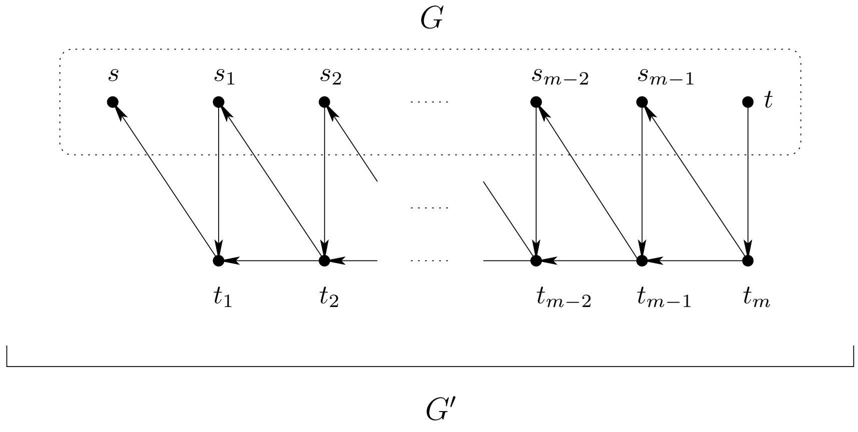


FIG. 7

LEMME 8. *Soit f un polynôme calculable par un circuit fortement multiplicativement disjoint de taille m, f est projection de* HC_{2m+1}.

Preuve. Soit f un polynôme calculable par un circuit fortement multiplicativement disjoint de taille m. On utilise encore une fois le graphe G obtenu via le lemme 6. Il comporte deux sommets s et t. Soit $s_1, \ldots, s_{m-1}$ ses autres sommets. On ajoute m sommets $t_1, \ldots, t_m$. Pour i compris entre 1 et $m-1$ inclus, on ajoute les arêtes (t_{i+1}, s_i), (s_i, t_i) et (t_{i+1}, t_i) en leur attribuant le poids 1. Enfin on ajoute les arêtes (t, t_m) et (t_1, s), de poids 1 également (cf. figure 7). Le graphe G' ainsi construit est de taille $2m+1$.

On s'intéresse aux cycles hamiltoniens de ce graphe. Un cycle hamiltonien passe évidemment par le sommet s, que nous considérons comme son origine. Il ne peut pas passer par le sommet t_1 avant de passer par le sommet t, car la seule arête partant de t_1 revient en s. Supposons alors qu'on a montré qu'aucun cycle hamiltonien de G', partant de s, ne peut passer par t_i avant de passer par t. Montrons alors qu'aucun cycle hamiltonien ne peut passer par t_{i+1} avant de paser par t. En effet, si un cycle passe par t_{i+1} avant de passer par t, il doit ensuite passer par s_i, car il ne peut passer par t_i par hypothèse. De s_i il ne peut aller en t_i, pour la même raison. Il ne pourra donc jamais passer par t_i, car ce sommet ne reçoit d'arêtes que des sommets t_{i+1} et s_i, et le cycle ne peut être hamiltonien. Un cycle hamiltonien partant de s commence donc par un chemin de s à t, sans passer par un des sommets t_i. Le retour en s est uniquement déterminé par le chemin choisi pour aller de s à t, car il faut visiter les sommets délaissés en allant de s à t. On a donc une bijection entre les chemins de s à t de G et les cycles hamiltoniens de G' et cette bijection respecte le poids. Le hamiltonien de la matrice correspondant au graphe G' est la somme des poids de ses cycles hamiltoniens, c'est-à-dire le polynôme f. □

En suivant la même méthode, nous obtenons une preuve simple de l'universalité du déterminant pour les polynômes calculés par des circuits fortement multiplicativement disjoints.

LEMME 9. *Soit f un polynôme calculable par un circuit fortement multiplicativement disjoint de taille m, f est projection de* $\det_{m+1}$.

Preuve. Soit f un polynôme calculable par un circuit fortement multiplicativement disjoint de taille m. Soit G le graphe fourni par le lemme 6. On considère le graphe G' de taille m construit à partir de G de la même manière que dans la démonstration de l'universalité du permanent et $A = (a_{i,j})$ la matrice associée. On a vu qu'à une permutation σ telle que $\prod_{i=1}^{m} a_{i,\sigma(i)}$ soit non-nul correspondait une couverture par cycles de G' consituée d'un cycle passant par s et de cycles de taille 1, les boucles des autres sommets. La signature de σ vaut alors $(-1)^{p+1}$, où p est la longueur du cycle passant par s. Soit G'' le graphe G' où pour chaque arête qui n'est pas une boucle on change le poids en son opposé, et $B = (b_{i,j})$ la matrice associée. Rappelons que :

$$\det_m(b_{i,j}) = \sum_{\sigma \in S_n} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^{n} b_{i,\sigma(i)}.$$

Soit σ une permutation correspondant à une couverture par cycles de G''. Soit p la longueur du cycle passant par s associé à σ. Alors $\prod_{i=1}^{m} b_{i,\sigma(i)}$ vaut $(-1)^p \prod_{i=1}^{m} a_{i,\sigma(i)}$. La signature de σ vaut $(-1)^{p+1}$, donc le déterminant de la matrice B est l'opposé du permanent de la matrice A, soit le polynôme $-f$. Il suffit enfin d'ajouter un sommet au graphe G'', relié uniquement à lui-même par une boucle de poids -1 : le déterminant de la matrice associée est le polynôme f. ☐

Le résultat précédent servira à la section suivante où nous montrerons la complétude du déterminant pour la classe VQP. Nous étudierons aussi la complétude d'autres suites de polynômes, notamment la suite (F_n) définie par $F_n = \mathrm{Tr}(X^n)$, où Tr représente la trace et X est une matrice carrée dont les entrées sont n^2 variables distinctes.

LEMME 10. *Soit f un polynôme calculable par un circuit fortement multiplicativement disjoint de taille m, f est projection de F_{2m+3} ou de F_{2m+5}.*

Preuve. Une *promenade de longueur k* dans un graphe orienté est simplement une suite de sommets $(t_1, \dots, t_k)$ telle que les arêtes (t_i, t_{i+1}) et l'arête (t_k, t_1) appartiennent au graphe. Une promenade peut passer plusieurs fois par un même sommet. Le sommet t_1 est appelé l'origine de la promenade. Le poids d'une promenade est le produit des poids de ses arêtes. Le k-poids d'un graphe G est la somme des poids de toutes les promenades de longueur k.

Si la matrice X est constituée des variables $x_{i,j}$, il est facile de montrer que le polynôme $\mathrm{Tr}(X^n)$ vaut :

$$\sum_{1 \le k_1, \dots, k_n \le n} x_{k_1,k_2} \cdots x_{k_{n-1},k_n} x_{k_n,k_1}.$$

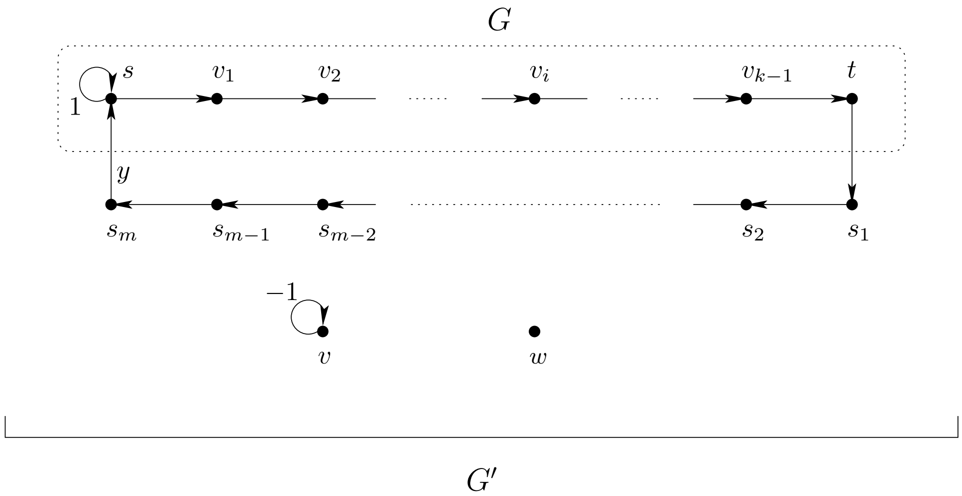


Fig. 8

En interprétant la matrice X comme la matrice d'adjacence d'un graphe orienté dont les arêtes sont munies de poids, on voit que $\mathrm{Tr}(X^n)$ calcule le n-poids du graphe à n sommets représenté par X. Ce que nous cherchons donc à construire maintenant c'est un graphe de taille l et dont le l-poids soit le polynôme f.

Le lemme 6 fournit un graphe orienté sans cycle G de taille $m+1$, avec deux sommets s et t tels que le poids de (s,t) dans le graphe soit le polynôme f. On commence par ajouter m sommets $s_1,\ldots,s_m$, ainsi que les arêtes (t,s_1), (s_i,s_{i+1}), toutes de poids 1, et enfin l'arête (s_m,s), en lui attribuant comme poids une nouvelle variable y. On ajoute aussi une boucle de poids 1 au sommet s, un sommet v uniquement relié à lui-même par une boucle de poids -1 et un sommet qui n'est relié à aucun sommet (cf. figure 8). La taille du graphe G' résultant est $2m+3$. Etudions donc les promenades de longueur $2m+3$ de G'.

Il y a une unique promenade de longueur $2m+3$ consistant à boucler au sommet v. L'entier $2m+3$ étant impair, elle est de poids -1.

Il y a une unique promenade de longueur $2m+3$ consistant à boucler au sommet s. Elle est de poids 1.

Soit $\tau = s, v_1, \ldots, v_{k-1}, t$ un chemin de s à t de longueur k dans G (et donc dans G'). Le sommet v_i est l'origine d'une unique promenade de longueur $2m+3$ passant par τ. Il s'agit de la promenade qui consiste à aller jusqu'à t via τ (longueur $k-i$), puis à rejoindre s via les sommets s_i (longueur $m+1$), à boucler $m+2-k$ fois en s (on a bien $m+2-k \geq 0$) et enfin à revenir à v_i via τ (longueur i). La longueur vaut bien $2m+3$. Le chemin τ induit aussi une unique promenade ayant pour origine chacun des sommets t, $s_1,\ldots,s_m$. Pour chacun de ces sommets, une autre promenade nécessiterait de faire deux tours, elle serait donc de longueur au moins $2(m+2)$, ce qui est strictement supérieur à $2m+3$. Par ailleurs, il existe $m+3-k$ promenades d'origine s, de longueur $2m+3$ et passant par τ, selon que l'on boucle $0,1,\ldots$ ou $m+2-k$ fois en s avant de suivre τ. Toutes ces promenades ont le même poids, à savoir le poids de τ multiplié par y. On a au total $2m+3$ promenades de longueur $2m+3$ associées à τ. Le $(2m+3)$-poids de G' vaut donc :

$$(-1)\ +\ 1\ +\ \sum_{\substack{\tau \text{ chemin} \\ \text{de } s \text{ à } t}} y(2m+3)\cdot \text{poids}(\tau).$$

En caractéristique nulle, il suffit donc de donner la valeur $(2m+3)^{-1}$ à la variable y. En effet, d'après la construction du graphe G, la somme des poids des chemins de s à t est le polynôme f.

En caractéristique positive p, il faut faire un peu attention. Pour m fixé, on peut faire la même construction si p ne divise pas $2m+3$, car cette valeur est alors inversible. Si p divise $2m+3$, alors p est strictement supérieur à 2, et p ne divise pas $2m+5$. Il suffit donc de refaire la construction précédente en ajoutant deux sommets supplémentaires s_{m+1} et s_{m+2}. □

6. La classe VQP

Nous montrons dans cette section que la notion de circuit fortement multiplicativement disjoint est bien adaptée pour étudier les propriétés de la classe VQP définie à la section 1. Ceci découle du lemme suivant.

LEMME 11. *Soit C un circuit de taille t et de degré formel complet d, il existe un circuit fortement multiplicativement disjoint calculant le même polynôme et de taille inférieure ou égale à $t^{\log d}$.*

Preuve. Comme pour le lemme 5, nous considérons des circuits qui peuvent éventuellement avoir plusieurs sorties et nous gardons la définition du degré formel complet d'un tel circuit comme le maximum des degrés formels complets des sorties. Nous utilisons encore la notion de porte réutilisable dans un circuit fortement multiplicativement disjoint définie pour la démonstration du lemme 6.

Nous allons montrer par induction sur n que pout tout entier d tel que $2^n \leq d < 2^{n+1}$, pour tout circuit à plusieurs sorties de taille t et de degré d, il existe un circuit fortement multiplicativement disjoint à plusieurs sorties C' tel que :

- C' est de taille inférieure ou égale à $t^{\log d}$.
- pour toute porte α de C, il existe une porte réutilisable de C' calculant le même polynôme que α dans C.

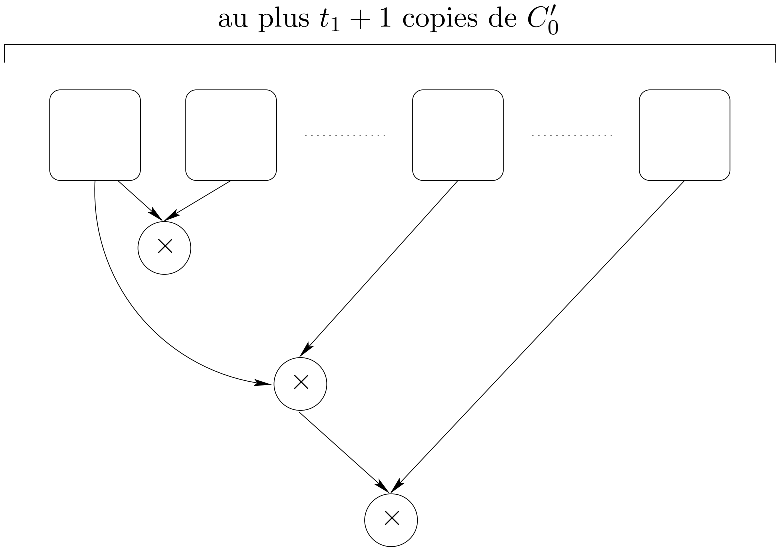


FIG. 9

Si n vaut 0, le degré formel complet de C vaut 1, donc C ne comporte pas de portes de multiplications. C est donc fortement multiplicativement disjoint et la propriété est vraie.

Supposons que la propriété soit vraie pour tout k strictement inférieur à n, avec n supérieur ou égal à 1, montrons qu'elle est vraie pour n. Soit C un circuit de taille t et de degré formel complet d, avec $2^n \leq d < 2^{n+1}$. Soit C_0 le circuit obtenu en enlevant toutes les portes de de C de degré formel complet strictement supérieur à $\lfloor d/2 \rfloor$. Soit t_0 la taille du circuit C_0 et t_1 le nombre de portes de C de degré strictement supérieur à $\lfloor d/2 \rfloor$. On applique l'hypothèse d'induction au circuit C_0, ce qui produit un circuit C'_0 de taille inférieure ou égale à $t_0^{\log \lfloor d/2 \rfloor}$. Pour toute porte de C_0 il existe une porte réutilisable de C'_0 qui calcule le même polynôme. Considérons une porte de multiplication de C de degré strictement supérieur à $\lfloor d/2 \rfloor$:

- si ses deux arguments sont de degré inférieur ou égal à $\lfloor d/2 \rfloor$, on ajoute à C' une porte correspondante reliée d'une part à une porte réutilisable de la première copie de C'_0, d'autre part à une porte réutilisable d'une nouvelle copie de C'_0 (cf. figure 9).
- sinon, l'un de ses arguments au moins étant de degré inférieur ou égal à $\lfloor d/2 \rfloor$ et l'autre étant alors déjà calculé par une porte de C', on ajoute à C' une porte correspondante reliée d'une part à la porte calculant l'argument de degré strictement supérieur à $\lfloor d/2 \rfloor$, d'autre part à la porte réutilisable adéquate d'une nouvelle copie de C'_0.

Les additions ne posent pas de problème. Le circuit obtenu est bien fortement multiplicativement disjoint et vérifie les propriétés demandées. En remarquant que t est la somme de t_0 et t_1 et que ces entiers sont supérieurs ou égaux à 1, on peut borner la taille de la manière suivante :

$$\begin{aligned}
& (t_1+1)\cdot t_0^{\log\left\lfloor\frac{d}{2}\right\rfloor}+t_1 \\
\leq\ & t\cdot t^{\log\left\lfloor\frac{d}{2}\right\rfloor} \\
\leq\ & t^{\log\left(2\cdot\left\lfloor\frac{d}{2}\right\rfloor\right)} \\
\leq\ & t^{\log d}.
\end{aligned}$$

□

Le lemme 11 montre qu'on peut supposer que le circuit calculant f_n est fortement multiplicativement disjoint dans la définition de la classe VQP. En effet, soit (C_n) une suite de circuits de taille quasi-polynomialement bornée (via les constantes a et b) calculant un polynôme dont le degré et le nombre de variables sont bornés par $c\cdot n^k$, alors pour n supérieur ou égal à 2 la taille de la suite (C'_n) obtenue par application du lemme 11 est bornée par :

$$\begin{aligned}
& \left(n^{a\cdot\log^b n}\right)^{\log(c\cdot n^k)} \\
\leq\ & n^{(a\cdot\log^b n)\cdot(\log c+k)\cdot\log n} \\
\leq\ & n^{a(\log c+k)\cdot\log^{b+1} n}
\end{aligned}$$

Après les propriétés d'universalité de la section précédente et le lemme ci-dessus, la suite est aussi prévisible que le dénouement d'un film de divertissement américain : nous déduisons du travail effectué jusqu'ici une preuve simple de la VQP-complétude du déterminant. La preuve originelle repose sur un puissant résultat de parallèlisation des circuits énoncé dans [**21**]. Celui-ci n'est pas nécessaire ici.

THÉORÈME 4. *La suite de polynômes* $(\det_n)$ *est* VQP-*complète.*

Preuve. Un déterminant se calcule par un circuit de taille polynomiale (cf. [**13**] et [**20**]), donc $(\det_n)$ appartient à VP et donc à VQP.

Soit donc (u_n) une suite de polynômes appartenant à la classe VQP. D'après le lemme 11, (u_n) est calculable par une suite de circuits fortement multiplicativement disjoint (C_n) de taille $t(n)$ quasi-polynomialement bornée. Le lemme 9 montre ensuite que (u_n) est une *qp*-projection de $(\det_n)$. □

Les résultats suivants fournissent une démonstration de la conjecture 8.1 énoncée par Bürgisser (cf. [**5**]). Notons qu'une démonstration d'une version faible de cette conjecture apparaît déjà dans [**3**]. Celle-ci utilise aussi le résultat de [**21**].

THÉORÈME 5. *La suite de polynômes* (F_n) *définie avant le lemme 10 est* VQP-*complète.*

Preuve. Cette suite de polynômes appartient à la classe VP, car le produit de n matrices de taille n se fait en $O(n^4)$ opérations. La VQP-complétude de la suite (F_n) se montre ensuite de la même manière que celle du déterminant, en utilisant les lemmes 10 et 11. $\square$

COROLLAIRE 2. *Les suites de polynômes (G_n) et (H_n) suivantes sont* VQP-*complètes ($X, X_1, \ldots, X_n$ représentent des matrices carrées dont les entrées sont n^2 variables distinctes) :*

- $G_n = \mathrm{Tr}(X_1 \cdots X_n)$.
- $H_n = \mathrm{Tr}(\det(X) \cdot X^{-1})$.

Preuve. Ces suites de polynômes appartiennent à la classe VP, donc aussi à la classe VQP. En effet, pour G_n, c'est encore le produit de matrices ; H_n est la trace de la comatrice, dont les coefficients sont des déterminants de taille $n-1$, et un déterminant se calcule avec un nombre polynomial d'opérations.

La suite (F_n) est clairement une *qp*-projection de la suite (G_n), donc celle-ci est VQP-complète.

Montrons que la suite (F_n) est une *qp*-projection de la suite (H_n). Pour cela nous allons adopter le point de vue matriciel. Soit I la matrice identité et O la matrice nulle, toutes deux de taille n. Soit J la matrice identité de taille $(n+1)n$. Soit N et P les matrices carrées de taille $(n+1)n$ définies par blocs de la manière suivante :

$$N = \begin{pmatrix} \mathrm{O} & -X & \mathrm{O} & \cdots & \mathrm{O} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \mathrm{O} \\ \vdots & & & \ddots & -X \\ \mathrm{O} & \cdots & \cdots & \cdots & \mathrm{O} \end{pmatrix} ; \quad P = \begin{pmatrix} \mathrm{O} & \mathrm{I} & \mathrm{O} & \cdots & \mathrm{O} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \mathrm{O} \\ \mathrm{O} & \cdots & \cdots & \mathrm{O} & \mathrm{I} \\ \mathrm{I} & \mathrm{O} & \cdots & \cdots & \mathrm{O} \end{pmatrix}.$$

N est une matrice nilpotente d'ordre $n+1$. Le déterminant de la matrice $J-N$ vaut alors 1 et on a :

$$(J-N)^{-1} = J + N + \cdots + N^n = \begin{pmatrix} \mathrm{I} & -X & (-X)^2 & \cdots & (-X)^{n-1} & (-X)^n \\ \mathrm{O} & \ddots & \ddots & \ddots & & (-X)^{n-1} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & (-X)^2 \\ \vdots & & & \ddots & \ddots & -X \\ \mathrm{O} & \cdots & \cdots & \cdots & \mathrm{O} & \mathrm{I} \end{pmatrix}.$$

Le déterminant de la matrice P vaut 1 ou -1 selon la valeur de n (la signature de la permutation sur les lignes qui fait passer de la matrice identité de taille $n(n+1)$ à la matrice P vaut 1 si n est pair et -1 si n est impair) et on a :

$$P \cdot (J-N)^{-1} = \begin{pmatrix} \mathrm{O} & \mathrm{I} & -X & (-X)^2 & \cdots & (-X)^{n-1} \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & (-X)^2 \\ \vdots & & & \ddots & \ddots & X \\ \mathrm{O} & \cdots & \cdots & \cdots & \mathrm{O} & \mathrm{I} \\ \mathrm{I} & -X & (-X)^2 & \cdots & (-X)^{n-1} & (-X)^n \end{pmatrix}.$$

Posons alors $Y = (J-N)P^{-1}$, la trace de la matrice $\det(Y) \cdot Y^{-1}$ vaut alors :

$$(-1)^n \mathrm{Tr}((-X)^n) = \mathrm{Tr}(X^n).$$

□

7. Classes de complexité potentielles

On pourrait définir la classe VQP′ comme la classe des suites de polynômes dont le nombre de variables est polynomialement borné, et dont le degré et la complexité sont quasi-polynomialement bornés. Cette nouvelle classe serait alors caractérisée par les circuits fortement multiplicativement disjoints. En effet, le lemme qui permet de passer d'un circuit à un circuit fortement multiplicativement disjoint montre que même si le degré est quasi-polynomialement bornée, la taille du circuit fortement multiplicativement disjoint résultant reste quasi-polynomialement bornée. Supposons en effet que notre circuit de départ soit de taille bornée par $n^{a \cdot \log^b n}$ et de degré borné par $n^{c \cdot \log^d n}$, on obtient un circuit fortement multiplicativement disjoint de taille bornée par :

$$\begin{aligned} & \left(n^{a \cdot \log^b n}\right)^{\log\left(n^{c \cdot \log^d n}\right)} \\ \leq \; & \left(n^{a \cdot \log^b n}\right)^{(c \cdot \log^d n) \log n} \\ \leq \; & n^{ac \cdot \log^{b+d+1} n}. \end{aligned}$$

Par ailleurs, comme les circuits fortement multiplicativement disjoints sont des cas particuliers des circuits multiplicativement disjoints, le degré d'un circuit fortement multiplicativement disjoint de taille quasi-polynomialement bornéee est quasi-polynomialement bornée. Les propriétés de complétude du déterminant et des autres exemples restent valables pour cette classe. On pourrait alors définir une classe VNQP′ associée, en suivant le modèle de définition des classes VNP et $\mathrm{VNP_e}$, en autorisant une somme exponentielle sur les valeurs booléennes d'un uple de longueur polynomiale. La preuve de la complétude du permanent ou du hamiltonien pour cette classe via les *qp*-projections serait alors simple et ne nécessiterait pas de prouver d'abord un théorème du type $\mathrm{VNP} = \mathrm{VNP}_\mathrm{e}$. En effet, une suite de polynômes (f_n) de la classe VNQP' est ainsi définie comme une somme à partir d'une suite de polynômes (g_n) de la classe VQP'. Cette suite est donc calculable par une suite de circuits fortement multiplicativement disjoint de taille quasi-polynomialement bornéee. Pour cette dernière, on peut construire via les lemmes 7 et 8 une suite de graphes de taille quasi-polynomialement bornéee dont la suite des poids (défini différemment selon qu'on étudie le permanent ou le hamiltonien) est la suite (g_n). A partir de cette suite de graphes, une construction similaire à celle de la preuve de complétude du permanent dans [**5**] ou à celle donnée à la section 2.2 du chapitre 3 permet d'éliminer la somme. Nous aurions alors des classes VQP' et VNQP' telles que le déterminant soit complet pour la classe VQP' et le permanent pour la classe VNQP'. A part cet équilibre entre le permanent et le déterminant et la relative simplicité des démonstrations nécessaires, ces classes sont moins intéressantes car moins naturelles que les classes VP et VNP, c'est pourquoi nous ne les définissons pas formellement. Nous les mentionnerons néanmoins à nouveau à la fin du chapitre 4.

On pourrait enfin définir la classe des suites de polynômes calculables par une suite de circuits fortement multiplicativement disjoints de taille polynomialement bornée, qui est incluse dans la classe VP. Le déterminant est difficile pour cette classe, au sens où toute suite de cette classe est une *p*-projection du déterminant. Montrer que cette classe est égale à la classe VP fournirait ainsi une preuve de la VP-complétude du déterminant. Sinon on sépare VP et VP_e. On pourrait en tout cas commencer par voir si le déterminant appartient à cette nouvelle classe, c'est-à-dire s'il est calculable par des circuits fortement multiplicativement disjoints de taille polynomialement bornée. Il serait alors complet pour cette classe, via des *p*-projections et non seulement des *qp*-projections, ce qui nous donnerait une autre classe capturant bien la complexité du déterminant. Remarquons que les suites (F_n), (G_n) et (H_n) définies ci-dessus peuvent être calculées par des circuits fortement multiplicativement disjoints de taille polynomiale. Ils sont donc complets pour cette nouvelle classe. Ceci peut laisser croire qu'il en est de même pour le déterminant. On peut probablement obtenir un tel résultat en utilisant l'algorithme présenté dans [**20**], qui ramène le calcul du déterminant à des calculs de puissances itérées de matrices.

CHAPITRE 3

Théorie de Valiant sans constantes

Nous allons nous intéresser aux rapports entre la complexité d'un polynôme et celle de sa fonction coefficient. Comme on le voit avec l'exemple du polynôme $(x+y)^n$, celle-ci devra calculer des entiers. Pour bien mettre en valeur le calcul de ces entiers, nous allons considérer des variantes des classes de Valiant, en ne s'autorisant que les constantes 0, 1 et -1. Nous choisissons ces constantes car sans -1 on a vu que la séparation des classes de Valiant était établie. Par ailleurs, -1 permet d'exprimer les connecteurs booléens et nous serons naturellement amenés à simuler des calculs booléens. Une fois qu'on a -1, les constantes 0 et 1 peuvent être obtenues par un circuit de taille constante, mais on se les donne pour des raisons esthétiques, les calculs de Valiant se faisant avec une somme sur des uples booléens, donc avec substitution de variables par 0 ou par 1. Après ces nouvelles définitions, nous montrons la complétude du hamiltonien et étudions certaines de ses propriétés. Enfin nous comparons très brièvement les classes sans constantes avec celles définies par Valiant.

1. Définitions

Les définitions ci-dessous sont exactement les mêmes que celles des classes de Valiant, mais il faut bien noter que les constantes arbitraires ne sont plus permises.

DÉFINITION 20. Une suite de polynômes (f_n) appartient à la classe VP^0 si le nombre de variables, le degré formel complet et la complexité de f_n sont bornés par un polynôme en n. Rappelons que la complexité d'un polynôme est ici définie par des circuits n'utilisant pas d'autres constantes que 0, 1 et -1.

Cette définition impose que le degré formel complet d'un polynôme de la suite soit polynomialement borné. La taille de ses coefficients entiers est alors également polynomialement bornée. C'est aussi le cas pour la classe VNP^0 définie ci-dessous.

DÉFINITION 21. Une suite de polynômes (f_n) appartient à la classe VNP^0 s'il existe une suite $(g_n(y_1,\ldots,y_{v(n)}))$ appartenant à la classe VP^0 telle que :

$$f_n(x_1,\ldots,x_{u(n)}) = \sum_{\bar{\epsilon}\in\{0,1\}^{v(n)-u(n)}} g_n(x_1,\ldots,x_{u(n)},\bar{\epsilon}).$$

Nous définissons encore une fois une notion de réduction pour laquelle les classes VP^0 et VNP^0 sont stables, ainsi qu'une notion de complétude.

DÉFINITION 22. Pour un entier k strictement positif, un polynôme f est une *k-projection bornée* d'un polynôme g si $f(\bar{x}) = g(a_1,\ldots,a_m)$, où chaque a_i est soit un entier relatif

calculable à partir de -1 par un circuit de taille et de degré formel complet inférieurs ou égaux à k, soit une variable choisie parmi $x_1, \ldots, x_n$.
Une suite (f_n) est une *projection bornée* d'une suite (g_n) s'il existe deux fonctions $s(n)$ et $t(n)$ polynomialement bornées telles que pour tout n, f_n est une $s(n)$-projection bornée de $g_{t(n)}$.

DÉFINITION 23. Une suite de polynômes (f_n) appartenant à VNP^0 est VNP^0-complète si toute suite (g_n) de VNP^0 est une projection bornée de (f_n).

LEMME 12. *Les classes* VP^0 *et* VNP^0 *sont stables par projection bornée.*

Preuve. Soit (g_n) une suite de polynômes de la classe VP^0 et (f_n) une projection bornée de (g_n) via les fonctions $s(n)$ et $t(n)$. Alors pour tout n le polynôme f_n est une $s(n)$-projection bornée du polynôme $g_{t(n)}$, en remplaçant par des variables ou des entiers relatifs calculables par un circuit de taille et de degré formel complet inférieurs ou égaux à $s(n)$. Si l'on effectue ces remplacements dans le circuit calculant $g_{t(n)}$, on obtient un circuit de taille et de degré formel complet polynomialement bornés en n calculant f_n. On montre facilement ensuite la stabilité pour la classe VNP^0. □

2. Le polynôme HC_n

La complétude du permanent est le résultat charnière des classes de Valiant originelles, mais elle repose sur des projections où l'on remplace des variables par la valeur 1/2. C'est pourquoi le permanent n'est pas complet en caractéristique 2. Afin d'obtenir des résultats indépendants de la caractéristique et de rester dans le cadre de nos classes sans constantes, nous allons utiliser le polynôme HC_n, qui calcule le hamiltonien d'une matrice (cf. section 5 pour la définition du polynôme HC_n).

2.1. Equivalence entre circuits et termes sous une somme de Valiant.

Comme pour la preuve de complétude du permanent, la première étape repose sur l'équivalence des circuits et des termes sous une somme de Valiant. On définit de manière similaire des classes VP_e^0 *et*VNP_e^0. Ce théorème reste valable dans le cadre des classes sans constantes. Il se démontre en reprenant la preuve de la section 4 du chapitre 2, car celle-ci se faisait sur des circuits de degré formel complet borné et elle convient pour des circuits sans constantes.

THÉORÈME 6. *Les classes* VNP_e^0 *et* VNP^0 *sont égales.*

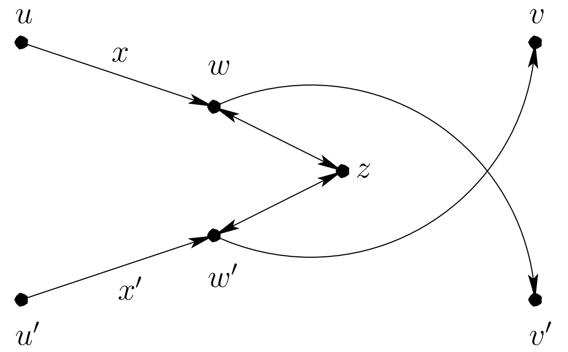


Fig. 1. Gadget de couplage.

2.2. Complétude.

Nous donnons ici une preuve différente de celle qui apparaît dans [**7**] ou dans [**17**], en nous inspirant de la preuve de complétude du permanent donnée dans [**5**].

Théorème 7. HC_n *est* VNP^0*-complet.*

Preuve. Soit donc un polynôme $f(x_1,\ldots,x_n)$ qui s'écrit $\sum_{\bar\epsilon} g(\bar a,\bar x,\bar\epsilon)$, où les a_i valent 0, 1 ou -1. On a vu qu'on pouvait supposer que g est calculable par un terme arithmétique de taille $p(n)$, avec p un polynôme. Par ailleurs on a trouvé une projection de $\mathrm{HC}_{2p(n)+1}$ sur g, projection qui remplace au plus $p(n)$ variables de $\mathrm{HC}_{2p(n)+1}$ par une variable de $\bar x$, les autres prenant les valeurs 0 ou 1. En effet, un terme arithmétique est un cas particulier d'un circuit fortement multiplicativement disjoint et il suffit d'appliquer le lemme 8 du chapitre 2. La remarque sur la projection est claire si on reprend la preuve.

Ce que nous voulons désormais, c'est montrer qu'on peut éliminer la somme sur tous les $\bar\epsilon$ booléens et l'écrire comme un hamiltonien, au prix d'une augmentation raisonnable de la taille du graphe. Nous suivons toujours le schéma de la preuve concernant le permanent. Commençons par donner les deux gadgets que nous utiliserons. Ils sont plus simples que dans le cas du permanent. Le poids d'un graphe est ici la somme des poids de tous les cycles hamiltoniens.

Le premier est le gadget de couplage. Soit G un graphe, (u,v) et (u',v') deux arêtes de G, de poids x et x', avec u distinct de u' et v distinct de v'. Soit G' le graphe obtenu à partir de G en ôtant les arêtes (u,v) et (u',v') et en connectant ces sommets par le graphe de couplage de la figure 1. Alors le poids de G' est la somme des poids des cycles de G qui passaient par exactement une des deux arêtes (u,v) et (u',v'). En effet, si un cycle de G' contient l'arête (u,w), il ne peut pas contenir l'arête (w,v'), car sinon ce cycle ne passe pas par z. Donc il contient aussi les arêtes (w,z) et (z,w'), et il ne peut pas contenir l'arête (u',w'). Le graphe de couplage se comporte dans ce cas comme s'il y avait une arête de u à v, de poids x, et pas d'arête de u' à v'. Le raisonnement réciproque est similaire.

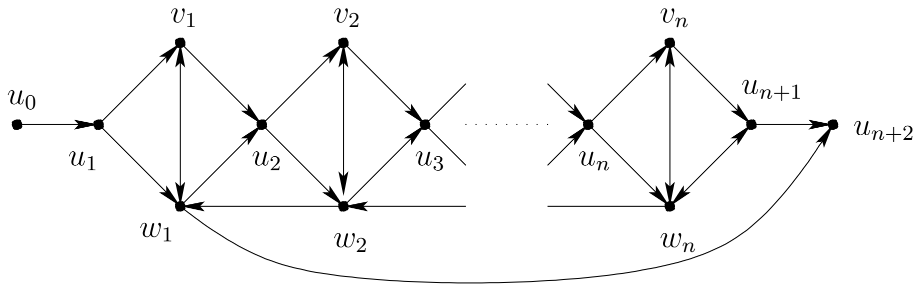


FIG. 2. Gadget de somme S_n.

Le second est le gadget de somme S_n pour tout n supérieur ou égal à 1 (cf. figure 2). Il est tel que pour tout sous-ensemble de $A = \{(u_1, v_1), \ldots, (u_n, v_n)\}$ distinct de A lui-même, il existe exactement un chemin hamiltonien de u_0 à u_{n+2} passant par ces arêtes et par aucune autre de A. De plus, il existe exactement *deux* chemins hamiltoniens passant par toutes les arêtes de A : le chemin u_0, $u_1, v_1, w_1, \ldots, u_n, v_n, w_n, u_{n+1}, u_{n+2}$ d'une part et le chemin $u_0, u_1, v_1, u_2, \ldots, u_n$, $v_n, u_{n+1}, w_n, w_{n-1}, \ldots, w_1, u_{n+2}$ d'autre part. Tous ces chemins sont de poids 1.

Soit $h(\bar{z}, y)$ un polynôme calculable par un terme arithmétique, on considère le graphe G fourni par le lemme 8 dont la somme des poids des cycles hamiltoniens vaut le polynôme h, où la variable y est l'étiquette de k arêtes. On veut montrer qu'il existe un graphe G'de taille raisonnable dont le poids total soit égal à $h(\bar{z}, 0) + h(\bar{z}, 1)$. Pour cela on disjoint le sommet s du graphe G, qui devient s_1 et s_2, en donnant les arêtes sortantes de s à s_1 et les arêtes entrantes à s_2, de sorte que les cycles hamiltoniens de G s'identifient aux chemins hamiltoniens de s_1 à s_2 du nouveau graphe. On adjoint ensuite le gadget S_k, et on relie u_{k+2} à s_1 d'une part, s_2 à u_0 d'autre part. Enfin soit $e_1, \ldots, e_k$ les arêtes de poids y, on leur affecte le poids 1 et on couple chaque arête e_i avec l'arête (u_i, v_i) du gadget de somme, via des copies du gadget de couplage (cf. 3). La somme $h(\bar{z}, 0) + h(\bar{z}, 1)$ correspond à prendre le poids de tous les cycles ne contenant pas les arêtes de poids y (c'est le terme $h(\bar{z}, 0)$) *plus* le poids de tous les cycles quand les arêtes e_i ont le poids 1. Si on partitionne les cycles par rapport aux arêtes e_i qu'ils traversent, i.e. si S est un sous-ensemble de $E = \{e_1, \ldots, e_k\}$ on considère les cycles hamiltoniens qui passent par les arêtes de S et par aucune autre arête de E, alors $h(\bar{z}, 0) + h(\bar{z}, 1)$ vaut deux fois le poids des cycles pour le sous-ensemble vide plus le poids des cycles passant exactement par les arêtes de S pour tout sous-ensemble non-vide des arêtes e_i. On a vu que justement tout cycle hamiltonien pourra passer de deux manières différentes par *toutes* les arêtes (u_i, v_i) et d'une manière unique pour chaque sous-ensemble. Comme le gadget de couplage agit comme un OU exclusif, le poids total du graphe est bien le poids recherché.

On répète cette opération pour toutes les variables à remplacer de g. A chaque fois il faut ajouter un nombre de noeuds constant pour chaque arête étiquetée par y, et on avait vu que le nombre d'arêtes etiquetées par une variable était borné par la taille de notre terme de départ, d'où le résultat. □

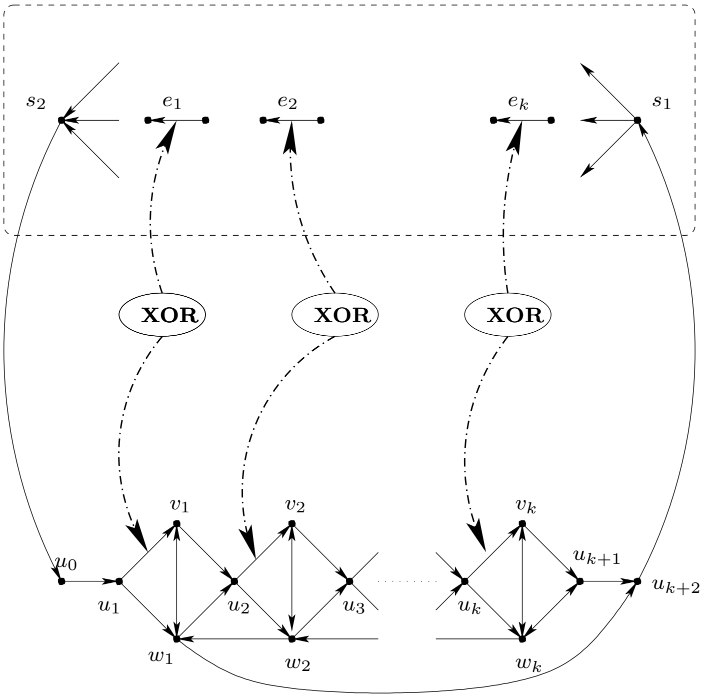


FIG. 3. Elimination.

2.3. Propriétés utiles.

Les propriétés suivantes seront utiles par la suite. Elles sont le pendant de celles énoncées à la section 2 du chapitre 2 et qui concernaient le permanent.

LEMME 13. *La fonction coefficient de* HC_n *est* VP^0.

Preuve. Nous allons écrire le hamiltonien sous la forme :

$$\mathrm{HC}_n(z_{i,j}) = \sum_{\bar{\epsilon}\in\{0,1\}^{n^2}} h_n(\bar{\epsilon})\bar{z}^{\bar{\epsilon}}.$$

La fonction h_n commence par vérifier que la matrice définie par $\bar{\epsilon}$ est bien une matrice de permutation, comme pour la fonction coefficient du permanent. Ensuite elle vérifie que cette permutation est un cycle de longueur n, en calculant les images successives de chacun des entiers $1, \ldots, n$ par l'itération de la permutation. Soit $(e^{(2)}_{i,j}), \ldots, (e^{(n)}_{i,j})$ les matrices correspondant à la matrice $(\epsilon_{i,j})$ élevée à la puissance $2, \ldots, n$ respectivement, la fonction h_n vérifie que :

- pour tout i compris entre 1 et n inclus, pour tout j compris entre 1 et $n-1$ inclus, $e^{(j)}_{i,i}$ vaut 0.
- pour tout i compris entre 1 et n inclus, $e^{(n)}_{i,i}$ vaut 1.

La suite de fonctions (h_n) peut être représentée par une suite de polynômes appartenant à VP^0. $\square$

S'il est connu que le permanent est coefficient d'un polynôme VP, il est plus difficile d'obtenir le même résultat pour le hamiltonien. C'est l'objet du lemme suivant.

LEMME 14. *Il existe une suite de polynômes (K_n) appartenant à VP^0 et telle que le polynôme HC_n soit le coefficient d'un monôme de K_n.*

Preuve. Nous allons définir une famille de polynômes $T_{p,k,l}$, pour les entiers p, k et l compris entre 1 et n inclus. Ces polynômes sont définis par récurrence sur les variables $x_{i,j}$, y_k et z_l, pour i, j, k et l compris entre 1 et n inclus :

- $T_{1,i,j} = x_{i,j} y_i z_j$.
- $T_{p+1,i,j} = \sum_{k=1}^{n} T_{p,i,k} \cdot T_{1,k,j}$.

Montrons par induction sur p que :

$$T_{p,i,j} = \sum_{1 \leq m_1,\ldots,m_{p-1} \leq n} x_{i,m_1} \left(\prod_{k=1}^{p-2} x_{m_k,m_{k+1}} \right) x_{m_{p-1},j} \left(\prod_{k=1}^{p-1} y_{m_k} z_{m_k} \right) y_i\, z_j$$

et qu'il existe un circuit de taille $3n^2 + n + (p-1)(2n^3 - n^2)$ calculant tous les $T_{k,i,j}$ pour i et j compris entre 1 et n inclus et k compris entre 1 et p inclus.

Pour $p = 1$, la première propriété est vérifiée si on pose par convention que le produit $x_{i,m_1} x_{m_1,m_2} \cdots x_{m_{p-2},m_{p-1}} x_{m_{p-1},j}$ vaut $x_{i,j}$ lorsque p vaut 1. De plus tous les $T_{1,i,j}$ sont calculables simultanément par un circuit de taille $3n^2 + n$.

Si les propriétés de récurrence sont vraies pour k inférieur ou égal à p, montrons qu'elles sont vraies pour $p + 1$. Le polynôme $T_{p+1,i,j}$ vaut alors :

$$\begin{aligned}
&\sum_{k=1}^{n} T_{p,i,k}\, T_{1,k,j} \\
= &\sum_{k=1}^{n} \left(\sum_{1 \leq m_1,\ldots,m_{p-1} \leq n} x_{i,m_1} \left(\prod_{i=1}^{p-2} x_{m_i,m_{i+1}} \right) x_{m_{p-1},k} \left(\prod_{i=1}^{p-1} y_{m_i} z_{m_i} \right) y_i\, z_k \right) x_{k,j}\, y_k\, z_j \\
= &\sum_{1 \leq m_1,\ldots,m_p \leq n} x_{i,m_1} \left(\prod_{i=1}^{p-1} x_{m_i,m_{i+1}} \right) x_{m_p,j} \left(\prod_{i=1}^{p} y_{m_i} z_{m_i} \right) y_i\, z_j.
\end{aligned}$$

Par ailleurs, si on a calculé tous les $T_{k,i,j}$ précédents par un circuit de taille $3n^2 + n + (p-1)(2n^3 - n^2)$, il faut ajouter $2n^3 - n^2$ portes pour calculer tous les $T_{p+1,i,j}$, ce qui donne la borne annoncée.

Le polynôme $T_{n,1,1}$ est donc calculable par un circuit de taille polynomiale.

$$T_{n,1,1} = \sum_{1 \leq m_1, \ldots, m_{n-1} \leq n} x_{1,m_1} x_{m_1,m_2} \cdots x_{m_{n-2},m_{n-1}} x_{m_{n-1},1} \left(\prod_{i=1}^{n-1} y_{m_i} z_{m_i} \right) y_1 \, z_1$$

Le coefficient du monôme $y_1 z_1 \cdots y_n z_n$ est le hamiltonien, car il faut choisir $m_1, \ldots, m_{n-1}$, chacun compris entre 2 et n, de telle sorte qu'on ait tous les entiers de 2 à n. Les variables $x_{i,j}$ associées à un tel choix constituent un cycle de longueur n et engendrent le monôme $x_{1,m_1} x_{m_1,m_2} \cdots x_{m_{n-2},m_{n-1}} x_{m_{n-1},1}$. Pour tout n, on pose $K_n = T_{n,1,1}$. ☐

3. Comparaison avec les classes de Valiant

Nous énonçons ici des résultats immédiats pour préciser un peu le lien entre les classes sans constantes et celles définies par Valiant. Rappelons que les classes strictes que nous définissons concernent les suites de polynômes à coefficients entiers pour une caractéristique fixée et non des fonctions sur un corps représentées par des polynômes.

LEMME 15. *Si p est un nombre premier, les propriétés suivantes sont équivalentes :*

(i) $\mathrm{VP}^0 = \mathrm{VNP}^0$ *en caractéristique p.*

(ii) sur tout corps de caractéristique p, $\mathrm{VP} = \mathrm{VNP}$.

(iii) sur le corps fini à p éléments $\mathbb{F}_p$, $\mathrm{VP} = \mathrm{VNP}$.

Preuve.

(i) → (ii) : si $\mathrm{VP}^0 = \mathrm{VNP}^0$, alors en caractéristique p le hamiltonien est calculable par une suite de circuits sans constantes de taille polynomialement bornée ; par VP-complétude du hamiltonien, VP = VNP sur tout corps de caractéristique p.

(ii) → (iii) est évident.

(iii) → (i) : si VP = VNP sur le corps $\mathbb{F}_p$, le hamiltonien est calculable en caractéristique p par une suite de circuits de taille polynomialement bornée, n'utilisant que des constantes appartenant à $\{0, 1, \ldots, p-1\}$, et donc par une suite de circuits sans constantes, car ces entiers peuvent se construire en temps constant à partir de 1. ☐

LEMME 16. *Si* $\mathrm{VP}^0 = \mathrm{VNP}^0$ *en caractéristique* 0*, alors* VP = VNP *sur tout corps de caractéristique* 0.

Cette propriété se démontre comme en caractéristique positive. Par contre la réciproque n'est pas évidente : si VP = VNP sur tout corps de caractéristique 0, est-ce que $\mathrm{VP}^0 = \mathrm{VNP}^0$ en caractéristique 0 ?

Cette question est liée aux propriétés du permanent pour les classes strictes. En toute caractéristique p strictement supérieure à 2, l'entier 2 a un inverse et le permanent est VNP^0-complet. Si le permanent était VNP^0-complet en caractéristique 0, il le serait aussi en caractéristique 2, ce qui est peu probable. Au lieu de se demander si le permanent est VNP^0-complet en caractéristique 0, on peut se demander si l'appartenance de (per_n) à VP^0 en caractéristique 0 implique $\mathrm{VP}^0 = \mathrm{VNP}^0$. Si (per_n) appartient à VP^0 en caractéristique 0, VP = VNP sur tout corps de caractéristique 0, donc cette question revient à la question précédente. Il faudrait montrer par exemple que VP = VNP sur $\mathbb{Q}$ implique $\mathrm{VP}^0 = \mathrm{VNP}^0$, en essayant de simuler les calculs avec des rationnels en caractéristique 0.

CHAPITRE 4

Coefficients d'un polynôme : cas du degré borné

Nous abordons ici le coeur de nos préoccupations, à savoir les rapports entre la complexité d'un polynôme et celle de sa fonction coefficient. Nous commençons par une remarque simple sur le cas des fonctions repésentées par des polynômes sur le corps $\{0,1\}$, avant de donner des résultats quand le degré du polynôme considéré est polynomialement borné : nous nous plaçons dans le cadre de la théorie de Valiant sans constantes présentée précédemment.

1. Position du problème

Si $f(x_1,\ldots,x_n)$ est un polynôme calculable par un circuit de taille polynomiale, il comporte un nombre simplement exponentiel de monômes dans son développement ; on peut donc identifier chaque monôme par un uple booléen de longueur polynomiale. Si le degré total est d, nous allons représenter le monôme $x_1^{m_1}\cdots x_n^{m_n}$ par l'uple $\bar\epsilon = (\bar\epsilon_1,\ldots,\bar\epsilon_n)$ où chaque $\bar\epsilon_i$ est de longueur $\lceil \log d\rceil$ et tel que $m_i = \epsilon_{i,0} + \epsilon_{i,1}\cdot 2 + \cdots + \epsilon_{i,\lfloor \log d\rfloor}\cdot 2^{\lfloor \log d\rfloor}$. On notera $\bar x^{\bar\epsilon}$ ou encore $x_1^{\bar\epsilon_1}\cdots x_n^{\bar\epsilon_n}$ le monôme ainsi codé.

Définition 24. Soit $f(x_1,\ldots,x_n)$ un polynôme de degré d, sa *fonction coefficient totale* est la fonction g, définie sur les variables $z_{i,j}$ pour i compris entre 1 et n et j compris entre 0 et $\lfloor \log d\rfloor$ inclus, telle que :

$$f(\bar x) = \sum_{\bar\epsilon\in\{0,1\}^{n\lceil \log d\rceil}} g(\bar\epsilon)\bar x^{\bar\epsilon}.$$

On peut aussi considérer les fonctions coefficients partielles, où on ne regarde les monômes que par rapport à un sous-ensemble des variables du polynôme.

Définition 25. Soit $f(x_1,\ldots,x_n,y_1,\ldots,y_m)$ un polynôme de degré d, sa *fonction coefficient par rapport aux variables $\bar x$* est la fonction g, définie sur les variables $\bar y$ et $z_{i,j}$ pour i compris entre 1 et n et j compris entre 0 et $\lfloor \log d\rfloor$ inclus, telle que :

$$f(\bar x,\bar y) = \sum_{\bar\epsilon\in\{0,1\}^{n\lceil \log d\rceil}} g(\bar y,\bar\epsilon)\cdot \bar x^{\bar\epsilon}.$$

Quand on dit que g est *une* fonction coefficient de f, on veut dire qu'il existe un choix de variables pour lequel g est la fonction coefficient de f associée à ce choix. Par la suite, nous négligerons souvent les longueurs des uples, en écrivant par exemple $\sum_{\bar\epsilon} g(\bar\epsilon)\bar x^{\bar\epsilon}$ afin de ne pas alourdir les notations.

Notons ici que le polynôme $f(\bar{x},\bar{y})$ d'une part et ses fonctions coefficients d'autre part sont a priori des objets très différents. Si le polynôme f est à coefficients entiers, la fonction coefficient totale est une fonction dont les entrées sont booléennes et à valeur dans $\mathbb{Z}$ et la fonction coefficient par rapport aux variables $\bar{x}$ est une fonction dont les entrées sont booléennes et à valeurs dans $\mathbb{Z}[\bar{y}]$. Dans le formalisme introduit jusqu'ici nous n'avons pas défini la complexité de calcul de telles fonctions. Nous définirons donc la complexité de calcul d'une fonction coefficient totale $g(\bar{z})$ comme la complexité minimale d'un polynôme en $\bar{z}$ dont la restriction aux valeurs booléennes de $\bar{z}$ coïncide avec g. La complexité de calcul de la fonction coefficient par rapport aux variables $\bar{x}$ est la complexité minimale d'un polynôme en $\bar{z}$ et $\bar{y}$ dont la restriction aux valeurs boolénnes de $\bar{z}$ coïncide avec g. Notre problème est de comparer la complexité de calcul d'un polynôme f et celle de ses fonctions coefficients.

2. Le corps $\{0,1\}$

Dans le cas du corps à deux éléments $\{0,1\}$, il n'y a pas d'autres constantes que 0 et 1 et il n'y a pas lieu d'introduire de soustraction, puisque addition et soustraction sont la même opération. De plus, chaque fonction de $\{0,1\}^n$ dans $\{0,1\}$ s'écrit de manière unique comme une somme de monômes dans lesquels chaque variable apparaît à la puissance 0 ou 1. On peut donc coder un tel monôme en les variables $y_1,\dots,y_n$ par l'uple booléen $(\epsilon_1,\dots,\epsilon_n)$. Nous étudions ici un problème différent de celui que nous avons présenté ci-dessus : nous nous intéressons aux fonctions sur $\{0,1\}$, en les représentant par des polynômes.

Soit $f(x_1,\dots,x_n)$ une fonction de $\{0,1\}^n$ dans $\{0,1\}$; appelons f^* le polynôme dont f est la fonction coefficient :

$$f^*(y_1,\dots,y_n) = \sum_{\bar{\epsilon}\in\{0,1\}^n} f(\bar{\epsilon})\ \bar{y}^{\bar{\epsilon}}.$$

Calculons maintenant f^{**} :

$$\begin{aligned} f^{**}(x_1,\dots,x_n) &= \sum_{\bar{\eta}\in\{0,1\}^n} f^*(\bar{\eta})\ \bar{x}^{\bar{\eta}} \\ &= \sum_{\bar{\eta}\in\{0,1\}^n} \left(\sum_{\bar{\epsilon}\in\{0,1\}^n} f(\bar{\epsilon})\ \bar{\eta}^{\bar{\epsilon}} \right) \bar{x}^{\bar{\eta}} \\ &= \sum_{\bar{\epsilon}\in\{0,1\}^n} f(\bar{\epsilon}) \cdot \sum_{\bar{\eta}\in\{0,1\}^n} \bar{\eta}^{\bar{\epsilon}} \bar{x}^{\bar{\eta}} \\ &= f(x_1,\dots,x_n), \end{aligned}$$

car $\sum_{\bar{\eta}\in\{0,1\}^n} \bar{\eta}^{\bar{\epsilon}}\bar{x}^{\bar{\eta}}$ vaut 1 si les uples $\bar{\epsilon}$ et $\bar{x}$ sont identiques et 0 sinon.

Donc une fonction sur $\{0,1\}$ est la fonction coefficient de sa propre fonction coefficient. Cela veut dire que passer du polynôme à sa fonction coefficient ou de la fonction coefficient au polynôme, dans cette représentation canonique des fonctions par des polynômes, est la même opération, si bien que supposer que le fait qu'une fonction soit calculable rapidement implique que sa fonction coefficient est calculable rapidement est équivalent à supposer que si la fonction coefficient d'une fonction est calculable rapidement alors la fonction est calculable rapidement. Ce qui est curieux, c'est que la propriété que nous venons d'établir à partir d'un calcul très simple reste vraie dans un cadre plus général mais un peu différent, quand on s'intéresse au calcul de polynômes.

3. Polynômes de degré polynomialement borné

Nous sommes alors dans le cadre de la théorie de Valiant (sans constantes), si bien que les résultats sont assez simples à obtenir grâce au travail effectué au chapitre précédent. La première proposition montre que la classe VNP^0 est stable pour le passage à la fonction coefficient et réciproquement. Valiant avait déjà remarqué que si, pour tout n, g_n est le coefficient d'un monôme dans le développement de f_n par rapport à certaines variables et si (f_n) appartient à VNP, alors (g_n) appartient à VNP. Ce qui suit est plus général au sens où on considère les fonctions coefficients décrites en début de chapitre.

Proposition 2. Les propositions suivantes sont équivalentes :

(i) (f_n) appartient à la classe VNP^0.

(ii) pour toute suite (g_n) telle que g_n soit une fonction coefficient de f_n, (g_n) appartient à la classe VNP^0.

(iii) il existe une suite (g_n) telle que g_n soit une fonction coefficient de f_n et que (g_n) appartienne à la classe VNP^0.

Preuve.
(ii) $\Rightarrow$(iii) est évident.

(iii) $\Rightarrow$(i) : il suffit de remarquer que $\bar{y}^{\bar{\epsilon}}$ est calculable par un circuit VP^0, et donc si :

$$g_n(\bar{x}, \bar{z}) = \sum_{\bar{\eta}} h_n(\bar{x}, \bar{z}, \bar{\eta}),$$

on obtient pour f_n :

$$f_n(\bar{x}, \bar{y}) = \sum_{\bar{\epsilon}, \bar{\eta}} h_n(\bar{x}, \bar{\epsilon}, \bar{\eta}) \bar{y}^{\bar{\epsilon}},$$

et la suite (f_n) appartient bien à VNP^0.

(i) $\Rightarrow$(ii). Soit $f(x_1, \ldots, x_m, y_1, \ldots, y_n)$ un polynôme de degré total d en les variables y_k qui est projection via σ du hamiltonien $(\mathrm{HC}_{q)})$:

$$\mathrm{HC}_q(\bar{z}) = \sum_{\bar{\epsilon}\in\{0,1\}^{p(m+n)^2}} h_q(\bar{\epsilon}) \prod_{i,j} z_{i,j}^{\epsilon_{i,j}}.$$

Intuitivement, on souhaite identifier les monômes du hamiltonien qui vont se projeter sur un monôme donné via σ. La fonction coefficient souhaitée revient à faire la somme des coefficients de ces monômes de HC_q.

Nous représentons un monôme en les variables $y_1, \ldots, y_n$ par l'uple $(\bar{\eta}_1, \ldots, \bar{\eta}_n)$ tel que $(\eta_{k,0}, \ldots, \eta_{k,\lfloor \log d \rfloor})$ est la décomposition binaire de la puissance de y_k. Nous allons commencer par construire un circuit qui calcule le polynôme $u(\bar{\epsilon}, \bar{\eta})$ valant 1 si et seulement si $\bar{\eta}$ représente le monôme en $\bar{y}$ qu'on obtient lorsqu'on applique la projection σ au monôme $\bar{z}^{\bar{\epsilon}}$. Pour chaque couple (i, j), avec i et j compris entre 1 et q, tel que $z_{i,j}$ se projette sur une variable y_k, on met l'uple $\bar{\alpha}$ dont toutes les coordonnées sont nulles sauf $\alpha_{k,0}$ qui vaut $\epsilon_{i,j}$. On somme ensuite tous ces uples de la manière suivante : la somme de $(\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ et $(\bar{\beta}_1, \ldots, \bar{\beta}_n)$ est l'uple $(\bar{\gamma}_1, \ldots, \bar{\gamma}_n)$ tel que $\bar{\gamma}_i$ est la représentation binaire de la somme des nombres représentés par $\bar{\alpha}_i$ et $\bar{\beta}_i$. Ce circuit calcule les puissances $\bar{\alpha}_1, \ldots \bar{\alpha}_n$ du monôme en $\bar{y}$ obtenu à partir de $\bar{z}^{\bar{\epsilon}}$ via la projection. On termine le circuit calculant $u(\bar{\epsilon}, \bar{\eta})$ en testant l'égalité de $\bar{\alpha}$ et $\bar{\eta}$. Ce calcul se fait par des sommes itérées d'entiers, donc en profondeur logarithmique (cf. [**22**]), ce qui permet de s'assurer que le degré reste polynomial.

On considère maintenant les polynômes suivants, pour tous i et j :

- si $z_{i,j}$ se projette sur une variable y_k, c'est le polynôme 1.
- si $z_{i,j}$ se projette sur un entier relatif a, c'est le polynôme $\epsilon_{i,j}\, a \; + 1 - \epsilon_{i,j}$
- si $z_{i,j}$ se projette sur une variable x_k, c'est le polynôme $\epsilon_{i,j}\, x_k \; + 1 - \epsilon_{i,j}$.

Le produit de ces polynômes calcule le polynôme $v(\bar{\epsilon}, \bar{x})$ dont la valeur est le coefficient du monôme en $\bar{y}$ qu'on obtient quand on applique σ au monôme $\bar{z}^{\bar{\epsilon}}$.

Il est facile de vérifier que tous ces circuits sont de taille et de degré formel complet polynomiaux en q. Enfin la fonction coefficient $g(\bar{x}, \bar{\eta})$ de f par rapport aux variables $\bar{y}$ vaut :

$$g(\bar{x}, \bar{\eta}) = \sum_{\bar{\epsilon}\in\{0,1\}^{q^2}} h_q(\bar{\epsilon})\; u(\bar{\epsilon}, \bar{\eta})\; v(\bar{\epsilon}, \bar{x}).$$

□

Notons que lorsqu'on dit que g_n est une fonction coefficient de f_n, ça veut dire que pour chaque n on choisit un sous-ensemble des variables et g_n est la fonction coefficient de f_n par rapport aux variables de ce sous-ensemble. C'est un choix non-uniforme, au sens où les variables choisies pour n n'ont pas forcément de rapport avec celles choisies pour $n + 1$. La propriété que nous exprimons ici avec des classes est en fait valide au niveau d'un polynôme individuel.

Ce premier résultat laisse supposer que VNP^0 est une bonne classe pour l'étude des fonctions coefficients, car elle est stable pour le passage d'un polynôme a sa fonction coefficient et réciproquement.

On en déduit ensuite le théorème suivant, qui rappelle le résultat simple obtenu dans le cas du corps $\{0,1\}$, avec en plus le fait que l'on a peu de chances de prouver mieux, car démontrer l'une des deux implications reviendrait à prouver que $\mathrm{VP}^0 = \mathrm{VNP}^0$.

THÉORÈME 8. *Les propositions suivantes sont équivalentes :*

(i) pour toute suite (f_n)*, si* (f_n) *appartient à* VP^0*, alors pour toute suite* (g_n) *telle que* g_n *soit une fonction coefficient de* f_n*,* (g_n) *appartient à la classe* VP^0*.*

(ii) pour toute suite (f_n)*, s'il existe une suite* (g_n) *de la classe* VP^0 *telle que* g_n *soit une fonction coefficient de* f_n *alors* (f_n) *appartient à* VP^0*.*

(iii) $\mathrm{VP}^0 = \mathrm{VNP}^0$*.*

Preuve.
(i) implique (iii) : on utilise la suite de polynômes VP^0 (K_n) définie dans la démonstration du lemme 14 et dont un coefficient est le hamiltonien. La suite des fonctions coefficients par rapport aux monômes en $\bar{y}$ appartient donc aussi à VP^0, et enfin en particulier la suite de ces fonctions appliquées au code du monôme $y_1 z_1 \cdots y_n z_n$, qui est la suite (HC_n). Par complétude du hamiltonien, on en déduit que $\mathrm{VP}^0 = \mathrm{VNP}^0$.

(iii) implique (i) : (f_n) appartient à VP^0, donc (f_n) appartient à VNP^0, (g_n) appartient à VNP^0 d'après la proposition 2, et enfin (g_n) appartient à VP^0 si on suppose (iii).

(ii) implique (iii) : d'après le lemme 13, la fonction coefficient du hamiltonien est VP^0, donc le hamiltonien aussi si on suppose (ii) et $\mathrm{VP}^0 = \mathrm{VNP}^0$.

(iii) implique (ii) : si (g_n) appartient à VP^0, (f_n) appartient à VNP^0, donc (f_n) appartient à VP^0 si on suppose (iii). □

Si l'on considère les classes de complexité VQP et VNQP telles qu'elles ont été décrites à la section 7 du chapitre 2, pour lesquelles le hamiltonien reste complet et en suivant la même démarche, on peut obtenir pour les suites de polynômes de degré quasi-polynomialement bornée des résultats similaires à ceux de la proposition 2 et du théorème 8, valables en toute caractéristique. Le cas où l'on considère des suites de polynômes sans borner la croissance du degré est étudié au chapitre suivant.

CHAPITRE 5

Coefficients d’un polynôme : cas du degré non borné

Les classes de degré polynomialement borné sont naturelles à cause des différents problèmes comme le calcul du permanent ou du hamiltonien qui sont complets sous cette condition. Cependant, nous avons vu que le nombre de monômes d'un polynôme calculé par un circuit de taille polynomiale, même de degré exponentiel, restait simplement exponentiel. On peut donc toujours représenter un monôme par un uple booléen de taille polynomiale. Pour étudier la complexité des fonctions coefficients sans la restriction sur le degré il nous faut définir des analogues des classes de Valiant de degré non borné. Nous tentons ensuite de montrer des résultats similaires à ceux de la question précédente, en introduiant une suite de polynômes complète et en étudiant ses propriétés. Nous ramenons ainsi le problème à celui du calcul de gros coefficients binomiaux, ce qui est faisable en caractéristique positive et semble difficile en caractéristique nulle.

1. Classes de degré non borné

Nous restons dans le cadre de nos classes sans constantes. La complexité dont il est question ici s'entend donc comme définie par des circuits calculant avec les seules constantes 0, 1 et -1.

Définition 26. Une suite de polynômes (f_n) appartient à la classe $\mathrm{VP}^0_{\mathrm{nb}}$ si le nombre de variables et la complexité de f_n sont bornés par un polynôme en n. Rappelons que la complexité d'un polynôme est ici définie par des circuits n'utilisant pas d'autres constantes que 0, 1 et -1.

Définition 27. Une suite de polynômes (f_n) appartient à la classe $\mathrm{VNP}^0_{\mathrm{nb}}$ s'il existe une suite $(g_n(y_1, \ldots, y_{v(n)}))$ appartenant à la classe $\mathrm{VP}^0_{\mathrm{nb}}$ telle que :

$$f_n(x_1, \ldots, x_{u(n)}) = \sum_{\bar{\epsilon} \in \{0,1\}^{v(n)-u(n)}} g_n(x_1, \ldots, x_{u(n)}, \bar{\epsilon}).$$

Définition 28. Un polynôme f est une k-projection d'un polynôme g si on peut écrire $f(\bar{x}) = g(a_1, \ldots, a_m)$, où chaque a_i est soit un entier relatif calculable à partir de -1 par un circuit de taille inférieur ou égale à k, soit une variable parmi $x_1, \ldots, x_n$.
Une suite (f_n) est une projection d'une suite (g_n) s'il existe deux fonctions $s(n)$ et $t(n)$ polynomialement bornées telles que pour tout n, f_n est une $s(n)$-projection de $g_{t(n)}$.

Définition 29. Une suite de polynômes (f_n) appartenant à $\mathrm{VNP}^0_{\mathrm{nb}}$ est $\mathrm{VNP}^0_{\mathrm{nb}}$-complète si toute suite (g_n) de $\mathrm{VNP}^0_{\mathrm{nb}}$ est une projection de (f_n).

On retrouve la propriété fondamentale de stabilité par projection, qui se démontre de la même manière.

Lemme 17. *Les classes* $\mathrm{VP}^0_{\mathrm{nb}}$ *et* $\mathrm{VNP}^0_{\mathrm{nb}}$ *sont stables par projection.*

Nous allons suivre la même démarche que dans le cas borné. Nous avons utilisé le polynôme HC_n, qui possède plusieurs propriétés intéressantes, notamment celle d'être complet. Nous commençons donc par construire un polynôme $\mathrm{VNP}^0_{\mathrm{nb}}$-complet.

2. Un polynôme complet

Cette construction se fait en plusieurs étapes, en obtenant d'abord un polynôme $\mathrm{VP}^0_{\mathrm{nb}}$ -complet, puis un polynôme $\mathrm{VNP}^0_{\mathrm{nb}}$-complet, et enfin en étudiant les propriétés de ce dernier. C'est essentiellement la construction d'un polynôme universel, calquée sur celle de [**5**].

2.1. Un polynôme $\mathrm{VP}^0_{\mathrm{nb}}$ -complet.

Proposition 3. Il existe une suite de polynômes (G_n^n) qui est complète pour la classe $\mathrm{VP}^0_{\mathrm{nb}}$.

Preuve. On construit en fait une famille de polynômes qui représente un calcul générique par un SLP de taille polynomiale. On commence par définir par récurrence des polynômes G_l^m :

- $G_{-m}^m = 1, G_{-m+1}^m = y_1, \dots, G_0^m = y_m$.
- pour $l \geq 1$,
$$G_l^m = \left(\sum_{i=-m}^{l-1} a_{l,i} G_i^m \right) \cdot \left(\sum_{i=-m}^{l-1} b_{l,i} G_i^m \right),$$
où les $a_{l,i}$ et $b_{l,i}$ sont de nouvelles variables.

On montre facilement par récurrence que :

- le nombre de variables de G_l^m est $2lm + l^2 + l + m$.
- tous les polynômes G_l^m sont calculables simultanément par un SLP de taille $4lm + 2l^2 - 3l + m$.

Montrons que (G_n^n) est complet pour la classe $\mathrm{VP}^0_{\mathrm{nb}}$. Soit $f(x_1, \dots, x_n)$ un polynome et C un SLP de longueur $t+n$ calculant f. On suppose d'abord que C est sans constantes. Nous allons spécialiser le calcul générique en substituant des valeurs adéquates aux $a_{l,i}$ et aux

$b_{l,i}$, afin de simuler les étapes du calcul de f par le SLP C. Soit k un entier plus grand que n (nombre de variables de f) et t (nombre d'étapes de calcul). Alors f est une projection de G_k^k. En effet, C est une suite $(c_1, \ldots, c_t)$ d'instructions de la forme $c_i = (\sigma_i, u_i, v_i)$, avec σ_i appartenant à $\{+, *\}$ et u_i et v_i compris entre $-k$ et $i-1$. On substitue chaque variable y_i de G_k^k par la variable x_i, et on donne la valeur 0 aux éventuelles variables supplémentaires (si k est plus grand que n). Nous allons donner des valeurs aux variables $a_{i,j}$ et $b_{i,j}$ selon l'instruction C_i pour i compris entre 1 et t :

- si $\sigma_i = +$ et si $u_i \neq v_i$, on donne la valeur 1 à a_{i,u_i}, a_{i,v_i} et $b_{i,-q(n)}$, et 0 aux autres $a_{i,j}$ et $b_{i,j}$.
- si $\sigma_i = +$ et si $u_i = v_i$, on donne la valeur 2 à a_{i,u_i}, la valeur 1 à $b_{i,-q(n)}$, et 0 aux autres $a_{i,j}$ et $b_{i,j}$.
- si $\sigma_i = *$, on donne la valeur 1 à a_{i,u_i} et b_{i,v_i}, et 0 aux autres $a_{i,j}$ et $b_{i,j}$.

Pour $t < i \leq k$, on donne la valeur 1 à $a_{i,t}$ et $b_{i,-k}$ et 0 aux autres. f est ainsi projection de G_k^k, et cette projection associe $x_1, \ldots, x_n$ à $y_{-k+1}, \ldots, y_0$ respectivement. On peut ensuite projeter de nouveau si on veut obtenir un polynôme qui utilise les constantes 0, 1 et -1. □

2.2. Un polynôme $\mathrm{VNP}^0_{\mathrm{nb}}$-complet.

PROPOSITION 4. Il existe une suite de polynômes polynôme (D_n) qui est complète pour la classe $\mathrm{VNP}^0_{\mathrm{nb}}$.

Preuve. On définit maintenant le polynôme suivant :

$$D_n = \sum_{k=0}^{n} c_k \sum_{\bar\epsilon \in \{0,1\}^{n-k}} G_n^n(\bar a, \bar b, y_1, \ldots, y_k, \epsilon_1, \ldots, \epsilon_{n-k}).$$

Soit $f(x_1, \ldots, x_n)$ un polynôme défini par une somme de Valiant à partir d'un polynôme de complexité polynomiale $g(z_1, \ldots, z_{r(n)})$:

$$f(x_1, \ldots, x_n) = \sum_{\bar\epsilon \in \{0,1\}^{r(n)-n}} g(x_1, \ldots, x_n, \epsilon_1, \ldots, \epsilon_{r(n)-n}).$$

On sait que g est la projection de $G_{q(n)}^{q(n)}(\bar a, \bar b, y_1, \ldots, y_{q(n)})$ pour un polynôme $q(n)$, c'est-à-dire qu'il existe des uples $\bar u, \bar v, w_1, \ldots, w_{q(n)-r(n)}$ de $\{-1, 0, 1, 2\}$ tels que :

$$g(z_1, \ldots, z_{r(n)}) = G_{q(n)}^{q(n)}(\bar u, \bar v, w_1, \ldots, w_{q(n)-r(n)}, z_1, \ldots, z_{r(n)}).$$

On a ensuite :

$$g(x_1,\dots,x_n,\epsilon_1,\dots,\epsilon_{r(n)-n}) = G_{q(n)}^{q(n)}(\bar{u},\bar{v},w_1,\dots,w_{q(n)-r(n)},x_1,\dots,x_n,\epsilon_1,\dots,\epsilon_{r(n)-n}).$$

Si on affecte en plus 1 à $c_{q(n)-r(n)+n}$ et 0 aux autres c_k, on a montré que f est une projection de $D_{q(n)}$.

Il reste à vérifier que la suite D_n est elle-même un polynôme définissable par une somme de Valiant à partir d'une suite de polynômes de complexité polynomiale. Soit :

$$H_n(\bar{a},\bar{b},y_1,\dots,y_n,e_1,\dots,e_n) = \sum_{k=0}^{n} c_k e_1\cdots e_k G_n^n(\bar{a},\bar{b},y_1,\dots,y_k,e_{k+1},\dots,e_n).$$

(H_n) est clairement de complexité polynomiale, et :

$$D_n = \sum_{\bar{\epsilon}\in\{0,1\}^n} H_n(\bar{a},\bar{b},y_1,\dots,y_n,\epsilon_1,\dots,\epsilon_n).$$

□

Maintenant que nous avons un polynôme $\mathrm{VNP}^0_{\mathrm{nb}}$-complet, il nous faut étudier sa fonction coefficient. Commençons par le polynôme G_n^n.

2.3. Fonction coefficient pour le polynôme (G_n^n).

2.3.1. *Les termes du développement.*

Développons le polynôme G_n^n, en suivant sa définition, sans regrouper les termes identiques qui apparaissent (nous appellerons ceci un développement complet).

$$G_n^n = \left(\sum_{i=-n}^{n-1} a_{n,i}G_i^n\right)\cdot\left(\sum_{i=-n}^{n-1} b_{n,i}G_i^n\right).$$

Il faut alors choisir un terme de la somme de gauche et un terme de la somme de droite. Si on choisit $a_{n,i}G_i^n$ et $b_{n,j}G_j^n$, un terme du développement complet de G_n^n correspondant à ce choix est le produit d'un terme du développement complet de G_i, d'un terme du développement complet de G_j^n et de $a_{n,i}b_{n,j}$. Pour chacun de ces polynômes G_i^n et G_j^n on choisit de nouveau un terme dans la somme de droite (avec sa variable a) et un terme dans la somme de gauche (avec sa variable b), sauf si l'indice correspondant (i ou j) est inférieur ou égal à 0, auquel cas on a une variable ou 1 et on s'arrête.

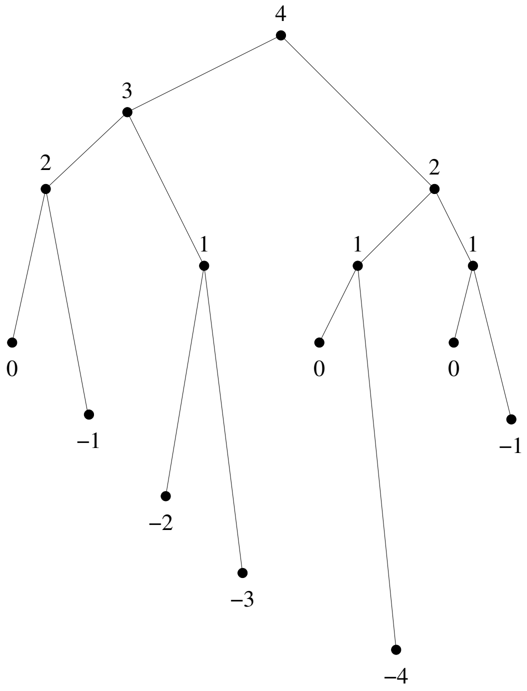


FIG. 1. L'arbre d'un terme du développement de G_4^4.

On peut ainsi identifier tout terme du développement complet du polynôme G_n^n par un arbre binaire dont chaque noeud est étiqueté par un entier compris entre $-n$ et n, de telle sorte que les conditions suivantes soient satisfaites.

(i) La racine est étiquetée par n.

(ii) L'étiquette d'un noeud est strictement supérieure à celle de ses deux fils.

(iii) Un noeud est une feuille si et seulement si il est étiqueté par un entier inférieur ou égal à 0.

Cet arbre indique comment on a obtenu le terme lors du développement. Dans l'exemple de la figure 1, le terme correspondant est :

$$a_{4,3}a_{3,2}a_{2,1}a_{2,0}a_{1,0}^2a_{1,-2}b_{4,2}b_{3,1}b_{2,1}b_{2,-1}b_{1,-1}b_{1,-3}b_{1,-4}y_4^3y_3^2y_2y_1.$$

De manière plus générale, déterminons le monôme correspondant à un arbre qui satisfait les conditions ci-dessus. Chaque noeud de l'arbre revient lors du développement à faire le produit de ses fils en multipliant par les variables a et b adéquates. Les variables y_i ne sont présentes qu'aux feuilles. A la racine de l'arbre, dans le monôme obtenu, on a le produit de toutes les feuilles et des variables correspondant aux branches. La puissance d'une variable $a_{i,j}$ (respectivement $b_{i,j}$) est le nombre d'arêtes gauches (respectivement droites) joignant un noeud étiqueté par i à un noeud étiqueté par j. Les puissances des variables $a_{i,j}$ et $b_{i,j}$ indiquent donc les choix effectués lors du développement ; elles déterminent donc l'arbre de développement et le terme correspondant. La puissance d'une variable y_i est le nombre de feuilles étiquetées par $-n+i$.

2.3.2. *Quels sont les monômes qui apparaissent ?*

Malheureusement le nombre d'arbres binaires de profondeur inférieure à k est doublement exponentiel en k et G_n^n a des termes dont les arbres peuvent être de profondeur $2n+1$. Si on avait eu un nombre simplement exponentiel de termes dans le développement complet, il aurait suffit de coder un tel arbre, et de faire la somme sur tous les codes possibles correspondant à un monôme donné pour montrer que la fonction coefficient était $\mathrm{VNP}^0_{\mathrm{nb}}$. Nous ne pouvons donc procéder de cette manière. De plus, nous aimerions pouvoir calculer effectivement la fonction coefficient, c'est-à-dire montrer que la suite des fonctions coefficients totales appartient à $\mathrm{VP}^0_{\mathrm{nb}}$.

Nous allons donc chercher à exprimer différemment cette somme de termes, en regroupant ceux qui donnent le même monôme. Au lieu des arbres binaires étiquetés décrits ci-dessus, nous allons considérer des graphes orientés à $2n+1$ sommets. Cela revient en fait à identifier les noeuds de notre arbre portant la même étiquette. On obtient ainsi une structure plus petite et plus facile à décrire car elle ne contient que $2n+1$ sommets. Entre les sommets de ce graphe il y aura des arêtes de deux types, gauche et droit, selon qu'un noeud de l'arbre était un fils droit ou gauche d'un autre. La figure 2 présente le graphe associé à l'arbre de dvéloppement de la figure 1. Notre graphe doit provenir d'un arbre ce qui impose les conditions suivantes.

(i) Le sommet n possède exactement une arête droite et une arête gauche.

(ii) Pour tout sommet d'indice i supérieur ou égal à 1, le nombre d'arêtes gauches le reliant aux sommets d'indice strictement inférieur à i est égal au nombre d'arêtes droites le reliant aux sommets d'indice strictement inférieur à i, et égal au nombre d'arêtes des deux types le reliant aux sommets d'indice strictement supérieur à i.

(iii) Tout sommet d'indice i inférieur ou égal à 0 n'est pas relié à un sommet d'indice strictement inférieur à i.

(iv) Un sommet ne peut être relié aux sommets d'indice strictement supérieurs.

Si on note $A_{i,j}$ (respectivement $B_{i,j}$) le nombre d'arêtes gauches (respectivement droites) allant du sommet i au asommet j, ceci se traduit par les conditions suivantes :

(i) $\sum_{i=-m}^{n-1} A_{n,i} = \sum_{i=-m}^{n-1} B_{n,i} = 1$.

(ii) Pour tout $i \geq 1$, $\sum_{j<i} A_{i,j} = \sum_{j<i} B_{i,j} = \sum_{j>i} (A_{j,i} + B_{j,i})$.

(iii) Pour tout $i \leq 0$, pour tout $j < i$, $A_{i,j} = B_{i,j} = 0$.

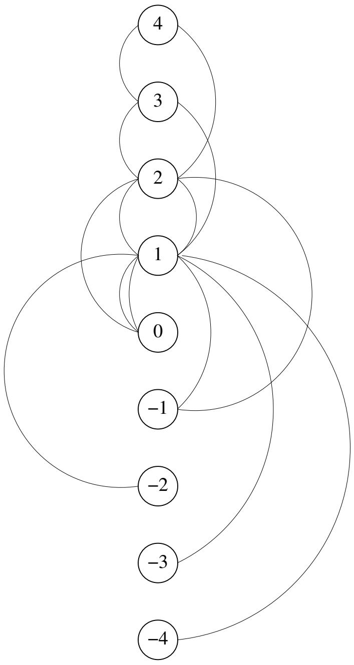


FIG. 2. Le graphe associé à l'arbre précédent.

(iv) Pour tout i et j, si $j < i$, , $A_{i,j} = B_{i,j} = 0$.

La donnée de $S = ((A_{i,j}), (B_{i,j}))$ détermine notre structure. Il est clair que si S satisfait ces conditions, il existe un arbre binaire étiqueté dont le graphe de monôme associé est S.

Déterminons le monôme associé à un tel graphe. Dans le monôme associé à un arbre, la puissance en $a_{i,j}$ était le nombre d'arêtes reliant un noeud étiqueté par i à un noeud étiqueté par j, ce nombre est exactement $A_{i,j}$. De manière similaire, la puissance en $b_{i,j}$ est $B_{i,j}$. Enfin, pour les y_i, le nombre de feuilles étiquetées par $-n+i$ était aussi le nombre d'arêtes arrivant à une feuille étiquetée par $-n+i$, ce qui dans le graphe est le nombre d'arêtes arrivant au sommet $-n+i$, soit :

$$\sum_{j\geq 1}(A_{j,i} + B_{j,i}).$$

On associe à un graphe le monôme dont les puissances ont été décrites ci-dessus. Cette application est surjective, car un monôme de G_n^n apparaît comme au moins un terme du développement, terme identifié par un arbre. Le monôme est donc l'image du graphe de monôme associé à cet arbre. Cette application est injective : si deux graphes $S = (A, B)$ et $S' = (A', B')$ sont différents, par exemple par $A_{i,j} \neq A'_{i,j}$, alors la puissance de la variable $a_{i,j}$ du monôme associé à S est différente de celle du monôme associé à S', et les monômes sont différents.

Cette représentation va nous permettre dans un premier temps de décrire quels sont les monômes présents dans G_n^n. On code par les uples $\alpha_{i,j,k}$ $(0 \leq k \leq n)$, $\beta_{i,j,k}$ $(0 \leq k \leq n)$ et $\epsilon_{i,k}$ $(0 \leq k \leq n)$ la puissance en base 2 des variables $a_{i,j}$, $b_{i,j}$ et y_i respectivement. Pour vérifer si un uple $\bar{\alpha}, \bar{\beta}, \bar{\epsilon}$ code un monôme présent dans G_n^n, on teste les conditions sur les nombres d'arêtes pour qu'un graphe corresponde à un monôme, ce qui revient à faire des opérations sur les $\bar{\alpha}_{i,j}$, $\bar{\beta}_{i,j}$ et $\bar{\epsilon}_i$. Notons $\mathrm{val}(\bar{u})$ l'entier codé en binaire par l'uple booléen $\bar{u}$. Les conditions à vérifier sont les suivantes.

(i) $\sum_{i=-m}^{n-1} \mathrm{val}(\bar{\alpha}_{n,i}) = \sum_{i=-m}^{n-1} \mathrm{val}(\bar{\beta}_{n,i}) = 1$.

(ii) Pour tout $i \geq 1$, $\sum_{j<i} \mathrm{val}(\bar{\alpha}_{i,j}) = \sum_{j<i} \mathrm{val}(\bar{\beta}_{i,j}) = \sum_{j>i}(\mathrm{val}(\bar{\alpha}_{i,j}) + \mathrm{val}(\bar{\beta}_{i,j}))$.

(iii) Pour tout $i \leq 0$, pour tout $j < i$, $\mathrm{val}(\bar{\alpha}_{i,j}) = \mathrm{val}(\bar{\beta}_{i,j}) = 0$.

(iv) Pour tout i et j, si $j < i$, $\mathrm{val}(\bar{\alpha}_{i,j}) = \mathrm{val}(\bar{\beta}_{i,j}) = 0$.

Ces calculs et ces tests se font sur des entiers inférieurs à 2^n et codés en binaire. Nous donnerons une description plus explicite de ces calculs à la section 3.1.

2.3.3. *Coefficient d'un monôme.*

Pour obtenir la fonction coefficient, il reste donc à calculer le nombre de termes qui donnent le même monôme lors du développement, c'est-à-dire le nombre d'arbres produisant le même graphe.

Pour obtenir un arbre à partir d'un graphe de monôme, il faut séparer chaque sommet en autant de noeuds qu'il reçoit d'arêtes venant des sommets d'indice supérieur, et distribuer un fils gauche et un fils droit à chacun parmi les arêtes droites et gauches partant de ce sommet vers des sommets d'indice inférieur. Nous évaluons le nombre de façons de faire ces séparations en partant du sommet n du graphe, qui donne la racine de l'arbre (étiquetée par n). Ce sommet n'apparaît qu'une fois dans un arbre, il n'a pas besoin d'être séparé. On suppose ensuite qu'on a construit tous les debuts d'arbre possibles jusqu'au niveau i (cf. figure 3). Pour chacun de ces arbres, on ordonne les noeuds de niveau i de la gauche vers la droite. On suppose qu'il y en a k. Cela veut dire que dans notre graphe on avait k arêtes qui arrivaient au sommet i. Il faut répartir entre ces noeuds de niveau i les arêtes gauches et droites que l'on avait dans le graphe. Il faut donc évaluer le nombre de façons différentes de répartir les fils gauches, sachant que l'on a $A_{i,j}$ arêtes allant vers le sommet j. On choisit donc d'abord $A_{i,i-1}$ noeuds parmi k, ce seront les noeuds auxquels on donnera comme fils gauche une arête allant vers un noeud étiqueté par $i-1$ puis $A_{i,i-2}$ noeuds parmi $k - A_{i,i-1}$, puis $A_{i,i-3}$ noeuds parmi $k - A_{i,i-1} - A_{i,i-2}$ et ainsi de suite. Le nombre de possiblités vaut donc (nous utilisons la notation anglo-saxonne pour les coefficients binomiaux pour des raisons de clarté) :

$$\begin{pmatrix} k \\ A_{i,i-1} \end{pmatrix} \begin{pmatrix} k - A_{i,i-1} \\ A_{i,i-2} \end{pmatrix} \cdots \begin{pmatrix} k - A_{i,i-1} - \cdots A_{i,-n+1} \\ A_{i,-n} \end{pmatrix},$$

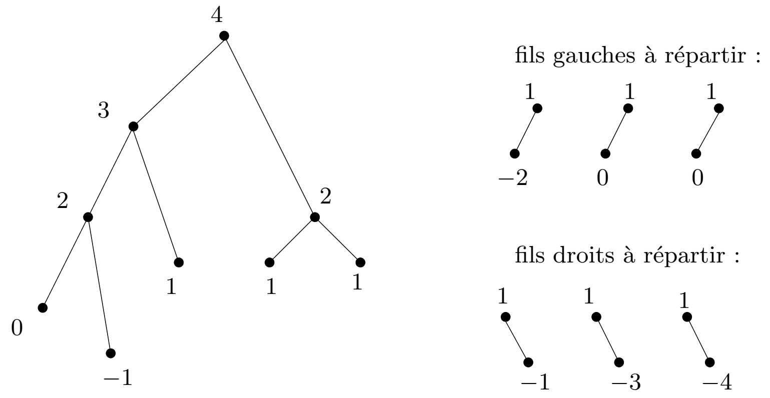


FIG. 3. Un début d'arbre donnant le graphe de la figure 2.

ce qui est encore égal à :

$$\frac{k!}{A_{i,i-1}!\cdots A_{i,-n}!}=\frac{\left(\sum_{j=-n}^{i-1}A_{i,j}\right)!}{\prod_{j=-n}^{i-1}A_{i,j}!}.$$

Le raisonnement est le même pour les fils droits, donc on multiplie les deux valeurs obtenues. Pour deux choix différents, quelle que soit la façon dont on séparera les sommets en-dessous, les arbres résultant seront différents. On doit donc faire le produit pour chaque noeud d'indice strictement positif de ces valeurs :

$$\prod_{i=1}^{n}\left(\frac{\left(\sum_{j=-n}^{i-1}A_{i,j}\right)!}{\prod_{j=-n}^{i-1}A_{i,j}!}\cdot\frac{\left(\sum_{j=-n}^{i-1}B_{i,j}\right)!}{\prod_{j=-n}^{i-1}B_{i,j}!}\right).$$

Comme tout arbre est obtenu ainsi, cela nous donne le coefficient du monôme.

2.3.4. *Pour le polynôme D_n.*

Le polynôme D_n contient en plus des variables de G_n^n les variables $c_0,\dots,c_n$. Nous codons la puissance de la variable c_i par le booléen γ_i, car la puissance de c_i vaut 0 ou 1 dans un monôme de D_n. Nous souhaitons donc déterminer et calculer par un polynôme la fonction $d_n(\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon)$ telle que :

$$D_n=\sum_{\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon}d(\bar\alpha,\bar\beta,\bar\gamma,\epsilon)\;\bar a^{\bar\alpha}\,\bar b^{\bar\beta}\,\bar c^{\bar\gamma}\,\bar y^{\bar\epsilon}.$$

Dans la section précédente, on a mis G_n^n sous la forme :

$$\sum_{\bar{\alpha},\bar{\beta},\bar{\epsilon}} v(\bar{\alpha},\bar{\beta})\, c(\bar{\alpha},\bar{\beta},\bar{\epsilon})\; \bar{a}^{\bar{\alpha}}\, \bar{b}^{\bar{\beta}}\, \bar{y}^{\bar{\epsilon}},$$

où $v(\bar{\alpha},\bar{\beta})$ calcule la valeur du coefficient et $c(\bar{\alpha},\bar{\beta},\bar{\epsilon})$ vérifie que $(\bar{\alpha},\bar{\beta},\bar{\epsilon})$ code bien un monôme de G_n^n, en particulier ce polynôme calcule les puissances des variables y_i en fonction de $\bar{\alpha},\bar{\beta}$ et teste l'égalité avec $\bar{\epsilon}$. Par définition de D_n :

$$D_n = \sum_{k=0}^{n} c_k \sum_{\bar{\eta}\in\{0,1\}^{n-k}} G_n^n(\bar{a},\bar{b},y_1,\ldots,y_k,\eta_1,\ldots,\eta_{n-k}),$$

ce qui donne :

$$\begin{aligned} D_n &= \sum_{k=0}^{n} c_k \sum_{\bar{\alpha},\bar{\beta},\bar{\epsilon},\bar{\eta}} v(\bar{\alpha},\bar{\beta})\, c(\bar{\alpha},\bar{\beta},\bar{\epsilon})\; \bar{a}^{\bar{\alpha}}\, \bar{b}^{\bar{\beta}}\, y_1^{\bar{\epsilon}_1}\cdots y_k^{\bar{\epsilon}_k}\, \eta_1^{\bar{\epsilon}_{k+1}}\cdots \eta_{n-k}^{\bar{\epsilon}_n} \\ &= \sum_{k=0}^{n} \sum_{\bar{\alpha},\bar{\beta},\bar{\epsilon}} v(\bar{\alpha},\bar{\beta})\, c(\bar{\alpha},\bar{\beta},\bar{\epsilon})\; c_k\, \bar{a}^{\bar{\alpha}}\, \bar{b}^{\bar{\beta}}\, y_1^{\bar{\epsilon}_1}\cdots y_k^{\bar{\epsilon}_k} \sum_{\bar{\eta}} \eta_1^{\bar{\epsilon}_{k+1}}\cdots \eta_{n-k}^{\bar{\epsilon}_n}. \end{aligned}$$

On a vue que pour $\bar{\alpha}$ et $\bar{\beta}$ fixés on pouvait calculer la valeur unique des $\bar{\epsilon}_i$ correspondant. La valeur de la somme :

$$\sum_{\bar{\eta}} \eta_1^{\bar{\epsilon}_{k+1}}\cdots \eta_{n-k}^{\bar{\epsilon}_n}$$

ne dépend plus que de $\bar{\alpha}$ et $\bar{\beta}$. En effet, notons u la fonction qui prend le code en binaire de k et des $\bar{\epsilon}_i$ et renvoie le code en binaire du nombre d'indices i compris entre $k+1$ et n tels que $\bar{\epsilon}_i$ soit complètement nul. La somme précédente vaut $2^{u(k,\bar{\epsilon})}$.

La fonction coefficient de D_n commence donc par tester qu'une seule des variables c_k apparaît avec une puissance non-nulle, et elle renvoie le code binaire de l'indice k correspondant. Elle calcule ensuite la fonction coefficient de G_n^n, elle multiplie par $2^{u(k,\bar{\epsilon})}$ et enfin elle vérifie que les puissances $\bar{\epsilon}_i$ des y_i pour $i > k$ sont nulles.

Le problème c'est que le calcul précédent fait intervenir des coefficients binomiaux $\binom{j}{i}$ pour des valeurs de i et j pouvant atteindre 2^n, qui paraissent difficiles à calculer rapidement par un circuit. L'apparition de ces gros coefficients n'est pas surprenante, car le polynôme G_n^n est complet pour les suites de polynômes de complexité polynomiale, donc le polynôme suivant doit s'obtenir par projection :

$$(x+y)^{2^n} = \sum_{i=0}^{2^n} \left(\begin{array}{c} 2^n \\ i \end{array} \right) x^i\, y^{2^n-i}.$$

Ses coefficients doivent s'exprimer, par projection, comme une somme au pire simplement exponentielle sur la fonction coefficient de G_n^n. Nous commençons par traiter un cas où ces gros entiers ne posent plus de problèmes, c'est-à-dire en caractéristique positive.

3. Corps de caractéristique positive

3.1. Calcul de la fonction coefficient.

Le calcul des coefficients binomiaux modulo p se fait rapidement grâce au théorème de Lucas.

THÉORÈME 9 (Lucas,1878). *Soit deux entiers m et n, $m = m_0 + m_1 p + \cdots + m_d p^d$ et $n = n_0 + n_1 p + \cdots + n_d p^d$ leurs décompositions respectives en base p, alors :*

$$\begin{pmatrix} n \\ m \end{pmatrix} \equiv \begin{pmatrix} n_0 \\ m_0 \end{pmatrix} \begin{pmatrix} n_1 \\ m_1 \end{pmatrix} \cdots \begin{pmatrix} n_d \\ m_d \end{pmatrix} \quad (mod\, p).$$

LEMME 18. *Dans un corps de caractéristique positive, la fonction coefficient totale du polynôme D_n est* VP^0.

Preuve. Nous montrons un peu plus que ce dont nous avons besoin. En suivant la méthode appliquée quand le degré était borné, il suffirait de montrer que cette fonction coefficient est $\mathrm{VP}^0_{\mathrm{nb}}$. Nous montrons donc qu'elle est VP^0, ce qui sera utile pour la suite. Nous allons reprendre les étapes du calcul de la fonction coefficient en vérifiant que tout peut se faire avec un degré polynomial, la plupart du temps en montrant que le calcul peut se faire en profondeur logarithmique.

Etape 1 : tester si un uple code un monôme qui apparaît dans le développement de G_n^n. Cela se fait en manipulant les uples $\bar{\alpha}_{i,j}$ et $\bar{\beta}_{i,j}$. Plus précisément, on effectue des sommes itérées, i.e. des sommes de (environ) n entiers de longueur n. Ces sommes itérées peuvent se faire en profondeur logarithmique en n (cf. [**22**]). Les tests d'égalité de deux entiers de longueur n codés en binaire se font en profondeur logarithmique.

Etape 2 : calcul des $\bar{\epsilon}_i$. C'est encore une somme itérée à partir des variables $\bar{\alpha}_{i,j}$ et $\bar{\beta}_{i,j}$.

Etape 3 : calcul du polynôme u, qui prend en entrée les $\bar{\epsilon}_i$ et un entier k codé en binaire et renvoie le code binaire du nombre d'indices i compris entre $k+1$ et n et tels que $\bar{\epsilon}_i$ soit complètement nul. On commence par tester en parallèle si chaque $\bar{\epsilon}_i$ est l'uple nul, ce qui se fait en profondeur logarithmique. Toujours en parallèle, pour chaque i on teste si i est strictement supérieur à k et on multiplie le résultat de ce test par celui du test sur $\bar{\epsilon}_i$, ce qui nous donne une valeur δ_i. Ceci se fait en profondeur logarithmique. Enfin on additionne en binaire les δ_i, pour obtenir une valeur u codée en binaire et de longueur $\lceil \log n \rceil$; c'est encore une somme itérée qui se fait en profondeur logarithmique.

Etape 4 : on veut calculer 2^u. On effectue le calcul suivant :

$$\prod_{i=0}^{\lfloor \log n \rfloor} (u_i \cdot 2^{2^i} + 1 - u_i),$$

ce qui est un calcul de taille et de degré polynomiaux.

Etape 5 : tester qu'exactement une seule des variables c_k a une puissance non-nulle se fait via le polynôme suivant :

$$\left(\prod_{0 \leq i < j \leq n} (1 - \gamma_i \gamma_j) \right) \left(\sum_{i \leq i \leq n} \gamma_i \right),$$

donc c'est bien de degré polynomial.

Etape 6 : renvoyer le code binaire de la variable k telle que la puissance de c_k est non-nulle. En parallèle, pour chaque i compris entre 1 et n, on écrit le code binaire de i et on multiplie chacun de ses bits par γ_i, ce qui nous donne le code d'un nombre qui est i si $\bar{\gamma}_i$ est l'entier 0 et 0 (codé en binaire) sinon. On effectue ensuite la somme itérée de ces nombres codés en binaire.

Etape 7 : vérifier que les puissances $\bar{\epsilon}_i$ des y_i pour i strictement plus grand que k sont nulles. En parallèle, pour chaque i, on écrit le code de i et on teste s'il est supérieur au code de k, et on teste si $\bar{\epsilon}_i$ est l'uple nul. On sélectionne ensuite par un circuit de taille constante, selon la valeur du test sur i et k : si $i > k$, on renvoie le résultat du test sur $\bar{\epsilon}_i$, sinon on renvoie 1. On effectue le produit des résultats obtenus pour chaque i, le tout en profondeur logarithmique.

Etape 8 : La décomposition d'un entier $m = \sum_{i=0}^{n} m_i 2^i$ en base p peut se faire en utilisant dans le circuit la décomposition en base p des puissances de 2 : $2^i = \sum_{j=0}^{n} d_{i,j} p^j$. Alors :

$$m = \sum_{i=0}^{n} m_i \sum_{j=0}^{n} d_{i,j} p^j = \sum_{i=0}^{n} \left(\sum_{j=0}^{n} m_i d_{i,j} p^j \right).$$

On a encore une fois affaire à la somme itérée de n nombres à n chiffres en base p, où chaque chiffre est représenté en base 2. Les opérations sur les chiffres se font avec un nombre constant d'opérations, donc ce calcul se fait en profondeur logarithmique.

Etape 9 : le calcul d'un coefficient binomial de deux nombres inférieurs à p se fait enfin par un circuit de profondeur constante. Il ne reste plus qu'à faire le produit d'un nombre polynomial de ces coefficients. □

3.2. Autres propriétés.

Nous avons aussi utilisé le fait que le polynôme HC_n est le coefficient d'un monôme d'un polynôme de la classe VP^0. Le lemme suivant permet d'avoir une propriété équivalente pour le polynôme D_n.

Lemme 19. *Dans un corps de caractéristique positive, il existe un polynôme* $\mathrm{VP}^0_{\mathrm{nb}}$ *dont un monôme a pour coefficient le polynôme* D_n.

Preuve. Nous allons en fait montrer que l'on peut séparer pour le polynôme D_n la partie qui consiste à calculer des puissances hautes des variables d'entrée de celle qui consiste à faire une somme de Valiant.

Considérons notre polynôme $\mathrm{VNP}^0_{\mathrm{nb}}$-complet D_n. On a vu qu'il se mettait sous la forme :

$$\sum_{\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon} d_n(\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon)\ \bar a^{\bar\alpha}\,\bar b^{\bar\beta}\,\bar c^{\bar\gamma}\,\bar y^{\bar\epsilon}.$$

On considère une nouvelle fonction $d'_n(\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon)$ qui prend en entrée des booléens et manipule des entiers codés en base 2, renvoyant à la fin la valeur que renvoyait d mais en la conservant en base 2, sans reconstruire l'élément du corps correspondant. On considère maintenant le polynôme :

$$P(u_0,\ldots,u_n,\alpha_0,\ldots,\alpha_n) = u_0^{\alpha_0}u_1^{\alpha_1}\cdots u_n^{\alpha_n} = \prod_{i=0}^{n}(\alpha_i u_i + 1 - \alpha_i).$$

Alors :

$$P(1,a,a^2,\ldots,a^n,\alpha_0,\alpha_1,\ldots,\alpha_n) = a^{\alpha_0+\alpha_1\cdot 2+\cdots+\alpha_n\cdot 2^n} = a^{\bar\alpha}.$$

Ainsi P, sur l'entrée des puissances de 2 successives d'une variable et d'une puissance en binaire, calcule la variable élevée à cette puissance. De même, $P(1,2,\ldots,2^{2^n},d'(\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon))$ est le polynôme $d(\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon)$.

On considère ensuite le polynôme $d''_n(\bar\alpha,\bar\beta,\bar\gamma,\bar\epsilon,\bar u,\bar v,\bar w,\bar z,\bar t)$, qui comporte, en plus des variables $\bar\alpha$, $\bar\beta$, $\bar\gamma$ et $\bar\epsilon$ les variables $u_{i,j,k}$ (pour $-n \le j < i \le n$ et $0 \le k \le n$), $v_{i,j,k}$ (pour $-n \le j < i \le n$ et $0 \le k \le n$), $w_{i,k}$ (pour $0 \le i \le n$ et $0 \le k \le n$), $z_{i,k}$ (pour $1 \le i \le n$ et $0 \le k \le n$) et t_i (pour $0 \le i \le n$) :

$$\begin{aligned}&P(t_0,t_1,\ldots,t_n,d'(\bar\alpha,\bar\beta,\bar\gamma,\ \bar ep))\\ &\qquad * \left(\prod_{i>j} P(\bar u_{i,j},\bar\alpha_{i,j})\right)\cdot\left(\prod_{i>j} P(\bar v_{i,j},\bar\beta_{i,j})\right)\cdot\left(\prod_{i=0}^{n} P(\bar w_i,\bar\gamma_i)\right)\cdot\left(\prod_{i=1}^{n} P(\bar z_i,\bar\epsilon_i)\right).\end{aligned}$$

Ce polynôme est VP^0. De plus, sur l'entrée de $a_{i,j}^{2^k}$ pour $u_{i,j,k}$, de $b_{i,j}^{2^k}$ pour $v_{i,j,k}$, de $c_i^{2^k}$ pour $w_{i,k}$, de $y_i^{2^k}$ pour $z_{i,k}$ et de 2^k pour t_k, il est égal à $d(\bar{\alpha},\bar{\beta},\bar{\gamma},\bar{\epsilon})\bar{a}^{\bar{\alpha}}\bar{b}^{\bar{\beta}}\bar{c}^{\bar{\gamma}}\bar{y}^{\bar{\epsilon}}$.

Le polynôme suivant est donc VNP^0 :

$$D'_n = \sum_{\bar{al},\bar{\beta},\bar{ga},\bar{\epsilon}} d''_n(\bar{\alpha},\bar{\beta},\bar{\gamma},\bar{\epsilon},\bar{u},\bar{v},\bar{w},\bar{z},\bar{t}).$$

Par complétude du hamiltonien pour la classe VNP^0, il existe une projection bornée σ qui donne le polynôme D'_n. Si on applique cette projection au polynôme K_n du lemme 14 du chapitre 3, D'_n est le coefficient du monôme $y_1z_1\cdots y_nz_n$ de $\sigma(K_n)$. Enfin on remplace dans $\sigma(K_n)$ les entrées $u_{i,j,k}$, $v_{i,j,k}$, $w_{i,k}$, $z_{i,k}$ et t_k par les valeurs adéquates énoncées ci-dessus et on obtient un polynôme calculable par un circuit de taille polynomiale et dont D_n est un coefficient. ☐

3.3. Complexité d'un polynôme et de sa fonction coefficient : cas du degré non borné.

Les résultats de la section précédente sont suffisants pour pouvoir réitérer les propriétés obtenues dans le cas du degré borné. Elles se démontrent de la même manière.

Proposition 5. Dans un corps de caractéristique positive, pour toute suite de polynômes (f_n) :

(i) si une fonction coefficient (f_n^c) appartient à $\mathrm{VNP}^0_{\mathrm{nb}}$, alors (f_n) appartient à $\mathrm{VNP}^0_{\mathrm{nb}}$.

(ii) si (f_n) appartient à $\mathrm{VNP}^0_{\mathrm{nb}}$, alors toute fonction coefficient (f_n^c) appartient à $\mathrm{VNP}^0_{\mathrm{nb}}$.

Théorème 10. *Dans un corps de caractéristique non-nulle, les propositions suivantes sont équivalentes :*

(i) pour toute suite (f_n), si (f_n) appartient à $\mathrm{VP}^0_{\mathrm{nb}}$, alors toute fonction coefficient (f_n^c) appartient à $\mathrm{VP}^0_{\mathrm{nb}}$.

(ii) pour toute suite (f_n), si une fonction coefficient (f_n^c) appartient à $\mathrm{VP}^0_{\mathrm{nb}}$, alors (f_n) appartient à $\mathrm{VP}^0_{\mathrm{nb}}$.

(iii) $\mathrm{VP}^0_{\mathrm{nb}} = \mathrm{VNP}^0_{\mathrm{nb}}$.

4. Conséquence pour l'hypothèse de Valiant non bornée

Par ailleurs, le travail effectué pour obtenir ces résultats a une conséquence brutale sur les classes de complexité avec degré non borné définies ici.

Théorème 11. *Sur un corps de caractérisique p non-nulle,* $\mathrm{VP}^0 = \mathrm{VNP}^0$ *si et seulement si* $\mathrm{VP}^0_{\mathrm{nb}} = \mathrm{VNP}^0_{\mathrm{nb}}$.

Preuve. Sur un corps de caractéristique p non-nulle. Soit (f_n) appartenant à $\mathrm{VNP}^0_{\mathrm{nb}}$. Par complétude, f_n est projection de D_n. Or on a vu que D_n était égal au polynôme g_n auquel on substitue les bonnes variables, avec g_n appartenant à VNP^0. Si $\mathrm{VP}^0 = \mathrm{VNP}^0$, (g_n) appartient à VP^0 et après substitution (D_n) appartient à $\mathrm{VP}^0_{\mathrm{nb}}$, et enfin par projection (f_n) appartient à $\mathrm{VP}^0_{\mathrm{nb}}$.

La partie réciproque de cette équivalence est vraie sur tout corps. Soit donc (f_n) appartenant à VNP^0. (f_n) appartient à $\mathrm{VNP}^0_{\mathrm{nb}}$, et donc sous l'hypothèse $\mathrm{VP}^0_{\mathrm{nb}} = \mathrm{VNP}^0_{\mathrm{nb}}$, (f_n) appartient à $\mathrm{VP}^0_{\mathrm{nb}}$. Cela veut dire que f_n est calculable par un circuit de taille polynomiale. De plus, comme (f_n) appartient à VNP^0, le degré de f_n est polynomial aussi. On peut donc calculer (f_n) par une suite de circuits de degré formel polynomialement borné, donc (f_n) appartient à VP^0. ☐

5. Corps de caractéristique nulle

Pour pouvoir utiliser les techniques précédentes, il faut savoir calculer rapidement les coefficients binomiaux. Notons ici que même avec les conventions de Valiant, qui offrent des constantes arbitraires, il n'est pas évident que la fonction coefficient totale de D_n soit calculable rapidement, car elle a besoin de pouvoir calculer des coefficeints binomiaux qui dépendent de ses entrées. En ce sens les nouvelles classes sans constantes n'étaient pas strictement nécessaires. Néanmoins, grâce aux lemmes 2 et 3, ces résultats restent valables si on s'autorise les constantes, et le travail supplémentaire est faible, une bonne partie des développements techniques ayant été causée par l'utilisation du hamiltonien pour ne pas négliger la caractéristique 2.

Soit $B_n(\bar{\beta}, \bar{\alpha})$ le polynôme calculant le coefficient binomial $\binom{\bar{\beta}}{\bar{\alpha}}$, considérons la suite de polynômes :

$$f_n(x_0, \ldots, x_n, y_1, y_2) = \prod_{i=0}^{n} \left(x_i (y_1 + y_2)^{2^i} + 1 - x_i \right).$$

Elle appartient bien à $\mathrm{VP}^0_{\mathrm{nb}}$. Si $\bar{\beta}$ est un uple booléen, $f_n(\bar{\beta}, y_1, y_2)$ est le polynôme :

$$(y_1+y_2)^{\bar\beta} = \sum_{\bar\alpha} \left(\begin{array}{c} \bar\beta \\ \bar\alpha \end{array} \right) y_1^{\bar\alpha} y_2^{\bar\beta-\bar\alpha}.$$

Soit donc $g_n(\bar x, \bar\epsilon, \bar\eta)$ la fonction coefficient de f_n par rapport aux variables y_1 et y_2 :

$$f_n(\bar x, y_1, y_2) = \sum_{\bar\epsilon,\bar\eta} g_n(\bar x, \bar\epsilon, \bar\eta)\, y_1^{\bar\epsilon} y_2^{\bar\eta}.$$

On en déduit que si on pose $\bar\gamma$ le code binaire de l'entier obtenu en soustrayant l'entier codé par $\bar\alpha$ à l'entier codé par $\bar\beta$, alors $B_n(\bar\beta, \bar\alpha) = g_n(\bar\beta, \bar\alpha, \bar\gamma)$.

Si l'on savait que les fonctions coefficients de suites $\mathrm{VP}^0_{\mathrm{nb}}$ sont $\mathrm{VP}^0_{\mathrm{nb}}$, on pourrait calculer rapidement ces coefficients binomiaux. Ceci est assez peu probable, car le lemme suivant montre que cela impliquerait un calcul rapide de la factorielle par un circuit numérique, ce qui est peu probable (cf. [**4**]).

Lemme 20. *Si $B_n(\bar\beta, \bar\alpha)$ est calculable par un circuit de taille polynomiale en n, alors $k!$ est calculable par un circuit de taille polynomiale en* $\log k$.

Preuve. On va d'abord montrer par induction que si $B_n(\bar\beta, \bar\alpha)$ est calculable par un circuit de taille polynomiale $q(n)$, alors pour tout n, $2^n!$ est calculable par un circuit de taille $p(n) = 1 + 2n + nq(n)$

Si $n = 0$, on a un circuit de taille 1.

Supposons que notre hypothèse soit vraie jusqu'à $n-1$. Alors :

$$2^n! = (2^{n-1}!)^2 \cdot \left(\begin{array}{c} 2^n \\ 2^{n-1} \end{array} \right).$$

Or le coefficient binomial est calculable par un circuit de taille $q(n)$, donc $2^n!$ est calculable par un circuit de taille :

$$\begin{array}{rcl} p(n-1) + 2 + q(n) & = & 1 + 2(n-1) + (n-1)q(n-1) + 2 + q(n) \\ & \leq & 1 + 2n + nq(n). \end{array}$$

Montrons maintenant que pour tout tout k tel que $2^n \leq k < 2^{n+1}$, $k!$ est calculable par un circuit de taille $1 + 2n + nq(n) + np(n)$.

Si k vaut 1 ou 2, $k!$ est calculable par un circuit de taille 1.

Supposons que la propriété soit vraie pour $n-1$. Soit k tel que $2^n \leq k < 2^{n+1}$. Alors :

$$k! = 2^n! \cdot (k-2^n)! \cdot \left(\begin{array}{c} k \\ 2^n \end{array} \right).$$

$\left(\begin{smallmatrix} k \\ 2^n \end{smallmatrix} \right)$ est calculable par un circuit de taille $q(n)$, $2^n!$ par un circuit de taille $p(n)$, donc :

$$\begin{array}{rcl} r(n+1) & = & q(n) + p(n) + r(n-1) + 2 \\ & = & q(n) + p(n) + 1 + 2(n-1) + (n-1)q(n) + (n-1)p(n) + 2 \\ & \leq & 1 + 2n + nq(n) + np(n). \end{array}$$

$\square$

CHAPITRE 6

Dérivation simultanée de polynômes

On a cité au chapitre 1 le fait que si un polynôme est calculable par un circuit de taille t, le polynôme correspondant à sa dérivée partielle par rapport à une variable est calculable par un circuit de taille $4t$. Par contre il semble difficile d'obtenir rapidement les dérivées partielles itérées, comme le montre le polynôme f_n de la section 2 du chapitre 2, ou encore le polynôme construit au lemme 14 du chapitre 3 :

$$f_n(\bar{z}, \bar{y}) = \prod_{1 \leq i \leq n} \left(\sum_{1 \leq j \leq n} z_{i,j} y_j \right).$$

Le monôme $y_1 \cdots y_n$, dont le permanent des $\bar{z}$ est le coefficient, est le seul à ne pas s'annuler quand on calcule $\partial^n f_n / \partial y_1 \cdots \partial y_n$, si bien que :

$$\frac{\partial^n f_n}{\partial y_1 \cdots \partial y_n} = \mathrm{per}(z_{i,j}).$$

Une méthode permettant de dériver rapidement par rapport à plusieurs variables conduirait donc à un calcul rapide du permanent.

Il est facile de voir que le rapport avec les classes de Valiant est un peu plus fort que l'obtention du permanent par dérivation.

Proposition 6. Les propriétés suivantes sont équivalentes.

(i) $\mathrm{VP}^0 = \mathrm{VNP}^0$.

(ii) Pour toute suite $(f_n(x_1, \ldots, x_{q(n)}))$ appartenant à VP^0, pour tout polynôme $p(n)$, pour tous entiers $p_{n,i}$ avec i compris entre 0 et $q(n)$ et dont la somme vaut $p(n)$, la suite :

$$\left(\frac{\partial^{p(n)} f_n}{\partial x_1^{p_{n,1}} \cdots \partial x_{q(n)}^{p_{n,q(n)}}} \right)_{n \in \mathbb{N}}$$

appartient à VP^0.

Preuve.
(i) →(ii). Si on suppose que $\mathrm{VP}^0 = \mathrm{VNP}^0$, alors la fonction coefficient totale de f_n appartient à VP^0 :

$$f_n(\bar{x}) = \sum_{\bar{\epsilon}} g_n(\bar{\epsilon}) \bar{x}^{\bar{\epsilon}},$$

avec (g_n) qui appartient à VP^0.

Les $p_{n,i}$ étant fixés, on construit d'abord le circuit $C_i(\bar{\epsilon}_i)$ qui prend en entrée $\bar{\epsilon}_i$, qui représente l'entier e_i, et calcule d'abord en parallèle les codes des entiers correspondant à $e_i + 1, \ldots, e_i + p_{n,i}$, ce qui se fait en profondeur logarithmique en n, car $p_{n,i}$ et e_i sont de taille logarithmique. Ensuite il convertit, toujours en parallèle, chacun de ces codes de taille logarithmique en l'entier lui-même, ce qui se fait en profondeur logarithmique, et enfin il les multiplie entre eux, toujours en profondeur logarithmique, car il y en a $p_{n,i}$. La fonction coefficient totale h_n de la dérivée partielle itérée souhaitée est calculée par le circuit qui prend des uples $\bar{\eta}_1, \ldots, \bar{\eta}_n$, ajoute en parallèle $p_{n,i}$ à chaque $\bar{\eta}_i$, appelle g_n sur les uples résultant, puis multiplie cela par le produit des $C_i(\bar{\eta}_i)$, qui ont été calculés en parallèle. La suite de polynômes (h_n) est donc bien VP^0, et si $\mathrm{VP}^0 = \mathrm{VNP}^0$, cela implique que la suite de polynômes dont (h_n) est la suite des fonctions coefficients totales est VP^0. Cette suite est la suite des dérivées partielles itérées souhaitées.

(ii) →(i). On fait le raisonnement qui vient d'être décrit au début de ce chapitre, mais en utilisant le polynôme du lemme 14 dont le hamiltonien est un coefficient. ☐

On obtient la même propriété avec les classes de degré non-borné, en caractéristique positive. La preuve est similaire mais on n'a pas besoin de faire attention à la profondeur.

Proposition 7. Les propriétés suivantes sont équivalentes :

(i) $\mathrm{VP}^0_{\mathrm{nb}} = \mathrm{VNP}^0_{\mathrm{nb}}$,

(ii) pour toute suite $(f_n(x_1, \ldots, x_{q(n)}))$ appartenant à $\mathrm{VP}^0_{\mathrm{nb}}$, pour tout polynôme $p(n)$, pour tous entiers $p_{n,i}$ avec i compris entre 0 et $p(n)$ et n positif ou nul, la suite :

$$\left(\frac{\partial^{p(n)} f_n}{\partial x_1^{p_{n,1}} \cdots \partial x_{q(n)}^{p_{n,q(n)}}} \right)_{n \in \mathbb{N}}$$

appartient à $\mathrm{VP}^0_{\mathrm{nb}}$.

Nous étudions ici plus en détail l'influence des dérivations partielles sur la complexité de calcul d'un polynôme. Dans le cas de la dérivation par rapport à une seule variable, nous affinons un résultat de Kaltofen, puis étudions les cas du calcul d'une ou de toutes les dérivées partielles d'ordre m. Pour des raisons de concision des résultats nous revenons ici à des circuits ou SLP pouvant utiliser des constantes dans un corps fixé au départ. Nous étudions donc des polynômes sur un corps et la manipulation des circuits qui les calculent.

1. Dérivée partielle itérée par rapport à une variable

Le premier théorème implique le théorème 3.1 de [**12**] et se démontre de manière similaire. C'est aussi un résultat proche du théorème de Portier [**15**], valable dans un anneau différentiel. Nous nous plaçons dans ce cadre, plus général et utile pour la suite.

Un anneau différentiel est un anneau commutatif $(A, 0, 1, +, -, \times)$ muni d'une dérivation, c'est-à-dire d'une fonction d de A dans A telle que $\mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y$ et $\mathrm{d}(xy) = x\mathrm{d}y + y\mathrm{d}x$ pour tous x, y éléments de A. Soit K un corps ; nous considérons ici l'anneau $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ des polynômes en $2n$ variables à coefficients dans K, muni de la dérivation d telle que $\mathrm{d}x_i = y_i$ et $\mathrm{d}y_i = 0$. Autrement dit $\mathrm{d}P = \sum_{i=1}^{n} y_i \cdot \partial P/\partial x_i$.

Notons respectivement $\mathrm{M}_s(m)$ et $\mathrm{M}_d(m)$ la taille et la profondeur d'un circuit calculant le produit de deux polynômes de degré inférieur ou égal à m : d'après [**6**], sur une algèbre quelconque, il existe un circuit de taille $O(m \cdot \log m \cdot \log\log m)$ et de profondeur $O(\log m)$ effectuant ce calcul.

THÉORÈME 12. *Soit* $P(x_1, \ldots, x_n)$ *un polynôme calculable par un circuit de taille* τ *et de profondeur* π *; alors il existe un circuit calculant les polynômes* $(\mathrm{d}^k P/k!)$*, pour* $0 \leq k \leq m$*, de taille* $\tau \cdot \mathrm{M}_s(m)$ *et de profondeur* $\pi \cdot \mathrm{M}_d(m)$*.*

Preuve. Nous reprenons la preuve de Kaltofen pour construire un circuit calculant $\mathrm{d}^k P/k!$ pour $0 \leq k \leq m$.

On commence par placer $m+1$ copies du circuit calculant P (numérotées de 0 à m) les unes à côté des autres. Le nœud $w^{[i]}$ de la ième copie du circuit va calculer $(d^i w/i!)$, où w est le polynôme calculé au noeud correspondant dans le circuit initial (numéroté 0). Cela s'obtient en ajoutant des portes de calcul :

- si w est une variable x_j, on pose $w^{[i]} = y_j$ si i vaut 1, et 0 si i est strictement supérieur à 1.
- si $w = u + v$, on pose $w^{[i]} = u^{[i]} + v^{[i]}$.
- si $w = u \times v$, on pose $w^{[i]} = \sum_{k=0}^{i} u^{[k]} v^{[i-k]}$.

On montre facilement par récurrence sur i que chaque noeud $w^{[i]}$ du circuit i calcule $(\mathrm{d}^i w/i!)$: par exemple, si $w = u \times v$, on a :

$$\begin{aligned} w^{[i+1]} &= \sum_{k=0}^{i+1} u^{[k]} v^{[i+1-k]} \\ &= \sum_{k=0}^{i+1} \frac{1}{k!}\mathrm{d}^k u \cdot \frac{1}{(i+1-k)!}\mathrm{d}^{i+1-k} v \\ &= \frac{1}{(i+1)!} \sum_{k=0}^{i+1} C_{i+1}^{k}\ \mathrm{d}^k u\ \mathrm{d}^{i+1-k} v \\ &= \frac{1}{(i+1)!}\mathrm{d}^{i+1} w. \end{aligned}$$

Evaluons maintenant la taille et la profondeur du circuit obtenu. Le calcul des portes de multiplication est le plus coûteux. Si on a calculé tous les $u^{[k]}$ et les $v^{[k]}$ pour $0 \leq k \leq m$, on calcule simultanément tous les $w^{[k]}$ en $\mathrm{M}_s(m)$ étapes, avec une profondeur de $\mathrm{M}_d(m)$, car ce calcul correspond exactement à l'obtention des coefficients du produit de deux polynômes. D'où les bornes du théorème. ☐

Le corollaire suivant correspond donc au théorème 3.1 de [**12**].

COROLLAIRE 3. *Soit $P(x_1, \ldots, x_n)$ un polynôme calculable par un circuit de taille τ et de profondeur π ; alors il existe un circuit calculant le polynôme $\partial^m P/\partial x_i^m$, de taille $\tau \cdot \mathrm{M}_s(m) + 1$ et de profondeur $\cdot\pi \cdot \mathrm{M}_d(m) + 1$*

Preuve. Nous avons construit un circuit qui calcule le polynôme $(d^m P/m!)$. Or nous souhaitons obtenir $\partial^m P/\partial x_i^m$. Le lien entre ces deux polynômes est le suivant :

$$d^m P = \sum_{m_1+\cdots+m_n=m} \left(\frac{m!}{m_1!\cdots m_n!}\right) \cdot \left(\frac{\partial^m P}{\partial x_1^{m_1}\cdots\partial x_n^{m_n}}\right)(y_1)^{m_1}\cdots(y_n)^{m_n},$$

si bien que notre circuit calcule

$$\sum_{m_1+\cdots+m_n=m} \left(\frac{1}{m_1!\cdots m_n!}\right) \cdot \left(\frac{\partial^m P}{\partial x_1^{m_1}\cdots\partial x_n^{m_n}}\right)(y_1)^{m_1}\cdots(y_n)^{m_n}.$$

Pour obtenir un circuit calculant le coefficient souhaité, il suffit donc de substituer toutes les variables dérivées y_j par 0, sauf y_i qu'on remplace par 1. Le seul monôme qui ne s'annule pas est $(y_i)^m$, on obtient ainsi $(1/m!) \cdot \partial^m P/\partial x_i^m$, et en multipliant par $m!$ on a le coefficient désiré, ce qui ajoute 1 à la taille et à la profondeur obtenues au théorème précédent. ☐

Ce premier résultat concerne la dérivation par rapport à une variable. La section suivante traite des dérivées partielles itérées et justifie le point de vue différent que nous avons adopté. En appliquant plusieurs fois ce corollaire, nous pouvons déjà dire que c'est le nombre de variables par rapport auxquelles on dérive qui fait exploser la taille, plus que l'ordre de dérivation : si on dérive un polynôme par rapport à un nombre fixe de variables, d'un ordre polynomial en chaque variable, la taille du polynôme augmente polynomialement seulement. Ce que nous souhaitons montrer c'est que, dans le calcul d'une dérivée partielle itérée, une partie du calcul est indépendante de la variable de dérivation, ce qui permet d'améliorer les bornes par rapport à une simple itération du corollaire 3.

2. Dérivation partielle par rapport à plusieurs variables

2.1. Calcul d'une dérivée partielle d'ordre m.

Nous voulons maintenant obtenir le coefficient suivant $\partial^m P/(\partial x_1^{m_1}\cdots\partial x_n^{m_n})$ avec la somme des m_i qui vaut m. Nous remplaçons y_1 par 1 et les variables $y_2,\ldots,y_n$ par les éléments nilpotents $u_2,\ldots,u_n$ de l'algèbre $A = K[u_2,\ldots,u_n]/I$, où I est l'idéal engendré par $u_2^{m_2+1},\ldots,u_n^{m_n+1}$. Le résultat obtenu alors est le polynôme :

$$\sum_{\substack{\epsilon_2\le m_2,\ldots,\epsilon_n\le m_n\\ \epsilon_1=m-(\epsilon_2+\cdots+\epsilon_n)}}\left(\frac{1}{\epsilon_1!\cdots\epsilon_n!}\right)\left(\frac{\partial^m P}{\partial x_1^{\epsilon_1}\cdots\partial x_n^{\epsilon_n}}\right)(u_2)^{\epsilon_2}\cdots(u_n)^{\epsilon_n}.$$

Ensuite, la difficulté réside uniquement dans l'extraction des coefficients de ce polynôme.

Notons respectivement $\mathrm{M}_s(d_1,\ldots,d_n)$ et $\mathrm{M}_d(d_1,\ldots,d_n)$ la taille et la profondeur d'un circuit calculant le produit de deux polynômes en les variables $x_1,\ldots,x_n$ et dont le degré en chaque variable x_i est inférieur ou égal à d_i.

THÉORÈME 13. *Soit $P(x_1,\ldots,x_n)$ un polynôme calculable par un circuit de taille τ et de profondeur π ; alors il existe un circuit calculant $\partial^m P/(\partial x_1^{m_1}\cdots\partial x_n^{m_n})$, de taille $\tau\cdot\mathrm{M}_s(m)\mathrm{M}_s(m_2,\ldots,m_n)+1$ et de profondeur $\pi\cdot\mathrm{M}_d(m)\mathrm{M}_d(m_2,\ldots,m_n)+1$.*

Preuve. En pratique, nous représentons un élément de cette algèbre A comme une somme de monômes en $u_2,\ldots,u_n$ où u_i apparaît avec une puissance inférieure ou égale à m_i. Posons $\bar{m}=(m_2,\ldots,m_n)$ et $I(\bar{m})=\{0,\ldots,m_2\}\times\cdots\times\{0,\ldots,m_n\}$. Nous allons considérer les uples $(a_{\bar{\epsilon}})_{\bar{\epsilon}\in I(\bar{m})}$ d'éléments de $K[x_1,\ldots,x_n]$, qui représentent les coefficients de la décomposition d'un résultat intermédiaire comme somme des monômes $u_2^{\epsilon_2}\cdots u_n^{\epsilon_n}$ pour $\bar{\epsilon}\in I(\bar{m})$. Le coefficient cherché est le dernier élément de l'uple calculé par notre circuit si on remplace en entrée y_1 par 1 et les variables $y_2,\ldots,y_n$ par les uples représentant $u_2,\ldots,u_n$. En effet ce dernier élément correspond à l'indice $(m_2,\ldots,m_n)$. Or notre polynôme de départ était homogène de degré m, donc ce coefficient est bien celui du monôme $y_1^{m_1}\cdots y_n^{m_n}$.

On part du circuit obtenu au théorème 12, et on doit simuler les opération sur des polynômes en plusieurs variables représentés par leurs monômes. Remplacer y_1 par 1 et $y_2,\ldots,y_n$ par les uples représentant $u_2,\ldots,u_n$ se fait sans augmentation de taille, car cela correspond juste à remplacer certains arguments par 0 ou 1. Ensuite chaque porte d'addition est remplacée par un circuit de taille $\prod_{i=2}^n(m_i+1)$ et de profondeur 1 et chaque porte de multiplication par un circuit de taille $\mathrm{M}_s(m_2,\ldots,m_n)$ et de profondeur $\mathrm{M}_d(m_2,\ldots,m_n)$, d'où les bornes du théorème, si on suppose que $\mathrm{M}_s(m_2,\ldots,m_n)\ge\prod_{i=2}^n(m_i+1)$ et en prenant en compte une multiplication finale par $(\prod_{i=1}^n m_i!)$. □

On peut si on le souhaite gagner un petit peu en complexité en choisissant i tel que m_i soit maximal et en remplaçant y_i par 1 et les autres dérivées premières par des éléments nilpotents, ce qui élimine le plus grand m_i des produits dans les bornes du théorème. On retrouve ainsi les résultats du théorème 12 si on applique celui-ci dans le cas où $m_i = m$ et $m_j = 0$ pour $j \neq i$, en notant que $\mathrm{M}_s(0, \dots, 0) = \mathrm{M}_d(0, \dots, 0) = 1$

Comparons les bornes obtenus avec l'itération du corollaire 3, dans le cas particulier où l'on souhaite dériver un polynôme n fois par rapport à chacune de ses n variables. En utilisant la substitution de Kronecker, on obtient les bornes suivantes pour la multiplication de polynômes de degré borné par n en chacune de leur $n-1$ variables : $\mathrm{M}_s(n, \dots, n) = O(2^n n^n (\log n)^2)$ et $\mathrm{M}_d(n, \dots, n) = O(n \log n)$. Comme m vaut ici n^2, on multiplie la taille du circuit calculant le polynôme par $O(2^n n^{n+2} (\log n)^3 \log\log n)$ et sa profondeur par $O(n (\log n)^2)$. L'itération, en prenant en compte les constantes “cachées” α et β dans la notation O, multiplie la taille par $\alpha^n n^n (\log n)^n (\log\log n)^n$ et la profondeur par $\beta^n (\log n)^n$.

2.2. Calcul de toutes les dérivées partielles d'ordre m.

Pour calculer une dérivée partielle itérée, on a donc été amené à extraire presque tous les coefficients du polynôme obtenu grace au théorème 12. Si on les extrait tous on obtient simultanément toutes les dérivées partielles itérées d'ordre m, et ça ne coûte pas beaucoup plus que d'en obtenir une.

Notons respectivement $\mathrm{I}_s(m, n)$ et $\mathrm{I}_d(m, n)$ la taille et la profondeur d'un circuit calculant les coefficients d'un polynôme de degré total m en n variables à partir de son évaluation sur $T(m, n)$ valeurs, où $T(m, n)$ est le nombre de monômes en n variables, de degré total inférieur ou égal à m.

THÉORÈME 14. *Soit $P(x_1, \dots, x_n)$ un polynôme calculable par un circuit de taille τ et de profondeur π et m un entier; alors il existe un circuit calculant les polynômes $\partial^m P/(\partial x_1^{m_1} \cdots \partial x_n^{m_n})$, pour tous $m_1 + \cdots + m_n = m$, de taille $\tau \cdot \mathrm{M}_s(m) T(m, n-1) + \mathrm{I}_s(m, n-1) + T(m, n-1)$ et de profondeur $\pi \cdot \mathrm{M}_d(m) + \mathrm{I}_d(m, n-1) + 1$.*

Preuve. Nous allons encore une fois utiliser le circuit calculant $(\mathrm{d}^m P/m!)$, mais en extrayant tous les coefficients. Nous remplaçons encore une fois la variable y_1 par 1. Nous obtenons alors le polynôme :

$$\sum_{m_1 + \cdots + m_n = m} \left(\frac{1}{(m_1! \cdots m_n!)} \right) \cdot \left(\frac{\partial^m P}{\partial x_1^{m_1} \cdots \partial x_n^{m_n}} \right) (y_2)^{m_2} \cdots (y_n)^{m_n}.$$

On souhaite obtenir tous les coefficients de ce polynôme qui comporte $T(m, n-1)$ monômes. Nous allons procéder par interpolation. Pour cela nous évaluons ce polynôme en $T(m, n-1)$ valeurs adéquates pour un algorithme d'interpolation rapide : on peut prendre les points $(1, 1, \dots, 1)$, $(p_1, \dots, p_{n-1})$, $(p_1^2, \dots, p_{n-1}^2)$, …, $(p_1^{T(m,n-1)-1}, \dots, p_{n-1}^{T(m,n-1)-1})$, en notant p_i

le ième nombre premier. Ceci multiplie la taille par $T(m, n-1)$ et ne change pas la profondeur. Les coefficients recherchés s'obtiennent ensuite par interpolation, en n'oubliant pas de multiplier chaque résultat par le produit convenable de factorielles. $\square$

Supposons qu'on veuille obtenir toutes les dérivées partielles itérées d'ordre n^2 d'un polynôme en n variables. En utilisant une interpolation naïve, i.e. en se donnant comme constantes les coefficients de l'inverse de la matrice de van der Monde, on obtient un circuit de taille $O(\tau \cdot n^2 \log n \log\log n T(n^2, n-1) + T(n^2, n-1)^2)$ et de profondeur $O(\pi \cdot \log n + \log T(n^2, n-1)$. On obtient des bornes proches de celles du circuit qui ne calculait que la dérivée partielle itérée n fois par rapport à chacune des variables.

2.3. Calcul de toutes les dérivées partielles d'ordre inférieur ou égal à m.

Il suffit maintenant de remarquer que le théorème 12 donnait en fait toutes les différentielles d'ordre 0 à m. Avec un calcul de taille similaire on peut donc calculer toutes les dérivées partielles itérées d'ordre inférieur ou égal à m.

Théorème 15. *Soit $P(x_1, \ldots, x_n)$ un polynôme calculable par un circuit de taille τ et de profondeur π et m un entier; alors il existe un circuit calculant les polynômes $\partial^m P/(\partial x_1^{m_1} \cdots \partial x_n^{m_n})$, pour tous $m_1 + \cdots + m_n \leq m$, de taille $\tau \cdot \mathrm{M}_s(m) T(m,n) + \sum_{k=0}^{m} (\mathrm{I}_s(k,n) + T(k,n))$ et de profondeur $\pi \cdot \mathrm{M}_d(m) + \mathrm{I}_d(m,n) + 1$.*

Preuve. On part du circuit calculant tous les $(\mathrm{d}^k P/k!)$. On ne remplace plus y_1 par 1, mais on évalue directement en $T(m,n)$ points, puis on interpole, ce qui ajoute à la taille la somme des interpolations pour chaque ordre, et à la profondeur celle de l'interpolation la plus grande, de degré m. $\square$

Conclusion

Nous avons donc présenté les rapports possibles entre la complexité d'un polynôme et celle de sa fonction coefficient. Pour cela nous avons introduit une variante sans constantes de la théorie de Valiant et développé les outils nécessaires pour en retrouver les résultats essentiels. Au passage nous avons donné une nouvelle caractérisation des classes VP et VQP, qui simplifient les preuves et permettent de trouver de nouvelles suites VQP-complètes. Nous avons aussi envisagé le cas le plus général, sans borne sur le degré des polynômes, et introduit les définitions et lemmes adéquats afin de montrer que le problème dans ce cas revient à calculer de gros entiers. Enfin nous avons montré que calculer toutes les dérivées partielles itérées jusqu'à un certain ordre ne coûtait pas beaucoup plus cher que d'en calculer une dans le pire des cas.

Il reste néanmoins à améliorer les résultats dans le cas où l'on ne sait pas calculer les gros entiers. De plus, les nouvelles classes introduites, sans degré borné, prendront un sens autre que technique seulement si on trouve un polynôme complet "naturel". Il serait par ailleurs intéressant de préciser les conséquences du travail effectué dans le cas du degré non borné sur les liens entre la théorie de Valiant et la complexité algébrique de [**4**]. Enfin, ces réflexions sur la théorie de Valiant et les nouvelles caractérisations permettent d'envisager l'existence de critères de complétude, en s'inspirant par exemple des travaux d'Agrawal et Biswas pour la classe NP. Il s'agit de porter notre attention sur le polynôme g_n par lequel est défini un polynôme VNP, dans le but de montrer qu'il est complet, plutôt que sur ce polynôme lui-même.

Bibliographie

[1] L. Babai & L. Fortnow, 'Arithmetization : a new method in structural complexity theory', *Comput. Complexity* 1 (1991), no. 1, 41–66.

[2] W. Baur & V. Strassen, 'The complexity of partial derivatives', *Theor. Comp. Sci.* 22 (1982) 317–330.

[3] M. Bläser, 'Complete problems for Valiant's class of *qp*-computable families of polynomials', *Proc. 7th Ann. Int. Computing and Combinatorics Conf. (COCOON)*, Lecture Notes in Comput. Sci., 2108, Springer, Berlin, 2001.

[4] L. Blum, F. Cucker, M. Shub & S. Smale, *Complexity and Real Computation.* Springer, 1998.

[5] P. Bürgisser, *Completeness and reduction in algebraic complexity theory* (Springer, New York, 2000).

[6] D.G. Cantor & E. Kaltofen, 'On fast multiplication of polynomials over arbitrary algebras', *Acta Informatica* **28**(7) (1991) 693–701.

[7] J. von zur Gathen, 'Feasible arithmetic computations : Valiant's hypothesis', *J. Symb. Comp.* 4 (1987) 137–172.

[8] J. Hammond, Question 6001. *Educ. Times* 32, 179, (1879).

[9] M. Jerrum & M. Snir, 'Some exact complexity results for straight-line computations over semirings', *J. Assoc. Comput. Mach.*, 29 (1982), 874–897.

[10] E. Kaltofen 'Factorization of polynomials given by straight-line programs', in S. Miscali, editor, *Randomness and Computation*,375–412. (JAI Press, Greenwich CT, 1989).

[11] E. Kaltofen, 'Single-factor Hensel lifting and its application to the straight-line complexity of certain polynomials', in *Proceedings 19th ACM STOC* (1987) 443–452.

[12] E. Kaltofen & M.F. Singer, 'Size efficient parallel algebraic circuits for partial derivatives', in : D. V. Shirkov, V. A. Rostovtsev, and V. P. Gerdt, *IV International Conference on Computer Algebra in Physical Research* (World Scientific Publ. Co., Singapore, 1991) 133–145.

[13] M. Mahajan & V. Vinay, 'Determinant : old algorithms, new insights'. *SIAM J. Discrete Math.* 12(4) (1999), 474–490.

[14] B. Poizat, *Les petits cailloux* (Nur al-mantiq wal-ma'rifah, Lyon, 1995).

[15] N. Portier, 'Stabilité polynomiale des corps différentiels', *J. Symb. Log.* 64(2) (1999) 803–816.

[16] R. Sengupta & H. Venkatsewaran, 'A lower bound for Monotone Arithmetic Circuits Computing 0-1 Permanent', *Theoret. Comput. Sci.* 209 (1998), no. 1-2, 389–398.

[17] L. G. Valiant, 'Completeness classes in algebra', *Proc. 11th ACM STOC* (1979), 249–261.

[18] L. G. Valiant, 'Reducibility by algebraic projections', *Logic and algorithmic : an international symposium held in honor of Ernst Specker*, Monogr. No. 30 de l'Enseign. Math. (1982), 365–380.

[19] L. G. Valiant, 'An algebraic approach to computational complexity', *Proc. Int. Congress of Mathematicians* volume 2, (Polish Scientific Publishers, Warsaw and Elsevier Science Publishers, Amsterdam, 1983), 1637–1644.

[20] L. G. Valiant, 'Why is boolean complexity difficult ?', in *Boolean Function Complexity*, M. S. Paterson ed., London Mathematical Society Lecture Notes Series 169, Cambridge University Press, 1992.

[21] L. G. Valiant, S. Skyum, S. Berkowitz & C. Rackoff, 'Fast parallel computation of polynomials using few processors', *SIAM J. Comp.*, 12(4) (1983), 641–644.

[22] H. Vollmer, *Introduction to circuit complexity. A uniform approach*. Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 1999.

[23] I. Wegener, *The complexity of Boolean functions*. Wiley-Teubner Series in Computer Science. John Wiley & Sons, Ltd., Chichester ; B. G. Teubner, Stuttgart, 1987.