Rapport - Relationless completeness and separations

Lucca Hirchi

28 novembre 2012

Résumé

Nous nous proposons de résumer l'article [2] "Relationless completeness and separations" écrit par P. Hrubes, A. Wigderson et A. Yehudayoff. Dans cet article, les auteurs proposent de revoir les définitions des classes de Valiant dans le cadre d'une algèbre de polynômes non associative ni commutative. Dans ce nouveau cadre, ils prouvent la complétude du permanent et parviennent à séparer les deux classes *VP* et *VNP* (problème ouvert dans le cadre général depuis 33 ans).

Table des matières

1 Introduction

En 1979, L. G. Valiant a étendu la théorie de la complexité au cadre algèbrique du calcul de polynômes. De la même façon que l'on peut définir les problèmes "faciles" (la classe *P*) et les problèmes "difficiles" (la classe *NP*), Valiant a considéré la classe des polynômes "facilement" calculables *VP* et la classe des polynômes "difficilement" calculables *VNP* . Dans la théorie de Valiant, on calcule un polynôme à l'aide d'un circuit dont les entrées sont des variables ou des constantes et où les noeuds dénotent l'addition ou la multiplication des entrées. La complexité se mesure alors sur la taille de ces circuits. On peut montrer que le déterminant est *VP* alors que le permanent est *VNP-complet* (i.e. il permet de simuler n'importe quel polynôme *VNP*). On peut alors se demander si $VP = VNP$. Tout comme dans le cadre des fonctions booléennes, ce problème est toujours ouvert et rien n'indique que les outils actuels puissent y venir à bout.

Il existe alors deux solutions orthogonales : soit il faut modifier les définitions de *VP* et *VNP* en réduisant l'expressivité des circuits, soit il faut modifier l'algèbre de polynômes. Les auteurs choisissent la seconde solution. Leur idée est de considérer une algèbre de polynômes non associative ni commutative. Cette algèbre possède strictement moins de relations ($P * X = X * P$ n'est plus vraie par exemple), il existe donc plus de polynômes différents. Ainsi, les chances de séparer *VP* de *VNP* paraissent plus grandes.

Les auteurs commencent par redéfinir les classes de Valiant dans ce nouveau cadre. Ces définitions ne sont pas du tout triviales et, par exemple, en l'absence d'associativité, il existe plusieurs façon de définir le permanent (une pour chaque façon de parenthéser les monômes et d'ordonner les variables). Leur solution consiste à considérer un parenthésage qui parrait "universel" (i.e. qui permet de simuler tous les autres). La section 2 traite de ces définitons et prouve quelques lemmes préliminaires. Les auteurs prouvent ensuite la complétude du permanent en adaptant une preuve existante. Nous verrons les étapes clés de cette preuve dans la section 3. Finalement, les auteurs en viennet à leur résultat principal : ils montrent que dans leur cadre, *VP* est *strictement* inclus dans *VNP* . La section 4 décrit cette preuve.

2 Définitions et lemmes préliminaires

Dans cette section, nous définissons les classes de polynômes ainsi que les classes de complexité. Nous introduisons le problème de l'universalité du parenthésage et nous définissons le permanent et le déterminant.

2.1 Classes de polynômes

Dans toute la suite $\mathbb{F}$ dénote un corps commutatif quelconque.

Définition 1 (Algèbre de polynôme)**.** $\mathbb{F}_{\overline{A},\overline{C}}[X]$ *désigne une* $\mathbb{F}$*-algèbre* $(\mathbb{F}[X], +, \cdot, *)$ *où* $(\mathbb{F}[X], +, \cdot))$ *est un espace vectoriel sur* $\mathbb{F}$ *et :*

- $* : \mathbb{F}[X] \times \mathbb{F}[X] \to \mathbb{F}[X]$ *est une loi multiplicative sur* $\mathbb{F}[X]$ *;*
- $*$ *est distributive par rapport à* $+$ *;*
- $\forall x, y \in \mathbb{F}\ \forall A, B \in \mathbb{F}[X], (x \cdot A) * (y \cdot B) = (xy) \cdot (A * B)$.

Ainsi $*$ n'est ni associative ni commutative dans $\mathbb{F}_{\overline{A},\overline{C}}[X]$ (contrairement à $+$). Nous définissons de la façon usuelle la notion de monôme dans $\mathbb{F}[X]$, le nombre de variables d'un polynôme ainsi que le degré d'un polynôme : $\deg(\_) : \mathbb{F}_{\overline{A},\overline{C}}[X] \to \mathbb{N}$. Enfin, nous définissons les *p*-familles de polynômes.

Définition 2 (*p*-famille)**.** *Une suite de polynômes $(f_i)_{i\in\mathbb{N}}$ est une p-famille s'il existe un polynôme $p \in \mathbb{R}[X]$ tel que pour tout $i \in \mathbb{N}$, $\deg(f_i) \leq p(i)$ et le nombre de variables de f_i est au plus $p(i)$.*

2.2 Classes de complexité

Il faut raffiner la notion de circuit usuelle pour le cadre non associatif et non commutatif. Toutes les portes étiquetées par $+$ ou $*$ (tous les noeuds internes du circuits) ont des entrées ordonnées : "gauche" et "droite". Cette modification est importante, elle permet par exemple de distinguer les deux circuits suivants (qui calculent les polynômes distincts $X(YZ)$ et $X(ZY)$) :

FIGURE 1 – Deux circuits différents

Nous définissons de la façon habituelle la taille d'un circuit $|C|$, les sous-circuits ainsi que les termes (i.e. circuits dont l'arité sortante de tout noeud est d'au plus 1).

Définition 3 (*VP*)**.** *Une famille (f_i) (i.e. série de polynômes) est dans* VP *si c'est une* p*-famille et s'il existe un polynôme $p \in \mathbb{R}[X]$ et une série de circuit (C_i) tels que pour tout $i \in \mathbb{N}$, C_i calcule f_i et $|C_i| \leq p(n)$.*

Définition 4 (*VNP*)**.** *Une famille (f_i) est dans* VNP *si c'est une* p*-famille et s'il existe une famille (g_i) dans* VP *ainsi qu'un polynôme $p \in \mathbb{R}[X]$ tel que pour tout $i \in \mathbb{N}$,*

$$f_i(x_1, \ldots, x_n) = \sum_{\epsilon_1,\ldots,\epsilon_{p(i)}\in\{0;1\}} g_i(x_1, \ldots, x_n, \epsilon_1, \ldots, \epsilon_{p(i)}).$$

Définition 5 (*VNP-complet*)**.** *Une famille (f_i) est* VNP-complet *si elle est dans* VNP *et si pour toute famille (g_i) dans* VNP *, il existe un polynôme $p \in \mathbb{R}[X]$ tel que pour tout $i \in \mathbb{N}$, $g_i(x_1, \ldots, x_n) = f_j(y_1, \ldots, y_m)$ avec $j \leq p(i)$ et $y_k \in \cup_{1\leq k\leq n}\{x_k\} \cup \mathbb{F}$ (i.e. (g_i) est une projection de (f_i)).*

2.3 Arbres binaires universels

Dans le cas non associatif, tout monôme doit être décrit avec sa structure multiplicative. Les arbres binaires ordonnés dont les feuilles sont étiquetées par des variables permettent une telle description. Ces arbres auront un rôle important dans le reste du développement.

Définition 6 (Arbre binaire et structure multiplicative)**.** *Un arbre binaire est une production de la grammaire suivante :*

$$T ::= v \mid (T_1, T_2)$$

La taille $|T|$ d'un arbre binaire est le nombre de ses feuilles. Si $(f_1, \ldots, f_n)$ est un vecteur de polynômes de $\mathbb{F}_{\overline{A},\overline{C}}[X]$ et T un arbre binaire de taille n, nous notons $\prod^T(f_1, \ldots, f_n)$ le polynôme produit des f_i de structure multiplicative T.

Notons que les arbres binaires que nous considèrons sont ordonnés. Ainsi $(v_1, (v_2, v_3))$ n'est pas $((v_1, v_3), v_4)$. Par contre, comme dans le cas non ordonné, (v_1, v_2) dénote le même arbre que (v_2, v_1).

Exemple 1. *Si $T = (v_1, (v_2, v_3))$ et $(f_1, f_2, f_3) = (X, Y, Z)$, alors $\Pi^T(f_1, f_2, f_3) = X(YZ)$.*

Le permanent de taille n est une somme de produit de n éléments. Il existe donc autant de façon d'écrire ce permanent que d'arbres binaires à n feuilles (i.e. $O(2^n)$). Mais rappelons que le but est de définir un permanent assez "universel" pour qu'il puisse simuler toutes les familles dans *VP* . L'idée des auteurs est de définir un arbre universel qui contient tous les arbres binaires "petits" comme mineur puis de définir le permanent avec cet arbre particulier. Dès lors, quand nous voudrons simuler une famille associée à une certaine structure multiplicative, nous pourrons utiliser un grand permanent associé à un arbre universel qui contient cette structure multiplicative.

Commençons par expliciter la notion de mineur dans le cas particulier des arbres binaires.

Définition 7 (Arbre induit par des feuilles)**.** *Soit T un arbre binaire et V un sous-ensemble des feuilles de T. On définit l'arbre induit par les feuilles V inductivement sur T. Si $T = \{v\}$, alors $\kappa(T, V) = T$; sinon $T = (T_1, T_2)$ et (en notant $V_1 = V(T_1) \cap V$ et $V_2 = V(T_2) \cap V$) :*

$$\kappa(T, V) = \begin{cases} \kappa(T_2, V_2) & \text{si } V_1 = \varnothing; \\ \kappa(T_1, V_1) & \text{si } V_2 = \varnothing; \\ (\kappa(T_1, V_1), \kappa(T_2, V_2)) & \text{sinon.} \end{cases}$$

Définition 8 (Universalité)**.** *Soit $t \in \mathbb{N}$. Un arbre binaire T est t-universel si pour tout arbre binaire T' de taille au plus t, il existe $V_{T'} \subseteq V(T)$ tel que $T' = \kappa(T, V_{T'})$.*

Remarquons que $\forall V \subseteq V(T)$, $\kappa(T, V)$ est un mineur de T. Une question importante est de savoir s'il existe des arbres t-universels pas trop grand par rapport à t. Le lemme suivant répond positivement.

Lemme 1 (Universalité polynomiale)**.** *Pour tout $t \leq 1$, il existe un arbre t-universel $\mathcal{T}_t$ de taille au plus t^4. De plus,il est possible de construire $\mathcal{T}_t$ en temps polynomial en t. Il est également possible pour un arbre binaire T' donné de taille au plus t de construire en temps polynomial en t un ensemble de feuilles $V_{T'} \subseteq V(\mathcal{T}_t)$ tel que $\kappa(\mathcal{T}_t, V_{T'}) = T'$.*

Nous admetterons ce résultat dont les arguments principaux sont de nature purement combinatoire.

2.4 Permanent et déterminant

Nous pouvons désormais définir le permanent et le déterminant de $\mathbb{F}_{\overline{A},\overline{C}}[X]$.

Définition 9 (Permanent)**.** *La famille* $(\mathrm{PERM}_i)_{i\in\mathbb{N}}$ *est définie par*

$$\mathrm{PERM}_n = \sum_{\sigma\in\mathfrak{S}_m} \prod^{\mathcal{T}_n} \left(M_{1,\sigma(1)}, \ldots, M_{m,\sigma(m)}\right)$$

où $\mathcal{T}_n$ *est l'arbre* n*-universel défini par le lemme 1,* $m = |\mathcal{T}_n|$ *et* M *est une matrice carrée de dimension* m*.*

Remarquons que la famille (PERM_i) n'est pas définie pour toute les tailles de matrices. Nous définissons le déterminant de la même façon.

Définition 10 (Déterminant)**.** *La famille* $(\mathrm{DET}_i)_{i\in\mathbb{N}}$ *est définie par*

$$\mathrm{DET}_n = \sum_{\sigma\in\mathfrak{S}_m} \epsilon(\sigma) \prod^{\mathcal{T}_n} \left(M_{1,\sigma(1)}, \ldots, M_{m,\sigma(m)}\right)$$

où $\mathcal{T}_n$ *est l'arbre* n*-universel défini par le lemme 1,* $m = |\mathcal{T}_n|$ *et* M *est une matrice carrée de dimension* m*.*

Ces familles forment de bons candidats pour simuler d'autres familles ; en voici l'intuition : Pour simuler une famille (f_i) de taille au plus $p(i)$, nous montrerons que $(\mathrm{PERM}_{p(n)})$ convient. Si T est la structure multiplicative de f_n, alors T est un mineur de $\mathcal{T}_{p(n)}$. Or nous verrons que $\mathrm{PERM}^T = \sum_{\sigma\in\mathfrak{S}_m} \prod^T \left(M_{1,\sigma(1)}, \ldots, M_{m,\sigma(m)}\right)$ simule f_n. La projection permet de sélectionner les feuilles de $\mathcal{T}_{p(n)}$ à garder pour retrouver PERM^T et ainsi $\mathrm{PERM}_{p(n)}$ simule f_n. Une preuve formelle est donnée en section 3.

3 Complétude du permanent

Nous montrons ici que la famille (PERM_i) est *VNP-complète*.

3.1 Plan de la preuve

La preuve suit le schéma classique en trois parties. Les auteurs donnent en référence le chapitre 2 du livre [1].

VNP$_e$ **= VNP** Dans un premier temps nous montrons que les sommes booléennes de termes simulent les sommes booléennes de circuits. C'est-à-dire que si (f_i) est dans *VNP* alors il existe une famille (h_i) calculable par une série polynomialmenent bornée de termes telle que $f_i(x_1, \ldots, x_n) = \sum_{\epsilon_1,\ldots,\epsilon_k\in\{0;1\}} h_i(x_1, \ldots, x_n, \epsilon_1, \ldots, \epsilon_k)$ (i.e. (f_i) est dans *VNP*$_e$). Nous prouverons cette première partie dans la section 3.2.

Le permanent simule les termes On montre ensuite que le permanent est *VP$_e$-complet*, c'est-à-dire que toute famille calculée par une série de termes polynomialement bornée s'écrit comme projection de la famille (PERM_i). Un résumé de la preuve est donné en section 3.3.

Le permanent simule les sommes booléennes Finalement on montre que si une famille (f_i) s'écrit comme projection de (PERM_i) alors une somme booléenne polynomiale de (f_i) s'écrit encore comme projection de (PERM_i). Ainsi, comme (PERM_i) simule les termes, (PERM_i) simule aussi les sommes booléennes de termes. Donc (PERM_i) est *VNP$_e$-complet* donc *VNP-complet* (première partie). Cette partie suit la méthode de Malod et Portier [3]. Nous détaillerons les étapes imortantes de la preuve dans la section 3.4. Finalemenent, les auteurs en déduisent le résultat également dans le cas associatif, non-commutatif et dans le cas non-associatif, commutatif.

3.2 VNP$_e$ = VNP

De la même façon que dans le cas associatif et commutatif, les auteurs introduisent les développements d'un circuit. Un développement est un sous-arbre connexe du circuit contenant la sortie et vérifiant les deux conditions suivantes :

- si une porte étiquetée par $*$ est dans le développement alors les deux portes correspondantes aux deux entrées sont également dans le développement (et dans le même ordre) ;
- si une porte étiquetée par $+$ est dans le développement alors exactement l'une des deux portes correspondantes aux deux entrées est également dans le développement.

Ainsi un développement est également un circuit et calcule un monôme du circuit (la structure multiplicative est conservée dans le développement). Plus précisemment, soit $\mu(T)$ le mineur de T contenant exactement toutes les portes multiplicatives et les entrées de T, alors le polynôme $\hat{T}$ calculée par T vérifie : $\hat{T} = \prod^{\mu(T)}(v_1, \ldots, v_k)$ où les v_i sont les feuilles de T.

Lemme 2. *Si C est un circuit multiplicativement disjoint alors :*

- *tous les développements sont des termes ;*
- *l'ensemble des développements ($\mathbb{T}_C$) calculent exactement tous les monômes ;*
- *le polynôme calculée par le circuit $\hat{C}$ vérifie : $\hat{C} = \sum_{T \in \mathbb{T}_C} \hat{T}$.*

La preuve de ce lemme dans le cas associatif et commutatif peut être appliquée ici sans aucune difficultée. De même il n'est pas difficile de reprouver le lemme suivant en introduisant le degré formel.

Lemme 3. *Soit C un circuit de taille n calculant un polynôme f de de degré r. Il existe un circuit multiplicativement disjoint calculant f de taille $O(r^4 s)$.*

Il reste donc à montrer que la somme des développements peut se réecrire comme une somme booléenne de termes.

Théorème 1. *Si f est un polynôme et C un circuit multiplicativement disjoint de taille t telle que $f = \sum_{T \in \mathbb{T}_C} \hat{T}$. Alors il existe un polynôme $q \in \mathbb{R}[X]$ tel que $f(x_1, \ldots, x_n) = \sum_{\epsilon_1, \ldots, \epsilon_m \in \{0;1\}} g(x_1, \ldots, x_n, \epsilon_1, \ldots, \epsilon_m)$ où $m \leq q(t)$ et g est un polynôme calculable par un terme de taille au plus $q(t)$.*

Démonstration. Pour tout $T \in \mathbb{T}_C$, $|T| \leq t$ donc il existe un ensemble V de feuilles de $\mathcal{T}_t$ calculée par l'algorithme du lemme 1 telle que $T = \kappa(\mathcal{T}_t, V)$. Dans la suite, σ dénote la bijection naturelle entre un tel V et les feuilles de T. Nous introduisons alors les variables booléennes suivantes : $a(v)$ pour tout porte v de C, $b(u)$ pour toute feuilles u de $\mathcal{T}_t$ et $c(u, w)$ pour toute feuille u de $\mathcal{T}_t$ et porte d'entrée w de C. Soit ζ un assignement des a, b et w. ζ est *correcte* si et seulement si les conditions suivantes sont réunies :

1. $T_\zeta = \{v \mid \zeta(a(v)) = 1\}$ est un développement de C (i.e. $T_\zeta \in \mathbb{T}_C$) ;
2. $V_\zeta = \{u \mid \zeta(b(u)) = 1\}$ est l'ensemble $V(\mu(T_\zeta))$ de feuilles de $\mathcal{T}_t$ induisant T_ζ ;
3. $\zeta(c(u, w)) = 1$ si et seulement si $u \in V(\mu(T_\zeta))$ et $\sigma(w) = u$.

Nous définissons ensuite la quantité suivante pour toute feuille u de $\mathcal{T}_t$: $L_u = (1 - b(u)) + \sum_w c(u, w)\hat{C_w}$ où $\hat{C_w}$ est l'étiquette (variable ou constante) de l'entrée w de C. Dès lors, si ζ est *correcte*,

$$\hat{T_\zeta} = \prod^{\mathcal{T}_t} (L_{u_1}, \ldots, L_{u_m})_{|\zeta}$$

où les u_i sont les feuilles de $\mathcal{T}_t$ et $_{|\zeta}$ dénote l'évaluation des variables booléennes par ζ.

Il ne reste plus qu'à montrer qu'il existe une formule qui décide les 3 conditions des assignements *correctes*. Puisque il est possible de déterminer si un assignement est *correcte* en temps polynomial, par le théorème de Cook, il existe une formule booléenne B de taille polynomiale en le nombre de variables $\overline{a}, \overline{b}$ et $\overline{w}$ (donc à fortiori en t) en les variables $\overline{a}, \overline{b}, \overline{w}$ et des variables additionnelles $\overline{d}$ telle que ζ est *correcte* si et seulement si il existe un assignement ζ_d des variables $\overline{d}$ (le certificat) tel que $B((\overline{a}, \overline{b}, \overline{w})_{|\zeta}, \overline{d}_{|\zeta_d}) = 1$. Finalement, on peut écrire :

$$f = \sum_T \hat{T} = \sum_{\zeta, \zeta_d} B((\overline{a}, \overline{b}, \overline{w})_{|\zeta}, \overline{d}_{|\zeta_d}) \prod_t^{\mathcal{T}} (L_{u_1}, \ldots, L_{u_m})_{|\zeta}$$

Enfin, $B((\overline{a}, \overline{b}, \overline{w})_{|\zeta}, \overline{d}_{|\zeta_d}) \prod_t^{\mathcal{T}} (L_{u_1}, \ldots, L_{u_m})_{|\zeta}$ est un terme de taille polynomial en s et ζ, ζ_d sont de tailles polynomial en s. □

3.3 Le permanent simule les termes

Contrairement à la précédente partie, la méthode usuelle (utilisant les programmes à branchement) est difficilement réutilisable. Les auteurs explicitent directement la traduction.

Théorème 2. *Soit C un terme. Il existe $s \leq |C| + 1$ et une matrice de taille $s \times s$ dont les entrées sont des variables ou des éléments de $\mathbb{F}$ et un arbre binaire T de taille s telle que $\hat{C} = \mathrm{PERM}^T(M)$. De plus M vérifie : $M_{i,i+1} = 1$ pour $i \leq s - 1$ et $M_{i,j} = 0$ pour $s \geq j > i \geq 0$.*

Ce théorème implique le résultat. En effet, l'arbre T de la preuve est un mineur de $\mathcal{T}_s$ donc $\mathrm{PERM}^T(M)$ s'exprime comme projection de $\mathrm{PERM}_s = \mathrm{PERM}^{\mathcal{T}_s}$ (il suffit de poser $M_{i,j} = 0$ si les feuilles correspondantes à i et à j de $\mathcal{T}_t$ ne sont pas toutes deux dans V_T). Noton également, que la preuve s'adapte très facilement pour le cas du déterminant.

Résumé de la preuve. Les auteurs prouvent ce théorème par induction sur $s = |C|$. Si $s = 1$ alors $M = \begin{bmatrix} 1 & 1 \\ 0 & \hat{C} \end{bmatrix}$ et T le seul arbre binaire à deux feuilles conviennent. Sinon alors nous distinguons deux cas :

1. Si la sortie de C est étiquetée par $*$. Soient C_1 et C_2 les deux sous circuis. Les hypothèses d'induction donnent $s_1, s_2, M_1, M_2, T_1, T_2$. Alors posons $s = s_1 + s_2 \leq |C| + 1$, E la matrice de dimension $s_1 \times s_2$ nulle partout sauf $E_{1,1} = 1$, $T = (T_1, T_2)$ et M la matrice définie par blocs par : $M = \begin{bmatrix} M_1 & E \\ 0 & M_2 \end{bmatrix}$. Alors en distinguant les permutations égales à la composée d'une permutation de $[s_1]$ et d'une permutation de $[s_2]$ des permutations qui possédent au moins un croisement $\sigma(i) > i$ il est facile de vérifer que $\mathrm{PERM}^T = 0 + \hat{C_1} * \hat{C_2} = \hat{C}$.
2. Sinon, alors la sortie de C est étiquetée par $+$. Nous ne montrons pas ce cas. Les auteurs explicitent une construction de M et de T qui mènent au résultat après une quantité de vérifications techniques.

□

3.4 Le permanent simule les sommes booléennes

Nous montrons le théorème suivant.

Théorème 3. *Soient M une matrice de dimension s dont les entrées sont sont des variables, des éléments de $\mathbb{F}$ ou une variable particulière e, s_e le nombre d'entrées de M égales à e et T un arbre binaire à s feuilles. Alors si $\mathbb{F}$ n'est pas de caractéristique 2, il existe une matrice M' de dimension $5s_e + s$ telle que*

$$\mathrm{PERM}^{T'}(M') = \mathrm{PERM}^{T}(M_{|e=0}) + \mathrm{PERM}^{T}(M_{|e=1})$$

où $T' = (T, P^{5s_e})$, $P^{(5s_e)}$ étant le peigne à $5s_e$ feuilles.

Ce théorème implique le résultat car la dimension de M' est polynomialement bornée en la dimension de M. Donc si la somme booléenne porte sur n variables ϵ_i, il suffit de répéter le procédé pour i de 1 à n en distinguant la variable $e = \epsilon_i$. La matrice résultat M^∞ est toujours de dimension bornée par un polynôme p en s (car n est aussi polynomialement borné). L'arbre binaire résultat T^∞ n'est pas forcément un $\mathcal{T}_t$ mais sa taille est bornée par un polynôme p en s donc $\mathrm{PERM}_{p(s)}(M_1^\infty) = \mathrm{PERM}^{T^\infty}(M^\infty)$ (où M_1^∞ est un élargissement de M^∞ telle qu'elle sélectionne le mineur T^∞ dans $\mathcal{T}_{p(n)}$).

Résumé de la preuve. L'idée principale des auteurs est d'exploiter le fait que le résultat est vrai dans le cas commutatif et associatif (en nettoyant l'énoncé des occurences de T). Supposons alors que dans l'algèbre commutative et associative $\mathbb{F}[X]$ l'on ait l'égalité suivante : $\mathrm{PERM}(M') = \mathrm{PERM}(M_{|e=0}) + \mathrm{PERM}(M_{|e=1})$. Les auteurs montrent ensuite une correspondence entre les monômes de $\mathrm{PERM}^T(M_{|e=0}) + \mathrm{PERM}^T(M_{|e=1})$ et de $\mathrm{PERM}(M_{|e=0}) + \mathrm{PERM}(M_{|e=1})$ d'une part et entre ceux de $\mathrm{PERM}^{T'}(M')$ et de $\mathrm{PERM}(M')$ d'autre part. On

note $x_{i,j}$ les entrées de M différentes de e. Soit $\alpha = \prod_{1\leq k\leq n} x_{i_k,j_k}$ un monôme de $\mathbb{F}[X]$ tel que les $i_k \in [s]$ soient croissants et distincts et les $j_k \in [s]$ soient distincts. Soient $u_1, \ldots, u_s$ les feuilles de T et $T_\alpha = \kappa(T, V)$ où $V = \{u_{i_1}, \ldots, u_{i_k}\}$. Soit α^* le monôme de $\mathbb{F}_{\overline{A},\overline{C}}[X]$ suivant : $\alpha^* = \prod^{T_\alpha}(x_{i_1,j_1}, \ldots, x_{i_n,j_n})$. Nous faisons alors une série de remarques :

- tout monôme de $\mathrm{PERM}^T(M_{|e=0}) + \mathrm{PERM}^T(M_{|e=1})$ ou de $\mathrm{PERM}^{(T,P^{(5s_e)})}(M')$ est de la forme α^* ;
- le coefficient pour un tel monôme α^* dans $\mathrm{PERM}^{(T,P^{(5s_e)})}(M')$ et égale au coefficient de α dans $\mathrm{PERM}(M')$;
- le coefficient pour un tel monôme α^* dans $\mathrm{PERM}^T(M_{|e=0}) + \mathrm{PERM}^T(M_{|e=1})$ et égale au coefficient de α dans $\mathrm{PERM}(M_{|e=0}) + \mathrm{PERM}(M_{|e=1})$.

L'égalite $\mathrm{PERM}(M') = \mathrm{PERM}(M_{|e=0}) + \mathrm{PERM}(M_{|e=1})$ permet alors de conclure. □

4 Séparation de *VP* et *VNP*

Les auteurs donnent une borne inférieure pour la complexité d'une famille dans le cas non-associatif, commutatif. Construisons cette famille.

Soit (S_n) la famille des peignes à n feuilles (i.e. S_n est le graphe peigne à n feuilles). Soit (V_n) la famille des S_n définie par :

$$V_n(z_0, z_1) = \sum_{\zeta<\zeta'} \prod^{S_n}(z_{\zeta(1)}, \ldots, z_{\zeta(n)}) \prod^{S_n}(z'_{\zeta(1)}, \ldots, z'_{\zeta(n)})$$

où $\zeta, \zeta' \in \{0;1\}^n$ et $\_ < \_$ est l'ordre lexicographique sur $\{0;1\}^n$.

Lemme 4. *La famille (V_n) est dans* VNP.

Démonstration. Remarquons que le degré de V_n est $2n$ et que le nombre de ses vaiables est toujours 2. De plus, tester si $\zeta < \zeta'$ peut se faire en évaluant une formule booléenne en les ζ_i, ζ'_i de taille $O(n^2)$ (i.e. $\zeta_1 <_{\mathbb{N}} \zeta'_1 \vee (\zeta_1 =_{\mathbb{N}} \zeta'_1 \wedge \zeta_2 <_{\mathbb{N}} \zeta'_2) \vee \ldots$). La somme $\sum_{\zeta<\zeta'}$ peut se réécrire en $\sum_{\zeta_1,\zeta'_1,\ldots,\zeta_n,\zeta'_n\in\{0;1\}} B(\zeta_i, \zeta'_i)$ qui est une somme booléenne de taille polynomiale en n. Finalement, comme $\prod^{S_n}(z_{\zeta(1)}, \ldots, z_{\zeta(n)}) \prod^{S_n}(z'_{\zeta(1)}, \ldots, z'_{\zeta(n)})$ est une famille dans *VP*, (V_n) est dans *VNP*. □

Nous voulons maintenant montrer que (V_n) n'est pas dans *VP*. Pour celà, nous montrons une borne inférieure polynomiale sur la taille des circuits qui calculent (V_n).

Théorème 4 (Séparation)**.** *Si $\mathbb{F}$ n'est pas de caractéristique 2, alors dans le cas non-associatif commutatif,* VP $\subsetneq$ VNP.

Démonstration. Soit C un circuit de taille s calculant V_n. Remarquons que V_n est homogène (i.e. tous ses monomes ont le même degré).

Lemme 5. *Si C calcule un polynôme homogène de degré n, il existe un circuit C' de taille $O(sn^2)$ calculant s dont tous les noeuds calculent un polynôme homogène.*

Nous amdettons ce résultat. Il existe alors un circuit C' de taille $S = O(sn^2)$ calculant V_n dont tous les noeuds calculent un polynôme homogène. Soient $v_1, \dots v_m$ les noeuds de C' étiquetés par des portes $*$ calculant un polynôme de degré $2n$. Notons que les v_i sont les portes multiplicatives les plus proches de la sortie. Alors $\hat{v_i} = \hat{u_i}\hat{w_i}$ avec u_i et w_i calculants des polynômes de degré au plus $2n-1$. Bien sûr, on a $m \leq S = |C'|$ et

$$V_n = \sum_{1 \leq i \leq m} a_i \hat{v_i} = \sum_{1 \leq i \leq m} a_i \hat{u_i} \hat{w_i} \tag{1}$$

où $a_i \in \mathbb{F}$ dépendent des portes étiquetées par $+$ entre les v_i et la sortie. Nous voulons désormais exploiter le lemme suivant (que nous admettons également).

Lemme 6. *Soit f_i, g_i des polynômes en les variables $x_i, 1 \leq i \leq k$ homogènes de degré 1 tels que*

$$\sum_{1 \leq i,j \leq k \ \wedge \ i<j} x_i x_j = \sum_{1 \leq i \leq m} f_i g_i,$$

alors $m \geq \frac{k-1}{2}$.

C'est ce lemme qui nous permet d'exploiter la non-associativité. L'idée est que les monômes de V_n sont trop nombreux et complexes pour que C' soit petit. Nous introduisons une nouvelle variable x_ζ par $\zeta \in \{0;1\}^n$. Nous définissons alors l'opérateur $(\_)^*$ sur les polynômes de variables z_0, z_1 qui remplace tout monôme $\prod^{S_n}(z_{\zeta(1)}, \dots, z_{\zeta(n)})$ par la variable x_ζ. Si $g = \sum_\zeta b_\zeta \prod^{S_n}(z_{\zeta(1)}, \dots, z_{\zeta(n)})$ avec $b_\zeta \in \mathbb{F}$, alors $g* = \sum_\zeta b_\zeta x_\zeta$ est soit le polynôme nul, soit un polynôme en les variables x_ζ homogène de degré 1. Les auteurs montrent ensuite que pour tout monôme de V_n qui s'écrit comme produit de deux polynômes non constants α_1, α_2, alors il existe $\zeta_i \in \{0;1\}^n, 1 \leq i \leq 2$ tels que $\alpha_i = \prod^{S_n}(z_{\zeta_i(1)}, \dots, z_{\zeta_i(n)})$. Nous avons donc grâce à l'équation 1 :

$$V_n^* = \sum_{1 \leq i \leq m} (a_i \hat{u_i})^* (\hat{w_i})^* = \sum_{\zeta, \zeta' \in \{0;1\}^n \ \wedge \ \zeta < \zeta'} x_\zeta x_{\zeta'}.$$

Finalement, nous obtenons $m \geq \frac{2^n-1}{2} = \Omega(2^n)$. Comme, $S \geq m$ et que $S = O(sn^2)$, nous avons $|C| = \Omega(2^{n-1})$. Comme c'est vrai pour tout C et pour tout n, (V_n) n'est pas dans *VP* or elle est dans *VNP* . Donc *VP* $\subsetneq$ *VNP*. □

5 Conclusion

Cet article propose une investigation très intéressante de la théorie de Valiant dans une algèbre de polynômes restreinte et propose un résultat positif conernant le problème *VP* $\neq$ *VNP*. Les résultats habituels s'adaptent relativement bien à ce nouveau cadre et le développement est très clair.

Il serait intéressant d'étudier les problèmes combinatoires qui peuvent être résolus par de telles familles de polynômes. On pourrait ainsi montrer que certains problèmes combinatoires sont strictement plus durs que d'autres sans supposer *P* $\neq$ *NP* ou *VP* $\neq$ *VNP*.

Références

[1] Peter Bürgisser, Leslie Ann Goldberg, and Mark Jerrum. 10481 Abstracts Collection – Computational Counting. In Peter Bürgisser, Leslie Ann Goldberg, and Mark Jerrum, editors, *Computational Counting*, number 10481 in Dagstuhl Seminar Proceedings, Dagstuhl, Germany, 2011. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany.

[2] Pavel Hrubes, Avi Wigderson, and Amir Yehudayoff. Relationless completeness and separations. In *Proceedings of the 2010 IEEE 25th Annual Conference on Computational Complexity*, CCC '10, pages 280–290, Washington, DC, USA, 2010. IEEE Computer Society.

[3] Guillaume Malod and Natacha Portier. Characterizing valiant's algebraic complexity classes. *J. Complex.*, 24(1) :16–38, February 2008.