Bornes inferieures et superieures dans les circuits arithmetiques

Sébastien Tavenas

THÈSE

en vue de l'obtention du grade de

Docteur de l'Université de Lyon, délivré par l'École Normale Supérieure de Lyon

Discipline : Informatique

Laboratoire de l'Informatique du Parallélisme

École Doctorale Informatique et Mathématiques

présentée et soutenue publiquement le 9 juillet 2014 par

Sébastien TAVENAS

Bornes inférieures et supérieures dans les circuits arithmétiques

---

Directeur de thèse : Pascal KOIRAN

Après avis de : Markus BLÄSER

Neeraj KAYAL

Mohab SAFEY EL DIN

Devant la commission d'examen formée de :

Frédéric BIHAN	Université de Savoie	Membre
Markus BLÄSER	Universität des Saarlandes	Rapporteur
Étienne GRANDJEAN	Université de Caen Basse-Normandie	Membre
Pascal KOIRAN	École normale supérieure de Lyon	Directeur
Natacha PORTIER	École normale supérieure de Lyon	Co-encadrante
Mohab SAFEY EL DIN	Université Pierre et Marie Curie	Rapporteur

Table des matières

Introduction

Commençons ce manuscrit par une simple question. Comment fait-on pour chercher un mot dans un dictionnaire ? On identifie la première lettre du mot et on la compare à la première lettre des mots sur la page où le dictionnaire est ouvert. Puis, selon leur position relative dans l'ordre alphabétique, on tourne les pages vers l'avant ou vers l'arrière jusqu'à ce que les premières lettres coïncident. Ensuite, on recommence avec la deuxième lettre, puis avec la troisième, et ainsi de suite...

Ce que nous venons de décrire correspond à ce que l'on appelle un *algorithme*. Il s'agit d'un procédé systématique, applicable mécaniquement, sans réfléchir, en suivant simplement un mode d'emploi précis. En bref, c'est une recette de cuisine qui répond aux questions "Comment faire telle chose ?", "Comment calculer telle opération ?", "Comment résoudre tel problème ?"... À l'origine, pour les mathématiciens, les algorithmes servaient plutôt à effectuer des calculs sur les nombres. Ainsi, les méthodes pour calculer des additions, soustractions, multiplications ou divisions en les posant que l'on apprend en primaire sont des algorithmes. Il en est de même par exemple du crible d'Érathostène pour déterminer si un nombre est premier.

Bien que cette notion d'algorithme soit très ancienne, sa formalisation mathématique provient des années 1930 et des travaux en particuliers de Kleene, Church, Gödel, Herbrand, Post et Turing. Différents modèles ont été introduits comme les fonctions récursives, le lambda-calcul, la machine de Turing ou la machine RAM. De façon assez surprenante, il a été prouvé que tous ces modèles permettent de résoudre exactement les mêmes problèmes, et qu'il existait d'autres problèmes que ces modèles ne pouvaient pas résoudre. Ainsi est née la calculabilité, l'étude de ce qui est calculable. L'équivalence de capacité de calculs des différents modèles a permis de conjecturer que ces modèles étaient capables de simuler tous les autres modèles mécaniques que l'on pourrait concevoir. Cette conjecture est connue sous le nom de "Thèse de Church" ou "Thèse de Church-Turing". L'apparition de l'ordinateur (qui est une réalisation marérielle de la machine RAM) dès la seconde guerre mondiale fut un grand succès de ces travaux.

Avec l'arrivée des premiers ordinateurs est apparue la notion d'*efficacité* des algorithmes. Ainsi, peut-on réllement dire qu'un algorithme nécessitant un temps de calcul de plusieurs milliers d'années soit "efficacement" calculable ? D'après Hartmanis et Stearn, l'efficacité d'un algorithme doit être mesurée comme une fonction de la taille de ses entrées. L'efficacité d'un algorithme se mesure alors par le nombre de ressources qu'il utilise (comme le nombre d'opérations ou le nombre de cases mémoires) en fonction de la taille des entrées. C'est le début de la théorie de la complexité. Ainsi, lorsqu'on pose une addition de deux entiers, le nombre de chiffres que l'on écrit est au plus grossièrement trois fois plus grand que le nombre de chiffres des entrées (on doit rajouter une ligne pour les retenues et une ligne pour la solu-

tion). On dira que cet algorithme est linéaire en le nombre de chiffres à écrire. En comparaison, lorsqu'on pose une multiplication, le nombre de chiffres à écrire sera quadratique car le nombre de lignes de chiffres sera proportionnel en le nombre de chiffres des entrées.

Quelques années plus tard, Cobham et Edmonds ont indépendamment proposé qu'un algorithme efficace est un algorithme qui n'effectue, dans le pire des cas, qu'*un nombre d'opérations polynomial en la taille de son entrée*. La classe P est ainsi définie comme l'ensemble des problèmes qui admettent de tels algorithmes. On pourrait en fait se demander si la classe P, qui contient des problèmes qui ont leur meilleur algorithme en temps n^{1000}, correspond bien à l'ensemble des problèmes efficacement calculables. En pratique ce modèle semble aujourd'hui assez satisfaisant puisque la grande majorité des problèmes naturels de cette classe nécessite en fait un nombre d'opérations en n^c avec c une constante relativement petite (disons $c \leq 5$). Toutefois, d'autres classes peuvent aussi prétendre représenter les problèmes décidables efficacement. Par exemple, la classe P ne considère que les algorithmes déterministes, or de nombreux algorithmes aujourd'hui utilisent des bits aléatoires. Ainsi, la classe BPP est définie comme l'ensemble des problèmes que l'on peut résoudre en temps polynomial en la taille des entrées en utilisant des bits aléatoires. D'autres candidats pour la classe des problèmes résolubles efficacement viennent des modèles non uniformes. Un modèle uniforme est un modèle (comme pour P et BPP) où les algorithmes sont les mêmes quelque soit la taille des entrées. Dans le cas de la cryptographie, pourrait-on dire que le problème de la factorisation soit vraiment difficile s'il existait un algorithme très rapide capable de factoriser tous les nombres d'au plus 100 000 bits ? Un exemple naturel de modèle de calcul non uniforme est celui des circuits. L'ensemble des problèmes qui possèdent une suite de circuits (un pour chaque taille d'entrée) de taille polynomiale correspond à la classe $\mathsf{P/poly}$.

La question duale à celle de savoir quels problèmes peuvent être efficacement calculables est celle de déterminer pour quels problèmes ce n'est pas le cas. Ainsi, imaginons le problème du touriste qui arrive en France et aimerait visiter certaines villes (par exemple Angers, Bordeaux, Caen, Clermont-Ferrand, Grenoble, Lille, Lyon, Nancy, Nice, Paris et Rennes) mais qui n'a, à sa disposition, qu'une voiture de location avec un forfait de 1500 kilomètres. Peut-il trouver un itinéraire passant par toutes ces villes ne dépassant pas les 1500 kilomètres ? Ce problème, connu sous le nom du "Voyageur de Commerce" semble difficile à implémenter efficacement sur les ordinateurs. Aucun algorithme de complexité polynomiale résolvant ce problème n'est aujourd'hui connu. En fait, nous pensons qu'il n'en existe pas. Mais pourquoi cela ? Comment pourrait-on montrer la non-existence d'un tel algorithme ?

Pour commencer, notons que pour ce problème, si un itinéraire est donné, il est facile (i.e. en temps polynomial) de vérifier s'il s'agit d'un itinéraire satisfaisant aux critères de départ. L'ensemble des problèmes ayant cette propriété forme une classe connue sous le nom de NP. Pourquoi pense-t-on alors qu'il n'existe pas d'algorithme polynomial qui décide l'existence d'un tel bon itinéraire ? En fait, il a été montré que ce problème était au moins aussi difficile que tous les autres problèmes de la classe NP (on dit que le problème du voyageur de commerce est NP-complet). Ce qui signifie que s'il existe un algorithme polynomial pour ce problème, alors il en existe aussi un pour tous les autres problèmes de cette classe NP. Or la classe NP comprend un très grand nombre de problèmes qui semblent difficiles. Depuis les premières preuves

de NP-complétude par Cook et Karp il y a trente ans, les chercheurs n'ont cessé d'augmenter la liste de ces problèmes NP-complets (cf. par exemple le livre [34] pour une liste déjà conséquente). Comme l'existence d'un algorithme polynomial pour le problème du voyageur de commerce impliquerait l'existence d'un tel algorithme pour tous ces autres problèmes, la communauté scientifique doute de cette existence. Mais comment le prouver ? Résoudre cette question connue sous le nom "$\mathsf{P} \neq \mathsf{NP}$?" (ou conjecture de Cook) est le plus grand défi de la recherche actuelle en informatique théorique. Cette conjecture fait partie des sept problèmes du millénaire exposés par l'Institut Clay. Très peu d'outils existent aujourd'hui pour trouver des bornes inférieures sur la complexité d'un problème, i.e. prouver que tel problème ne peut pas être résolu en moins de tant d'opérations.

Un autre problème classique est celui des mariages parfaits (en anglais "perfect matching"). Anne, Bertrand, Charles et Daniel doivent se répartir quatre gâteaux, un au chocolat, un à la vanille, un au citron et un à la fraise. Anne et Bertrand n'aiment pas beaucoup les fruits, mais raffolent du chocolat et de la vanille. Charles est preneur des gâteaux au citron, à la fraise ou à la vanille, mais laisserait bien celui au chocolat. Quant à Daniel, gourmand, sera satisfait quelque soit le gâteau qu'il recevra. Le problème des mariages parfaits est celui de savoir s'il y a une affectation des gâteaux qui convient aux quatre amis. Ce problème est en fait dans P. Toutefois, la variante de ce problème qui consiste à compter le nombre de telles affectations valables est supposée difficile (ce problème est connu #P-complet). En fait compter ce nombre d'assignations revient à évaluer un polynôme particulier, le *permanent*, en un certain point. Cela signifie qu'il est possible de résoudre ce problème en effectuant seulement *les opérations arithmétiques* que sont l'addition, la soustraction ou la multiplication. Dans ce manuscrit, nous nous intéresserons essentiellement à de tels problèmes arithmétiques. Il est envisageable que l'utilisation d'autres opérations (comme modifier directement les bits des nombres considérés) permette d'évaluer ces polynômes plus rapidement, mais en pratique ce n'est généralement pas le cas des algorithmes connus actuellement. Nous considérerons ainsi des modèles de calcul arithmétiques, i.e. des modèles où seules les opérations arithmétiques sont utilisées. Le modèle arithmétique probablement le plus répandu de nos jours est celui des *circuits arithmétiques*. Ce modèle a été particulièrement étudié par Valiant dans les années 70, 80. Ce dernier a introduit des classes analogues aux classes booléennes. Ainsi, la classe VP correspond aux familles de polynômes calculables efficacement dans ce modèle, alors que la classe VNP est l'analogue de la classe VP. Valiant montra que le polynôme Permanent est en fait VNP-complet. La conjecture $\mathsf{VP} \neq \mathsf{VNP}$, connue sous le nom de *conjecture de Valiant* fait figure de version arithmétique de la conjecture de Cook. Toutefois, comme on se limite ici seulement aux opérations arithmétiques, la robustesse des objets algébriques sur lesquels on travaille (comme les anneaux ou les corps) et les nombreuses propriétés qu'ont les opérations associées permettent d'imaginer que cette version arithmétique de la conjecture $\mathsf{P} \neq \mathsf{NP}$ soit beaucoup plus accessible.

Dans le premier chapitre, nous rappelerons les définitions et premières propriétés autour de ces circuits arithmétiques dont nous aurons besoin dans la suite de ce manuscrit.

Nous avons mentionné précédemment que le principal challenge en complexité informatique est de trouver des bornes inférieures. Agrawal et Vinay [4] ont mon-

tré que trouver une borne inférieure en $2^{o(d+d\log(n/d))}$ pour la taille des circuits de profondeur 4 calculant une suite de polynômes P_n de degré d à n indéterminées est équivalent à trouver une borne inférieure (aussi en $2^{o(d+d\log(n/d))}$) pour les circuits généraux calculant cette suite de polynômes. Ce résultat traduit que le problème de trouver des bornes inférieures est aussi difficile dans le cas des circuits de profondeur 4 que dans le cas des circuits généraux. Depuis, beaucoup de travaux ont été réalisés sur les circuits arithmétiques de profondeur constante (en particulier de profondeur 3 et 4). Nous exposerons dans le deuxième chapitre les résultats sur ce sujet. Nous commencerons par donner les résultats récents sur des bornes inférieures non triviales pour les circuits de profondeur 4. Puis nous nous intéresserons plus particulièrement aux bornes supérieures correspondantes et verrons que dans un grand nombre de cas les bornes optimales ont été trouvées.

En 2007, Bürgisser [21] a montré qu'une célèbre conjecture, la *τ-conjecture* introduite par Shub et Smale [92], implique une borne inférieure sur la taille des circuits arithmétiques calculant le permanent. Cette τ-conjecture suggère qu'un polynôme calculé par un petit circuit ne peut pas avoir beaucoup de racines entières. Cependant cette conjecture est fausse si on considère les racines réelles au lieu des racines entières. En effet les polynômes de Tchebychev possèdent un nombre de racines réelles exponentiellement plus grand que la taille des circuits les calculant. Koiran [61] a proposé une variante de cette τ-conjecture, nommée la *τ-conjecture réelle*. Cette dernière stipule qu'il existe un polynôme universel p tel que les polynômes univariés de la forme

$$\sum_{i=1}^{k}\prod_{j=1}^{m} f_{i,j}(X)$$

ont au plus $p(ktm)$ racines réelles dès que les $f_{i,j}$ ont au plus t monômes. L'intérêt de cette conjecture est que, tout en impliquant encore la conjecture de Valiant, elle considère le nombre de racines réelles, et permet d'espérer que les outils d'analyse réelle puissent aider à la résoudre. Dans le troisième chapitre, nous étudierons cette τ-conjecture réelle ainsi que d'autres variantes ayant toutes la propriété d'impliquer des bornes inférieures pour le permanent. Le quatrième chapitre sera consacré à des premiers résultats concernant deux de ces variantes : la τ-conjecture réelle monotone ainsi que la version combinatoire.

Nous nous attarderons ensuite sur nos travaux pour tenter de prouver la τ-conjecture réelle dans le chapitre cinq. Nous verrons alors pourquoi le wronskien est un outil très adapté pour borner le nombre de zéros de sommes de puissances. Même si nous sommes encore loin de prouver la τ-conjecture réelle, nous montrerons comment obtenir des bornes sur le nombre de racines pour des polynômes de la forme

$$\sum_{i=1}^{k}\prod_{j=1}^{m} (f_{i,j}(X))^{\alpha_{i,j}}$$

où les $f_{i,j}$ ont au plus t monômes. Ces bornes améliorent à la fois les résultats de Khovanskiĭ [59] sur ce sujet et les résultats précédents de Grenet, Koiran, Portier et Strozecki [38]. Ces outils sont assez robustes et permettent d'améliorer les bornes supérieures connues sur le nombre de racines pour d'autres familles de polynômes.

Enfin, au chapitre six, nous essaierons d'utiliser la pleine puissance des outils développés au chapitre cinq pour attaquer les variantes "creuses" du théorème de Bézout. Dans le corps des complexes, le nombre de racines d'un polynôme est borné par son degré. La règle des signes de Descartes assure, elle, que le nombre de racines réelles est aussi borné par le nombre de termes du polynôme. Par ailleurs, pour un système de plusieurs équations, le théorème de Bézout affirme que le nombre de solutions complexes, s'il est fini, est borné par le produit des degrés des différents polynômes. Qu'en est-il alors du cas d'un système de polynômes creux ? Cette question a été soulevée par Kushnirenko en 1977. Les résultats de Khovanskiĭ sur la théorie des "fewnomials" assurent que le nombre de solutions réelles est borné par une fonction du nombre de termes. Cependant cette fonction est exponentielle en le nombre de termes. La question de savoir s'il existe une borne supérieure polynomiale en le nombre de termes comme pour le théorème de Bézout est encore largement ouverte. Dans ce même chapitre nous examinerons un cas particulier, celui d'un système d'un polynôme de petit degré avec un polynôme creux. Nous montrerons que dans ce cas, il existe effectivement une borne supérieure polynomiale sur le nombre de composantes connexes des solutions.

Notations

Dans ce manuscrit nous utiliserons abondamment la notation de Landau pour apprécier le comportement asymptotique de nos mesures. Par comportement asymptotique, nous sous-entendons en fait le comportement des fonctions au voisinage de $+\infty$. Si f et g sont des fonctions $\mathbb{R} \to \mathbb{R}$, on dira que $f = O(g)$ s'il existe deux réels positifs c et N tels que pour tout $n \geq N$, on ait $f(n) \leq cg(n)$. De plus, on notera $f = o(g)$ si pour tout réel positif ε, il existe un réel N tel que pour tout $n \geq N$, on ait $f(n) \leq \varepsilon g(n)$. Ces notations permettent de borner supérieurement le comportement asymptotique de f. Il existe des notations symétriques pour les bornes inférieures. Ainsi, on notera $f = \Omega(g)$, respectivement $f = \omega(g)$ si $g = O(f)$, respectivement $g = o(f)$. Enfin, la notation $f = \Theta(g)$ exprime que $f = O(g)$ et $g = O(f)$, i.e. que f et g sont de même ordre de grandeur. Finalement nous utiliserons la même notation dans le cas de fonctions de $\mathbb{Z} \to \mathbb{R}$.

Chapitre 1

Préliminaires : notations et introduction à la théorie de Valiant

Dans ce chapitre, nous définirons les outils ainsi que les notations que nous allons utiliser dans la suite de ce manuscrit. Nous donnerons ensuite une brève introduction à la théorie des circuits arithmétiques (appelée généralement théorie de Valiant). Toutefois, nous considérerons ici seulement les bases et les résultats qui nous seront utiles pour la suite. Pour un aperçu plus complet de cette théorie, le lecteur interessé pourra se tourner vers les références suivantes [19, 23, 35, 91].

L'idée de cette théorie est de mesurer la complexité des polynômes en termes de nombres d'opérations arithmétiques à effectuer. Commençons par fixer quelques notations pour les polynômes.

1 Polynômes

Un *polynôme univarié* f est défini comme une expression de la forme

$$f = c_0 + c_1 X + c_2 X^2 + \ldots + c_d X^d = \sum_{i=0}^{d} c_i X^i$$

où les c_i (pour $0 \leq i \leq d$) sont des éléments d'un anneau commutatif $\mathbb{A}$ avec $c_d \neq 0$ et où X est un symbole formel appelé *indéterminée* (ou même *variable*). La constante d est appelée le *degré* (notée aussi $\deg(f)$) et les $(c_i)_{0 \leq i \leq d}$ les *coefficients* de f. Par convention, le degré du polynôme nul sera $-\infty$. L'ensemble des polynômes à coefficients dans un anneau $\mathbb{A}$ est encore un anneau et sera noté $\mathbb{A}[X]$.

Remarque 1.1. *Dans la suite du manuscrit, les anneaux seront toujours supposés unitaires et commutatifs.*

Un polynôme est donc une somme de *termes* où chaque terme est le produit d'un coefficient c_i et d'un *monôme* X^i. Les coefficients c_d (où d est le degré) et c_0 sont traditionnellement appelés respectivement le *coefficient dominant* et le *terme constant*.

Si $\mathbb{A}$ est un sous-anneau de $\mathbb{B}$, alors, on associera à un polynôme f sa *fonction*

polynomiale sur $\mathbb{B}$. Il s'agit de la fonction :

$$\begin{aligned} f \ : \mathbb{B} &\to \mathbb{B} \\ x &\mapsto c_0 + c_1 x + \ldots + c_d x^d. \end{aligned}$$

En fait, nous nous intéresserons essentiellement dans la suite à des anneaux très simples. En particulier $\mathbb{A}$ correspondra généralement à $\mathbb{Z}$ ou $\mathbb{Q}$ et $\mathbb{B}$ sera $\mathbb{R}$ ou $\mathbb{C}$. Les polynômes *multivariés* sont des polynômes en plusieurs indéterminées. Il s'agit d'expression de la forme

$$\begin{aligned} f &= c_{0,0,\ldots,0} + c_{1,0,\ldots,0} X_1 + \ldots + c_{0,0,\ldots,1} X_n + \ldots + c_{i_1,i_2,\ldots,i_n} X^{i_1} X^{i_2} \cdots X^{i_n} \\ &= \sum_{\boldsymbol{\alpha} \in \mathbb{N}^n} c_{\boldsymbol{\alpha}} \mathbf{X}^{\boldsymbol{\alpha}} \end{aligned}$$

où la somme est finie. Les coefficients $c_{i_1,i_2,\ldots,i_n}$ sont encore des éléments d'un anneau $\mathbb{A}$. Le coefficient $c_{0,0,\ldots,0}$ sera encore appelé le terme constant. Le degré d'un monôme $m = X^{\alpha_1} \cdots X^{\alpha_n}$ sera alors défini par $\deg(m) = \sum_{i=1}^{n} \alpha_i$. Le degré total du polynôme sera le maximum des degrés de ses monômes, c'est-à-dire $\deg(f) = \max_{\boldsymbol{\alpha}}(\alpha_1 + \ldots + \alpha_n)$. Un polynôme est dit *homogène* si tous les termes associés à un coefficient non nul ont même degré. Un polynôme est *constant* s'il est de degré au plus 1.

1.1 Propriétés élémentaires des polynômes

Un outil pratique pour les polynômes est la *décomposition en facteurs irréductibles*. Plus formellement, si $\mathbb{K}$ est un corps commutatif, un polynôme f est dit *irréductible* s'il est de degré au moins 1 et si pour toute écriture de f comme un produit $g \cdot h$ alors, un des deux polynômes g ou h est constant. La décomposition en facteurs irréductibles assure que pour tout polynôme f sur un corps $\mathbb{K}$, il existe des polynômes $g_1, \ldots, g_p$ irréductibles et une constante λ de $\mathbb{K}$ tels que :

$$f = \lambda g_1 \ldots g_p.$$

De plus, ces nouveaux polynômes sont uniques à constante multiplicative près. Un anneau qui possède cette propriété de décomposition unique en irréductible est appelé *factoriel*. La théorie sur ces anneaux est beaucoup plus générale que celle présentée ici (en particulier, pour les anneaux de polynômes, l'anneau de base n'a pas besoin d'être un corps) et peut être trouvée dans tout livre d'algèbre.

Une *racine* d'un polynôme f en n variables est un point $(a_1, \ldots, a_n)$ de $\mathbb{A}^n$ tel que f s'annule en ce point (i.e. $f(a_1, \ldots, a_n) = 0$). Dans le cas des polynômes univariés, le fait que a soit une racine de $f(X)$ est équivalent au fait que $(X - a)$ soit un facteur de f. Un corollaire direct de l'unicité de la décomposition en irréductibles est que si $f(X)$ est un polynôme non identiquement nul, alors son nombre de racines est borné par son degré.

1.2 Fractions rationnelles

On peut tout d'abord remarquer que l'ensemble des polynômes est le plus petit ensemble qui contient les constantes, les variables et qui est stable par les trois lois $+$, $-$ et $\times$. Mais que se passe-t-il si on veut rajouter les divisions ?

Il est alors naturel de se placer dans le cas où l'anneau de base est un corps $\mathbb{K}$ (comme pour les anneaux, nos corps seront toujours commutatifs). On définit les *fractions rationnelles* comme les quotients de deux polynômes : f est fraction rationnelle si et seulement s'il existe deux polynômes g et h (avec h non identiquement nul) tels que $f = g/h$. On dira que g/h est sous forme simplifiée si g et h sont premiers entre eux (i.e. que si un polynôme ϕ divise g et h, alors ϕ est constant). De même que pour les polynômes, on peut associer à chaque écriture g/h *la fonction rationnelle associée* (où $\mathbb{B}$ est un sur-corps de $\mathbb{K}$) :

$$\begin{aligned} g/h \ : \mathbb{B} &\to \mathbb{B} \\ x &\mapsto g(x)/h(x). \end{aligned}$$

Toute fraction rationnelle peut se mettre sous une forme simplifiée, la seule perturbation de cette transformation est que le domaine de la nouvelle fonction associée a potentiellement été étendu par continuité. Ces singularités qui ont disparu sont appelées *singularités effaçables*. Dans la suite, les fractions rationnelles (ainsi que les fonctions associées) seront par défaut sous forme simplifiée. On peut encore définir les *racines* d'une fonction rationelle comme les points où elle s'annule. On définira les *pôles*, comme les points où la fonction rationnelle est non définie. L'ensemble des fractions rationnelles sera noté $\mathbb{K}(X_1, \ldots, X_n)$.

1.3 Polynômes classiques

Un premier exemple de polynôme est le produit itéré de matrices. Il s'agit du produit matriciel $\left(\mathcal{X}^{(0)}\right)^t \mathcal{X}^{(1)} \cdots \mathcal{X}^{(d-1)}$ où

$$\mathcal{X}^{(0)} = \left(X_i^{(0)}\right)_{1 \leq i \leq n} \text{ et } \mathcal{X}^{(d-1)} = \left(X_i^{(d-1)}\right)_{1 \leq i \leq n}$$

sont deux vecteurs colonnes, et pour $1 \leq k \leq d-2$ les

$$\mathcal{X}^{(k)} = \left(X_{i,j}^{(k)}\right)_{1 \leq i,j \leq n}$$

sont des matrices $n \times n$.

Le polynôme obtenu, appelé $\mathrm{IMM}_{n,d}$ (le nom vient de l'anglais "Iterated Matrix Multiplication") est défini comme suit. Pour d, n des entiers tels que $d \geq 2$ et $n \geq 1$, on considère le polynôme suivant sur les $(d-2)n^2 + 2n$ indéterminées $\left(X_i^{(0)}, X_i^{(d-1)}, X_{i,j}^{(l)}\right)$ pour $1 \leq i, j \leq n$ et $l \in \{1, \ldots, d-2\}$:

$$\mathrm{IMM}_{n,d} = \sum_{(i_0,\ldots,i_{d-2}) \in \{1,\ldots,n\}^{d-1}} X_{i_0}^{(0)} X_{i_0,i_1}^{(1)} \cdots X_{i_{d-3},i_{d-2}}^{(d-2)} X_{i_{d-2}}^{(d-1)}.$$

Un autre exemple classique de polynôme est celui du *déterminant*. Les bijections de l'ensemble $\{1, \ldots, n\}$ vers lui-même sont appelées *permutations* à n éléments. On notera leur ensemble $\mathfrak{S}_n$. Soient $i < j$ deux éléments distincts compris entre 1 et n. On dit que la paire $\{i, j\}$ est *en inversion* pour la permutation σ quand $\sigma(i) > \sigma(j)$. Une permutation est dite *paire* quand elle présente un nombre pair d'inversions, *impaire* sinon. Par définition, la *signature* d'une permutation paire est 1, celle d'une permutation impaire est -1. La signature d'une permutation σ sera notée $\varepsilon(\sigma)$. Nous

pouvons enfin définir le polynôme déterminant. Soit $X = (X_{i,j})_{1 \leq i,j \leq n}$ la matrice de taille $n \times n$ où chaque case correspond à une indéterminée particulière. Le polynôme

$$\textsc{Det}_n = \sum_{\sigma \in \mathfrak{S}_n} (-1)^{\varepsilon(\sigma)} \prod_{i=1}^{n} X_{i,\sigma(i)}$$

est alors défini comme le déterminant de la matrice $X = (X_{i,j})_{1 \leq i,j \leq n}$. Il s'agit d'un polynôme homogène de degré n. Par exemple,

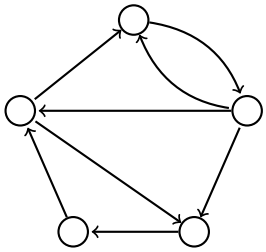
$$\textsc{Det}_2 = X_{1,1}X_{2,2} - X_{1,2}X_{2,1}.$$

Le déterminant ne se résume pas à la formule ci-dessous. Il s'agit d'un outil primordial en mathématiques, à la base par exemple de l'algèbre linéaire. Muir lui a consacré un livre [74].

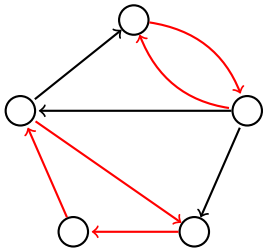
On s'intéressera dans ce manuscrit plus particulièrement au *permanent*, un polynôme en partie similaire au déterminant. Il est défini par :

$$\textsc{Perm}_n = \sum_{\sigma \in \mathfrak{S}_n} \prod_{i=1}^{n} X_{i,\sigma(i)}.$$

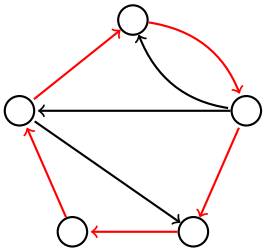
Il s'agit exactement de la formule du déterminant à laquelle on a retiré les "-1". $\textsc{Perm}_n$ est aussi un polynôme homogène de degré n en n^2 variables. Même s'il est loin d'avoir l'ampleur du déterminant en mathématiques, il a tout de même des significations combinatoires. En particulier, si G est un graphe orienté à n sommets où chaque arête e est pondérée par un poids $\pi(e)$, alors le *permanent de* G compte le nombre de couvertures par cycles. Plus précisément, une *couverture par cycle* $\mathfrak{C}$ est un sous-ensemble des arêtes couvrant G par des cycles, i.e. pour chaque sommet v de G, exactement une arête sortante et une arête entrante de v (possiblement la même) sont dans $\mathfrak{C}$.



Graphe G



Couverture par cycles (en rouge)



Cycle hamiltonien (en rouge)

Le *poids* de la couverture par cycle $\mathfrak{C}$ est le produit des poids des arêtes de $\mathfrak{C}$. Si $M = (m_{i,j})_{1 \leq i,j \leq n}$ est la matrice d'adjacence du graphe G (la case $m_{i,j}$ correspond au poids associé à l'arête allant du sommet i au sommet j, s'il n'y a pas d'arête, le poids est 0), alors le permanent de M vaut la somme des poids de $\mathfrak{C}$ où $\mathfrak{C}$ parcourt l'ensemble des couvertures par cycle de G :

$$\textsc{Perm}_n(G) = \sum_{\substack{\mathfrak{C} \text{ couverture} \\ \text{par cycles de } G}} \left(\prod_{\substack{e \text{ arête} \\ \text{de } \mathfrak{C}}} \pi(e) \right).$$

Le polynôme obtenu si on se restreint alors aux *cycles hamiltoniens* au lieu des couvertures par cycles est appelé le *hamiltonien* (un cycle hamiltonien est un cycle qui passe une et une seule fois par chaque sommet du graphe).

$$\textsc{Ham}_n(G) = \sum_{\substack{\mathfrak{C} \text{ cycle} \\ \text{hamiltonien de } G}} \left(\prod_{\substack{e \text{ arête} \\ \text{de } \mathfrak{C}}} \pi(e) \right).$$

2 Circuits arithmétiques

2.1 Les circuits

La façon la plus naturelle de calculer un polynôme $f(x_1, \ldots, x_n)$ sur un anneau $\mathbb{A}$ est de commencer avec les variables $x_1, \ldots, x_n$ puis d'effectuer une succession d'opérations arithmétiques basiques telles que des additions, des soustractions, des multiplications ou des divisions (c.f. Remarque1.3) jusqu'à obtenir le polynôme désiré. Un tel calcul est appelé un SLP (de l'anglais "Straight-line program"). Nous représenterons ces SLP par des circuits arithmétiques.

Définition 1.2. *Un* circuit arithmétique *sur un anneau commutatif $\mathbb{A}$ de portes d'opération $\mathcal{P}$ est un graphe fini orienté acyclique avec les propriétés suivantes : les sommets d'un circuit sont habituellement nommés* portes. *Ceux de degré entrant* 0 *sont appelés les* entrées *et sont étiquetés par une constante de $\mathbb{A}$ ou une variable. Les autres sommets (de degré entrant > 0) sont étiquetés par des opérations de $\mathfrak{P}$ et sont appelés les* portes de calcul *ou* nœuds internes. *Pour une porte de calcul, le degré entrant sera souvent noté* arité. *Les sommets de degré sortant* 0 *seront nommés les* sorties.

Enfin, nous appellerons formule, *un circuit tel que le graphe sous-jacent est un arbre.*

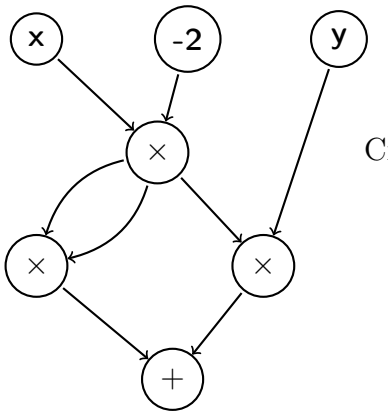
Comme nous avons introduit les circuits comme une représentation des SLP, il est intéressant de remarquer que la taille d'un circuit n'est rien d'autre que la longueur du SLP correspondant.

Comme nous l'avons mentionné à la remarque 1.1, nous nous limitons dans ce manuscrit au cas des anneaux commutatifs, mais il est aussi possible de définir les circuits pour des anneaux non-commutatifs (voir par exemple sur ce sujet le célèbre résultat de Nisan [75] ou la section consacrée dans [91]).

Nous utiliserons aussi le vocabulaire classique *successeur/arguments* pour mettre en évidence les liens entre les portes. S'il existe une arête du graphe allant de la porte α vers la porte β, nous dirons que α est un *argument* de β ou que β est un *successeur* de α.

Chaque porte d'un circuit calcule un polynôme (défini par récurrence). Les polynômes calculés par un circuit correspondent aux polynômes calculés par les sorties du circuit. Comme dans l'exemple ci-dessous, on considérera généralement des circuits avec une seule sortie (et donc calculant un unique polynôme).

Pour une porte α, nous noterons $[\alpha]$ le polynôme calculé par cette porte.



Circuit calculant le polynôme $f = 4x^2 - 2xy$.

Remarque 1.3. *Quand rien n'est signalé, l'ensemble des portes d'opérations sera par défaut :* $\mathcal{P} = \{+, \times\}$.

Rajouter des portes de soustraction ne changera pas grand chose, vu qu'il est possible de simuler le calcul $a - b$ *par le calcul* $a + ((-1) \times b)$. *Pour calculer des polynômes, Strassen a montré ([95], cf. lemme 1.6) que l'on pouvait aussi facilement se passer des portes de division. Enfin, nous utiliserons aussi (au chapitre 2) les portes de multiplication par un scalaire* $\odot$.

Remarque 1.4. *Encore par défaut, l'arité des portes de calcul sera bornée par deux. On mentionnera dans la suite quand l'arité des portes (essentiellement* $+$ *et* $\times$*) sera bornée par une autre valeur ou non bornée.*

Comme mentionné précédemment, nous nous intéresserons à la complexité des circuits arithmétiques. Pour cela, nous aurons besoin de "mesures" de la "taille" de tels circuits.

Définition 1.5. *La* taille *d'un circuit compte le nombre de portes. La* profondeur *du circuit mesure la longueur maximale d'un chemin orienté depuis une entrée jusqu'à une sortie.*

Nous avons déjà mentionné précédemment que l'on peut en général se passer des portes de division. Plus précisément, le résultat suivant a été démontré par Strassen [95]. Une preuve peut être trouvée au chapitre 7.1 du livre [22].

Lemme 1.6. *Sur un corps infini, si un polynôme* f *de degré* d *est calculable par un circuit de portes* $\{+, -, \times, \div\}$ *et de taille* s*, alors il est aussi calculé par un circuit de portes* $\{+, -, \times\}$ *et de taille* $O(d^2 s)$.

Le résultat reste valide en fait pour tout corps assez grand. Hrubeš et Yehudayoff ont généralisé ce résultat à tout corps [49].

2.2 Degré formel

Définition 1.7. *Pour un circuit de portes* $\{+, \times\}$*, on définit, par récursivité, le degré (formel) d'une porte :*

- *Le degré d'une entrée étiquetée par* 0 *est* $-\infty$.
- *Le degré d'une entrée étiquetée par une constante non nulle est* 0.
- *Le degré d'une entrée étiquetée par une variable est* 1.

— *Le degré d'une porte* + *d'arguments* $\alpha_1, \ldots, \alpha_p$ *est le maximum des degrés des portes* $\alpha_1, \ldots, \alpha_p$.
— *Le degré d'une porte* $\times$ *d'arguments* $\alpha_1, \ldots, \alpha_p$ *est la somme des degrés des portes* $\alpha_1, \ldots, \alpha_p$.

*Un circuit est qualifié d'*homogène *si pour chacune de ses portes d'addition* α*, tous les arguments de* α *ont le même degré.*

Remarque 1.8. *Dans la suite de ce manuscrit nous supposerons que les nœuds internes ne calculent jamais le polynôme identiquement nul. Si c'est le cas, il suffit de remplacer ces portes par des portes d'entrée étiquetées par la constante* 0.

Un premier résultat découle immédiatement de la définition par récurrence des circuits homogènes.

Lemme 1.9. *Dans un circuit homogène, toutes les portes calculent des polynômes homogènes. De plus le degré de la porte correspond au degré du polynôme homogène calculé par la porte.*

Démonstration.
— Le lemme est avéré pour toutes les portes d'entrée.
— Si α est une porte + d'arguments $\alpha_1, \ldots, \alpha_p$, alors par homogénéité, ces arguments ont le même degré d. Par hypothèse de récurrence, les portes $\alpha_1, \ldots, \alpha_p$ calculent des polynômes homogènes de degré d. Donc $[\alpha]$ est un polynôme homogène de degré d ou $-\infty$. Par la remarque 1.8, le degré de $[\alpha]$ est d.
— Si α est une porte de multiplication d'arguments $\alpha_1, \ldots, \alpha_p$, alors par hypothèse de récurrence les polynômes $[\alpha_1], \ldots, [\alpha_p]$ sont homogènes et leurs degrés correspondent au degré des portes correspondantes. Donc $[\alpha]$ est homogène et le degré de $[\alpha]$ égale le degré de α.

□

Les portes $\odot$ correspondant à la multiplication par un scalaire sont donc des cas particuliers de portes de multiplication. On peut rajouter maintenant une restriction syntaxique pour que ces portes calculent bien des multiplications scalaires. Dans la suite, ces portes sont toujours d'arité deux et au moins l'un des arguments est de degré formel 0.

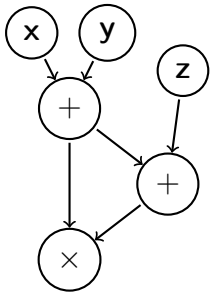
2.3 Arbres monomiaux

Pour un circuit donné à une seule sortie, nous allons définir une famille de formules particulières que nous appellerons les arbres monomiaux. Dans l'esprit, un arbre monomial correspond au calcul d'un monôme particulier.

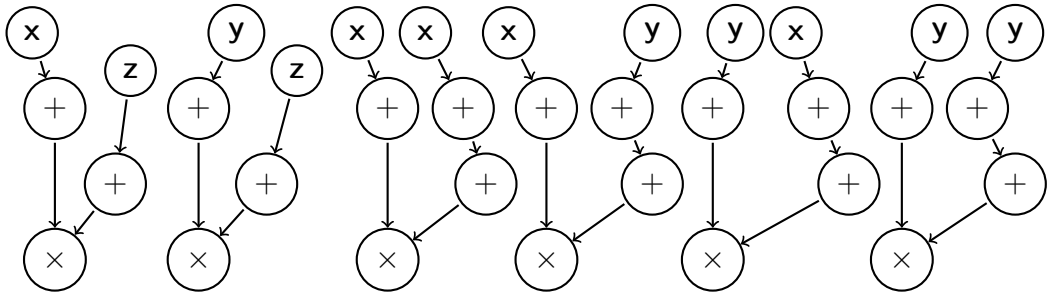
Définition 1.10. *L'ensemble des arbres monomiaux d'un circuit* C *qui a une seule sortie* o *est défini par récurrence sur sa taille :*
— *Si* C *est de taille* 1*, il a seulement un arbre monomial, lui-même.*
— *Si la sortie* o *de* C *est une porte* + *d'arguments* $\alpha_1, \ldots, \alpha_p$*, alors les arbres monomiaux de* C *sont obtenus en choisissant un arbre monomial du sous-circuit enraciné en* α_i *et l'arc reliant* α_i *à la sortie* o *pour une valeur de* i *dans l'ensemble* $\{1, \ldots, p\}$.

— *Si la porte de sortie o de C est une porte de multiplication (ou une porte $\odot$) dont les arguments sont $\alpha_1, \ldots, \alpha_p$, les arbres monomiaux de C sont obtenus en prenant des copies disjointes pour chaque $1 \leq i \leq p$ d'un arbre monomial enraciné en α_i, puis en prenant les p arcs reliant les portes α_i à la sortie o.*

Par exemple, le circuit suivant



possède six arbres monomiaux.



On remarque ici qu'un arbre monomial peut avoir une taille (exponentiellement) plus grande que celle du circuit original. Cela ne posera pas de problème dans la suite de ce manuscrit. Toutefois, il est possible d'éviter cette explosion en travaillant avec des circuits multiplicativement disjoints comme dans [72].

À chaque arbre monomial, on peut associer un monôme correspondant au produit de ses feuilles.

Le lemme suivant qui montre comment revenir au circuit à partir des arbres monomiaux provient de [72].

Lemme 1.11. *Un polynôme f calculé par un circuit C correspond exactement à la somme des monômes des arbres monomiaux :*

$$f = \sum_{\substack{T \text{ arbre} \\ \text{monomial}}} m(T)$$

où $m(T)$ est le monôme associé à l'arbre T.

2.4 Notations en profondeur constante

Dans le cas des circuits de profondeur constante de portes $\{+, \times\}$, l'arité des portes sera non bornée. En fait, pour un circuit de profondeur δ, si l'arité des portes est bornée par a, alors le polynôme calculé ne dépend que d'au plus a^δ variables. Or comme dans le cas de la complexité booléenne, nous ne voulons pas que la taille des entrées du problème soient bornée par une constante.

Pour les circuits de profondeur constante, il est traditionnel (et très pratique) de les partitionner en niveaux. Le niveau 0 contient les entrées, puis pour tout $i \geq 1$, le niveau i correspond à un unique opérateur et chaque porte de ce niveau a tous ses arguments dans le niveau $i-1$. On peut remarquer que cette transformation est presque anodine pour les circuits à une seule sortie, de portes $\{+, \times\}$ (plus précisément, elle n'augmente pas la profondeur p et multiplie la taille par au plus p).

Nous utiliserons quelques notations pratiques qui sont définies dans l'article [45]. Un circuit, par exemple de profondeur 4, tel que les portes des niveaux 1 et 3 sont des portes de multiplication et les portes de niveau 2 et 4 sont des portes d'addition est noté : circuit $\sum\prod\sum\prod$. De plus un circuit $\sum\prod^{[\alpha]}\sum^{[\beta]}\prod$ correspond à un circuit de type $\sum\prod\sum\prod$ où l'arité des portes de multiplication au niveau 3 est borné par α et l'arité des portes d'addition du niveau 2 est borné par β. Par exemple, un circuit $\sum\prod^{[\alpha]}\sum^{[\beta]}\prod$ calcule un polynôme de la forme :

$$\sum_{i=1}^{t}\prod_{j=1}^{u_i}\sum_{k=1}^{v_{i,j}}\prod_{l=1}^{w_{i,j,k}} x_{i,j,k,l}$$

où $u_i \leq \alpha$, $v_{i,j} \leq \beta$.

De même, nous aurons besoin de portes d'*exponentiation* $\bigwedge$. Nous ne les avons pas définies précédemment car elles ne serviront que dans le cas des circuits de profondeur bornée. Elles correspondent à l'opérateur "puissance". Par exemple un circuit $\sum\bigwedge^{[\gamma]}\sum$ calcule des polynômes de la forme :

$$\sum_{i=1}^{t}\left(\sum_{j=1}^{v_i} x_{i,j}\right)^{u_i}$$

où les exposants u_i sont bornés par γ.

3 Classes de Valiant

3.1 Un soupçon de complexité booléenne

Commençons ce chapitre par une petite digression sur la complexité booléenne. En fait, dans la suite, seul le chapitre 3 nécessitera quelques outils de cette théorie. L'intérêt ici est aussi de donner au lecteur une petite intuition des classes P et NP avant d'aller voir les classes VP et VNP qui en seront inspirées. De plus, on supposera connue la définition d'une machine de Turing (le lecteur pourra sinon, pour l'intuition, imaginer la machine de Turing comme un ordinateur ou un programme informatique). D'ailleurs, beaucoup plus d'informations sur la complexité booléenne (comme la définition des machines de Turing) pourront être trouvées dans les références [7, 37, 79, 82].

Définition 1.12. *L'ensemble* $\{0,1\}^\star$ *désigne l'ensemble des mots finis sur l'alphabet* $\{0,1\}$. *Par exemple* 011 *et* 00000 *sont deux mots de* $\{0,1\}^\star$. *Le premier est un mot de longueur* 3, *le second, un mot de longueur* 5. *On utilisera la notation* $|x|$ *pour désigner la taille du mot* x. *Un* langage *est une partie de* $\{0,1\}^\star$.

Nous pouvons maintenant définir la classe P constituée des langages supposés "facilement calculables".

Définition 1.13. *La classe* P *contient l'ensemble des langages* A *tels qu'il existe une constante* c *et une machine de Turing* $\mathcal{M}$ *telles que*

— *sur toute entrée* $x \in \{0,1\}^\star$, $\mathcal{M}(x)$ *fonctionne en temps* $\leq |x|^c + c$,

— $\mathcal{M}$ *reconnaît le langage* A, *i.e.* $x \in A \Leftrightarrow \mathcal{M}(x) = 1$.

Une des plus grandes réussites de cette théorie réside dans la classe NP. Dans l'idée, un langage A est dans cette classe, lorsque l'appartenance d'un mot à A est facilement vérifiable.

Définition 1.14. *On définit la classe* NP *comme l'ensemble des langages* A *tels qu'il existe un polynôme* p *et un langage* $B \in \mathsf{P}$ *où*

$$x \in A \Leftrightarrow \exists y \in \{0,1\}^{p(|x|)}, (x,y) \in B.$$

Le succès de la classe NP vient du fait que de nombreux langages ont été prouvés NP-complets (comprendre, au moins aussi difficiles que tous les autres de cette classe). Le livre référence sur le sujet est [34]. On conjecture que les deux classes précédentes sont distinctes, i.e. que les problèmes NP-complets n'ont pas d'algorithme de complexité polynomiale, mais cette question reste toujours ouverte. Cette conjecture figure dans la liste des sept problèmes du millénaire rédigée par l'Institut de mathématiques Clay.

Conjecture 1.15. *Les classes* P *et* NP *sont distinctes.*

3.2 Classes VP, VNP

Nous sommes en mesure de définir les classes de complexité du modèle de Valiant [99, 100]. Puisqu'on veut mesurer la complexité comme une fonction de la taille des entrées, on considérera en fait des suites infinies de polynômes comme $(\textsc{Det}_n)_{n\in\mathbb{N}}$. Ces suites de polynômes (P_n) seront calculées par des suites de ciruits C_n si et seulement si pour tout n, le circuit C_n calcule le polynôme P_n. Au début, nous considérerons bien ces suites de polynômes, mais rapidement, par abus de notation, nous identifierons ces suites aux polynômes : ainsi, par exemple, on parlera du polynôme $\textsc{Det}_n$ pour parler de la suite $(\textsc{Det}_n)_{n\in\mathbb{N}}$.

Comme dans le modèle booléen, nous aurons besoin d'une notion de réduction.

Définition 1.16. *Un polynôme* f *est une* projection *d'un polynôme* g *si* $k \leq l$ *et si*

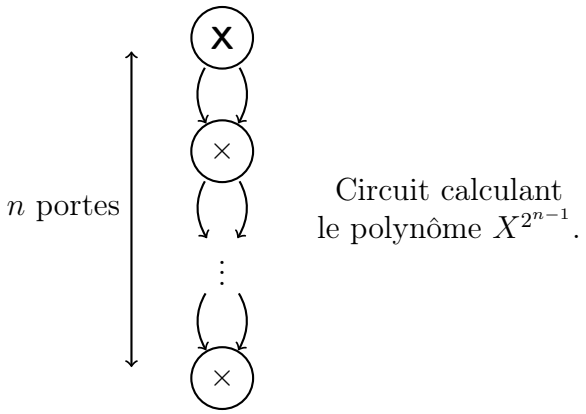
$$f(X_1, \ldots, X_k) = g(Y_1, \ldots, Y_l)$$

où les Y_i *sont soit des variables* X_i, *soit des constantes de* $\mathbb{A}$.

La suite de polynômes (f_n) *est une* projection polynomiale *de la suite de polynômes* (g_n) *s'il existe un polynôme* p *tel que pour tout* n, *le polynôme* f_n *soit une projection du polynôme* $g_{p(n)}$.

Les définitions des classes VP et VNP sont basées sur celles des classes booléennes P et NP (le V rajouté est pour Valiant). Intuitivement, nous voulons définir VP comme l'ensemble des suites de polynômes calculables par des circuits de taille

polynomiale. On va en fait rajouter une autre contrainte sur VP : nous voulons que le degré des polynômes de cette classe soit aussi polynomialement borné. Pourquoi rajouter une telle contrainte ? L'idée derrière est encore que l'on souhaite que VP ressemble à P. Les fonctions calculables polynomialement par une machine de Turing sont telles que la taille de leur sortie est polynomialement bornée par la taille de leur entrée. Ce n'est pas le cas des polynômes de degré exponentiel. Cependant dans le modèle des circuits, la multiplication et l'addition coûtent toujours un temps constant, quelque soit la taille des entrées. En particulier, il est possible de calculer des polynômes de degré exponentiel par des circuits de taille polynomiale, comme le montre le circuit suivant de taille n :



Commençons par la définition de la classe VP.

Définition 1.17. *Soit $\mathbb{A}$ un anneau commutatif. La suite C_n de polynômes (f_n) est dans $\mathsf{VP}_{\mathbb{A}}$ s'il existe des polynômes p, q et r et une suite de circuits arithmétiques sur $\mathbb{A}$ de portes $\{+, \times\}$ tels que pour tout n, les propriétés suivantes sont avérées :*

- *le nombre de variables de f_n est borné par $p(n)$,*
- *le degré de f_n est borné par $q(n)$,*
- *le circuit C_n calcule f_n*
- *et la taille de C_n est bornée par $r(n)$.*

Suivant la tradition, on pose $\mathsf{VP} = \mathsf{VP}_{\mathbb{Q}}$.

Considérons par exemple la famille $(\textsc{Det}_n)$. Le nombre de variables ainsi que le degré de ces circuits est polynomialement borné. La méthode du pivot fournit directement un circuit de portes $\{+, \times, -, \div\}$ de taille $O(n^3)$. D'après la remarque 1.1 et le lemme 1.6, il existe un circuit arithmétique de portes $\{+, \times\}$ de taille $O(n^5)$. En particulier, $(\textsc{Det}_n) \in \mathsf{VP}$.

Un autre exemple de polynôme est le produit itéré de matrices $\mathrm{IMM}_{n,n}$. Comme le produit de deux matrices se fait directement en utilisant $O(n^3)$ opérations, il est facile de vérifier que $\mathrm{IMM}_{n,n} \in \mathsf{VP}$.

La classe VNP correspond alors à la classe NP. L'idée de la définition est de partir de la définition par certificats de la classe booléenne NP et de remplacer le "$\exists y \in \{0,1\}^{p(n)}$" par une somme $\sum_{y \in \{0,1\}^{p(n)}}$.

Définition 1.18. *Soit $\mathbb{A}$ un anneau commutatif. La suite de polynômes (g_n) est dans $\mathsf{VNP}_{\mathbb{A}}$ s'il existe une suite de polynômes $(h_n) \in \mathsf{VP}_{\mathbb{A}}$ et un polynôme p tels que*

$$g_n(x) = \sum_{\varepsilon \in \{0,1\}^{p(n)}} h_n(x, \varepsilon)$$

De même on note VNP *la classe* $\mathsf{VNP}_{\mathbb{Q}}$.

Les suites de polynômes $(\textsc{Perm}_n)$ et $(\textsc{Ham}_n)$, définies à la section 1 sont des exemples d'éléments de la classe VNP (une preuve pourra être trouvée par exemple dans [19]) :

Lemme 1.19. *Pour tout anneau* $\mathbb{A}$*, on a* $(\textsc{Perm}_n), (\textsc{Ham}_n) \in \mathsf{VNP}_{\mathbb{A}}$.

En fait, il est possible de se passer, a priori, de la borne sur le degré des polynômes f_n en considérant que la "mesure" du circuit correspond à son nombre de sommets combiné à son degré formel. Ceci évite a posteriori les polynômes de degré exponentiel. Le prochain lemme (folklore) assure que l'on obtient les mêmes classes en contraignant le degré formel des circuits au lieu du degré des polynômes.

Lemme 1.20. *Si une suite de polynômes* (f_n) *de degré* (d_n) *est dans* VP*, alors il existe une suite de circuits* (C_n) *calculant* f_n *de taille polynomiale telle que le degré de* C_n *est* d_n *pour tout* n.

3.3 Classes sans constantes

L'importance du rôle des constantes est une question intéressante. Par exemple remarquons que pour calculer le produit itéré de matrices, aucune constante n'est utilisée. Pour mette en évidence leur rôle, Malod introduit des variantes *sans constantes* VP^0 et VNP^0 des classes de Valiant [71]. Par "sans constantes", nous voulons en fait dire utilisant seulement la constante -1. Les constantes 0 et 1 s'obtiennent facilement à l'aide de -1 et vu que nous n'autorisons pas la soustraction, nous avons besoin d'une constante strictement négative.

Ainsi, si un circuit a besoin d'une constante non triviale, il doit la calculer à partir de -1. En particulier, la notion de degré formel (qui ignore le calcul des constantes) devient alors un peu bancal. Malod [71] introduit ainsi le degré formel complet :

Définition 1.21. *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 en prend la somme.*

Nous pouvons maintenant définir les classes VP^0 et VNP^0.

Définition 1.22. f_n *est dans* VP^0 *s'il existe une suite de circuits arithmétiques*
- *calculant* f_n*,*
- *utilisant comme seule constante* -1
- *et de taille et de degré formel complet polynomiaux.*

g_n *est dans* VNP^0 *s'il existe un polynôme* p *tel que :*

$$g_n(x) = \sum_{\varepsilon \in \{0,1\}^{p(n)}} h_n(x, \varepsilon)$$

avec $h_n \in \mathsf{VP}^0$.

En fait les polynômes considérés précédemment ne nécessitent pas de constantes. En particulier :

$$\textsc{Det}_n \in \mathsf{VP}^0 \text{ et } \textsc{Perm}_n, \textsc{Ham}_n \in \mathsf{VNP}^0.$$

La réduction définie précédemment (la projection polynomiale) utilise les constantes de l'anneau courant. Les classes VP^0 et VNP^0 ne sont donc pas stables pour cette réduction. Nous sommes alors amenés à considérer une variante sans constante de cette réduction [71].

Définition 1.23. *Une suite de polynômes (f_n) est une* projection bornée *d'une suite (g_n) s'il existe deux polynômes p et q tels que pour tout n :*

$$f_n(X_1, \ldots, X_k) = g_n(Y_1, \ldots, Y_l)$$

où les Y_i sont soit des variables X_i, soit des constantes calculables par des circuits de taille et degré formel bornés par $q(n)$ utilisant seulement la constante -1.

Une autre mesure classique quantifie la complexité des circuits sans constantes. Il s'agit de la mesure τ introduite dans [27].

Définition 1.24. *La complexité $\tau(f)$ d'un polynôme f entier (i.e. de $\mathbb{Z}[X_1, \ldots, X_n]$) est défini comme la taille minimale d'un circuit calculant f, de portes $\{+, -, \times\}$ et utilisant seulement la constante* 1.

Remarquons que la définition (traditionnelle) donnée ici ne correspond pas exactement aux conventions actuelles. On utilise ici la constante 1, mais on autorise la porte de soustraction. Cette mesure est en particulier restée célèbre grâce à la τ-conjecture introduite par Shub et Smale [92]. On reviendra plus en détail sur cette conjecture au chapitre 3.

3.4 Polynômes complets

Le problème est alors de trouver pour chaque polynôme la plus petite classe qui la contient. Comme dans le cas booléen, les bornes inférieures non conditionnelles sont généralement inconnues, mais on peut encore obtenir des "preuves de difficulté" grâce à la notion de complétude.

Définition 1.25. *Une suite de polynômes (f_n) est VNP-complète si et seulement si la suite (f_n) fait partie de la classe VNP et pour toute suite (g_n) de VNP, g_n est une projection polynomiale de f_n.*

On peut de même obtenir une définition de VNP^0-complétude en utilisant la classe VNP^0 au lieu de VNP et en n'autorisant que les projections polynomiales bornées.

En particulier, bien qu'on ne soit pas capable de montrer qu'un polynôme $f \in \mathsf{VNP}$ n'est pas dans VP, il est possible pour un certain nombre de polynômes, de prouver qu'ils sont VNP-complets et donc, non supposés être dans VP. Si tel était le cas, $\mathsf{VNP} = \mathsf{VP}$.

Valiant a montré [99] que sur tout corps $\mathbb{K}$ de caractéristique différente de 2, le permanent est VNP-complet.

Théorème 1.26. *Soit $\mathbb{K}$ un corps de caractéristique différente de* 2*. Alors la famille $\textsc{Perm}_n$ est VNP-complète.*

On remarque qu'en caractéristique 2, le permanent correspond exactement au déterminant, il tombe donc dans la classe $\mathsf{VP}_{\mathbb{K}}$.

Plus précisément, la preuve du théorème précédent nécessite la constante 2^{-1}. Ceci explique l'hypothèse du corps de caractéristique différente de 2. L'intérêt des classes sans constantes est justement de mettre en évidence le rôle particulier que certaines constantes peuvent avoir. En particulier la proposition suivante généralise le théorème 1.26 et vient de [62]. Intuitivement, il signifie que le permanent appartient à la classe VNP^0 et est presque complet pour cette classe.

Proposition 1.27. *Supposons que* $\textsc{Perm}_n \in \mathsf{VP}^0$. *Alors, pour toute famille* (f_n) *dans* VNP^0, *il existe un polynôme* $p(n)$ *tel que la famille* $\left(2^{p(n)} f_n\right)$ *soit dans* VP^0.

Le permanent étant probablement le polynôme complet pour VNP le plus étudié, nous suivrons la tradition dans ce manuscrit et nous l'utiliserons systématiquement comme polynôme complet pour VNP. Toutefois, il est possible d'éviter les difficultés provoquées par la constante 2^{-1} en choisissant un autre polynôme VNP-complet comme le hamiltonien (défini en section 1.3).

Théorème 1.28. *Dans tout anneau* $\mathbb{A}$, *le polynôme* $\textsc{Ham}_n$ *est* VNP^0*-complet et donc aussi* $\mathsf{VNP}_{\mathbb{A}}$*-complet.*

La grande conjecture classique du domaine est que les classes VP et VNP sont distinctes :

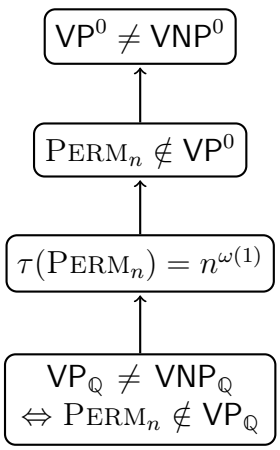
Conjecture 1.29 (Hypothèse de Valiant)**.** $\mathsf{VP} \neq \mathsf{VNP}$.

La complétude du permanent assure que cette conjecture est équivalente au fait que le permanent n'appartient pas à la classe VP, i.e. ne possède pas de circuit arithmétique de taille polynomiale.

Les implications sont moins simples dans le cas sans constantes. En fait, si $\mathsf{VP}^0 = \mathsf{VNP}^0$ alors on a $\textsc{Perm}_n \in \mathsf{VP}^0$ et si $\textsc{Perm}_n \in \mathsf{VP}^0$ alors $\tau(\textsc{Perm}_n) = n^{O(1)}$, mais les réciproques ne sont pas connues. Pour la première réciproque, nous avons déjà vu que le permanent n'est que "presque complet" pour VNP^0. Le second cas est plus subtil. Si $\tau(\textsc{Perm}_n) = n^{O(1)}$, il est possible que le circuit utilise des portes de très grand degré formel complet pour calculer des constantes. Cependant, l'astuce classique d'homogénéisation ne semble pas être efficace contre le calcul des constantes.

Toutefois si $\tau(\textsc{Perm}_n) = n^{O(1)}$, alors le permanent admet une suite de circuit de taille polynomiale et ainsi $\mathsf{VP} = \mathsf{VNP}$.

La figure suivante (directement inspirée de l'article de Bürgisser [21]) tente de résumer les différentes implications connues.



Chapitre 2

Circuits de profondeur bornée

Valiant, Skyum, Berkowitz et Rackoff [101] ont prouvé que si un circuit de taille s et de profondeur p calcule un polynôme de degré d, alors ce polynôme peut aussi être calculé par un circuit de profondeur $O(\log(d))$ et de taille bornée par un polynôme en s. Ce résultat est essentiellement à la base de toutes les avancées sur la parallélisation des circuits arithmétiques. Quelques années plus tard, Miller, Ramachandran et Kaltofen [73] puis Allender, Jiao, Mahajan et Vinay [6] ont étudié la complexité de cette méthode de parallélisation. À l'aide de ces résultats, Agrawal et Vinay [4] ont prouvé que si un polynôme f n-varié de degré $d = O(n)$ possède un circuit de taille $2^{o(d+d\log(n/d))}$, alors f peut aussi être calculé par un circuit de profondeur quatre $(\sum\prod\sum\prod)$ de taille $2^{o(d+d\log(n/d))}$. Ce résultat indique que pour prouver des bornes inférieures dans les circuits arithmétiques ou pour dérandomiser le test d'identité polynomial, le cas des circuits de profondeur quatre est dans un certain sens le cas général.

L'hypothèse du résultat d'Agrawal et Vinay est assez faible : ils considèrent des circuits de taille $2^{o(d+d\log(n/d))}$ (nous pouvons remarquer au passage que tous les polynômes ont une formule de taille $d\binom{n+d}{d} = 2^{O(d\log(\frac{n+d}{d}))}$). Mais, serait-il possible d'obtenir une conclusion plus forte si on demandait des hypothèses plus fortes ? Koiran [60] a montré que c'était effectivement le cas. Si le circuit de départ est de taille s, alors le polynôme peut être calculé par un circuit de profondeur quatre de taille $2^{O(\sqrt{d}\log(d)\log(s))}$. Par exemple, si la famille du permanent est calculée par des circuits de taille polynomiale (i.e. de taille n^c), alors elle est aussi calculée par des circuits de profondeur quatre et de taille $2^{O(\sqrt{n}\log^2(n))}$. De plus, la transformation conserve l'homogénéité du circuit. La parallélisation semble être un outil intéressant pour obtenir des bornes inférieures pour les circuits généraux : une borne inférieure en $2^{\omega(\sqrt{n}\log^2(n))}$ sur la taille des circuits $\sum\prod^{[O(\sqrt{n})]}\sum\prod^{[\sqrt{n}]}$ calculant le permanent implique qu'il n'y a pas de circuits de taille polynomiale pour le permanent. Et il paraît plus facile d'obtenir des bornes inférieures pour ces circuits particuliers que pour les circuits généraux. C'est d'ailleurs le cas. Bien qu'aucune borne inférieure superpolynomiale ne soit encore connue pour les circuits généraux, Gupta, Kamath, Kayal et Saptharishi [44] ont obtenu une borne inférieure superpolynomiale pour le permanent s'appliquant à des circuits de profondeur 4 particuliers. Plus précisément, ils ont montré que si un circuit homogène $\sum\prod\sum\prod^{[t]}$ (i.e. un circuit de profondeur 4 dont le degré entrant des portes de multiplication du premier niveau est borné par t) calcule le permanent d'une matrice de taille $n \times n$, alors sa taille est $2^{\Omega(n/t)}$. En

particulier, un circuit homogène $\sum\prod\sum\prod^{[\sqrt{n}]}$ calculant le permanent est de taille $2^{\Omega(\sqrt{n})}$. L'année suivante, les mêmes auteurs [45] ont trouvé comment réduire encore un peu la profondeur des circuits. Ils montrent comment transformer des circuits à n variables de taille s et de profondeur d ($= n^{O(1)}$) en des circuits de profondeur 3 et de taille $\exp(O(\sqrt{d\log s\log n\log d}))$. De plus, si l'entrée est un programme à branchements (et non un circuit), la borne supérieure devient $\exp(O(\sqrt{d\log s\log n}))$. Ce résultat implique l'existence d'un circuit de profondeur 3 et de taille $2^{O(\sqrt{n}\log n)}$ calculant le déterminant d'une matrice $n\times n$. Toutefois, ce résultat n'est pas comparable aux réductions à la profondeur 4 car le circuit de profondeur 3 obtenu est non homogène, et utilise au milieu de son calcul des portes calculant des polynômes de très haut degré. En 2013, Fournier, Limaye, Malod et Srinivasan [31] ont obtenu une borne inférieure de $2^{\Omega(\sqrt{d/t}\log n)}$ pour la taille des circuits homogènes $\sum\prod\sum\prod^{[t]}$ calculant le produit itéré de matrices. Tous ses résultats récents sur les circuits arithmétiques peuvent être trouvés dans l'article de synthèse [58].

Dans ce chapitre, nous allons commencer par étudier des bornes inférieures sur la taille des circuits de profondeur bornée. Nous allons voir deux résultats intermédiaires sur les circuits de profondeur 4 et 3, avant d'évoquer les résultats récents relatifs à la profondeur 4. Puis dans la section suivante, nous allons nous attaquer aux résultats de parallélisation (i.e. aux bornes supérieures). Nous [98] améliorons la borne de parallélisation de Koiran : un circuit de taille s peut être parallélisé de manière homogène à la profondeur 4 en un circuit de taille $\exp(O(\sqrt{d\log(ds)\log(n)}))$. De plus, le degré entrant de chaque porte de multiplication est borné par $O\left(\sqrt{d\frac{\log ds}{\log n}}\right)$. Remarquons que comme $n\leq s$, le résultat implique la borne de Koiran et est en général meilleur : dans le cas où $d, s = n^{\Theta(1)}$, la borne de Koiran est $2^{O(\sqrt{n}\log^2 n)}$ tandis que la nouvelle borne est $2^{O(\sqrt{n}\log n)}$. En particulier, la nouvelle borne est optimale puisqu'elle correspond exactment à la borne inférieure obtenue par [31]. Cela implique aussi qu'une borne inférieure en $2^{\omega(\sqrt{n}\log(n))}$ pour les circuits homogènes de profondeur 4 calculant le permanent induit une borne inférieure super-polynomiale pour la taille des circuits généraux calculant le permanent. En fait, nous généralisons cette réduction au cas d'une profondeur bornée. Enfin, nous étudierons le cas des parallélisations non homogènes introduites par Gupta, Kamath, Kayal et Saptharishi [45]. Comme ils utilisent dans leur preuve la borne de Koiran, nous pourrons légèrement améliorer leur borne en utilisant à la place la borne décrite plus haut. Un circuit n-varié de taille s et de profondeur d peut être simulé par un circuit de profondeur 3 et de taille $\exp\left(O(\sqrt{d\log(ds)\log n})\right)$. Enfin, nous remarquons que cette parallélisation peut elle aussi être généralisée aux profondeurs constantes, ce qui nous donnera, en particulier, le résultat intéressant que les circuits de taille s et de degré d peuvent en fait être simulés par des circuits de profondeur 4 et de taille $(ds)^{\sqrt[3]{d}}$. Cette borne est bien en-dessous des bornes inférieures connues pour les circuits n'utilisant que des petits degrés. Cela montre bien que l'utilisation de portes intermédiaires de très haut degré s'avère très puissante. Aujourd'hui, on ne sait pas comment obtenir des bornes inférieures non triviales pour de tels circuits.

1 Les formules de Ryser, Glynn et Fischer

Les travaux autour de l'hypothèse de Valiant tendent à essayer de montrer que le permanent est difficile à calculer. Mais qu'est ce que cela veut dire plus précisément ? On entend parfois que le calcul du permanent devrait nécessiter un nombre exponentiel d'opérations arithmétiques. Ce n'est pas encore un énoncé très précis. Souvent (vu que le terme est suffisamment vague, c'est loin d'être toujours vrai), on utilise le terme exponentiel pour désigner une fonction $f(n) = 2^{\theta(n^c)}$ pour une constante $c \geq 1$ (si c est une constante strictement inférieur à 1, on préfère habituellement le terme sous-exponentiel). Ensuite, il pourrait être tentant (et naturel) de paramétriser les polynômes par leur nombre de variables. Le polynôme PERM_n est un polynôme en n^2 variables. La conjecture émise plus haut pourrait être décrite plus formellement :

Conjecture (Première conjecture sur la complexité du permanent)**.** *Si C_n est une suite de circuits de taille s_n calculant PERM_n, alors*

$$s_n = 2^{\Omega(n^2)}.$$

Cependant, cette conjecture est trivialement fausse puisque le polynôme PERM_n est une somme de $(n!)$ monômes. Il peut être calculé par une suite de circuits de taille $n \times (n!)$. En fait une meilleure borne existe depuis 1963 et les travaux de Ryser [88]. Il trouva une formule simple, de taille $n^2 2^n$ pour le permanent d'une matrice $A = (A_{i,j})_{1 \leq i,j \leq n}$:

Proposition 2.1 (Formule de Ryser)**.**

$$\text{PERM}_n(A) = (-1)^n \sum_{S \subseteq \{1,\ldots,n\}} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \in S} a_{i,j}.$$

On peut donc émettre une nouvelle conjecture. Celle-ci est encore ouverte :

Conjecture 2.2 (Conjecture sur la complexité du permanent)**.** *Si C_n est une suite de circuits de taille s_n calculant PERM_n, alors*

$$s_n = 2^{\Omega(n)}.$$

La formule de Ryser est assez étonnante car malgré sa grande simplicité, homogène et de profondeur 3, elle est une des formules connues les plus efficaces pour calculer le permanent. Une autre formule, devenue classique, mais trouvée beaucoup plus récemment par Glynn [36] possède ces mêmes propriétés :

Proposition 2.3 (Formule de Glynn)**.**

$$\text{PERM}_n(A) = \frac{1}{2^{n-1}} \sum_{\varepsilon_2,\ldots,\varepsilon_n \in \{\pm 1\}} (-1)^{p(\varepsilon)} \prod_{i=1}^{n} \left(a_{i,1} + \sum_{j=2}^{n} \varepsilon_j a_{i,j} \right)$$

où $p(\varepsilon) = |\{i \mid \varepsilon_i = -1\}|$.

Ces formules assurent que le permanent peut être calculé par des circuits de type $\sum^{[2^n]} \prod^{[n]} \sum^{[n]}$. Ce résultat est d'autant plus surprenant que le même résultat est inconnu et plutôt conjecturé faux pour le déterminant :

Conjecture 2.4. DET_n *n'a pas de circuits de type* $\sum^{[2^{O(n)}]}\prod^{[n]}\sum$.

La formule de Glynn ressemble particulièrement à une formule plus vieille d'une quinzaine d'années, la formule de Fischer [30] :

Lemme 2.5 (Formule de Fisher)**.**

$$n!\cdot x_1x_2\dots x_n=\frac{1}{2^{n-1}}\sum_{r_2,\dots,r_n\in\{\pm1\}}(-1)^{p(r)}\left(x_1+\sum_{i=2}^{n}r_ix_i\right)^n$$

où $p(r)=|\{i\mid r_i=-1\}||$.

Dans [86], les auteurs montrent que la taille de la somme (en 2^{n-1}) est exactement la taille optimale pour transformer des monômes en sommes de puissances de formes lineaires.

En fait, comme Amir Shpilka me l'a fait remarquer lors d'une discussion, il est facile d'obtenir la formule de Fischer à partir de celle de Glynn. Il suffit pour cela de calculer le permanent de la matrice

$$\begin{bmatrix} x_1 & x_2 & \dots & x_n\\ \vdots & \vdots & \vdots & \vdots\\ x_1 & x_2 & \dots & x_n\end{bmatrix}$$

qui vaut $n!\cdot x_1\dots x_n$.

Ainsi, on se dit que la même astuce devrait marcher en utilisant la vraie formule de Ryser. On obtient effectivement une nouvelle formule du type de celle de Fischer :

Proposition 2.6.

$$n!\cdot x_1x_2\dots x_n=(-1)^n\sum_{S\subseteq\{1,\dots,n\}}(-1)^{|S|}\left(\sum_{j\in S}x_j\right)^n.$$

2 Quelques bornes inférieures

2.1 Comptage de monômes

Nous allons commencer cette section par une borne inférieure très simple mais relativement précise. On va montrer :

Proposition 2.7. *Si une suite de circuits* $\sum^{[s]}\prod^{[a]}\sum^{[v]}\prod$ *calcule* PERM_n *ou* DET_n*, alors* $s\cdot v^a\geq n!$.

En particulier, si une suite de circuits $\sum^{[s]}\prod^{[O(\sqrt{n})]}\sum^{[s]}\prod$ *calcule* PERM_n *ou* DET_n*, alors* $s\geq 2^{\Omega(\sqrt{n}\log n)}$.

Les bornes supérieures en a et v sur les degrés entrants des portes de multiplication du troisième niveau et les portes d'addition du second niveau s'avérent être cruciales. Une telle contrainte impliquera directement en général une bonne borne inférieure seulement grâce à un argument de comptage de monômes. On peut comparer ainsi ce résultat avec la proposition 2.10 plus loin.

Nous ferons la preuve dans le cas du permanent. Le cas du déterminant est complètement identique. L'approche ici, est de transformer un tel circuit en un circuit de profondeur 2, puis d'obtenir une borne inférieure pour le circuit de profondeur 2. En fait, dans le cas des circuits de profondeur 2, l'écriture d'un polynôme comme une somme de produits est unique (une fois qu'on a effectué toutes les annulations possibles). Il s'agit de la forme développée du polynôme. La taille de la somme est alors simplement le nombre de monômes. Vu que PERM_n a $n!$ monômes, on vient de prouver

Lemme 2.8. *Si un circuit* $\sum^{[s]} \prod$ *calcule* PERM_n*, alors* $s \geq n!$.

D'un autre côté, pour calculer dans un circuit $\sum^{[s]} \prod^{[a]} \sum^{[v]} \prod$ une porte du troisième niveau, il suffit de calculer un polynôme $\prod^{[a]} \sum^{[v]}$ qui a pour entrées les portes du premier niveau. En appellant V l'ensemble de ces entrées, les polynômes du troisième niveau sont donc de la forme $g = \prod_{i=1}^{a} \sum_{j=1}^{v} z_{i,j}$ avec $z_{i,j} \in V$. Or si on développe g, on obtient $g = \sum_{(j_1,\ldots,j_a)\in\{1,\ldots,v\}^a} z_{1,j_1} \ldots z_{a,j_a}$. Donc on peut transformer tout circuit $\sum^{[s]} \prod^{[a]} \sum^{[v]} \prod$ en un circuit $\sum^{[s]} \sum^{[v^a]} \prod^{[a]} \prod$, c'est-à-dire un circuit $\sum^{[sv^a]} \prod$. Ceci prouve la proposition 2.7.

2.2 Quasi-optimalité des formules de Ryser et de Glynn

Dans toute la suite de cette section sur les bornes inférieures, nous utiliserons la dimension des espaces vectoriels engendrés par certaines familles de polynômes. Donc l'anneau de base des polynômes sera en fait un corps.

Pour obtenir des bornes inférieures, un des outils principaux est l'espace engendré par les dérivées partielles. Nisan et Wigderson [76] ont trouvé des bornes inférieures pour la taille des circuits homogènes de profondeur 3 calculant les polynômes symétriques élémentaires ou le produit itéré de matrices. Ces techniques sont développées dans les articles de synthèse [91] et [23]. Depuis 2012, cet outil est au cœur des travaux relatifs aux bornes inférieures pour les circuits arithmétiques homogènes de profondeur 4. Pour ce dernier point, on y reviendra un peu plus tard.

Un autre résultat, très proche de ceux de Nisan et Wigderson [76], peut être obtenu à l'aide de ces techniques : montrer que les formules de Ryser et de Glynn sont "presque optimales". Après quelques discussions, ce résultat – qui découle de [76] – semble connu de certaines personnes, mais à la connaissance de l'auteur, il n'est écrit nulle part.

Proposition 2.9. *Soit* C_n *une suite de circuits de type* $\sum^{[s]} \prod^{[n]} \sum$ *calculant* PERM_n *(ou* DET_n*), alors*

$$s \geq \binom{n}{n/2} \geq \frac{2^n}{\sqrt{2n}}.$$

Pour les formules de Ryser et de Glynn, s vaut respectivement $2^n - 1$ et 2^{n-1}. Les résultats sont donc optimaux à un facteur multiplicatif près de $\frac{1}{\sqrt{n}}$. Nous allons donner maintenant une preuve de cette proposition. D'ailleurs, cette preuve illustre bien l'utilisation typique des dérivées partielles.

Démonstration. Soit k un entier que l'on fixera plus tard. Posons $X = \{x_{i,j} \mid 1 \leq i, j \leq n\}$ l'ensemble des variables de PERM_n. Nous allons considérer l'espace vectoriel engendré par les dérivées partielles $k$ièmes du polynôme PERM_n. Notons $\langle \boldsymbol{\partial}^{=k} f \rangle$ l'espace vectoriel engendré par l'ensemble

$$\left\{ \frac{\partial^k}{\partial y_1 \dots \partial y_k} f \mid (y_1, \dots, y_k) \in X^k \right\}.$$

La preuve se fait en deux parties. Nous allons commencer par borner inférieurement la dimension de $\langle \boldsymbol{\partial}^{=k} \text{PERM}_n \rangle$, puis nous allons borner supérieurement la dimension de tout espace $\langle \boldsymbol{\partial}^{=k} g \rangle$ où g est un polynôme calculé par un circuit $\sum^{[s]} \prod^{[n]} \sum$.

Définissons les p-mineurs (mineurs permanentaux) de taille $s \times s$ d'une matrice M de taille $n \times n$ comme les permanents de N où N parcourt les sous-matrices de M obtenues en supprimant $(n-s)$ lignes et $(n-s)$ colonnes. Si $k < n$, alors les dérivées partielles d'ordre k de PERM_n sont soit le polynôme nul (si on dérive deux fois dans la même ligne ou la même colonne), soit les p-mineurs de tailles $(n-k) \times (n-k)$. Il est facile de vérifier que chacun de ces p-mineurs de taille $(n-k) \times (n-k)$ peut être obtenu comme une dérivée $k$ième de PERM_n. De plus comme un même monôme ne peut pas apparaître dans deux p-mineurs différents, cela signifie que la famille des p-mineurs est une famille libre. La dimension de l'espace est donc exactement le nombre de p-mineurs distincts. Vu qu'un p-mineur de taille $(n-k) \times (n-k)$ est obtenu de manière unique en choisissant k lignes et k colonnes, on obtient :

$$\dim(\langle \boldsymbol{\partial}^{=k} \text{PERM}_n \rangle) = \binom{n}{k}^2.$$

De l'autre côté, si g est un polynôme de degré n pouvant être exprimé de la forme $\sum^{[s]} \prod^{[n]} \sum$, alors $g(\mathbf{x}) = \sum_{i=1}^{s} h_i(x)$ où chaque h_i est un produit de n formes linéaires. De plus, notre mesure de complexité (la dimension des sous-espaces engendrés par le dérivées partielles) est une mesure sous-additive. En effet, comme $\boldsymbol{\partial} g = \sum_{i=1}^{t} \boldsymbol{\partial} h_i$, on a

$$\langle \boldsymbol{\partial}^{=k} g \rangle \subseteq \text{ev}\left(\bigcup_{i=1}^{s} \langle \boldsymbol{\partial}^{=k} h_i \rangle \right)$$

où $\text{ev}(A)$ correspond à l'espace engendré par A. D'où

$$\dim\left(\langle \boldsymbol{\partial}^{=k} \rangle\right) \leq s \cdot \max_h \dim\left(\langle \boldsymbol{\partial}^{=k} h \rangle\right)$$

où h parcourt les produits de taille n de formes linéaires. Posons $h = l_1 \dots l_n$ avec les l_i des formes linéaires. Toute dérivée $k$ième de h est engendrée par des polynômes $l_{i_1} \dots l_{i_{n-k}}$ (où $1 \leq i_1 < \dots < i_{n-k} \leq n$). Cette famille est de taille $\binom{n}{k}$. D'où

$$\dim\langle \boldsymbol{\partial}^{=k} g \rangle \leq s \binom{n}{k}.$$

En remettant tout ensemble, on en déduit que si PERM_n peut être écrit comme $\sum^{[s]} \prod^{[n]} \sum$, alors

$$\binom{n}{k}^2 \leq s \binom{n}{k}.$$

En choisissant $k = \frac{n}{2}$, on en déduit la proposition. □

2.3 Quelques résultats récents de bornes inférieures

Avant d'attaquer, dans la prochaine partie, les bornes supérieures pour les circuits de profondeur bornée, nous allons juste évoquer les bornes inférieures connues qui vont leur faire écho.

La technique des dérivées partielles a été vraiment remise au goût du jour depuis l'article de Gupta, Kamath, Kayal et Saptharishi [44]. Ils considèrent en fait l'espace engendré par les dérivées partielles décalées :

$$\langle \boldsymbol{\partial}^{=k} f \rangle_{\leq l} = \left\{ x_1 \dots x_l \frac{\partial^k}{\partial y_1 \dots \partial y_k} f \mid (x_1, \dots, x_l, y_1, \dots, y_k) \in X^{k+l} \right\}.$$

Dans leur article, ils prouvent que :

Proposition 2.10. *Tout circuit homgène* $\sum^{[s]} \prod \sum \prod^{[t]}$ *qui calcule* DET_n *(ou* PERM_n*) doit être tel que*

$$s \geq 2^{\Omega(\frac{n}{t})}.$$

En particulier, tout circuit homogène $\sum^{[s]} \prod \sum \prod^{[\sqrt{n}]}$ *qui calcule* DET_n *(ou* PERM_n*) est tel que*

$$s \geq 2^{\Omega(\sqrt{n})}.$$

Le résultat fut d'autant bien accueilli que c'est la première borne inférieure superpolynomiale pour les circuits de profondeur 4. De plus, on verra dans la prochaine section que ce résultat est presque optimal, on peut donner une borne supérieure en $n^{\sqrt{d}}$ (où d est le degré du polynôme). La technique a alors été adaptée à d'autres familles de polynômes. Peu après, Kayal, Saha et Saptharishi obtinrent la borne inférieure $n^{\sqrt{d}}$ pour les polynômes de Nisan-Wigderson définis dans [57].

Définition 2.11. *Soient* n *une puissance de* 2 *et* $\mathbb{F}_n$ *le corps fini où les* n *éléments sont identifiés avec l'ensemble* $\{1, \dots, n\}$*. Pour tout* $0 \leq k \leq n$*, le polynôme* NW_k *est un polynôme à* n^2 *inconnues de degré* n *défini comme suit :*

$$\mathsf{NW}_k(x_{1,1}, \dots, x_{n,n}) = \sum_{\substack{p \in \mathbb{F}_n[t] \\ \deg(p) < k}} x_{1,p(1)} \dots x_{n,p(n)}.$$

Nous pouvons déjà décrire une variante NW_k^d *de ce polynôme. Soit* d *un nombre premier, nous identifierons les éléments du corps* $\mathbb{F}_{d^2}$ *à l'ensemble* $\{1, \dots, d^2\}$*. Alors,*

$$\mathsf{NW}_k^d(x_{1,1}, \dots, x_{d,d_2}) = \sum_{\substack{p \in \mathbb{F}_{d^2}[t] \\ \deg(p) < k}} x_{1,h(1)}, \dots, x_{d,h(d)}.$$

Plus précisément, Kayal, Saha et Saptharishi ont montré [57] :

Proposition 2.12. *Si une suite de circuits* $\sum^{[s]} \prod^{[O(\sqrt{n})]} \sum \prod^{[\sqrt{n}]}$ *calcule le polynôme* NW_k *avec* $k = \varepsilon\sqrt{n}$ *pour un certain* $\varepsilon > 0$ *suffisamment petit, alors*

$$s \geq 2^{\Omega(\sqrt{n}\log(n))}.$$

Cette famille de polynôme fait partie de la classe VNP. Toutefois, une borne inférieure similaire (en $n^{\sqrt{d}}$) a été trouvée pour le produit itéré de matrices. Fournier, Limaye, Malod et Srinivasan [31] ont montré que :

Proposition 2.13. *Si un circuit* $\sum^{[s]}\prod^{[O(D)]}\sum\prod^{[\sqrt{d}]}$ *calcule le polynôme* $\mathrm{IMM}_{n,d}$*, alors*

$$s \geq 2^{\Omega(\sqrt{d}\log(n/D))}.$$

Les techniques de preuve pour cette proposition ainsi que pour la proposition 2.12 ont été unifiés dans l'article [24].

Nous finirons cette présentation de l'état de l'art sur les bornes inférieures par deux résultats tout récents. Jusqu'à présent, toutes les bornes inférieures requièrent des bornes supérieures sur le degré entrant de certaines portes de multiplication. Peut-on s'affranchir de telles contraintes ? On verra à la section 4 que si on s'autorise à ce que les portes intermédiaires calculent des polynômes de très hauts degrés, alors les bornes en $n^{\sqrt{d}}$ ne marchent plus du tout. Toutefois, une contrainte intermédiaire, naturelle, pourrait être que le circuit soit homogène, sans donner de conditions supplémentaires sur les degrés. On peut remarquer qu'une telle contrainte implique en particulier que les portes ne calculent pas des polynômes de degré strictement plus grand que d. Des bornes inférieures superpolynomiales ont été trouvées par Kumar et Saraf [67], puis indépendamment par Kayal, Limaye, Saha et Srinivasan [56]. Ainsi,

Proposition 2.14. *Soit* C_n *une famille de circuits homogènes* $\sum^{[s]}\prod\sum\prod$*.*

- *Si* C_n *calcule* NW_r^d *alors* $s \geq 2^{\Omega(\sqrt{d}\log d)}$*.*
- *Si* C_n *calcule* $\mathsf{IMM}_{n,d}$ *avec* $d = \Omega(\log^2 n)$*, alors* $s \geq n^{\Omega(\log n)}$*.*
- *Si* C_n *calcule* DET_n*, alors* $s \geq n^{\Omega(\log n)}$*.*

3 Bornes supérieures pour circuits homogènes

Comme on l'a mentionné précédemment, il existe une borne supérieure sur la taille des circuits de profondeur 4 calculant des polynômes de VP en $n^{\sqrt{d}}$ où d est le degré. Nous allons en fait montrer un résultat un peu plus général qui traite toutes les profondeurs constantes paires. L'idée étant que les circuits de profondeur 6 nous permettront par exemple d'obtenir une borne supérieure pour les circuits non homogènes de profondeur 4 dans la prochaine section.

On rappelle (Remarque 1.4) que si rien n'est mentionné l'arité des portes $+$ et $\times$ est deux.

Théorème 2.15. *Soient* p *un entier supérieur à* 2 *et* f *un polynôme à* n *variables calculé par un circuit de taille* s *et de degré* d*. Alors* f *est calculé par* C*, un circuit* $\sum\prod^{[O(\alpha)]}\cdots\sum\prod^{[O(\alpha)]}\sum\prod^{[\beta]}$ *de profondeur* $2p$ *et de taille* $2^{O(d^{1/p}\log^{(p-1)/p}(ds)\log^{1/p} n)}$ *où :*

$$\alpha = \left(d\frac{\log n}{\log ds}\right)^{\frac{1}{p}} \text{ et } \beta = d^{\frac{1}{p}}\left(\frac{\log ds}{\log n}\right)^{\frac{p-1}{p}}.$$

De plus, si f *est homogène, ce sera aussi le cas pour* C*.*

Nous donnerons une preuve de cette parallélisation un peu plus loin, à la sous-section 3.3.

Le cas de la profondeur 4 est largement le plus étudié de nos jours. Le théorème précédent donne alors :

Théorème 2.16. *Soit f un circuit à n variables calculé par un circuit de taille s et de degré d. Alors f est calculé par un circuit $\sum\prod^{[O(\alpha)]}\sum\prod^{[\beta]}$ de taille $2^{O(\sqrt{d\log(ds)\log n})}$ où :*

$$\alpha = \sqrt{d\frac{\log n}{\log ds}} \text{ et } \beta = \sqrt{d\frac{\log ds}{\log n}}.$$

De plus si f est homogène ce sera aussi le cas pour le nouveau circuit.

D'ailleurs le théorème précédent peut être directement appliqué dans le cas du permanent.

Théorème 2.17. *Si le permanent $n \times n$ est calculé par un circuit de taille polynomiale en n, alors il est aussi calculé par un circuit homogène $\sum\prod^{[O(\sqrt{n})]}\sum\prod^{[O(\sqrt{n})]}$ de taille $2^{O(\sqrt{n}\log(n))}$.*

3.1 Propositions sur les circuits arithmétiques

Pour prouver le théorème 2.15, nous aurons besoin de quelques résultats préalables.

Le résultat suivant est considéré comme du folklore. Toutefois on peut trouver une preuve dans le livre de Bürgisser [19] (Lemma 2.14).

Proposition 2.18. *Si f est un polynôme de degré d calculé par un circuit C de portes $\{+,\times\}$ de taille s tel que le degré entrant des portes $\times$ est borné par 2 (on ne met pas de borne sur celui des portes $+$), alors il existe un circuit $\tilde{C}$ de taille $s(d+1)^2$ avec $d+1$ sorties $O_0, O_1, \ldots, O_d$ tel que :*

- *le degré entrant des portes $+$ n'est pas borné,*
- *le degré entrant de chaque porte $\times$ est borné par 2,*
- *pour tout i, la porte O_i calcule la composante homogène de f de degré i,*
- *$\tilde{C}$ est homogène.*

On rappelle le lemme 1.9 montré au chapitre 1.

Lemme (Rappel du lemme 1.9)**.** *Dans un circuit homogène, toutes les portes calculent des polynômes homogènes. De plus le degré de la porte correspond au degré du polynôme homogène calculé par la porte.*

Enfin, nous avons déjà mentionné le fait que les preuves de parallélisation sont presque toujous basées sur la réduction de Valiant, Skyum, Berkowitz et Rackoff [101]. Celle-ci ne déroge pas à la règle. Toutefois, nous aurons besoin d'un résultat légèrement plus fort. En effet leur résultat est complètement global : leur circuit d'arrivée est de profondeur $O(\log d)$. Nous aurons besoin ici, d'un résultat local sur le comportement de chacune des portes de multiplication.

Définition 2.19. *Un circuit C de portes $\{\times, +, \odot\}$ sera dit* équilibré pour les portes $\times$ *si et seulement si toutes les propriétés suivantes sont vérifiées :*

- *le degré entrant de chaque porte $\times$ est au plus 5,*
- *le degré entrant de chaque porte $+$ est non borné,*
- *le degré entrant de chaque porte $\odot$ est au plus 2,*
- *pour chaque porte $\times$ (appelée α), chacune de ses entrées est de degré au plus la moitié du degré de α,*
- *le degré de chaque porte égale le degré du polynôme calculé par la porte (obtenu grâce au lemme 1.9).*

La dernière condition ne peut pas être vraie pour la multiplication par un scalaire. C'est la raison pour laquelle nous avons introduit l'opérateur $\odot$.

La proposition suivante a été trouvée par Agrawal et Vinay [4]. Elle généralise légèrement le célèbre résultat de Valiant, Skyum, Berkowitz et Rackoff [101] en rajoutant une contrainte sur toutes les portes $\times$.

Proposition 2.20. *Soit f un polynôme homogène de degré d calculé par un circuit $\tilde{C}$ de taille s et défini comme dans la conclusion de la proposition 2.18. Alors f est calculé par un circuit $\{\times, +, \odot\}$ homogène équilibré pour les portes $\times$, de taille $s^6 + s^4 + 1$ et de degré d.*

Nous présentons une preuve de ce résultat à la sous-section 3.2 vu que l'énoncé ci-dessus est légèrement différent de ceux que l'on peut trouver dans [4] ou dans [91] (les constantes sont un peu améliorées). En particulier, le circuit obtenu vérifie le résultat classique de VSBR.

Corollaire 2.21 (VSBR)**.** *Soit f un polynôme de degré d calculé par un circuit de taille s. Alors f est calculé par un circuit $\{+, \times\}$ de taille $(sd)^{O(1)}$ et de profondeur $O(\log(d))$ où chaque porte $\times$ est de degré entrant 2 et où le degré entrant des portes $+$ n'est pas borné.*

3.2 Réduction à la VSBR

Nous allons prouver ici la proposition 2.20.

Soit f un polynôme homogène calculé par un circuit $\tilde{C}$ de taille s tel que :

- le degré entrant de chaque porte $+$ est non borné,
- le degré entrant de chaque porte $\times$ est borné par 2,
- $\tilde{C}$ est homogène.

Pour commencer, nous supprimons le "calcul de constantes" (cela signifie que l'on peut supposer que toutes les portes de calculs calculent un polynôme de degré non nul). Pour faire cela, il suffit de remplacer chaque porte calculant un polynôme de degré 0 par une entrée étiquetée par la valeur constante de cette porte. Nous pouvons remarquer que par homogénéité, les entrées constantes ne peuvent être des arguments d'une porte $+$. De plus, pour chaque porte $\times$ dont une entrée est une constante, nous remplaçons l'étiquette de cette porte par l'étiquette $\odot$. Nous remarquons que jusque là, nous n'avons pas augmenté la taille du circuit. Ensuite, nous pouvons réordonner les entrées de chaque porte $\times$ et $\odot$ de façon que pour chacune de ces portes, le degré de l'argument de droite soit plus grand que le degré de l'autre argument. Après ces préparations, nous obtenons alors un circuit C_1 de taille au plus s.

Nous rappellons que la définition des arbres monomiaux (en anglais "parse tree") a été donnée dans l'introduction. Définissons maintenant un nouveau circuit C_2 qui satisfait aux critères de la proposition. Pour chaque paire de portes α et β dans C_1, nous définissons la porte $(\alpha;\beta)$ dans C_2 comme suit (nous verrons dans la suite comment les calculer) :

— Si β est une feuille, alors $[(\alpha;\beta)]$ équivaut à la somme des arbres monomiaux enracinés en α tels que β apparaît dans le chemin le plus à droite (i.e., la feuille du chemin le plus à droite correspond au sommet β).

— Si β n'est pas une feuille, alors $[(\alpha;\beta)]$ equivaut à la somme des arbres monomiaux enracinés en α tels que la porte β apparaît dans le chemin le plus à droite et tels que le sous-arbre au dessus de cette porte β la plus à droite est supprimé. C'est comme si nous remplacions l'occurence la plus à droite de la porte β par l'entrée 1 et que nous calculions $[(\alpha;\beta)]$ avec $\beta = 1$ une feuille.

Notons ici qu'il est facile de récupérer le polynôme calculé par la porte α :

$$\begin{aligned}[\alpha] &= \sum_{T_\alpha \text{ arbre monomial}} \text{valeur}(T_\alpha) \\ &= \sum_{l \text{ feuille de } C_1} \sum_{\substack{T_\alpha \text{ arbre monomial tq la feuille} \\ \text{du chemin le plus à droite de } T_\alpha \\ \text{est une copie de } l}} \text{valeur}(T_\alpha) \\ &= \sum_{l \text{ feuille de } C_1} [(\alpha; l)].\end{aligned}$$

Nous remarquons que le nombre d'arbres monomiaux peut être exponentiel mais que la somme extérieure est toujours de taille polynomiale.

Montrons maintenant comment calculer les portes $(\alpha;\beta)$.

— Si β n'apparait pas dans un chemin le plus à droite d'un arbre monomial enraciné en α, alors $(\alpha;\beta) = 0$.

— Dans le cas où $\alpha = \beta$, si α est une feuille, alors $(\alpha;\beta) = \alpha$ et sinon $(\alpha;\beta) = 1$.

— Autrement α et β sont deux portes différentes et α n'est pas une feuille. Si α est une porte $+$, alors $[(\alpha;\beta)]$ est simplement la somme de tous les $[(\alpha';\beta)]$, où α' est un fils de α.

— Si α est une porte $\odot$, alors un fils est une constante c et l'autre fils est une porte α'. Alors, $(\alpha;\beta)$ est simplement l'opération multiplication par un scalaire $[(\alpha;\beta)] = [(c;c)] \odot [(\alpha';\beta)]$.

— Si α est une porte $\times$. Il y a deux cas.

  — Premier cas : β est une feuille. Alors $\deg(\alpha) > \deg(\beta)$ et $\deg(\beta) \leq 1$. Sur le chemin le plus à droite finissant en β de chaque arbre monomial enraciné en α, il existe exactement une porte $\times$, que l'on notera γ, et son fils droit sur ce chemin γ_r tels que :

$$\deg(\gamma) > \deg(\alpha)/2 \geq \deg(\gamma_r). \tag{2.1}$$

  Remarquons que γ n'est unique que pour un arbre monomial fixé. Réciproquement, on peut remarquer que pour chaque porte γ satisfaisant (2.1), si $[(\alpha;\gamma)]$ et $[(\gamma_r;\beta)]$ ne sont pas les polynômes nuls, alors γ est sur un

chemin le plus à droite allant de α vers β. Alors,

$$[(\alpha;\beta)] = \sum_{\substack{l \text{ feuille de } C_1,\\ \gamma \text{ porte } \times \text{ vérifiant (2.1)}}} [(\alpha;\gamma)][(\gamma_l;l)][(\gamma_r;\beta)].$$

Comme β est une feuille, $\deg(\alpha;\beta) = \deg(\alpha)$. Utilisant (2.1) et le fait que nous avons préalablement réordonné les entrées des portes de multiplication de façon à ce que le degré des fils droits soit au moins aussi grand que celui des fils gauches :

$$\begin{aligned} \deg(\alpha;\gamma) = \deg(\alpha) - \deg(\gamma) &< \deg(\alpha)/2 \\ \deg(\gamma_r;\beta) = \deg(\gamma_r) &\leq \deg(\alpha)/2 \\ \deg(\gamma_l;l) = \deg(\gamma_l) \leq \deg(\gamma_r) &\leq \deg(\alpha)/2. \end{aligned}$$

Par conséquent, $[(\alpha;\beta)]$ est calculé par un circuit de profondeur 2 de taille au plus s^2+1 : une porte $+$, d'arité s^2, où chaque fils est une porte $\times$ de degré entrant 3. Chaque fils de ces portes $\times$ est de degré au plus la moitié du degré de la porte $\times$.

— Second cas : β n'est pas une feuille. Alors il existe, sur le chemin le plus à droite de chaque arbre monomial enraciné en α, une porte $\times$, dénoté γ, et son fils sur ce chemin γ_r tels que :

$$\deg(\gamma) \geq (\deg(\alpha) + \deg(\beta))/2 > \deg(\gamma_r). \tag{2.2}$$

De même par un argument similaire :

$$[(\alpha;\beta)] = \sum_{\substack{l \text{ feuille de } C_1\\ \gamma \text{ porte } \times \text{ vérifiant (2.2)}}} [(\alpha;\gamma)][(\gamma_l;l)][(\gamma_r;\beta)]. \tag{2.3}$$

On utilise alors (2.2) :

$$\begin{aligned} \deg(\alpha;\beta) &= \deg(\alpha) - \deg(\beta) \\ \deg(\alpha;\gamma) = \deg(\alpha) - \deg(\gamma) &\leq (\deg(\alpha) - \deg(\beta))/2 \\ \deg(\gamma_r;\beta) = \deg(\gamma_r) - \deg(\beta) &< (\deg(\alpha) - \deg(\beta))/2. \end{aligned}$$

Le problème est ici que le degré de $(\gamma_l;l)$ pourrait être plus grand que $(\deg(\alpha) - \deg(\beta))/2$. La porte α est une porte $\times$ et son fils gauche est de degré non constant (sinon α serait une porte $\odot$). Donc, $\deg(\alpha;\beta) > \deg(\gamma_l;l)$. Si γ_l est de degré au plus 1 (et donc exactement 1 car γ n'est pas une porte $\odot$), alors $(\alpha;\beta)$ est de degré au moins 2. Le calcul de la porte $(\alpha;\beta)$ par la formule (2.3) marche (i.e., le degré de $(\gamma_l;l)$ est plus petit que la moitié du degré de $(\alpha;\beta)$). Enfin sinon, le degré de γ_l est au moins 2 et au plus $\deg(\alpha;\beta)$. Comme l est une feuille, nous pouvons appliquer le premier cas à la porte γ_l (même si γ_l n'est pas une porte $\times$). Il existe encore sur chaque chemin le plus à droite finissant en l et enracinés en γ_l une porte $\times$, notée μ, et son fils μ_r sur ce chemin tels :

$$\deg(\mu) > \deg(\gamma_l)/2 \geq \deg(\mu_r). \tag{2.4}$$

Alors,

$$[(\gamma_l; l)] = \sum_{\substack{l_2 \text{ feuille de } C_1 \\ \mu \text{ porte } \times \text{ vérifiant (2.4)}}} [(\gamma_l; \mu)][(\mu_l; l_2)][(\mu_r; l)].$$

Ainsi,

$$[(\alpha; \beta)] = \sum_{l,l2,\gamma,\mu} [(\alpha; \gamma)][(\gamma_r; \beta)][(\gamma_l; \mu)][(\mu_l; l_2)][(\mu_r; l)] \tag{2.5}$$

où la somme est prise sur toutes les feuilles l, l_2 de C_1, toutes les portes $\times$, notées γ, vérifiant (2.2) et toutes les portes $\times$, notées μ vérifiant (2.4). Les degrés des portes $(\gamma_l; \mu)$, $(\mu_l; l_2)$ et $(\mu_r; l_1)$ sont bornés par la moitié du degré de γ_l. Donc, $[(\alpha; \beta)]$ est calculé par un circuit de profondeur 2 de taille $s^4 + 1$. Les portes $\times$ sont de degré entrant borné par 5 et le degré de leurs enfants est borné par la moitié de leur degré.

En conclusion, pour chaque couple de portes α et β dans C_1, la porte $(\alpha; \beta)$ est calculée dans C_2 par un sous-circuit de taille au plus $s^4 + 1$. À la fin, nous obtenons un circuit de taille au plus $s^6 + s^2$ qui calcule toutes les portes $(\alpha; \beta)$. Finalement, f est calculé par un circuit de taille $s^6 + s^2 + 1$.

Cela prouve la proposition.

3.3 Réduction à une profondeur bornée constante

Nous allons prouver ici le théorème 2.15.

Pour réaliser la réduction à la profondeur quatre, Koiran [60] commence par transformer le circuit considéré en un programme à branchements équivalent. Ensuite, il parallélise ce programme à branchements, et finalement revient à un circuit. Le problème avec cette stratégie est que la transformation des circuits aux programmes à branchements nécessite une augmentation de la taille de notre objet. Si le circuit est de taille s, le nouveau programme à branchements sera de taille $s^{\log(d)}$. L'approche, ici, est de directement paralléliser le circuit, et d'éviter ainsi l'augmentation de la taille due au passage aux programmes à branchements.

L'idée de la preuve pour paralléliser un circuit à la profondeur 4 est de diviser le circuit en deux parties : les portes de degré moins que $\sqrt{d}$ et les portes de degré plus grand. Un circuit tel que le degré de chacune de ses portes est borné par $\sqrt{d}$ calcule un polynôme de degré $\sqrt{d}$ et peut donc être écrit comme une somme d'au plus $s^{O(\sqrt{d})}$ monômes. Ainsi, si chaque partie de notre circuit calcule des polynômes de degré borné par $\sqrt{d}$, il suffit d'obtenir les circuits de profondeur 2 pour chacune des parties, et de les reconnecter ensemble. La principale difficulté vient du fait qu'il n'est toujours vrai que le sous-circuit obtenu par les portes de degré plus grand que $\sqrt{d}$ est de degré inférieur à $\sqrt{d}$. Par exemple, dans le cas du graphe "peigne" avec $n-1$ portes $\times$ et n variables d'entrée :

$$x_1 \cdot (x_2 \cdot (x_3 \cdot (\ldots)))$$

le degré de la première partie est $\sqrt{n}$, alors que le degré de la seconde est $n - \sqrt{n}$. En fait, nous montrerons que ce problème ne peut pas se présenter si on travaille

avec des circuits équilibrés pour les portes $\times$. Dans ce cas, les deux parties auront un degré borné par $\sqrt{d}$.

Bien que la profondeur quatre soit probablement le cas le plus important de notre réduction, nous allons directement traiter un cas plus général, celui de la profondeur $2p$.

Lemme 2.22. *Soient $p \geq 2$ un entier et f un polynôme homogène n-varié, de degré d et calculé par un circuit de portes $\{\times, +, \odot\}$ noté C, homogène, équilibré pour les portes $\times$ et de taille σ.*

Si $d_1, d_2, \ldots, d_p$ sont p réels strictement positifs tels que $d = d_1 d_2 \ldots d_p$, alors f est calculé par un circuit de profondeur $2p$ de la forme

$$\sum \prod^{[15d_p]} \sum \prod^{[15d_{p-1}]} \cdots \sum \prod^{[15d_2]} \sum \prod^{[d_1]}$$

homogène de taille $\sigma + \sigma\binom{n+d_1}{d_1} + \binom{\sigma+15d_p}{15d_p} + \sigma \sum_{i=2}^{p-1} \binom{\sigma+15d_i}{15d_i}$.

Pour obtenir des expressions plus agréables, nous utiliserons l'approximation suivante, conséquence de la formule de Stirling : (On peut trouver une preuve dans [4])

Lemme 2.23.

$$\binom{k+l}{l} = 2^{O\left(l + l \log \frac{k}{l}\right)}$$

Voyons pour commencer comment le lemme 2.22 implique le théorème 2.15.

Preuve du théorème 2.15. Soit f un polynôme n-varié de degré d calculé par un circuit de taille s. Soit $\tilde{C}$ le circuit homogène obtenu alors pour le polynôme f par la proposition 2.18. Le circuit $\tilde{C}$ est de taille $t = s(d+1)^2$ et calcule tous les polynômes $f_0, \ldots, f_d$ où f_i est la composante homogène de f de degré i. Ainsi, grâce à la proposition 2.20, pour chaque $i \leq d$, il existe un circuit C_1 de portes $\{+, \times, \odot\}$ équilibré pour les portes $\times$ de taille $\sigma = t^6 + t^4 + 1$ calculant f_i. Utilisons maintenant le lemme 2.22 pour le circuit C_1 avec $d_1 = d^{1/p} \frac{\log^{(p-1)/p} \sigma}{\log^{(p-1)/p} n}$ et $d_2 = \ldots = d_p = d^{1/p} \frac{\log^{1/p} n}{\log^{1/p} \sigma}$. Ces valeurs satisfient bien que $d_1 d_2 \ldots d_p = d$. Ainsi, le lemme 2.23 fournit un circuit $\sum \prod^{[O(\alpha)]} \cdots \sum \prod^{[O(\alpha)]} \sum \prod^{[\beta]}$ homogène, de profondeur $2p$ et de taille

$$\sigma + \sigma\binom{n+d_1}{d_1} + \binom{\sigma+15d_p}{15d_p} + \sigma \sum_{i=2}^{p-1} \binom{\sigma+15d_i}{15d_i} = 2^{O(d^{1/p} \log^{(p-1)/p} \sigma \log^{1/p} n)}$$

en choisissant

$$\alpha = d^{1/p} \frac{\log^{1/p} n}{\log^{1/p} \sigma} \text{ et } \beta = d^{1/p} \frac{\log^{(p-1)/p} \sigma}{\log^{(p-1)/p} n}.$$

À la fin, il suffit d'additionner ensemble les différentes composantes homogènes f_i. Comme $\sigma = O(s^6 d^{12})$, cela donne une borne supérieure de $2^{O(d^{1/p} \log^{(p-1)/p}(ds) \log^{1/p} n)}$ pour la taille. □

Il suffit alors de prouver le lemme 2.22 pour achever la preuve.

Preuve du lemme 2.22. Posons $(D_i)_{1\leq i\leq p}$ la suite des produits partiels des (d_i). Plus précisément, pour $i \leq p$, nous posons $D_i = \prod_{j=1}^{i} d_j$. En outre, $D_p = d$. Définissons $C_1, C_2, \ldots, C_p$, p sous-circuits de C, comme suit. C_1 est le sous-circuit de C que nous obtenons en gardant seulement les portes de C de degré $\leq d_1$. Puis pour i entre 2 et p, le circuit C_i est constitué non seulement des portes dont le degré est strictement supérieur à D_{i-1} et inférieur à D_i mais aussi des entrées de ces portes. Ces entrées sont les seules portes qui appartiennent à la fois à plusieurs C_i.

Chaque porte α de C_1 a degré au plus d_1, donc calcule un polynôme de degré au plus d_1. Par homogénéité de C, le polynôme calculé en α est homogène. Par conséquent, α est une somme homogène d'au plus $\binom{n+d_1}{d_1}$ monômes, et ainsi, peut être calculé par un circuit de profondeur deux homogène et de taille $1 + \binom{n+d_1}{d_1} + n$ (le "1" encode la porte $+$, le "n" les portes d'entrées, et le reste tient pour les portes $\times$).

Nous allons montrer que pour $i \geq 2$, le degré de C_i est borné par $15d_i$. Fixons ainsi un tel i.

Soit δ le degré de C_i (défini par rapport aux entrées de C_i). Il existe un monôme m de degré δ dans C_i. Soit T un arbre monomial calculant m.

Remarquons qu'une porte de C_i peut à la fois apparaître dans beaucoup d'arbres monomiaux, mais aussi apparaître plusieurs fois dans un même arbre monomial.

Nous partitionnons l'ensemble des portes $\times$ de T en 3 ensembles :

- $\mathcal{G}_0 = \{\alpha \in T \mid \alpha$ est une porte $\times$ et tous les fils de α sont des feuilles de $T\}$
- $\mathcal{G}_1 = \{\alpha \in T \mid \alpha$ porte $\times$ et exactement un fils de α n'est pas une feuille$\}$
- $\mathcal{G}_2 = \{\alpha \in T \mid \alpha$ porte $\times$ et au moins deux fils de α ne sont pas des feuilles$\}$.

Alors, si nous considérons le sous-arbre S de T où toutes les portes de S sont exactement les portes de T qui n'apparaissent dans aucun des C_j avec $j < i$, alors $\mathcal{G}_0$ correspond exactement aux feuilles de S, $\mathcal{G}_1$ correspond aux sommets internes de degré entrant 1 et $\mathcal{G}_2$ aux sommets internes de degré entrant au moins 2.

La preuve se fait en deux parties. Nous allons commencer par borner supérieurement la taille des ensembles $\mathcal{G}_0$, $\mathcal{G}_1$ et $\mathcal{G}_2$. Puis, nous bornerons le degré de m.

Dans C, d'après le lemme 1.9, le degré de m est au moins la somme des degrés des portes de $\mathcal{G}_0$ (car deux de ces portes ne peuvent pas appartenir à un même chemin). Chacune de ces portes est dans C_i, donc est de degré au moins D_{i-1} dans C. Comme m est de degré au plus D_i dans C, cela signifie que le nombre de portes dans $\mathcal{G}_0$ est au plus $\frac{D_i}{D_{i-1}} = d_i$.

Dans C, nous savons encore grâce au lemme 1.9 que le degré de m est au moins la somme des degrés des feuilles de C_i qui sont directement reliées à une porte de $\mathcal{G}_1$. Pour chaque porte α de $\mathcal{G}_1$, exactement une de ses entrées β est dans C_i, donc de degré au moins D_{i-1} dans C. Par la proposition 2.20, le degré de α est au moins deux fois le degré de β, cela implique que la somme des degrés dans C des fils de α qui sont des feuilles de T est aussi au moins D_{i-1}. Ainsi, le nombre de sommets de $\mathcal{G}_1$ est au plus d_i.

Enfin, dans un arbre, le nombre de feuilles étant plus grand que le nombre de sommets de degré entrant au moins 2, nous pouvons en déduire que dans S :

$$|\mathcal{G}_2| \leq |\mathcal{G}_0| \leq d_i.$$

Dans C_i, le degré du monôme m est le nombre de feuilles non étiquetées par une constante dans l'arbre T. Il suffit de mettre en correspondance chaque feuille

avec la plus proche porte $\times$ qui lui est reliée. Comme dans T, le degré entrant des portes $\times$ est borné par 5, celui des portes $+$ est borné par 1 et chaque porte $\odot$ ne rajoute qu'une entrée constante, nous en déduisons que le nombre de feuilles, non constantes, relié à une même porte $\times$ est au plus 5. D'où le nombre de feuilles dans T est au plus

$$5 \times (|\mathcal{G}_0| + |\mathcal{G}_1| + |\mathcal{G}_2|) \leq 15d_i.$$

Ceci prouve que le degré de C_i est au plus $15d_i$. Le nombre d'entrées de C_i est borné par le nombre de portes de C (qui est σ). Ainsi pour chaque porte α de C_i, il existe un circuit de profondeur 2 de type $\sum\prod$ qui calcule $[\alpha]$, avec pour entrées des portes dans C_j (avec $j < i$) et utilisant $\binom{\sigma+15d_i}{15d_i}$ portes de multiplication.

Posons σ_i le nombre de portes internes dans C_i. En particulier, $\sigma = n + \sum_{i=1}^{p} \sigma_i$. Ainsi, le polynôme f peut être calculé par un circuit homogène

$$\sum \prod^{[15d_p]} \sum \prod^{[15d_{p-1}]} \cdots \sum \prod^{[15d_2]} \sum \prod^{[d_1]}$$

de profondeur $2p$ et de taille

$$\begin{aligned} &1 + \binom{\sigma + 15d_p}{15d_p} + \left[\sum_{i=2}^{p-1} \sigma_i \left(1 + \binom{\sigma + 15d_i}{15d_i}\right)\right] + \sigma_1 + \sigma_1 \binom{n + d_1}{d_1} + n \\ &\leq \sigma + \sigma \binom{n + d_1}{d_1} + \binom{\sigma + 15d_p}{15d_p} + \sigma \sum_{i=2}^{p-1} \binom{\sigma + 15d_i}{15d_i}. \end{aligned}$$

□

4 Bornes supérieures pour circuits non homogènes

Koiran [60] prouve une borne en $2^{\sqrt{d}\log^2(s)}$ pour la réduction des circuits à la profondeur 4. Dans leur article [45], Gupta, Kamath, Kayal et Saptharishi affinent cette borne et obtiennent $2^{O(\sqrt{d \log n \log s \log d})}$. De plus, ils utilisent cette borne pour montrer que :

Proposition 2.24 (Théorème 1.1 dans [45]). *Soit $f(x) \in \mathbb{Q}[x_1, \ldots, x_n]$ un polynôme à n variables, de degré $d = n^{O(1)}$ calculé par un circuit arithmétique de taille s.*

Alors, il peut aussi être calculé par un circuit $\sum\prod\sum$ de taille $2^{O(\sqrt{d \log n \log s \log d})}$ où les coefficients sont des éléments de $\mathbb{Q}$.

En fait leur preuve est divisée en trois parties. Premièrement, ils transforment les ciruits généraux en circuits homogènes de profondeur 4. Puis ils transforment ces circuits de profondeur 4 en circuits de profondeur 5 utilisant seulement des portes d'addition et d'exponentiation. Pour faire cela, ils utilisent la formule de Fisher [30].

Lemme 2.25 (Rappel de la formule de Fischer, lemme 2.5). *Pour tout n, le monôme $x_1 \ldots x_n$ peut être exprimé comme une combinaison linéaire de 2^{n-1} puissances de formes linéaires.*

$$x_1 x_2 \ldots x_n = \frac{1}{2^{n-1} n!} \sum_{r_2, \ldots, r_n \in \{\pm 1\}^{n-1}} \left(x_1 + \sum_{i=2}^{n} r_i x_i\right)^n \cdot (-1)^{p(\mathbf{r})}$$

où $p(\mathbf{r}) = |\{i \mid r_i = -1\}|$.

Ainsi, un produit $\prod_{i=1}^{n} x_i$ *peut être transformé en une somme de puissances de sommes :*

$$\sum_{i=1}^{2^{n-1}} \bigwedge^{[n]} \sum_{j=1}^{n} y_{i,j}$$

où les $y_{i,j}$ *valent* $\pm x_j$.

L'idée d'utiliser la formule de Fisher pour transformer un produit en somme de puissances provient de [45]. D'autres utilisations récentes de cette formule dans le cas de la complexité des circuits arithmétiques peuvent être trouvées dans [45, 55].

Enfin, ils transforment ces derniers circuits en circuits de profondeur 3. L'outil principal ici est l'astuce de dualité de Saxena [89]. Reformulant cette astuce combinée aux lemmes 4.7 à 4.9 de [45], on obtient :

Lemme 2.26. *Soit* f *un polynôme de la forme* $\bigwedge^{[d]} \sum^{[m]} \sum^{[b]}$ *dans* $\mathbb{Q}[\mathbf{X}]$. *Alors* f *peut être écrit de la forme*

$$\sum^{[O(m^2b^2d^4)]} \prod^{[mbd]} (X_{i,j} + C_{i,j})$$

où $X_{i,j}$ *est une coordonnée de* $\mathbf{X}$ *et* $C_{i,j}$ *est une constante dans* $\mathbb{Q}$.

Utiliser le théorème 2.16 au lieu du théorème 4.1 dans leur article améliore la première partie de leur preuve. Cela donne une petite amélioration au théorème 1.1 de [45] :

Corollaire 2.27. *Soit* $f(x) \in \mathbb{Q}[x_1, \ldots, x_n]$ *un polynôme à* n *variables de degré* $d = n^{O(1)}$ *calculé par un circuit arithmétique de taille* s. *Alors il peut aussi être calculé par un circuit* $\sum \prod \sum$ *de taille* $2^{O(\sqrt{d \log n \log s})}$ *où les coefficients sont dans* $\mathbb{Q}$.

En fait, de même que lors de la section précédente, ces résultats se généralisent facilement à toute profondeur bornée.

Théorème 2.28. *Soient* $p \geq 2$ *et* $f(x) \in \mathbb{Q}[x_1, \ldots, x_n]$ *un polynôme à* n *variables de degré* d *calculé par un circuit arithmétique de taille* s. *Alors* f *est calculable par un circuit de profondeur* p *de taille* $2^{O(d^{1/(p-1)} \log ds)}$ *où les coefficients sont dans* $\mathbb{Q}$.

Démonstration. Si $p = 2$, alors il va être suffisant de réécrire ce polynôme comme une somme de monômes. Vu qu'il est de degré au plus d, il a au plus $\binom{n+d}{n}$ monômes, ce qui est plus petit que s^d.

Si p est impair et supérieur à deux. Posons $p = 2q + 1$. Si $q = 1$, il s'agit du cas de la profondeur 3. Réduisons f à un circuit de profondeur $4q$ grâce au théorème 2.16. Nous obtenons C un circuit $\sum \prod^{[O(\alpha)]} \cdots \sum \prod^{[O(\alpha)]} \sum \prod^{[\alpha]}$ de profondeur $4q$ et de taille $t = 2^{O(d^{1/2q} \log(ds))}$ avec $\alpha = d^{1/(2q)}$. Appliquons le lemme 2.25 relatif à la formule de Fischer pour chaque niveau de multiplications pour obtenir un circuit $\sum \bigwedge^{[O(\alpha)]} \cdots \sum \bigwedge^{[O(\alpha)]} \sum \bigwedge^{[\alpha]} \sum$ de profondeur $4q+1$ et de taille au plus t^2. Il y a en fait, intercalés, $2q + 1$ niveaux de portes d'addition et $2q$ niveaux de portes d'exponentiation. Groupons les niveaux d'exponentiation deux par deux, nous obtenons un

circuit de la forme $\sum(\bigwedge\sum\bigwedge)\sum\cdots\sum(\bigwedge\sum\bigwedge)\sum$ avec q parenthèses. Remplaçons finalement ces parenthèses par des sommes de produits de sommes comme dans le lemme 2.26. Nous obtenons un circuit $\sum\prod\cdots\prod\sum$ de profondeur $2q+1$ de taille polynomiale en $t = 2^{O(d^{1/(p-1)}\log(ds))}$ et où les portes de multiplication sont aussi de degré polynomial en t.

Si $p = 2q$ est un entier pair plus grand que trois, nous allons faire la même chose à part que nous n'allons pas toucher au dernier niveau de multiplication. Nous réduisons le circuit à la profondeur $4q-2$. Le circuit est de la forme $\sum\prod\cdots\sum\prod$ avec $2q-1$ niveaux de portes d'addition ainsi que $2q-1$ niveaux de multiplication. Nous allons transformer les $2q-2$ derniers niveaux de multiplications (i.e. du côté de la sortie du circuit) en niveaux d'exponentiation. On obtient un circuit de la forme $\sum\bigwedge\cdots\sum\bigwedge\sum\prod$ avec $2q-2$ niveaux d'exponentiations. De même que pour le cas impair, il suffit alors de grouper les niveaux d'exponentiations par deux et de transformer les $\bigwedge\sum\bigwedge$ en $\sum\prod\sum$ pour obtenir un circuit $\sum\prod\cdots\sum\prod$ de profondeur $2q$ et de taille $2^{O(d^{1/(2q-1)}\log(ds))}$. Ce qui prouve le résultat. □

On peut ainsi découvrir une autre réduction à la profondeur quatre, utilisant des portes intermédiaires calculant de très hauts degrés. Ce résultat met en évidence la nécessité des contraintes d'homogénéité des polynômes ou de bornes sur les degrés entrants des portes de multiplication dans les propositions 2.10, 2.12 et 2.13.

Corollaire 2.29. *Soit $f(\mathbf{x}) \in \mathbb{Q}[x_1,\ldots,x_n]$ un polynôme à n variables de degré d calculé par un circuit arithmétique de taille s. Alors il peut aussi être calculé par un circuit $\sum\prod\sum\prod$ de taille $2^{O(d^{1/3}\log s)}$ où les coefficients sont dans $\mathbb{Q}$.*

Par conséquent les polynômes DET_n et $\mathrm{IMM}_{n,d}$ possèdent des circuits $\sum\prod\sum\prod$ de taille respective $n^{O(\sqrt[3]{n})}$ et $n^{O(\sqrt[3]{d})}$. De plus, si tout circuit de type $\sum\prod\sum\prod$ pour le langage PERM_n nécéssite une taille d'au moins $n^{\omega(\sqrt[3]{n})}$, alors $\mathsf{VP} \neq \mathsf{VNP}$.

Chapitre 3

De l'hypothèse de Valiant aux τ-conjectures

En 1995, Shub et Smale [92] ont trouvé un lien entre la complexité des polynômes univariés à coefficients entiers et la question $\mathsf{P}_{\mathbb{C}}$ vs. $\mathsf{NP}_{\mathbb{C}}$ dans le modèle de Blum-Shub-Smale sur $\mathbb{C}$. Nous ne détaillerons pas ici les classes citées ci-dessus vu que nous ne les utiliserons pas. Le lecteur intéressé pourra se référer par exemple à l'article où elles sont introduites [15] ou à la référence [13].

Pour un polynôme à coefficients entiers $f \in \mathbb{Z}[X_1, \ldots, X_n]$, nous rappellons que la τ-complexité de f notée $\tau(f)$ correspond à la taille du plus petit circuit calculant f, de portes $\{+, \times, -\}$ et utilisant seulement la constante 1. La τ-conjecture, introduite par Shub et Smale [92] est :

Conjecture 3.1 (τ-conjecture)**.** *Il existe une constante universelle $c > 0$ telle que pour tout polynôme univarié $f \in \mathbb{Z}[X]$,*

$$Z_{\mathbb{Z}}(f) \leq (1 + \tau(f))^c$$

où $Z_{\mathbb{Z}}(f)$ correspond au nombre de racines entières distinctes de f.

Shub et Smale ont prouvé dans le même article que cette conjecture impliquait $\mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$. La résolution de la τ-conjecture apparaît sous le titre "Integer zeros of a polynomial of one variable" comme le quatrième problème de la liste de Smale [93] des plus importants problèmes pour les mathématiciens du XXI$^{\text{ème}}$ siècle. Toutefois, cette conjecture reste complètement ouverte.

Une autre implication importante de cette conjecture a été mise en évidence par Bürgisser [21]. Il montre que la τ-conjecture implique aussi que le permanent n'admet pas de circuits arithmétiques sans constantes de taille polynomiale, et donc en particulier que $\mathsf{VP}^0 \neq \mathsf{VNP}^0$.

Un des obstacles aux avancées sur cette conjecture vient du fait que l'on cherche des racines entières. Cependant cette contrainte est nécessaire car la conjecture devient fausse dans le cas des racines réelles. C'est le cas pour les polynômes de Tchebychev. Ces polynômes T_n de degré n sont définis sur l'intervalle $[-1, 1]$ par la relation $T_n(\cos\theta) = \cos(n\theta)$. Le polynôme T_n a n racines réelles simples, mais est calculé par un circuit de taille $O(\log n)$. Un autre exemple de polynômes avec beaucoup de racines réelles a été trouvé plus tôt par Borodin et Cook [18]. Certains rapprochements entre des bornes inférieurs en complexité et des bornes supérieures sur le nombre de racines réelles avaient déjà été trouvés dans [18, 39, 87].

Toutefois, Koiran [61] réussit à renforcer l'hypothèse pour que la borne tienne pour les racines réelles tout en conservant l'implication de $\mathsf{VP}^0 \neq \mathsf{VNP}^0$. Il définit la conjecture suivante :

Conjecture 3.2 (τ-conjecture réelle)**.** *Il existe une constante universelle $c > 0$ telle que pour tous paramètres entiers positifs k, m et t et tout polynôme univarié $f \in \mathbb{Z}[X]$ de la forme*

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}(X)$$

avec $f_{i,j}$ des polynômes t-creux, on a

$$Z_{\mathbb{R}}(f) \leq (1 + k + m + t)^c$$

où $Z_{\mathbb{R}}(f)$ correspond au nombre de racines réelles distinctes de f.

On rappelle que les polynômes t-creux, introduits au chapitre 1 désignent les polynômes ayant au plus t monômes dans leur forme développée.

Koiran montre [61] :

Théorème 3.3. *Si la τ-conjecture réelle est avérée, alors le permanent n'admet pas de circuits arithmétiques sans constantes de taille polynomiale, c'est-à-dire $\tau(\text{PERM}_n) = n^{omega(1)}$.*

Un des arguments en faveur de cette version réelle de la τ-conjecture est sa similarité avec l'estimation de Descartes.

Lemme 3.4 (Estimation de Descartes)**.** *Soit $f = \sum_{i=1}^{t} a_i x^{\alpha_i}$ un polynôme tel que $\alpha_1 < \alpha_2 < \ldots < \alpha_t$ et a_i sont des réels non nuls. Alors le nombre de racines réelles strictement positives de f, compté avec multiplicité, est borné par $t - 1$. De plus, le résultat tient encore dans le cas où les exposants sont réels.*

Cette estimation découle directement d'un résultat classique, la règle des signes de Descartes :

Lemme 3.5 (Règle des signes)**.** *Soit $f = \sum_{i=1}^{t} a_i x^{\alpha_i}$ un polynôme tel que $\alpha_1 < \alpha_2 < \ldots < \alpha_t$ et a_i sont des réels non nuls. Soit N le nombre de changements de signes dans la suite $(a_1, \ldots, a_t)$. Alors le nombre de racines réelles strictement positives de f, compté avec multiplicité, est borné par N.*

En particulier, le cas $k = 1$ de la τ-conjecture réelle est vérifié. Comme chaque $f_{i,j}(X)$ a au plus $2t - 1$ racines réelles, on obtient si $k = 1$:

$$Z_{\mathbb{R}}(f) \leq 2(t-1)m + 1.$$

A contrario, la meilleure borne supérieure connue pour la conjecture 3.2 est $(2kt^m - 1)$. Pour obtenir cette borne, il suffit de développer f en somme de kt^m monômes et d'utiliser encore l'estimation de Descartes.

Dans ce chapitre, nous étudierons premièrement comment obtenir des bornes inférieures à partir d'une variante de la τ-conjecture. Ainsi, nous pourrons alors dériver de nouvelles variantes de cette conjecture impliquant encore des bornes inférieures pour les circuits arithmétiques.

1 Des bornes sur la taille du permanent aux bornes sur le nombre de racines

Nous montrons dans cette section la preuve du théorème 3.3. La raison étant que nous cherchons à comprendre ce transfert de bornes inférieures dans le but d'énoncer d'autres variantes de cette τ-conjecture réelle. Nous allons devoir commencer par présenter quelques outils. La plupart viennent de l'article [21].

1.1 Quelques définitions de classes booléennes

Dans la suite, nous voudrons considérer des polynômes de la classe VNP^0. Or pour trouver de tels polynômes, le critère de Valiant (proposition 3.10) – exposé un peu plus loin – nécessite que les coefficients des polynômes considérés soient calculables dans la classe $\mathsf{GapP/poly}$. Ainsi, nous commençons par exposer ici quelques définitions classiques de classes booléennes. Il va s'agir essentiellement de classes de comptage.

Rappelons la définition des deux classes de comptage $\#\mathsf{P}$ et GapP.

Définition 3.6. *La classe* $\#\mathsf{P}$ *est l'ensemble de fonctions* $f : \{0,1\}^\star \to \mathbb{N}$ *tel qu'il existe un langage* $\mathrm{A} \in \mathsf{P}$ *et un polynôme* $p(n)$ *satisfiant :*

$$f(x) = |\{y \in \{0,1\}^{p(|x|)} \mid (x,y) \in \mathrm{A}\}|.$$

Une fonction $f : \{0,1\}^\star \to \mathbb{Z}$ *est dans* GapP *si elle correspond à une différence de deux fonctions dans* $\#\mathsf{P}$*.*

Définissons maintenant la hiérarchie de comptage. Un lien entre la hiérarchie de comptage et la théorie de la complexité algébrique a été mis en évidence dans [5]. Ce lien a été approfondi dans [21] et [63]. Par exemple, dans [21], Bürgisser montre que les polynômes $\prod_{i=1}^{2^n}(X-i)$ ont des circuits de taille polynomiale s'il en est de même pour la famille du permanent.

La hiérarchie de comptage définie dans [103] est une classe de langages plutôt que de fonctions. Elle est définie à partir de l'opérateur de majorité C comme suit.

Définition 3.7. *Si* K *est une classe de complexité, alors la classe* $C \cdot \mathsf{K}$ *correspond à l'ensemble de langages* A *tels qu'il existe un langage* $\mathrm{B} \in \mathsf{K}$ *et un polynôme* $p(n)$ *satisfiant*

$$x \in \mathrm{A} \Leftrightarrow |\{y \in \{0,1\}^{p(|x|)} \mid (x,y) \in \mathrm{B}\}| \geq 2^{p(|x|)-1}.$$

Le $i^{ème}$ *niveau* $C_i\mathsf{P}$ *de la hiérarchie de comptage est défini récursivement par* $C_0\mathsf{P} = \mathsf{P}$ *et* $C_{i+1}\mathsf{P} = C \cdot C_i\mathsf{P}$*. La hiérarchie de comptage* CH *est l'union de tous les* $\mathsf{C}_i\mathsf{P}$ *pour* $i \geq 0$*.*

Situons la hiérarchie de comptage parmi les autres classes booléennes classiques. Elle contient toute la hiérarchie polynomiale PH et est contenue dans PSPACE (des définitions et beaucoup d'informations sur ces dernières classes peuvent être trouvées dans [7, 37, 79, 82]).

Les classes de circuits arithmétiques que nous considérons sont non uniformes. Par conséquent nous travaillerons en fait avec des versions non uniformes des classes de comptage définies ci-dessus. Nous utilisons la notation standard de Karp et Lipton [54] :

Définition 3.8. *Si* K *est une classe de complexité, la classe* K/poly *est l'ensemble des langages* A *tels qu'il existe un langage* $B \in K$*, un polynôme* $p(n)$ *et une famille* $(a_n)_{n\geq 0}$ *de mots (*les conseils*) satisfiant*

— *pour tout* $n \geq 0$, $|a_n| \leq p(n)$

— *et pour tout mot* x, $x \in A \Leftrightarrow (x, a_{|x|}) \in B$.

Remarquons que les conseils a_n dépendent seulement de la taille de x.

1.2 Les polynômes définissables

Comme mentionné en début de ce chapitre, nous aurons besoin de manipuler ici les classes de la théorie de Valiant. Nous renvoyons le lecteur au premier chapitre pour les définitions des différentes classes de complexité ou au livre de Bürgisser [19].

Dans le prochain lemme, prouvé dans [21], l'auteur montre un premier lien entre la complexité arithmétique et la hiérarchie de comptage.

Lemme 3.9. *Si* PERM_n *est dans* VP^0 *alors* $\mathsf{CH/poly} = \mathsf{P/poly}$.

En particulier, ce lemme a été utilisé dans le même article pour montrer que les sommes et produits exponentiels sont calculables dans la hiérarchie de comptage.

Le résultat suivant a été démontré par Valiant [99]. La formulation provient en fait de l'article de Koiran [62].

Proposition 3.10 (Critère de Valiant)**.** *Supposons que* $n \mapsto p(n)$ *soit une fonction polynomialement bornée et que* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Z}$ *est telle que la fonction* $1^n\#j \mapsto f(j,n)$ *soit dans la classe de complexité* GapP/poly *(où* $1^n\#j$ *correspond à la concaténation du mot "n" écrit en unaire, du caractère* # *et du mot "j" écrit en binaire). Alors la famille* (f_n) *de polynômes multilinéaires définie par*

$$f_n(X_1, \ldots, X_{p(n)}) = \sum_{\mathbf{j}\in\{0,1\}^{p(n)}} f(j,n) X_1^{j_1} \cdots X_{p(n)}^{j_{p(n)}}$$

est dans VNP^0*. L'exposant* j_k *correspond au bit de* j *de poids* 2^{k-1}.

Remarquons que n est codé en unaire alors que j est codé en binaire.

Remarquons aussi que dans la proposition précédente, la classe booléenne utilisée est GapP/poly une classe de fonctions. Or il est souvent plus aisé de travailler avec des langages. C'est pourquoi, nous allons définir maintenant la notion de définissabilité d'un polynôme.

Les paragraphes suivants sont directement tirés de l'article de Koiran et Périfel [63] qui est lui-même basé sur [21].

On va être amené à introduire une notion de complexité des suites d'entiers. Dans le but d'éviter de traiter les signes séparément, nous suivons ce qui est fait dans [63], ie. nous supposons que nous pouvons retrouver le signe dans l'encodage des entiers. Par exemple, le premier bit code le signe et les suivants, la valeur absolue de l'entier considéré.

Définition 3.11. *Une* suite d'entiers de taille exponentielle *est une suite d'entiers* $a(n, \alpha_1, \ldots, \alpha_k)$ *telle qu'il existe deux polynômes* $p(n)$ *et* $q(n)$ *satisfaisant :*

— *le paramètre* k*, dépendant de* n*, vérifie* $k \leq p(n)$*,*

— *$a(n, \alpha_1, \ldots, \alpha_k)$ est défini pour $n, \alpha_1, \ldots, \alpha_k \in \mathbb{N}$ avec $0 \leq \alpha_i < 2^{p(n)}$ pour tout $1 \leq i \leq k$,*
— *pour tout $n \geq 1$ et tous $\alpha_1, \ldots, \alpha_k < 2^{p(n)}$, la taille de l'encodage binaire de $a(n, \alpha_1, \ldots, \alpha_k)$ est inférieure à $2^{q(n)}$.*

On définit à partir de $a(n, \alpha_1, \ldots, \alpha_k)$ le langage suivant :

$$\textsc{Bit}(a) = \{(1^n \# \alpha_1, \ldots, \alpha_k, j) \mid \text{ le } j^{\text{ème}} \text{ bit de } a(n, \boldsymbol{\alpha}) \text{ est } 1\}.$$

Attention, dans la définition analogue de Bürgisser [21], l'entier n est codé en binaire.

Définition 3.12. *Une suite d'entiers $a(n, \boldsymbol{\alpha})$ de taille exponentielle est dite* définissable *dans la classe* K *si le langage* $\textsc{Bit}(a)$ *est dans* K.

Une suite de polynômes $f_n(X_1, \ldots, X_k) = \sum_{\boldsymbol{\alpha}} a(n, \boldsymbol{\alpha}) \mathbf{X}^{\boldsymbol{\alpha}}$ est dite définissable *dans* K *si sa suite de coefficient a est de taille exponentielle et définissable dans* K.

Dans la suite, nous considérerons essentiellement des polynômes définissables dans $\mathsf{P/poly}$ ou dans $\mathsf{CH/poly}$. La seconde classe est assez large et englobe de nombreux polynômes classiques, comme par exemple, le polynôme de Pochhammer-Wilkinson. Le résultat suivant, prouvé dans [21] est très utile pour montrer qu'une suite est dans cette classe.

Théorème 3.13. *Soient $p(n)$ un polynôme et $(a(n, \boldsymbol{\alpha}))_{\alpha_i < 2^{p(n)}}$ une suite définissable dans* $\mathsf{CH/poly}$. *Considérons les suites*

$$b(n) = \sum_{\boldsymbol{\alpha}} a(n, \boldsymbol{\alpha}) \text{ et } d(n) = \prod_{\boldsymbol{\alpha}} a(n, \boldsymbol{\alpha}).$$

Alors $(b(n))$ et $(d(n))$ sont définissables dans $\mathsf{CH/poly}$.

Supposons que $(s(n))$ et $(t(n))$ soient définissables dans $\mathsf{CH/poly}$. *Alors la suite des produits $(s(n)t(n))$, ainsi que si $t(n) > 0$ la suite des quotients $\lceil s(n)/t(n) \rceil$, sont définissables dans* $\mathsf{CH/poly}$.

En fait, comme mentionné précédemment, Bürgisser utilise une notation binaire pour n. Le résultat précédent est une simple "mise à l'échelle" du résultat qui peut être trouvé dans [21] (poser $a'(2^{p(n)}, \boldsymbol{\alpha}) = a(n, \boldsymbol{\alpha})$).

Dans [63], les auteurs définissent une autre caractérisation des polynômes :

Définition 3.14. *Soit $(f_n(X_1, \ldots, X_k))$ une famille de polynômes à coefficients entiers. Nous disons que (f_n) peut être évaluée dans* K *aux points entiers si les conditions suivantes sont vérifiées pour un certain polynôme p :*

— *le paramètre k est polynomialement borné en n,*
— *le degré de f_n ainsi que la taille binaire de ses coefficients sont bornés par $2^{p(n)}$,*
— *le langage*

$$\{(1^n \# i_1, \ldots, i_k, j) \mid 0 \leq i_1, \ldots, i_k \leq 2^{p(n)} \text{ et le } j^{\text{ème}} \text{ bit de } f_n(i_1, \ldots, i_k) \text{ est } 1\}$$

est dans K, *où les entiers $i_1, \ldots, i_k, j$ sont donnés en binaire.*

Le résultat suivant est énoncé (et prouvé) dans le théorème principal (Theorem 3.5) de [63] :

Théorème 3.15. *Si (f_n) est une suite de polynômes qui peut être évaluée dans* CH/poly *aux points entiers, alors (f_n) est définissable dans* CH/poly.

Nous avons tous les résultats pour montrer, par exemple, que la suite des polynômes $U_n(X,Y) = \prod_{i=1}^{2^n}(X^i + Y)$ est définissable dans CH/poly.

Les suites $s_1(n,x,y,i,j) = y$ et $s_2(n,x,y,i,j) = (\sigma_{i,j})_{1\leq x,y,i,j\leq 2^n}$ où

$$\sigma_{i,j} = \begin{cases} x \text{ si } j \leq i \\ 1 \text{ sinon,} \end{cases}$$

sont par définition définissables dans CH/poly. Par le théorème 3.13, c'est aussi le cas pour la suite

$$t(n,x,y,i) = (x^i + y)_{1\leq x,y,i\leq 2^n} = \left(y + \prod_{j=1}^{2^n} \sigma_{i,j}\right),$$

ainsi que pour la suite

$$u(n,x,y) = \left(\prod_{i=1}^{2^n}(x^i + y)\right)_{1\leq x,y\leq 2^n}.$$

Donc $U_n(X,Y)$ peut être évalué dans CH/poly aux points entiers, ce qui par le théorème 3.15, montre que les polynômes U_n sont définissables dans CH/poly.

La même preuve marche pour les autres polynômes suivants :

Lemme 3.16. *Les polynômes suivants*

$$\mathrm{PW}_n(X) = \prod_{i=1}^{2^n}(X - i),\ \mathrm{PW}_n^-(X) = \prod_{i=1}^{2^n}(X + i),\ T_n(X) = \prod_{i=1}^{2^n}(X - 1),$$

$$\text{et } U_n(X,Y) = \prod_{i=1}^{2^n}(X^i + Y)$$

sont tous définissables dans CH/poly.

Le cas des polynômes de Pochhammer-Wilkinson (PW_n) était déjà établi dans l'article de Bürgisser [21]. Il prouve même que ces polynômes sont en fait définissables dans CH.

1.3 Preuve du théorème 3.3

Dans la suite de ce chapitre, nous utiliserons le résultat de complétude du permanent (théorème 1.26). C'est pourquoi, nous fixons un corps $\mathbb{K}$ de caractéristique nulle dans lequel travailler. Les circuits utiliseront comme constantes les éléments de $\mathbb{K}$. En particulier, les résultats sont souvent utilisés et cités dans le cas où $\mathbb{K} = \mathbb{Q}$.

Nous allons prouver dans cette sous-section le théorème 3.3 mentionné en début de ce chapitre. L'idée de la preuve est similaire à celle que l'on peut trouver dans l'article original [61] sauf que le découpage de la preuve est différent. En fait, nous avons voulu extraire ici la proposition 3.17 implicite dans la preuve originale, pour

pouvoir dans la suite, obtenir des variantes du théorème 3.3. Cette sous-section correspond donc aux lemme 3, théorèmes 6 et 7 et proposition 2 de l'article [61], bien que le découpage ainsi que les notations aient changés.

Nous voulons extraire la proposition suivante :

Proposition 3.17. *Soit p un polynôme et soit (f_n) une suite de polynômes entiers de $\mathbb{Z}[X_1, \ldots, X_{p(n)}]$ définissables dans* P/poly*, de degré maximal en chaque variable $2^d - 1$ et tels que la valeur absolue des coefficients soit bornée par $2^{2^r} - 1$ avec $r, d = n^{O(1)}$.*

Si PERM_n est calculé par une suite de circuits C_n, alors il existe un polynôme q et une projection D_n du circuit $C_{q(n)}$ tel que f_n peut être calculé par un circuit $D_n(Y_1, \ldots, Y_k)$ où les Y_i sont des puissances de X_{j_i} d'exposants au plus 2^{d-1} et où k est un entier tel que $k \leq dp(n) + r$. De plus, les circuits D_n calculent des polynômes homogènes en les Y_k.

Enfin, le polynôme q ne dépend que du choix de la famille de polynômes (f_n).

Un corollaire immédiat dans le cas où les C_n sont des circuits de taille polynomialement bornée est le suivant :

Corollaire 3.18. *Soit p et f_n définis comme dans la proposition 3.17. Si PERM_n admet une suite (C_n) de circuits de taille polynomiale, alors c'est aussi le cas pour f_n.*

Preuve du corollaire 3.18. D'après la proposition 3.17, f_n est calculé par un circuit $D_n(Y_1, \ldots, Y_k)$ où les $Y_j = X_{i_j}^{\alpha_j}$ pour des valeurs $1 \leq i_j \leq p(n)$ et $1 \leq \alpha_j \leq 2^{d-1}$ et où le circuit D_n est la projection d'un circuit $C_{q(n)}$ pour un polynôme q. Donc (D_n) est une suite de circuits de taille polynomiale. De plus, les puissances $X_{i_j}^{\alpha_j}$ avec $\alpha_j \leq 2^{d-1}$ peuvent être calculées par exponentiation rapide par des circuits de taille au plus $2d = n^{O(1)}$. On obtient ainsi, en rebranchant les circuits, un circuit de taille polynomiale pour la famille (f_n). □

La preuve de la proposition 3.17 est similaire à celle que l'on peut trouver dans l'article de Koiran [61]. Le fait que le nombre de variables soit $p(n)$ et non 1 n'introduit aucune complication.

Preuve de la proposition 3.17. Nous travaillerons à n fixé. Posons de plus $p = p(n)$. Commençons par exprimer le polynôme f_n sous sa forme développée (somme d'au plus 2^{dp} monômes) :

$$f_n(X_1, \ldots, X_p) = \sum_{\alpha_1, \ldots, \alpha_p} a(n, \alpha_1, \ldots, \alpha_p) X_1^{\alpha_1} \cdots X_p^{\alpha_p}.$$

Alors développons les coefficients entiers $a(n, \boldsymbol{\alpha})$ en base 2 :

$$a(n, \boldsymbol{\alpha}) = \sum_{i=0}^{2^r - 1} a_i(n, \boldsymbol{\alpha}) 2^i$$

où $a_i(n, \boldsymbol{\alpha}) \in \{0, 1\}$. Grâce à ces deux développements, nous obtenons

$$f_n(\mathbf{X}) = \sum_{i, \boldsymbol{\alpha}} a_i(n, \boldsymbol{\alpha}) 2^i \mathbf{X}^{\boldsymbol{\alpha}}.$$

Ce qui mène à l'égalité

$$f_n(\mathbf{X}) = h_n(X_1^{2^0}, X_1^{2^1}, \ldots, X_1^{2^{d-1}}, X_2^{2^0}, \ldots, X_p^{2^{d-1}}, 2^{2^0}, 2^{2^1}, \ldots, 2^{2^{r-1}}) \tag{3.1}$$

où $h_n(x_{1,0}, x_{1,1}, \ldots, x_{1,d-1}, x_{2,0}, \ldots, x_{p,d-1}, z_0, z_1, z_2, \ldots, z_{r-1})$ est le polynôme multilinéaire

$$\sum_{i,\boldsymbol{\alpha}} a_i(n, \boldsymbol{\alpha}) x_{1,0}^{\alpha_{1,0}} x_{1,1}^{\alpha_{1,1}} \ldots x_{1,d-1}^{\alpha_{1,d-1}} x_{2,0}^{\alpha_{2,0}} \ldots x_{p,d-1}^{\alpha_{p,d-1}} z_0^{i_0} z_1^{i_1} z_2^{i_2} \ldots z_{r-1}^{i_{r-1}}.$$

Ici les exposants $i_j, \alpha_{h,j}$ correspondent aux bits des entiers $i, (\alpha_h)_{1 \leq h \leq p}$. Remarquons que h_n est un polynôme multilinéaire en $(dp + r) = n^{O(1)}$ variables. La fonction $\phi : 1^n \# \boldsymbol{\alpha}, i \mapsto a_i(n, \boldsymbol{\alpha})$ est une fonction à valeurs dans $\{0,1\}^\star$ qui est la fonction indicatrice du langage $\textsc{Bit}(a)$. Par hypothèse, ce langage est dans $\mathsf{P/poly}$, donc $\phi \in \mathsf{GapP/poly}$. Par le critère de Valiant [19] (proposition 3.10), cela implique que la famille polynomiale (h_n) appartient à la classe de complexité VNP^0. Comme la famille du permanent est VNP-complète et est calculée par les circuits (C_n), il existe un polynôme q tel que pour tout n, la fonction h_n est calculée par D_n une projection de $C_{q(n)}$. Il suffit alors de brancher en entrée les constantes et les puissances de variables correspondantes pour obtenir un circuit pour f_n du type $D_n(Y_1, \ldots, Y_k)$. □

Remarque 3.19. *Nous pouvons noter que nous n'utilisons pas réellement dans la preuve le fait que les polynômes soient définissables dans* $\mathsf{P/poly}$. *Nous avons seulement besoin que la fonction indicatrice du langage* $\textsc{Bit}(a)$ *soit dans* $\mathsf{GapP/poly}$.

Remarque 3.20. *Notons aussi que nous autorisons les constantes du corps* $\mathbb{K}$ *pour* f_n *comme pour le permanent. Toutefois, il est possible d'obtenir un résultat plus fin pour les constantes. Remarquons que le seul moment où des nouvelles constantes peuvent apparaître est lors de l'utilisation de la* VNP*-complétude du permanent. En particulier, en utilisant la proposition 1.27 du chapitre 1, on peut aussi obtenir un circuit utilisant juste les constantes de* (C_n) *mais calculant* $2^{q(n)} f_n$ *pour un certain polynôme* q.

L'idée de Koiran est alors d'appliquer les résultats de réduction à la profondeur 4 aux circuits D_n.

Proposition 3.21. *Soit* c *un entier strictement positif fixé et soit* (f_n) *une suite de polynômes dans* $\mathbb{Z}[X_1, \ldots, X_c]$ *définissables dans* $\mathsf{P/poly}$, *de degré maximal en chaque variable* $2^d - 1$ *et tels que la valeur absolue des coefficients soit bornée par* $2^{2^r - 1}$ *avec* $r \leq d = n^{O(1)}$.

Si $\textsc{Perm}_n$ *admet une suite de circuits* C_n *de taille* $n^{O(1)}$, *alors* (f_n) *est calculé par des circuits*

$$\sum_{i=1}^{n^{O(\sqrt{d})}} \prod_{j=1}^{O(\sqrt{d})} f_{i,j}(X_1, \ldots, X_c)$$

où les $f_{i,j}$ *sont des polynômes* $n^{O(\sqrt{d})}$*-creux.*

Démonstration. D'après la proposition 3.17, la famille de polynômes (f_n) est calculée par des circuits de type $D_n(Y_1, \ldots, Y_k)$ où D_n de taille $n^{O(1)}$, calcule un polynôme h_n multivarié d'au plus $(c+1)d = O(d)$ variables. D'après le théorème 2.16, il suit que les polynômes h_n sont calculables par des circuits de profondeur 4 de taille $2^{O(\sqrt{d}\log n)}$ avec des portes de multiplication de degré entrant $O(\sqrt{d})$. D'où (f_n) est calculé par des circuits

$$\sum^{[n^{O(\sqrt{d})}]} \prod^{[O(\sqrt{d})]} \sum^{[n^{O(\sqrt{d})}]} \prod^{[2^d\sqrt{d}]},$$

ie. par des circuits

$$\sum_{i=1}^{n^{O(\sqrt{d})}} \prod_{j=1}^{O(\sqrt{d})} f_{i,j}(X_1, \ldots, X_c)$$

où les $f_{i,j}$ sont des polynômes $n^{O(\sqrt{d})}$-creux. □

On a tout ce qu'il faut pour prouver le théorème 3.3 énoncé au début du chapitre : la τ-conjecture réelle (conjecture 3.2) implique que le permanent n'admet pas de circuits sans constantes de taille polynomiale.

Preuve du théorème 3.3. Montrons ce résultat par l'absurde.

Supposons que le permanent est calculé par des circuits sans constantes de taille polynomiale, ie. $\text{PERM}_n \in \mathsf{VP}^0$. D'après le lemme 3.9, on a $\mathsf{CH/poly} = \mathsf{P/poly}$. Donc d'après le lemme 3.16, le polynôme univarié $\text{PW}(X) = \prod_{i=1}^{2^n}(X - i)$ est définissable dans $\mathsf{P/poly}$. Par la proposition 3.21, PW est calculé par des circuits

$$\sum_{i=1}^{n^{O(\sqrt{n})}} \prod_{j=1}^{O(\sqrt{n})} f_{i,j}(X)$$

où les $f_{i,j}$ sont des polynômes $n^{O\sqrt{n})}$-creux. La conjecture 3.2 implique qu'il existe une constante c telle que $Z_{\mathbb{R}}(\text{PW}) \leq (1 + n^{O(\sqrt{n})})^c = 2^{O(\sqrt{n}\log(n))}$. Ce qui contredit le fait que $Z_{\mathbb{R}}(\text{PW}) = 2^n$. □

Remarque 3.22. *Notons qu'avec la conditon légèrement plus faible* $\text{PERM}_n \in \mathsf{VP}$*, l'effondrement de la hiérarchie de comptage n'est connu qu'en supposant l'hypothèse de Riemann généralisée [20]. Nous verrons plus loin (théorème 3.38) comment l'éviter pour la* τ*-conjecture réelle.*

2 Variations

2.1 Raffinement de la τ-conjecture réelle

Nous pouvons déjà remarquer dans la preuve précédente (preuve du théorème 3.3) que nous avons un peu de marge sur le paramètre m. Plus précisément, en utilisant la conjecture 3.23 suivante, au lieu de la conjecture 3.2, on a encore l'inégalité $Z_{\mathbb{R}}(\text{PW}) \leq (1 + n^{O(\sqrt{n})})^c = 2^{O(\sqrt{n}\log(n))}$.

Conjecture 3.23 (τ-conjecture réelle)**.** *Il existe un polynôme p tel que si $f(x) \in \mathbb{R}[x]$ est un polynôme de la forme $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}(x)$ où les polynômes $f_{i,j}$ sont des polynômes t-creux, alors le nombre de racines réelles distinctes de f est au plus $p(kt2^m)$.*

Nous pouvons au passage noter que la borne supérieure ici ne semble plus très loin de la borne kt^m que nous avons obtenue en développant le polynôme.

Une autre idée pour renforcer cette conjecture est d'utiliser, comme au chapitre 2 la formule de Fisher (lemme 2.5) pour remplacer les produits par des puissances.

Conjecture 3.24 (τ-conjecture réelle avec puissances)**.** *Il existe un polynôme p tel que si $f(x) \in \mathbb{R}[x]$ est un polynôme de la forme $\sum_{i=1}^{k} f_i^{\alpha_i}(x)$ où les polynômes f_i sont des polynômes t-creux et les puissances α_i sont des entiers tels que $0 \leq \alpha_i \leq m$, alors le nombre de racines réelles distinctes de f est au plus $p(kt2^m)$.*

Ainsi,

Théorème 3.25. *Si la τ-conjecture réelle avec puissances est avérée, alors le permanent n'admet pas de circuits arithmétiques sans constantes de taille polynomiale, c'est-à-dire $\tau(\text{PERM}_n) = n^{\omega(1)}$.*

En fait, pour montrer ce théorème, il est suffisant de montrer que la conjecture 3.24 implique la conjecture 3.23.

Lemme 3.26. *Les conjectures 3.23 et 3.24 sont équivalentes.*

Démonstration. La conjecture 3.23 implique directement la conjecture 3.24. Réciproquement choisissons un polynôme p qui vérifie la conjecture 3.24. Soit f un polynôme de la forme $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}(x)$ où les polynômes $f_{i,j}$ sont des polynômes t-creux. Alors d'après la formule de Fisher, f peut être écrit de la forme

$$\sum_{i=1}^{k} \sum_{j=1}^{2^{m-1}} \left(\sum_{l=1}^{m} \tilde{f}_{i,j,l} \right)^m$$

où les $\tilde{f}_{i,j,l}$ sont des polynômes t-creux. Par hypothèse, $Z_{\mathbb{R}}(f) \leq p(k2^m 2^m mt) = (kt2^m)^{O(1)}$. Ce qui prouve le lemme. □

2.2 Différentes τ-conjectures

Nous donnons dans la suite différentes variantes de la τ-conjecture réelle.

Version adélique

La pemière remarque est que nous bornons le nombre de racines réelles alors que les racines du polynôme de Pochhammer-Wilkinson sont en fait entières. En particulier, ils suffit de borner le nombre de racines sur un ensemble qui étend $\mathbb{N}$. L'idée de la τ-conjecture réelle est de pouvoir utiliser le fait que $\mathbb{R}$ soit complet. Toutefois, $\mathbb{R}$ n'est pas la seule complétion de $\mathbb{Q}$. Ainsi, Kaitlyn Phillipson et Maurice Rojas [83] ont introduit la τ-conjecture adélique (par rapport à la version de [83], nous lui faisons bénéficier ici des améliorations de la sous-section 2.1).

Conjecture 3.27 (τ-conjecture adélique avec puissances)**.** *Soit $\mathbb{L}$ un des corps de $\{\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots\}$ où p est premier est $\mathbb{Q}_p$ est le corps des nombres p-adiques. Il existe un polynôme p tel que pour tout polynôme $f(x) \in \mathbb{R}[x]$ univarié, si f est de la forme $\sum_{i=1}^{k} \bigwedge_{j=1}^{m} f_{i,j}(x)$ où les polynômes $f_{i,j}$ sont des polynômes t-creux, alors le nombre de racines distinctes de f dans $\mathbb{L}$ est au plus $p(kt2^m)$.*

Version monotone

Une autre remarque simple est que l'on aurait pu tout aussi bien utiliser dans les preuves le polynôme $\mathrm{PW}_n^- = \prod_{i=1}^{2^n}(X+i)$ au lieu du polynôme PW_n. En particulier les conjectures peuvent être reformulées dans le cas où on ne considère que des polynômes dont tous les coefficients sont positifs. On appellera de tels polynômes des *polynômes à coefficients positifs*. On propose alors la conjecture :

Conjecture 3.28. *Les propriétés suivantes sont vérifiées :*

- *Il existe un polynôme p tel que si $f(x) \in \mathbb{R}[x]$ est un polynôme de la forme $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}(x)$ où les polynômes $f_{i,j}$ sont des polynômes t-creux à coefficients positifs, alors le nombre de racines réelles distinctes de f est au plus $p(kt2^m)$.*
- *Il existe un polynôme p tel que si $f(x) \in \mathbb{R}[x]$ est un polynôme de la forme $\sum_{i=1}^{k} f_i^{\alpha_i}(x)$ où les polynômes f_i sont des polynômes t-creux à coefficients positifs et les puissances α_i sont des entiers tels que $0 \leq \alpha_i \leq m$, alors le nombre de racines réelles distinctes de f est au plus $p(kt2^m)$.*

On remarque que les deux énoncés sont en fait équivalents et que cela peut être prouvé de la même manière que pour le lemme 3.26. On montrera au chapitre 4 que cette version de la conjecture est en faite équivalente aux conjectures 3.23 et 3.24.

Version avec multiplicités

La τ-conjecture réelle s'appuie sur l'idée qu'une somme de produits de polynômes creux ne pourrait pas avoir un nombre exponentiel de racines distinctes. Nous pouvons cependant imaginer d'autres caractéristiques. Par exemple, considérons la multiplicité des racines non nulles au lieu du nombre de racines. La conjecture suivante a été introduite dans [48].

Conjecture 3.29. *Il existe un polynôme p tel que pour tout polynôme $f(x) \in \mathbb{R}[x]$ univarié, si f est de la forme $\sum_{i=1}^{k} \bigwedge^{m} f_i(x)$ où les polynômes f_i sont des polynômes t-creux, alors pour toute racine complexe non nulle r de f, la multiplicité de r est bornée par $p(kt2^m)$.*

La preuve que cette conjecture implique que $\textsc{Perm}_n \notin \mathsf{VP}^0$ est similaire à celle de la conjecture 3.24 mais en remplaçant les polynômes PW_n par les polynômes T_n du lemme 3.16.

Version combinatoire

Nous pouvons même définir une version combinatoire de cette conjecture.

Nous introduisons ici la notion de polygone de Newton. Plus d'informations sur le sujet pourront par exemple être trouvées dans l'article de synthèse de Sturmfels [96].

Les polytopes de Newton sont une façon géométrique de représenter la structure d'un polynôme. Par structure, il faut comprendre qu'ici seul l'ensemble des monômes présents (ie. où le coefficients correspondant est non nul) sera considéré et qu'on ne se préoccupera pas des valeurs prises par les coefficients. En particulier, les polynômes DET_n et PERM_n correspondent au même polytope.

Vis à vis des polytopes de Newton, on s'intéressera dans la suite seulement au cas particulier où les polynômes sont bivariés. On parle alors de polygone de Newton. Nous allons ainsi définir nos objets dans ce cadre là, bien que la plupart des définitions pourraient, sans difficultés, être généralisées à "n" variables.

Si E est un ensemble du plan $\mathbb{R}^2$, cet ensemble est appelé *convexe*, si pour tout couple de points (a, b) de E^2, le segment réel $[a, b]$ est inclus dans E. Si C est un ensemble convexe, un point e de C est dit *extrémal* s'il n'appartient à aucun segment strict $]a, b[$ inclus dans C. Si P est un ensemble de points du plan, l'*enveloppe convexe* est définie comme le plus petit ensemble convexe (au sens de l'inclusion) contenant P. On la notera $\text{conv}(P)$. Les polygones sont les enveloppes convexes des ensembles finis de points, en particulier, ils sont convexes et exactement cactérisés par l'ensemble de leurs points extrémaux. Enfin, si E et F sont deux sous-ensembles du plan euclidien, la *somme de Minkowski* de E et de F désigne l'ensemble

$$\{p + q \in \mathbb{R}^2 \mid p \in E \wedge q \in F\}.$$

Considérons un polynôme bivarié $f \in \mathbb{A}[X, Y]$ où $\mathbb{A}$ est un anneau. À chacun des monômes $X^i Y^j$ apparaissant dans f avec un coefficient non nul, nous pouvons lui associer le point de coordonnées (i, j) du plan euclidien. Nous noterons $\text{Mon}(f)$ cet ensemble fini de points. Par définition, *le polytope de Newton* de f, noté $\text{Newt}(f)$, est l'enveloppe convexe de $\text{Mon}(f)$ (en particulier, $\text{Newt}(f) = \text{conv}(\text{Mon}(f))$). Remarquons que $\text{Newt}(f)$ a au plus t points extrémaux si f a t monômes, et donc au plus t arêtes. En 1921, Ostrowski a montré [78] que le polygone de Newton d'un produit de polynômes est la somme de Minkowski de leurs polygones de Newton (une preuve simple peut être trouvée dans [33], lemme 2.1) :

Proposition 3.30 (Ostrowski)**.**

$$\text{Newt}(fg) = \text{Newt}(f) + \text{Newt}(g) = \{p + q \mid p \in \text{Newt}(f), q \in \text{Newt}(g)\}.$$

Il en résulte que si f a s monômes et g a t monômes, alors $\text{Newt}(fg)$ a au plus $s + t$ arêtes. Plus généralement, pour un produit $f = g_1 g_2 \dots g_m$, $\text{Newt}(f)$ a au plus $\sum_{i=1}^{m} t_i$ arêtes où t_i est le nombre de monômes de g_i ; mais f peut bien sûr avoir jusqu'à $\prod_{i=1}^{m} t_i$ monômes. Le nombre d'arêtes d'un polygone de Newton est donc facilement controlable dans le cas d'un produit de polynômes. En comparaison, la situation n'est plus du tout claire pour une somme de produits. Nous proposons dans l'article [66] la conjecture suivante.

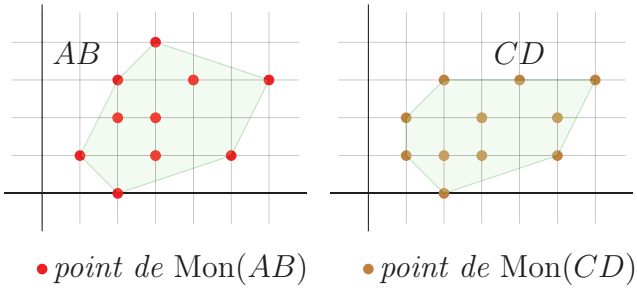
Conjecture 3.31. *Soit p un polynôme, si f est un polynôme de la forme*

$$f(X, Y) = \sum_{i=1}^{k} a_i f_i(X, Y)^m \tag{3.2}$$

où $a_i \in C$ et les f_i ont au plus t monômes, alors le nombre d'arêtes de $\text{Newt}(f)$ est borné supérieurement par $p(kt2^m)$.

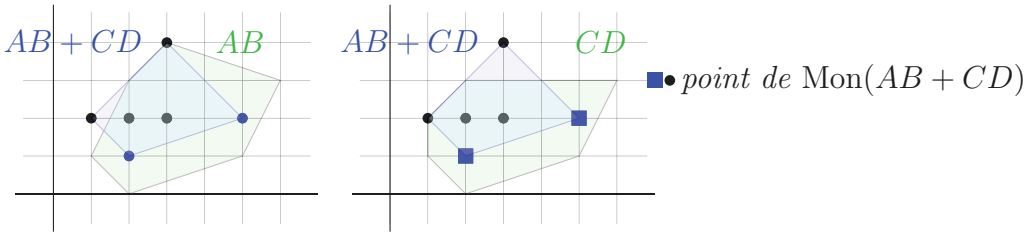
En développant les produits dans (3.2) nous observons que f a au plus kt^m monômes, et ceci est une borne supérieure sur le nombre d'arêtes de son polygone de Newton. Dans le but d'améliorer cette borne si grossière, la principale difficulté que l'on rencontre vient du fait que la somme de taille k dans la définition de f peut créer des annulations de monômes. Ainsi, il se peut que certains sommets de $\mathrm{Newt}(f)$ ne correspondent à aucun des sommets des polygones de Newton des produits $\prod_{j=1}^{m} f_{i,j}(X,Y)$ pour $1 \leq j \leq k$. Nous donnons deux exemples de telles annulations ci-dessous. Nous pouvons remarquer que contrairement aux versions considérant le nombre de racines réelles (conjecture 3.28), la question ici devient très simple si tous les coefficients sont positifs. S'il n'y a pas d'annulations (par exemple, si les $f_{i,j}$ ont seulement des coefficients positifs) alors nous avons effectivement une borne supérieure polynomiale. Dans ce cas, $\mathrm{Newt}(f)$ est l'enveloppe convexe de l'union des polygones de Newton des k produits. Chacun de ces k polygones de Newton a au plus mt sommets, donc $\mathrm{Newt}(f)$ a au plus kmt sommets et autant d'arêtes.

Exemple 3.32. *Considérons les polynômes* $A(X,Y) = XY + X^2 + X^2Y^2 + X^3Y + X^5Y$, $B(X,Y) = 1 + XY^2$, $C(X,Y) = -X - XY - X^2Y^2$ *et* $D(X,Y) = Y + X + X^2Y + X^4Y$.



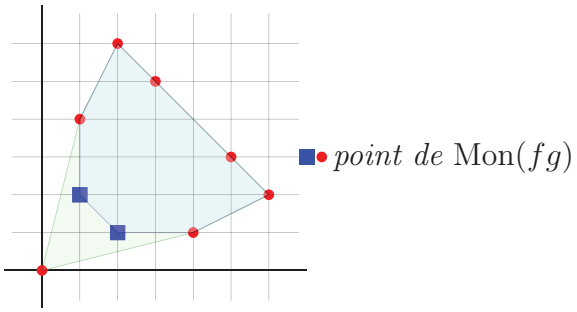
Alors,

$$\begin{aligned} AB + CD =& (XY + X^2 + X^2Y^2 + X^3Y + X^5Y + X^2Y^3 + X^3Y^2 + X^3Y^4 \\ &+ X^4Y^3 + X^6Y^3) - (XY + X^2 + X^3Y + X^5Y + XY^2 \\ &+ X^2Y + 2X^3Y^2 + X^5Y^2 + X^2Y^3 + X^4Y^3 + X^6Y^3) \\ =& X^2Y^2 + X^3Y^4 - XY^2 - X^2Y - X^3Y^2 - X^5Y^2 \end{aligned}$$



Les deux points bleus ("rectangles") apparaissent dans l'enveloppe convexe de $\mathrm{Mon}(AB+CD)$*, mais ni dans celle de* $\mathrm{Mon}(AB)$*, ni dans celle de* $\mathrm{Mon}(CD)$.

Exemple 3.33. *Posons* $f(X,Y) = 1 + X^2Y + Y^2X$, $g(X,Y) = 1 + X^4Y + XY^4$ *et considérons* $\mathrm{Mon}(fg-1)$.



Les deux points bleus ("rectangles") font partie de l'enveloppe convexe de $\mathrm{Mon}(fg-1)$*, mais pas de l'enveloppe de* $\mathrm{Mon}(fg)$*.*

Nous montrons dans [66] que la conjecture 3.31 implique que le permanent est difficile pour les circuits arithmétiques. C'est ce que nous allons voir maintenant.

Considérons le polynôme

$$U_n = \prod_{i=1}^{2^n} (X + Y^i). \tag{3.3}$$

défini au lemme 3.16.

Le polygone de Newton de U_n a exactement 2^{n+1} arêtes : chaque facteur $X + Y^i$ contribue pour une arête de longueur horizontale 1 et de pente $-i$. Pour $1 \leq i \leq 2^n$, notons E_i l'arête (définie à translation près) qui relie les points (X, Y) et $(X+1, Y-i)$. Alors nous pouvons dessiner le polygone de Newton de U_n :

— les points $P = (0, \sum_{i=1}^{2^n} i)$ et $Q = (2^n, 0)$ sont deux points extrémaux,

— l'enveloppe convexe inférieure, allant de P à Q, correspond à la suite ordonnée d'arêtes : $E_{2^n}, E_{2^n-1}, \ldots, E_1$.

— L'enveloppe convexe supérieure, allant aussi de P à Q, correspond à la suite : $E_1, E_2, \ldots, E_{2^n}$.

Chaque arête (qui rappellons-le est définie à translation près) apparait deux fois sur le pourtour de $\mathrm{Newt}(U_n)$, une fois sur l'enveloppe inférieure et une fois sur l'enveloppe supérieure.

Nous obtenons alors le résultat suivant :

Théorème 3.34. *Si la conjecture 3.31 est avérée, alors le permanent n'est pas calculable par des circuits sans constantes et de taille polynomiale.*

Démonstration. Supposons encore que $\tau(\mathrm{PERM}_n) = n^{O(1)}$. De manière similaire à la preuve du théorème 3.25, mais en utilisant les polynômes $U_n(X, Y) = \prod_{i=1}^{2^n}(X^i + Y)$ du lemme 3.16 au lieu des polynômes de Pochhammer-Wilkinson, nous obtenons que la famille de polynômes $U_n(X, Y)$ est aussi calculée par des circuits

$$\sum_{i=1}^{n^{O(\sqrt{n})}} f_i(X, Y)^{\alpha_i}$$

où $\alpha_i = O(\sqrt{n})$ et les f_i sont des polynômes bivariés $n^{O(\sqrt{n})}$-creux. D'après l'hypothèse du théorème, le polygône de Newton associé à U_n a au plus $2^{O(\sqrt{n}\log n)}$ arêtes. Ce qui contredit le fait que les polygônes de Newton associés à U_n ont 2^{n+1} arêtes. □

Avec la définissabilité dans P

Un problème de toutes ces "τ-conjectures" est que des bornes intermédiaires (par exemple en $2^{p(\log(kmt))}$ sur le nombre de racines) ne permettent pas d'obtenir des bornes inférieures plus faibles pour la taille du permanent. En fait, en regardant le schéma des preuves par contradiction d'un peu plus près, on s'aperçoit qu'on utilise à deux reprises le fait que $\tau(\text{PERM}_n) = n^{O(1)}$. La première fois pour appliquer la proposition 3.17 et la seconde, pour utiliser le lemme 3.9. Alors que dans le second cas, la condition $\text{PERM} \in \mathsf{VP}^0$ est nécessaire, on peut s'apercevoir que la condition pour la proposition 3.17 est plus souple. Elle peut encore s'appliquer avec une hypothèse plus faible.

Dans ces preuves, le lemme 3.9 sert à montrer – toujours sous l'hypothèse $\tau(\text{PERM}_n) = n^{O(1)}$ – que les polynômes définissables dans $\mathsf{CH/poly}$ sont aussi définissables dans $\mathsf{P/poly}$. Pour ne pas avoir à utiliser ce lemme, il suffit de trouver une famille de polynômes définissable dans $\mathsf{P/poly}$ ayant aussi un nombre exponentiel de racines réelles.

Bien qu'à la connaissance de l'auteur, nous ne connaissons pas de telle famille qui a, comme pour PW_n, un nombre exponentiel de racines entières, il est possible d'utiliser aussi le fait qu'on a seulement besoin de racines réelles distinctes dans la τ-conjecture réelle.

Le résultat suivant a été prouvé par Hutchinson [51]. Une autre preuve apparaît dans [68].

Théorème 3.35. *Soit $f_n(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme réel de degré $n \geq 2$ où les coefficients sont positifs. Si*

$$a_i^2 - 4a_{i-1}a_{i+1} > 0 \qquad i = 1, 2, \ldots, n-1,$$

alors toutes les racines de f_n sont réelles et distinctes.

On peut appliquer directement ce résultat à la famille suivante.

Lemme 3.36. *Soit*

$$V_n(X) = \sum_{i=0}^{2^n-1} 2^{2\cdot 2^n i - 2i(i+1)} X^i.$$

Alors $V_n \in \mathbb{Z}[X]$ et pour tout $n \geq 1$, le polynôme V_n a 2^n racines réelles distinctes.

Démonstration. Fixons n. Comme pour tout $0 \leq i \leq 2^n - 1$, on a $2\cdot 2^n i - 2i(i+1) \geq 0$, le polynôme V_n est bien dans $\mathbb{Z}[X]$. De plus :

$$\begin{aligned}
\log_2(4a_{i-1}a_{i+1}) &= 2 + 2\cdot 2^n(i-1) - 2(i-1)i + 2\cdot 2^n(i+1) - 2(i+1)(i+2) \\
&= 4\cdot 2^n i - 4i(i+1) - 2 \\
&< 2(2\cdot 2^n i - 2i(i+1)).
\end{aligned}$$

Donc,

$$a_i^2 > 4a_{i-1}a_{i+1}.$$

La preuve du lemme suit du théorème 3.35. □

La suite de coefficients de V_n est $v_n = 2^{2\cdot 2^n i - 2i(i+1)}$. Ainsi

$$\textsc{Bit}(v) = \{1^n \# i, j \mid 0 \leq i \leq 2^n - 1 \text{ et } j = 2 \cdot 2^n i - 2i(i+1)\} \in \mathsf{P}.$$

Le polynôme V_n est définissable dans P, donc en particulier dans $\mathsf{GapP/poly}$.

On obtient alors le corollaire suivant en appliquant directement la proposition 3.17 à la famille (V_n) (avec $d = n$ et $r = 2n + 1$) :

Corollaire 3.37. *Il existe un polynôme q tel que si $\textsc{Perm}_n$ est calculé par une suite de circuits C_n, alors il existe une projection D_n du circuit $C_{q(n)}$ tel que V_n soit calculé par un circuit $D_n(Y_1, \ldots, Y_k)$ où les Y_i sont des puissances de X d'exposants au plus 2^{n-1} et où k est un entier inférieur à $3n + 1$. De plus, les circuits D_n calculent des polynômes homogènes en les Y_k.*

Comme on l'avait mentionné à la remarque 3.22, la définissabilité dans P permet d'éviter de dépendre du lemme 3.9 et donc de pouvoir travailler avec des constantes. En particulier, utiliser la famille de polynômes (V_n) au lieu de (PW_n) permet d'améliorer un peu le théorème 3.25.

Théorème 3.38. *Si la τ-conjecture réelle avec puissances est avérée, alors* $\textsc{Perm} \notin \mathsf{VP}$.

Enfin, la définissabilité dans P permet aussi d'améliorer (et de simplifier) la version combinatoire. Considérons le polynôme $W_n = \sum_{i=1}^{2^n} X^i Y^{i^2}$. Le polygone de Newton associé a 2^n arêtes. De plus W_n est définissable dans P. D'où

Théorème 3.39. *Si la version combinatoire de la τ-conjecture (conjecture 3.31) est avérée, alors* $\textsc{Perm} \notin \mathsf{VP}$.

Cependant, on ne sait pas se passer de la hiérarchie de comptage pour la version avec multiplicité (conjecture 3.29). Pour cela, il faudrait trouver un polynôme P_n définissable dans P tel que P_n ait une racine non nulle de multiplicité 2^n.

Question ouverte. *Existe-t-il un tel polynôme ?*

2.3 Problèmes $fg + 1$

Vu que chacune des conjectures exposées ci-dessus reste encore ouverte, on pourrait déjà s'intéresser à essayer de comprendre les "cas de bases". Pour un polynôme donné, on s'intéressera ici aux trois paramètres suivants :

— le nombre Z de racines réelles,
— la multiplicité μ d'une racine complexe non nulle
— et le nombre d'arêtes π du polygone de Newton correspondant.

Pour le cas des polynômes t-creux, Z, μ et π sont tous bornés linéairement en t.

Pour Z, il s'agit de l'estimation de Descartes, pour μ un résultat de Hajós [46] et pour π, il s'agit juste du fait que dans le plan, l'enveloppe convexe de t points est un polygone avec au plus t sommets.

L'étape suivante, des produits, ne rajoute aucune complexité dans chacun de ces cas. Les racines d'un produit sont l'union des racines des facteurs, et la multiplicité d'une racine d'un produit est la somme des multiplicités des racines des facteurs. Enfin, on a vu au chapitre 1 (proposition 3.30) que le nombre d'arêtes d'une somme de

Minkowski de m polygones à t sommets est borné par mt. Donc les trois paramètres considérés sont bornés par $O(mt)$.

Toute la difficulté arrive lorsque la dernière somme intervient. Considérons alors le cas – qui semble basique – des polynômes $fg+1$ où f et g sont des polynômes t-creux. Le paragraphe précédent assure que pour le produit fg, les trois paramètres sont bornés par $O(t)$. La borne linéaire tient-elle encore pour $fg+1$?

Conjecture 3.40 (Conjecture $fg+1$)**.** *Si f et g sont des polynômes t-creux, alors les trois paramètres Z, μ et π sont linéairement bornés en t.*

Pour ces trois cas, on obtient une borne supérieure quadratique en t en développant le polynôme. Pour les paramètres Z et μ, c'est, à la connaissance de l'auteur, la meilleure borne connue. Pour le cas du paramètre π. on verra un peu plus loin (théorème 4.9) que l'on peut obtenir une borne supérieure en $O(t^{4/3})$.

Chapitre 4

Premiers résultats sur les τ-conjectures

Dans ce chapitre, nous nous intéresserons à deux variantes de la τ-conjecture réelle que nous avons introduites au chapitre précédent. Nous montrerons en premier lieu que la version monotone est en fait équivalente à la τ-conjecture réelle. Puis nous étudierons une attaque de la version combinatoire.

1 Équivalence de la version monotone

Bien que les différentes versions de la τ-conjecture réelle du chapitre précédent impliquent toutes que $\text{PERM} \notin \mathsf{VNP}^0$, on ne sait en général pas les comparer entre elles. On a cependant déjà remarqué (lemme 3.26) que les conjectures 3.23 et 3.24 sont équivalentes. On se propose de montrer ici que ces dernières sont, en fait, aussi équivalentes à la conjecture 3.28 (la version monotone) :

Proposition 4.1. *Les conjectures 3.23 et 3.28 sont équivalentes.*

Commençons par poser quelques notations.

Définition 4.2. *Notons $\mathbb{R}[X]^+$ l'ensemble des polynômes sur $\mathbb{R}$ qui n'ont que des coefficients positifs dans leur forme développée. Nous noterons enfin $\mathbb{R}[X]_t$ (resp. $\mathbb{R}[X]_t^+$) l'ensemble des polynômes de $\mathbb{R}[X]$ (resp. de $\mathbb{R}[X]^+$) qui sont t-creux.*

Le cœur de la preuve repose sur le lemme suivant :

Lemme 4.3. *Soient $f \in \mathbb{R}[X]_t$, $g \in \mathbb{R}[X]$ et $h \in \mathbb{R}[X]$ où f et g sont non identiquement nuls. Supposons que $P(X) = f(X) \cdot g(X) + h(X)$ soit aussi non identiquement nul. Soit r le nombre de racines strictement négatives de P. Alors il existe $\tilde{f} \in \mathbb{R}[X]_t^+$ non nul et $m \in \mathbb{N}$ tels que $\tilde{f}(X) \cdot g(X^m) + X \cdot h(X^m)$ ait au moins r racines strictement négatives.*

Démonstration. Notons $f(X) = f_+(X) - f_-(X)$ où f_+ et f_- sont à coefficients positifs. Si f_- est le polynôme nul, alors le lemme est montré avec $\tilde{f} = f$ et $m = 1$.

Supposons donc que f_- n'est pas identiquement nul. On a

$$f(x) \cdot g(x) = -h(x) \Leftrightarrow -f_-(x) \cdot g(x) = -h(x) - f_+(x) \cdot g(x)$$
$$\Leftrightarrow \begin{cases} -1 = \left(\frac{-h - gf_+}{gf_-}\right)(x) \\ \text{ou } \ (gf_-(x) = 0 \text{ et } \ -h(x) - gf_+(x) = 0)\,. \end{cases}$$

Considérons les solutions strictement négatives du premier cas. Posons

$$F(X) = -\frac{h(X) + g(X)f_+(X)}{g(X)f_-(X)}$$

où F est prolongée par continuité au niveau des singularités effaçables. Comme P n'est pas le polynôme nul, F n'est pas la constante -1. Soient

$$\alpha_1 < \alpha_2 < \ldots < \alpha_p < -1 < \beta_1 < \ldots < \beta_q < 0$$

les zéros strictement négatifs et distincts de -1 de la fraction rationnelle $F(X)+1$. Notons

$$\alpha_i^- = \begin{cases} 1 \text{ si } F(X)+1 > 0 \text{ sur un voisinage à gauche de } \alpha_i \\ -1 \text{ sinon.} \end{cases}$$

De même,

$$\alpha_i^+ = \begin{cases} 1 \text{ si } F(X)+1 > 0 \text{ sur un voisinage à droite de } \alpha_i \\ -1 \text{ sinon.} \end{cases}$$

Les familles $\left(\beta_i^+\right)$ et $\left(\beta_i^-\right)$ sont formées de même. Nous noterons dans la suite $(\alpha, i, -)$ un tel voisinage à gauche de α_i, $(\alpha, i, +)$ un tel voisinage à droite de α_i et de même pour $(\beta, i, -)$ et $(\beta, i, +)$. Par abus de notation, nous dirons que ces "voisinages" appartiennent aux intervalles correspondants (par exemple, $(\alpha, 1, -) \in [2\alpha_1, \alpha_1[$ et $(\beta, 2, +) \in]\beta_2, \beta_3[$).

Nous allons considérer l'ensemble d'intervalles défini par

$$\mathcal{I} = \Big\{ [2\alpha_1, \alpha_1[,]\alpha_1, \alpha_2[, \ldots,]\alpha_{p-1}, \alpha_p[, \Big]\alpha_p, \frac{\alpha_p - 1}{2}\Big], \\ \Big[\frac{-1+\beta_1}{2}, \beta_1\Big[,]\beta_1, \beta_2[, \ldots,]\beta_{q-1}, \beta_q[, \Big[\beta_q, \frac{\beta_q}{2}\Big] \Big\}$$

(remarquons que si p et/ou q sont nuls, l'ensemble est encore bien défini). Posons pour chaque intervalle, $l_I = \|F(X)+1\|_{I,\infty}$, ie. la norme infinie prise sur l'intervalle I et posons $L = \min_{I \in \mathcal{I}}(l_I)$. Enfin, soit $m \in \mathbb{N}$ un entier impair tel que

$$\begin{cases} (-1-L)^m < \min(2\alpha_1, \frac{2}{\beta_q}) \\ (-1+L)^m > \max(\frac{1}{2\alpha_1}, \frac{\beta_q}{2}) \end{cases}$$

(m est bien défini car $L > 0$ et $\alpha_1, \beta_q < 0$). F est une fraction rationnelle. Donc pour chaque intervalle I, soit F est définie sur I et forme ainsi une "bosse", soit F a une singularité essentielle sur I et donc $l_I = \infty$. L'idée de la preuve est d'amplifier ces "bosses" sur chaque intervalle pour que la courbe "$Y = F(X)$" coupe la première bissectrice ou l'hyperbole $Y = X^{-1}$ au moins autant de fois qu'elle coupe l'axe des abcisses.

Posons $A_+ = \{(\alpha, i, \varepsilon) \mid 1 \leq i \leq p \text{ et } \alpha_i^\varepsilon = +1\}$ et $A_- = \{(\alpha, i, \varepsilon) \mid 1 \leq i \leq p \text{ et } \alpha_i^\varepsilon = -1\}$ (avec $\varepsilon \in \{+, -\}$). On définit de même B_+ et B_- pour les $(\beta_i^\varepsilon)_{1 \leq i \leq q}$. Alors $|A_+| + |A_-| + |B_+| + |B_-| = 2(p+q)$. Deux cas sont possibles :

— Si $|A_-| + |B_+| \geq p + q$.

Lemme 4.4. *Dans ce cas, l'équation*

$$X = (F(X))^m \tag{4.1}$$

a au moins $p+q$ solutions strictement négatives distinctes et différentes de -1.

Démonstration. On montre que pour chaque intervalle I de $\mathcal{I}$, l'équation a au moins autant de solutions distinctes dans I que d'éléments dans $(A_- \cup B_+) \cap I$ (où les couples (i, ε) de A_- et B_+ sont assimilés aux voisinages correspondants). Le lemme découle alors du fait que $|A_- \cup B_+| \geq p+q$. Étudions les cas possibles pour les différents intervalles I :

— Intervalle $[2\alpha_1, \alpha_1[$: seul $(\alpha, 1, -)$ est dans cet intervalle. Donc,
  — Si $(\alpha, 1, -) \notin A_-$, c'est immédiat car l'équation (4.1) a bien au moins 0 solutions sur cet intervalle.
  — Si $(\alpha, 1, -) \in A_-$, alors on a encore deux cas :
    — Soit F a un pôle sur cet intervalle, dans ce cas, comme $F(\alpha_1) = -1$, comme $F(X)+1$ ne s'annule pas sur l'intervalle et comme $F(X) < -1$ sur un voisinage à gauche de α_1, la branche à gauche de $x = \alpha_1$ part vers $-\infty$. Cela est encore vrai pour F^m (car m est impair). $F^m(\alpha_1) = -1 > \alpha_1$. Donc $F^m(X) = X$ a au moins une solution dans l'intervalle par le théorème des valeurs intermédiaires (que l'on notera ensuite TVI).
    — Sinon, F est définie (et donc continue) sur $[2\alpha_1, \alpha_1]$. Sur cet intervalle, $F(X) < -1$. Donc, d'après la définition de $l_{[2\alpha_1,\alpha_1[}$, et par le théorème des bornes atteintes, il existe $a \in [2\alpha_1, \alpha_1]$ tel que $F(a) \leq \left(-1 - l_{]2\alpha_1,\alpha_1[}\right)$ et donc par définition de m :

$$F^m(a) \leq \left(-1 - l_{]2\alpha_1,\alpha_1[}\right)^m \leq (-1-L)^m < 2\alpha_1 \leq a.$$

    Or $F^m(\alpha_1) = -1 > \alpha_1$. Par le TVI, $F^m(X) = X$ a au moins une solution sur l'intervalle $[a, \alpha_1[\subseteq [2\alpha_1, \alpha_1[$.

— Intervalle $]\alpha_i, \alpha_{i+1}[$.
  — Si F a un pôle en a dans l'intervalle, on se ramène au cas précédent pour chacune des branches partant de α_i et α_{i+1}.
  — Si F est définie sur $[\alpha_i, \alpha_{i+1}]$, alors par le TVI $\alpha_i^+ = \alpha_{i+1}^-$ (car $F+1$ ne s'annule pas sur l'intervalle).
    — Si $\alpha_i^+ = \alpha_{i+1}^- = +1$, alors, on a bien au moins 0 solutions dans l'intervalle.
    — Si $\alpha_i^+ = \alpha_{i+1}^- = -1$, comme précédemment, il existe $a \in]\alpha_i, \alpha_{i+1}[$ tel que $F(a) \leq \left(-1 - l_{]\alpha_i,\alpha_{i+1}[}\right)$. D'où, $F^m(a) < a$. Par le TVI, $F^m(X) = X$ a au moins une solution sur $]\alpha_i, a[$ et au moins une sur $]a, \alpha_{i+1}[$. Donc, l'équation (4.1) a bien au moins deux solutions sur l'intervalle.

— Intervalle $\left[\alpha_p, \frac{\alpha_p - 1}{2}\right]$: ce cas est symétrique au cas $[2\alpha_1, \alpha_1[$.

— Intervalle $\left[\frac{-1+\beta_1}{2}, \beta_1\right[$: seul $(\beta, 1, -)$ est dans cet intervalle. Donc,
  — Si $(\beta, 1, -) \notin B_+$, c'est immédiat. L'équation (4.1) a bien au moins 0 solutions sur cet intervalle.
  — Si $(\beta, 1, -) \in B_+$, alors on a encore 2 cas :

— Soit F a un pôle sur cet intervalle, dans ce cas, comme $F(\beta_1) = -1$, comme $F(X)+1$ ne s'annule pas sur l'intervalle et comme $F(X) > -1$ sur un voisinage à gauche de β_1, la branche à gauche de $x = \beta_1$ part vers $+\infty$. Cela est encore vrai pour F^m. Donc $F^m(X) = X$ a au moins une solution dans l'intervalle (toujours par le TVI).
— Sinon, F est définie (et donc continue) sur $\left[\frac{-1+\beta_1}{2}, \beta_1\right]$. Sur cet intervalle, $F(X) + 1 > 0$. Donc, d'après la définition de $l_{\left[\frac{-1+\beta_1}{2}, \beta_1\right[}$, et par le théorème des bornes atteintes, il existe $b \in \left[\frac{-1+\beta_1}{2}, \beta_1\right]$ tel que $F(b) \geq \left(-1 + l_{\left[\frac{-1+\beta_1}{2}, \beta_1\right[}\right)$. D'où,

$$F^m(b) \geq \left(-1 + l_{\left[\frac{-1+\beta_1}{2}, \beta_1\right[}\right)^m > \frac{\beta_q}{2} > b.$$

Or $F^m(\beta_1) = -1 < \beta_1$. Par le théorème des valeurs intermédiaires, $F^m(X) = X$ a au moins une solution sur l'intervalle $[b, \beta_1] \subseteq \left[\frac{-1+\beta_1}{2}, \beta_1\right[$.

— Intervalles $]\beta_i, \beta_{i+1}[$ et $]\beta_q, 0[$: ces cas sont similaires.

On remarque que l'on a trouvé $p+q$ solutions distinctes à l'équation $F^m(X) = X$. Ces solutions se trouvent dans des intervalles de $\mathcal{I}$, donc ces solutions sont strictement négatives et distinctes de -1. □

Quitte à remplacer m par un entier impair plus grand on peut supposer que les nouvelles solutions de $F^m(X) = X$ n'étaient pas solution de

$$\begin{cases} f_-(X) \cdot g(X) = 0 \\ -h(X) - f_+(X) \cdot g(X) = 0 \end{cases}$$

(possible car $f_- g$ est non identiquement nul). De plus, si -1 est solution de $F(X) = -1$, alors -1 est encore solution de $F^m(X) = X$. Ainsi, le système

$$\begin{cases} X = \left(\frac{-h(X)-f_+(X)g(X)}{f_-(X)g(X)}\right)^m \\ \text{ou } (f_-(X)g(X) = 0 \text{ et } -h(X) - f_+(X)g(X) = 0) \end{cases}$$

a au moins autant de solutions strictement négatives que le système

$$\begin{cases} -1 = \left(\frac{-h-f_+g}{f_-g}\right)(X) \\ \text{ou } (f_-(X)g(X) = 0 \text{ et } -h(X) - f_+(X)g(X) = 0)\,. \end{cases}$$

Donc $X^{1/m} \cdot f_-(X) \cdot g(X) = -h(X) - f_+(X)g(X)$ a au moins r solutions strictement négatives. Il en est donc de même pour

$$[X \cdot f_-(X^m) + f_+(X^m)]g(X^m) + h(X^m) = 0$$

(changement de variables bijectif $X \mapsto X^m$). Ainsi,

$$X \cdot [X \cdot f_-(X^m) + f_+(X^m)]g(X^m) + X \cdot h(X^m)$$

a au moins r racines. En posant $\tilde{f}(X) = X \cdot [X \cdot f_-(X^m) + f_+(X^m)]$, on obtient le lemme.

— Sinon, $|A_+| + |B_-| \geq p + q$. Le cas est similaire en remplaçant les égalités à X par des égalités à $1/X$.

Lemme 4.5. *L'équation*

$$\frac{1}{X} = (F(X))^m$$

a au moins $p + q$ solutions strictement négatives distinctes et différentes de -1.

Démonstration. La preuve de l'affirmation est similaire à celle du lemme 4.4. □

De même, $X^{-1/m} \cdot f_-(X) \cdot g(X) = -h(X) - f_+(X) \cdot g(X)$ a au moins r solutions strictement négatives. C'est donc aussi le cas de

$$\frac{1}{X} \cdot f_-(X^m) \cdot g(X^m) + f_+(X^m) \cdot g(X^m) + h(X^m)$$

(changement de variables bijectif $X \mapsto X^m$), ie.

$$[f_-(X^m) + X \cdot f_+(X^m)]\, g(X^m) + X \cdot h(X^m).$$

En posant $\tilde{f}(X) = [f_-(X^m) + X \cdot f_+(X^m)]$, on obtient le lemme.

□

L'équivalence de la proposition 4.1 suit alors directement du résultat suivant :

Théorème 4.6. *Soient une suite d'entiers $(t_{i,j})_{i \leq m, j \leq n}$ et un polynôme*

$$P(X) = \sum_{i=1}^{m} \prod_{j=1}^{n} f_{i,j}(X)$$

avec $f_{i,j} \in \mathbb{R}[X]_{t_{i,j}}$. Posons ρ le nombre de racines réelles distinctes de P. Alors, il existe des polynômes $g_{i,j} \in \mathbb{R}[X]^+_{t_{i,j}}$ tels que le polynôme

$$\sum_{i=1}^{m} \prod_{j=1}^{n} g_{i,j}(X)$$

a au moins $\frac{\rho+1}{2}$ racines réelles distinctes.

Démonstration. $P(X)$ a au moins $\rho - 1$ racines non nulles. Donc, quitte à remplacer $P(X)$ par $P(-X)$, on peut supposer que $P(X)$ a au moins $\frac{\rho-1}{2}$ racines strictement négatives distinctes. Appliquer alors le lemme 4.3 successivement à chaque facteur permet d'obtenir une famille de polynômes $(\tilde{g}_{i,j}) \in \mathbb{R}[X]^+_{t_{i,j}}$ telle que

$$\sum_{i=1}^{m} \prod_{j=1}^{n} \tilde{g}_{i,j}(X)$$

a au moins $\frac{\rho-1}{2}$ racines réelles strictement négatives. Il suffit alors de poser $g_{i,1}(X) = X \cdot \tilde{g}_{i,1}(X)$ et $g_{i,j}(X) = \tilde{g}_{i,j}(X)$ pour $2 \leq j \leq n$, ce qui rajoute la racine 0. □

2 Par les polygones de Newton

2.1 Bornes supérieures grâce à la convexité

La conjecture 3.31 affirme que le nombre d'arêtes des polygones de Newton des polynômes de la forme de (3.2) est bornée polynomialement. Cette question reste complètement ouverte, mais dans cette section, nous allons améliorer la borne supérieure grossière en $k.t^m$. Avec Koiran, Portier et Thomassé [66], nous obtenons une borne en $O(kt^{2m/3})$. Notre principal outil est un résultat de géométrie convexe [29]. Un ensemble de points du plan S sera appelé extrémal s'il est égal à l'ensemble des points extrémaux de son enveloppe convexe (ie. les éléments de S sont les sommets d'un polygone convexe).

Théorème 4.7. *Soient P et Q deux ensembles de points du plan avec $|P| = s$ et $|Q| = t$. Soit S un sous-ensemble de la somme de Minkowski $P + Q$. Si S est extrémal, alors nous avons $|S| = O(s^{2/3}t^{2/3} + s + t)$.*

Cette borne supérieure est connue être optimale à un facteur constant près [12] (une borne inférieure non-optimale peut aussi être trouvée dans [97]).

Considérons tout d'abord les sommes de produits de deux polynômes.

Théorème 4.8. *Considérons un polynôme bivarié $f \in \mathbb{C}[X, Y]$ de la forme*

$$f(X, Y) = \sum_{i=1}^{k} f_i g_i(X, Y) \tag{4.2}$$

où les f_i ont au plus r monômes et les g_i ont au plus s monômes. Le polygone de Newton de f a $O(k(r^{2/3}s^{2/3} + r + s))$ arêtes.

Démonstration. Soit S_i l'ensemble des points du plan correspondant aux monômes de $f_i g_i$ qui apparaissent dans f avec un coefficient non nul. Comme $\mathrm{Newt}(f)$ est l'enveloppe convexe de $\bigcup_{i=1}^{k} \mathrm{conv}(S_i)$, il est suffisant de borner le nombre de sommets de $\mathrm{conv}(S_i)$. Ces sommets forment un sous-ensemble extrémal de la somme de Minkowski $\mathrm{Mon}(f_i) + \mathrm{Mon}(g_i)$. Par le théorème 4.7, il suit que $\mathrm{conv}(S_i)$ a $O(r^{2/3}s^{2/3} + r + s)$ arêtes. Multiplier cette borne par k fournit une borne supérieure sur le nombre de sommets et donc d'arêtes de $\mathrm{Newt}(f)$. □

À partir de ce résultat, il est facile d'obtenir une borne supérieure pour le cas général, où nous avons des produits de $m \geq 2$ polynômes. Nous avons juste à diviser les m facteurs en deux groupes d'approximativement $m/2$ facteurs, puis dans chaque groupe nous développons le produit par force brute.

Théorème 4.9. *Considérons un polynôme bivarié $f \in \mathbb{C}[X, Y]$ de la forme*

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{i,j}(X, Y) \tag{4.3}$$

où $m \geq 2$ et les $f_{i,j}$ ont au plus t monômes. Le polygone de Newton de f a $O(k.t^{2m/3})$ arêtes.

Démonstration. Comme nous l'avions suggéré plus haut, nous réécrivons chacun des k produits comme un produit de deux polynômes $F_i = \prod_{i=1}^{\lceil m/2 \rceil} f_i$ et $G_i = \prod_{i=1}^{\lfloor m/2 \rfloor} f_i$. Nous pouvons alors appliquer le théorème 4.8 à $f = \sum_{i=1}^{k} F_i G_i$, avec $r = t^{\lceil m/2 \rceil}$ et $s = t^{\lfloor m/2 \rfloor}$. Dans la borne supérieure obtenue $O(k(r^{2/3}s^{2/3}+r+s))$, le terme $kr^{2/3}s^{2/3}$ est dominant car $r^{2/3}s^{2/3} = t^{2(\lceil m/2 \rceil + \lfloor m/2 \rfloor)/3} = t^{2m/3}$ et $m \geq 2$. □

Remarque 4.10. *La borne donnée par ces deux théorèmes est la meilleure connue même lorsqu'on se restreint à des cas qui semblent nettement plus basiques, comme c'est le cas pour les deux exemples suivants.*

- *Considérons deux polynômes $f, g \in \mathbb{C}[X, Y]$ avec au plus t monômes chacun. Quel est le nombre maximum d'arêtes pour le polygone de Newton de $fg + 1$? Le seul cas difficile est quand le terme constant de fg vaut -1. Le théorème 4.8 fournit une borne supérieure en $O(t^{4/3})$, mais la vraie borne pourait tout aussi bien être linéaire en t.*
- *Plus généralement, quel est le nombre maximum d'arêtes du polygone de Newton de $f_1 \dots f_m + 1$, où les f_i ont encore au plus t monômes ? Le théorème 4.9 fournit une borne supérieure en $O(t^{2m/3})$, mais la vraie borne pourrait être de la forme $2^{O(m)}t^{O(1)}$; elle pourrait même aussi être polynomiale en m et t, comme l'impliquerait la conjecture 3.31.*

Afin d'éviter le développement par force brute dans la preuve du théorème 4.9, il est naturel de considérer pour tout i un sous-ensemble extrémal S_i de la somme de Minkowski des m ensembles $\mathrm{Mon}(f_{i1}), \dots, \mathrm{Mon}(f_{im})$. Il s'agit exactement du problème ouvert présent à la fin de [12] : déterminer la plus grande cardinalité possible $M_m(t)$ d'un sous-ensemble extrémal d'une somme de Minkowski de m ensembles $P_0, \dots, P_{m-1}$, chacun composé de t points du plan euclidien. Par exemple la borne inférieure de [12] combinée avec la borne supérieure de [29] montrent que $M_2(t) = \Theta(t^{4/3})$. Malheureusement, nous verrons que $M_m(t) = t^{\Omega(m)}$, donc le développement par force brute n'est pas très éloigné de l'optimal.

Exemple 4.11. *Fixons un entier $b \geq 2$ Soit P_k la grille $b_2 \times b$ composée des points entiers dont tous les digits en base b des ordonnées et tous les digits en base b^2 des abscisses valent zéro, sauf éventuellement le digit de poids b^k pour les ordonnées et le digit de poids b^{2k} pour les abscisses. Plus précisément,*

$$P_k = \{(b^{2k}.i, b^k.j) \mid 0 \leq i \leq b^2 - 1 \text{ et } 0 \leq j \leq b - 1\}.$$

Clairement la somme de Minkowski $P_0 + \ldots + P_{m-1}$ est la grille $\{0, \dots, b^{2m} - 1\} \times \{0, \dots, b^m - 1\}$ de taille $b^{2m} \times b^m$.

Le prochain lemme (qui n'est probablement pas optimal) montre comment trouver un ensemble extrémal suffisamment grand dans une grille.

Lemme 4.12. *Si $n(n-1)/2 < M$ et $n < N$ il est possible de trouver n points formant un ensemble extrémal dans la grille $M \times N$.*

Démonstration. Nous commençons à partir de l'origine et construisons une suite de $n - 1$ segments (qui correspondront aux arêtes du polygone). Le $i^{\text{ème}}$ segment possède une longueur horizontale i et une pente $1/i$. Nous construisons ces segments un à un aussi longtemps que nous pouvons le faire sans sortir de la grille, ie. tant que $n(n-1)/2 < M$ et $n < N$. Ensemble, les $n - 1$ segments relient n points qui forment un ensemble extrémal. □

Proposition 4.13. *Pour tout m et pour une infinité de valeurs de t nous avons :*

$$M_m(t) \geq t^{m/3} - 1.$$

Démonstration. À partir de l'exemple 4.11 et du lemme 4.12 (en posant $M = b^{2m}$ et $N = b^m$) nous obtenons que $M_m(b^3) \geq n$ si $n(n-1) < 2b^{2m}$ et $n < b^m$. Donc $M_m(b^3) \geq b^m - 1$. Le résultat suit en chosissant $t = b^3$. □

Ce résultat montre que d'autres ingrédients que le théorème 4.7 seraient nécessaires si l'on veut obtenir une preuve de la conjecture 3.31. Un argument similaire peut être trouvé pour le cas où les ensembles $P_0, P_1, \ldots, P_{m-1}$ dans la somme de Minkowski sont tous égaux (c'est un cas naturel à étudier vu le résultat du théorème 3.34, qui montre qu'il est suffisant de traiter seulement les sommes de puissances pour obtenir une borne inférieure pour le permanent). Plus précisément, posons $M'_m(t)$ la cardinalité maximale d'un sous-ensemble extrémal d'une somme de Minkowski $P + P + \cdots + P$ de taille m où P est une ensemble d'au plus m points. Par définition, nous savons que $M'_m(t) \geq M_m(\lceil t/m \rceil)$: il suffit de remplacer les m ensembles de taille $\lceil t/m \rceil$ par leur union. Donc nous avons $M'_m(t) \geq \lceil t/m \rceil^{m/3} - 1$.

Chapitre 5

Approche de la τ-conjecture réelle à l'aide du wronskien

Dans le chapitre 3, nous avons vu que prouver une des versions de la τ-conjecture réelle impliquerait une borne inférieure superpolynomiale sur la taille des circuits calculant le permanent. Nous étudierons dans ce chapitre des pistes pour attaquer cette τ-conjecture réelle. Nous rappellons la forme la plus faible (et donc potentiellement la plus facile à prouver).

Conjecture (Rappel de la conjecture 3.24)**.** *Il existe un polynôme p tel que pour tout polynôme $f(x) \in \mathbb{R}[x]$ univarié et de la forme $\sum_{i=1}^{k} \bigwedge^{m} f_i(x)$ où les polynômes f_i sont des polynômes t-creux, le nombre de racines réelles distinctes de f est au plus $p(kt2^m)$.*

Un premier pas a été fait pour résoudre cette conjecture par Grenet, Koiran, Portier et Strozecki [38]. Ils ont considéré en fait une famille un peu plus générale : les sommes de produits de puissances de polynômes creux.

$$\sum_{i=1}^{k} \prod_{j=1}^{m} f_j^{\alpha_{i,j}}. \tag{5.1}$$

La borne supérieure sur le nombre de racines rélles obtenue dans [38] est polynomiale en t, mais exponentielle en m et doublement exponentielle en k.

Les bornes sur le nombre de zéros réels pour les systèmes de polynômes creux ont été abondamment étudié par Khovanskĭ [59]. Ses travaux ont débouché sur une théorie très générale, communément appelée "Théorie des fewnomials". Un peu plus de détails sur cette théorie seront donné au prochain chapitre. Les résultats issus de cette théorie impliquent une borne supérieure exponentielle en k, m et t sur le nombre de racines réelles des polynômes de la forme (5.1). Dans ce chapitre, nous allons montrer une borne de l'ordre de $t^{O(k^2m)}$, c'est-à-dire sans la double exponentielle de [38], mais tout en restant polynomial en t. Cette borne ainsi que les autres résultats dans ce chapitre ont été obtenu dans l'article [64] coécrit avec Koiran et Portier.

En outre, les résultats s'étendent à d'autres familles de fonctions. En particulier, Avendaño [8] a étudié le nombre d'intersections dans le plan réel entre une courbe creuse et une droite. Il prouve une borne linéaire sur le nombre de racines réelles des polynômes de la forme $\sum_{i=1}^{k} x^{\alpha_i}(ax+b)^{\beta_i}$ où α_i et β_i sont des entiers. Cependant, il

donne aussi un contre-exemple à sa borne dans le cas d'exposants non entiers. Nous obtenons une borne polynomiale pour la famille plus générale de type (5.1) où les polynômes f_j sont de degrés bornés et les $\alpha_{i,j}$ sont des exposants réels.

En plus de borner le nombre de racines réelles, nous établirons à la section 3 des algorithmes déterministes pour le problème du test de l'identité de polynômes (en anglais "Polynomial Identity Testing", et que l'on notera "PIT") dans le cas des polynômes de la forme (5.1). Le temps d'exécution de l'algorithme est polynomial en t et en la taille en bits des coefficients et des puissances $(\alpha_{i,j})$ et exponentiel en k et m.

Présentons maintenant le principal outil technique. Trouver les racines d'un produit de polynômes est facile : il s'agit de la réunion des racines des différents facteurs. Mais trouver les racines d'une somme est nettement plus difficile : par exemple comment borner le nombre de racines rélles de $fg + 1$ lorsque f et g sont t-creux ? La question de savoir si la borne est ou non linéaire en t est ouverte. L'outil principal pour outrepasser la difficulté des sommes est le wronskien. Rappelons que le wronskien d'une famille de fonctions $f_1, \ldots, f_k$ est le déterminant de la matrice des dérivées d'ordre 0 jusqu'à $k-1$. Plus formellement,

$$W(f_1, \ldots, f_k) = \det\left(\left(f_j^{(i-1)}\right)_{1 \leq i,j \leq k}\right).$$

Un autre outil classique et très utile est la règle des signes de Descartes (lemme 3.5) qui a été donnée au chapitre 3. Nous utiliserons surtout l'estimation qu'elle implique (nous rappelons cette borne qui a déjà été donnée au chapitre 3, lemme 3.4) :

Lemme 5.1 (Estimation de Descartes)**.** *Soit $f = \sum_{i=1}^{t} a_i x^{\alpha_i}$ un polynôme tel que $\alpha_1 < \alpha_2 < \ldots < \alpha_t$ et a_i sont des réels non nuls. Alors le nombre de racines réelles strictement positives de f, compté avec multiplicité, est borné par $t-1$. De plus, le résultat tient encore dans le cas où les exposants sont réels.*

Dans leur livre [85], Pólya et Szegő utilisent déjà le wronskien pour généraliser la règle des signes à d'autres familles. Dans notre cas, nous aurons seulement besoin de l'estimation originale concernant les polynômes creux (présentée ci-dessus). D'autres liens étaient déjà connus entre les wronskiens et les polynômes creux (cf. par exemple [42], [43] et [41]). Nous montrons dans le théorème 5.6 que borner le nombre de racines du wronskien implique une borne supérieure sur le nombre de racines de la somme correspondante. En général, le wronskien semble plus compliqué que la somme des fonctions, mais pour les familles étudiées ici, la structure du déterminant permet de les factoriser (cf. théorèmes 5.14 et 5.16).

Commençons donc, dès la prochaine section, à nous occuper des liens entre les wronskiens et les sommes de fonctions avant de pouvoir utiliser ces résultats pour borner le nombre de racines réelles de certaines familles en section 2, puis pour élaborer des algorithmes pour certains cas du PIT en section 3.

1 Zéros des wronskiens

Rappelons que pour une famille finie de fonctions réelles $f_1, \ldots, f_k$ suffisamment dérivables, le wronskien est défini par

$$W(f_1, \ldots, f_k) = \det\left(\left(f_j^{(i-1)}\right)_{1\leq i,j\leq k}\right).$$

Nous utiliserons les propriétés suivantes du wronskien.

Lemme 5.2. *Soient $f_1, \ldots, f_k$ et g des fonctions réelles $k-1$ fois dérivables. Alors,*

$$W(gf_1, \ldots, gf_k) = g^k W(f_1, \ldots, f_k).$$

Et le corollaire :

Lemme 5.3. *Soient $f_1, \ldots, f_k$ des fonctions réelles $k-1$ fois dérivables et I un intervalle où aucune de ces fonctions ne s'annule. Alors, sur I, nous avons*

$$W(f_1, \ldots, f_k) = (f_1)^k W\left(\left(\frac{f_2}{f_1}\right)', \ldots, \left(\frac{f_k}{f_1}\right)'\right).$$

Ces résultats peuvent être trouvés dans [85] (ex. 57, 58 en Partie 7). Notons que le wronskien d'une famille de fonctions linéairement dépendantes est identiquement nul (si une famille est dépendante, alors la famille des dérivées est aussi dépendante avec les mêmes coefficients). Mais la réciproque n'est pas systématiquement vraie. Peano puis Bôcher trouvèrent des contrexemples [16, 80, 81] (cf. [28] pour un historique de ces résultats). Toutefois, Bôcher [17] a prouvé que la réciproque est vérifiée lorsque les fonctions sont analytiques [50].

Lemme 5.4. *Si $f_1, \ldots, f_k$ sont des fonctions analytiques, alors la famille (f_i) est linéairement dépendante si et seulement si $W(f_1, \ldots, f_k) = 0$.*

Définition 5.5. *Pour toute fonction g et tout intervalle I, nous noterons $Z_I(g)$ le nombre de racines réelles distinctes de g sur I. Nous écrirons juste $Z(g)$ quand le choix de l'intervalle considéré est clair d'après le contexte.*

Dans la suite de ce chapitre, nous considérerons seulement des intervalles non triviaux, c'est-à-dire ceux qui ne sont pas réduits à des points (et nous autoriserons les intervalles non-bornées). Le prochain théorème est presque impliqué par les résultats de Voorhoeve et Van der Porten (cf. le théorème 5.8 plus bas).

Théorème 5.6. *Soit k un entier non-nul. Soit (f_i) une famille de k fonctions $(k-1)$ fois dérivables sur un intervalle I et telle que pour tout $i \leq k$, le wronskien $W(f_1, \ldots, f_i)$ ne s'annule pas sur I.*

Si les constantes réelles $a_1, \ldots, a_k$ ne sont pas toutes égales à 0, alors

$$a_1 f_1 + a_2 f_2 + \ldots + a_k f_k$$

a au plus $k-1$ zéros réels sur I comptés avec multiplicité.

Démonstration. Nous allons montrer ce résultat par récurrence sur k.

Si $k = 1$, alors $f_1 = W(f_1)$ n'a aucun zéro. De plus, a_1 n'est pas la constante nulle. Donc $a_1 f_1$ n'a pas de zéro.

Soit $k \geq 2$ et supposons que la propriété est vraie pour toutes les combinaisons linéaires de taille $k-1$. Appellons z le nombre de zéros de $a_1 f_1 + \ldots + a_k f_k$. Si $a_2 = a_3 = \ldots = a_k = 0$, alors $a_1 \neq 0$ et $a_1 f_1 + a_2 f_2 + \ldots + a_k f_k = a_1 f_1$ n'ont aucun zéro, et la conclusion du théorème est vérifiée. Autrement, $a_1 + \frac{a_2 f_2}{f_1} + \ldots + \frac{a_k f_k}{f_1}$ a z zéros (car $f_1 = W(f_1)$ n'a pas de racine par hypothèse). En appliquant le théorème de Rolle, $a_2 \left(\frac{f_2}{f_1}\right)' + \ldots + a_k \left(\frac{f_k}{f_1}\right)'$ a au moins $z-1$ zéros sur I.

La fonction f_1 ne s'annule pas sur I, donc les fonctions $\left(\frac{f_2}{f_1}\right)', \ldots, \left(\frac{f_k}{f_1}\right)'$ sont $k-2$ fois dérivables. De plus, pour tout $2 \leq i \leq k$,

$$W\left((f_2/f_1)', \ldots, (f_i/f_1)'\right) = W(f_1, \ldots, f_i)/f_1^i$$

ne s'annule pas non plus sur I. Comme les coefficients $a_2, \ldots, a_k$ ne sont pas tous nuls, on obtient avec l'hypothèse de récurrence que

$$a_2 \left(\frac{f_2}{f_1}\right)' + \ldots + a_k \left(\frac{f_k}{f_1}\right)'$$

a au plus $k-2$ zéros. Donc $a_1 f_1 + a_2 f_2 + \ldots + a_k f_k$ a au plus $k-1$ racines selon le théorème de Rolle. □

1.1 Borner les zéros des sommes par les zéros des wronskiens

Nous pouvons directement déduire du théorème 5.6 un premier résultat. Le théorème suivant nous donne une méthode pour trouver des bornes supérieures sur le nombre de racines. Nous montrerons dans la section 4 que cette borne et en quelque sorte optimale.

Théorème 5.7. *Soient $f_1, \ldots, fk$ des fonctions analytiques définies sur un intervalle I. Si les constantes réelles $a_1, \ldots, a_k$ ne sont pas toutes nulles,*

$$Z(a_1 f_1 + \ldots + a_k f_k) \leq \left(1 + \sum_{i=1}^{k} Z(W(f_1, \ldots, f_i))\right) k - 1. \tag{5.2}$$

Plus précisément, si $\Upsilon = \{x \in I \mid \exists i \leq k, W(f_1, \ldots, f_i)(x) = 0\}$ est fini, alors

$$Z(a_1 f_1 + \ldots + a_k f_k) \leq (1 + |\Upsilon|)k - 1. \tag{5.3}$$

De plus, les inégalités restent vérifiées si, du côté gauche des inégalités, les zéros qui ne sont pas des zéros de l'un des wronskiens $W(f_1, \ldots, f_i)$ sont comptés avec multiplicité.

Démonstration. Si $a_1 f_1 + \ldots + a_k f_k$ est le polynôme nul, alors la famille est linéairement dépendante et donc le wronskien $W(f_1, \ldots, f_k)$ est aussi le polynôme identiquement nul. Cela signifie que $\Upsilon = I$ est infini et que l'inégalité est vérifiée.

Autrement, $a_1 f_1 + \ldots + a_k f_k$ a un nombre fini de zéros. Nous avons

$$\Upsilon = \bigcup_{i=1}^{k} Z(W(f_1, \ldots, f_i)).$$

Donc, $|\Upsilon| \leq \sum_{i=1}^{k} |Z(W(f_1, \ldots, f_i))|$. L'ensemble $I \setminus \Upsilon$ est une union de $|\Upsilon| + 1$ intervalles. Soit J un de ces intervalles. D'après le théorème 5.6, on a $Z_J(a_1 f_1 + \ldots + a_k f_k) \leq k - 1$. D'où $a_1 f_1 + \ldots + a_k f_k$ a au plus $(1 + |\Upsilon|)(k-1)$ zéros sur $I \setminus \Upsilon$ et au plus $(1 + |\Upsilon|)(k-1) + |\Upsilon|$ zéros sur I. □

Remarquons que Voorhoeve et van der Poorten [102] ont prouvé un résultat similaire au théorème 5.7, excepté que dans leur cas, les zéros sont comptés avec multiplicité.

Théorème 5.8 (Voorhoeve et van der Poorten, 1975)**.** *Soient $f_1, \ldots, f_k$ des fonctions réelles analytiques sur un intervalle I. Alors,*

$$N(f_1 + \ldots + f_k) \leq k - 1 + \sum_{j=1}^{k-2} N(W_j) + \sum_{j=1}^{k} N(W_j)$$

où $N(f)$ désigne le nombre de racine de f sur I comptées avec multiplicité.

Ce résultat implique immédiatement le théorème 5.6 dans le cas analytique. Cependant dans nos applications, les wronskiens auront des racines de grandes multiplicité. Nous aimerions donc ne pas compter la multiplicité pour éviter que la borne obtenue par la partie droite de l'inégalité soit trop large. Toutefois en réutilisant des idées de la preuve de leur théorème, nous pouvons prouver la variation suivante du théorème 5.7. La preuve sera donnée en sous-section 1.2.

Théorème 5.9. *Soit $f_1, \ldots, f_k$ des fonctions analytiques linéairement indépendantes sur un intervalle I. Alors,*

$$Z(f_1 + \ldots + f_k) \leq k - 1 + Z(W_k) + Z(W_{k-1}) + 2 \sum_{j=1}^{k-2} Z(W_j).$$

Dans la plupart des applications, ce résultat implique une meilleure borne que les précédents théorèmes 5.6 et 5.7. Plus précisément, le théorème 5.6 sera plus fort si les $W(f_1, \ldots, f_i)$ ont les mêmes zéros, car ils ne seront pas recomptés. Sinon, la borne du théorème 5.9 sera plus précise. Nous conjecturons d'ailleurs la borne suivante qui généraliserait les deux bornes :

Conjecture 5.10. *Soit $f_1, \ldots, f_k$ des fonctions analytiques linéairement indépendantes sur un intervalle I. Alors,*

$$Z(f_1 + \ldots + f_k) \leq k - 1 + \sum_{j=1}^{k} Z(W_j).$$

1.2 Seconde version de la borne supérieure

Dans cette section, nous allons donner une preuve du théorème 5.9.

Nous noterons $W_i = W(f_1, f_2, \ldots, f_i)$ pour $i \geq 1$ quand la famille $(f_1, \ldots, f_i)$ est explicite d'après le contexte. Finalement, nous poserons $W_0 = 1$.

En plus du lemme 5.4, plusieurs liens entre le wronskien et les combinaisons linéaires des fonctions sont connus. Nous utiliserons d'ailleurs un résultat de Frobenius [32, 77, 84] :

Lemme 5.11. *Soit (f_i) une famille de fonctions analytiques. Soit (R_i) la famille de fonctions définie par :*

$$R_0 = f_1 + \ldots + f_k$$
$$R_{i+1} = \frac{W_{i+1}^2}{W_i} \left(\frac{R_i}{W_{i+1}} \right)'.$$

Alors les fonctions R_i sont analytiques et $R_{k-1} = W_k$.

Nous pouvons maintenant donner une preuve du théorème 5.9.

Si la famille (f_i) est linéairement dépendante, alors le membre droit de l'inégalité est infini. Ainsi, le résultat est avéré. Nous supposerons donc dans la suite que la famille est linéairement indépendante.

Soit (R_i) la famille des fonctions analytiques définie par :

$$R_0 = f_1 + \ldots + f_k$$
$$R_{i+1} = \frac{W_{i+1}^2}{W_i} \left(\frac{R_i}{W_{i+1}} \right)'.$$

Nous allons prouver par récurrence sur i, que pour tout $0 \leq i \leq k-1$, la fonction analytique R_i a au moins

$$Z(f_1 + \ldots + f_k) - i - Z(W_i) - 2\sum_{j=1}^{i-1} Z(W_j)$$

racines sur I. Ceci implique le théorème lorsque $i = k - 1$ d'après le lemme 5.11.

Si $i = 0$, alors $R_0 = f_1 + \ldots + f_k$ et R_0 a exactement (et donc au moins) $Z(f_1 + \ldots + f_k)$ zéros.

Supposons que la propriété soit vérifiée pour une valeur particulière de i telle que $i \leq k - 2$. Nous noterons $m_x(F)$ la multiplicité de F en x pour tout $x \in \mathbb{R}$ et toute fraction de fonctions analytiques F. Nous définissons enfin quatre valeurs :

— Z_i^+ est le nombre de $x \in \mathbb{R}$ tels que $m_x(R_i) > m_x(W_{i+1}) > 0$.
— $Z_i^=$ est le nombre de $x \in \mathbb{R}$ tels que $m_x(R_i) = m_x(W_{i+1}) > 0$.
— $Z_i^{->}$ est le nombre de $x \in \mathbb{R}$ tels que $m_x(W_{i+1}) > m_x(R_i) > 0$.
— Z_i^{-0} est le nombre de $x \in \mathbb{R}$ tels que $m_x(W_{i+1}) > 0 = m_x(R_i)$.

Nous avons : $Z(W_{i+1}) = Z_i^+ + Z_i^= + Z_i^{-0} + Z_i^{->}$.

Nous savons d'après le lemme 5.11 que R_i est en fait analytique. Alors par hypothèse de récurrence, la fraction $\frac{R_i}{W_{i+1}}$ a au moins

$$Z(f_1 + \ldots + f_k) - i - Z(W_i) - 2\left(\sum_{j=1}^{i-1} Z(W_j)\right) - Z_i^= - Z_i^{->}$$

racines et au plus $Z_i^{->} + Z_i^{-0}$ pôles. D'après le théorème de Rolle, le nombre de zéros de $\left(\frac{R_i}{W_{i+1}}\right)'$ est au moins

$$\left[Z(f_1 + \ldots f_k) - i - Z(W_i) - 2\left(\sum_{j=1}^{i=1} Z(W_j)\right) - Z_i^{=} - Z_i^{->}\right] - Z_i^{->} - Z_i^{-0} - 1.$$

Donc le nombre de zéros de $R_{i+1} = \frac{W_{i+1}^2}{W_i}\left(\frac{R_i}{W_{i+1}}\right)'$ est au moins

$$\left[Z(f_1 + \ldots + f_k) - i - Z(W_i) - 2\left(\sum_{j=1}^{i+1} Z(W_j)\right) - Z_i^{=} - Z_i^{->}\right] - \left[Z_i^{->} + Z_i^{-0} + 1\right] + Z_i^{->} - Z(W_i).$$

Nous utilisons pour la dernière borne le fait que si x est tel que

$$0 < m_x(R_i) < m_x(W_{i+1}),$$

alors

$$-m_x(W_{i+1}) < m_x(R_i) - m_x(W_{i+1}) < 0$$

et donc

$$m_x\left(W_{i+1}^2\left(\frac{R_i}{W_{i+1}}\right)'\right) > m_x(W_{i+1}) - 1 > 0.$$

D'où

$$Z(R_{i+1}) \geq Z(f_1 + \ldots + f_k) - (i+1) - Z(W_{i+1}) - 2\left(\sum_{j=1}^{i} Z(W_j)\right).$$

Ce qui prouve le théorème.

2 Retour aux sommes de produits de polynômes

Dans cette section, nous prouvons le théorème 5.14 qui borne le nombre de zéros des polynômes de la forme (5.1). La borne donnée améliore à la fois le résultat de Grenet, Koiran, Portier et Strozecki [38] et la borne obtenue par la théorie des "fewnomials" développée par Khovanskiĭ [59]. À la fin de cette section, nous étendons aussi le résultat d'Avendaño aux exposants réels. Nous avons vu précédemment (dans la section 1) que le nombre de zéros d'une combinaison linéaire de fonctions réelles peut être bornée par une fonction du nombre de zéros du wronskien de ces fonctions. Ainsi, pour montrer notre résultat nous avons juste à borner le nombre de racines des wronskiens des polynômes de la forme $\prod_{j=1}^{m} f_j^{\alpha_{i,j}}$. On va pouvoir montrer qu'un tel wronskien a peu de zéro distincts grâce au fait qu'un tel déterminant se factorise beaucoup : après avoir factorisé les grandes puissances, il ne nous restera plus qu'un déterminant dont les entrées sont des polynômes de petit degré (ou des polynômes creux, selon le modèle que l'on considèrera). Il sera alors immédiat de borner le nombre de racines du déterminant.

2.1 Dérivées d'une puissance

Nous allons utiliser les suites presque nulles d'entiers, c'est-à-dire des suites infinies d'entiers qui ont seulement un nombre fini d'éléments non-nuls. Nous noterons cet ensemble $\mathbb{N}^{(\mathbb{N})}$. Pour tout entier strictement positif p, posons $\mathscr{S}_p = \{(s_1, s_2, \ldots) \in \mathbb{N}^{(\mathbb{N})} \mid \sum_{i=1}^{\infty} i s_i = p\}$ (donc pour tout p, cet ensemble est infini). Alors si s est dans $\mathscr{S}_p$, nous pouvons observer que pour tout $i \geq p+1$, nous avons $s_i = 0$. De plus, pour tout p et pour tout $s = (s_1, s_2, \ldots) \in \mathbb{N}^{(\mathbb{N})}$, nous noterons $|s| = \sum_{i=1}^{\infty} s_i$ (la somme a un sens car elle est finie).

Lemme 5.12. *Soient p un entier strictement positif et $\alpha \geq p$ un nombre réel. Alors*

$$(f^\alpha)^{(p)} = \sum_{s \in \mathscr{S}_p} \left[\beta_{\alpha,s} f^{\alpha-|s|} \prod_{k=1}^{p} \left(f^{(k)}\right)^{s_k} \right]$$

où $(\beta_{\alpha,s})$ sont des constantes.

Nous définissons l'ordre total de dérivation d'un polynôme différentiel d'une fonction avec un exemple : si f est une fonction, l'ordre total de dérivation de $f^3(f')^2\left(f^{(4)}\right)^3 + 3ff'$ est $\max(3*0+2*1+3*4, 0*1+1*1) = 14$.

Le lemme 5.12 signifie juste que la $p^{\text{ième}}$ dérivée d'une puissance α d'une fonction f est une combinaison linéaire de termes tels que chacun de ces termes est un produit de dérivées de f de degré total α et d'ordre total de dérivation p.

Démonstration. Dans la suite, e_i correspond à la suite infinie $(0, 0, \ldots, 0, 1, 0, 0, \ldots)$ où le seul 1 apparaît au niveau de la $i^{\text{ème}}$ coordonnée. Nous montrons ce lemme par récurrence sur p. Si $p = 1$, alors $(f^\alpha)' = \alpha f' f^{\alpha-1}$. Il s'agit du cas de base puisque $\mathscr{S}_1 = \{(1, 0, 0, \ldots)\}$. Remarquons que $\beta_{\alpha,(1,0,\ldots)} = \alpha$. Supposons que le lemme est avéré pour un p fixé. Par hypothèse de récurrence, nous avons

$$\begin{aligned}(f^\alpha)^{(p+1)} &= \left(\sum_{s \in \mathscr{S}_p} \beta_{\alpha,s} f^{\alpha-|s|} \prod_{k=1}^{p} \left(f^{(k)}\right)^{s_k} \right)' \\ &= g_1 + g_2\end{aligned}$$

où

$$g_1 = \sum_{s \in \mathscr{S}_p} \beta_{\alpha,s} \left(f^{\alpha-|s|}\right)' \left(\prod_{k=1}^{p} \left(f^{(k)}\right)^{s_k} \right)$$

$$\text{et } g_2 = \sum_{s \in \mathscr{S}_p} \beta_{\alpha,s} f^{\alpha-|s|} \left(\prod_{k=1}^{p} \left(f^{(k)}\right)^{s_k} \right)'.$$

En réécrivant chaque terme nous obtenons

$$\begin{aligned}
g_1 &= \sum_{s\in\mathscr{S}_p} \beta_{\alpha,s}(\alpha-|s|)f'f^{\alpha-|s|-1}\prod_{k=1}^{p}\left(f^{(k)}\right)^{s_k}\\
&= \sum_{\substack{s\in\mathscr{S}_p\\ s'=s+e_1}} \beta_{\alpha,s}(\alpha-|s'|+1)f^{\alpha-|s'|}\prod_{k=1}^{p}\left(f^{(k)}\right)^{s'_k}\\
g_2 &= \sum_{s\in\mathscr{S}_p} \beta_{\alpha,s}f^{\alpha-|s|}\sum_{j=1}^{p} s_j f^{(j+1)}\left(f^{(j)}\right)^{s_j-1}\prod_{k\neq j}\left(f^{(k)}\right)^{s_k}\\
&= \sum_{j=1}^{p}\left[\sum_{\substack{s\in\mathscr{S}_p\\ s_j\neq 0\\ s'=s-e_j+e_{j+1}}} \beta_{\alpha,s'+e_j-e_{j+1}}f^{\alpha-|s'|}(s'_j+1)\prod_{k=1}^{p+1}\left(f^{(k)}\right)^{s'_k}\right].
\end{aligned}$$

Si s est dans $\mathscr{S}_p$, alors $s+e_1\in\mathscr{S}_{p+1}$ et si de plus $s_j\neq 0$ alors $s-e_j+e_{j+1}\in\mathscr{S}_{p+1}$. Ce qui prouve le théorème. Les constantes β sont définies par : $\beta_{\alpha,(1,0,0,\ldots)}=\alpha$; et si $s\in\mathscr{S}_p$ avec $p>1$, alors

$$\begin{aligned}
\beta_{\alpha,s} =& \mathbb{1}_{s_1\neq 0}(\alpha-|s|+1)\beta_{\alpha,(s_1-1,s_2,s_3,\ldots)}\\
&+\sum_{\substack{2\leq j\leq p\\ s_j\neq 0}}(s_{j-1}+1)\beta_{\alpha,(s_1,\ldots,s_{j-1},s_{j-1}+1,s_j-1,s_{j+1},\ldots)}.
\end{aligned}$$

□

2.2 Application aux $\sum\prod\bigwedge\sum\prod$

Dans [38], les auteurs donnèrent une borne en $t^{O(m2^k)}$ sur le nombre de racines réelles distinctes des polynômes de la forme $f=\sum_{i=1}^{k}a_i\prod_{j=1}^{m}f_j^{\alpha_{i,j}}$, où les f_j sont des polynômes avec au plus t monômes. Nous améliorons leur résultat avec le théorème 5.14 dont la preuve est basée sur propriétés du wronskien développées dans la section 1.

Lemme 5.13. *Soient M un ensemble de T monômes et $f_1,\ldots,f_s$ des polynômes dont les monômes sont dans M. Pour tout polynôme formel P en les s^2 variables $f_1,f_1',\ldots,f_1^{s-1},f_2,f_2',\ldots,f_s^{s-1}$ de degré d et d'ordre de dérivation e, le nombre de monômes dans x de $P(f_1,f_1',\ldots,f_s^{s-1})(x)$ est borné par $\binom{d+T-1}{T-1}$. Plus précisément, l'ensemble de ces monômes est inclus dans un ensemble $E_{d,e}$ de taille au plus $\binom{d+T-1}{T-1}$ qui ne dépend pas de P.*

Démonstration. Soit M^d l'ensemble des monômes qui sont des produits de d monômes de M non nécessairement distincts. Le cardinal de cet ensemble est borné par le cardinal de l'ensemble des multi-ensembles de taille d d'éléments dans M, c'est-à-dire $\binom{T+d-1}{T-1}$. Il est alors aisé de voir que nous pouvons choisir l'ensemble $E_{d,e}$ défini comme l'ensemble des monômes de $x^{-e}M^d$. Son cardinal est borné par la cardinalité de M^d. □

Théorème 5.14. *Soit* $f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$ *une fonction non identiquement nulle telle que* f_j *est un polynôme avec au plus* t *monômes et telle que* $a_i \in \mathbb{R}$ *et* $\alpha_{i,j} \in \mathbb{N}$. *Alors,* $Z_{\mathbb{R}}(f) \leq 4ktm + 4\left(\mathrm{e}(1+t)\right)^{\frac{mk^2}{2}} = O(t^{\frac{mk^2}{2}})$.

De plus, si I *est un intervalle réel tel que pour tout* j, $f_j(I) \subseteq]0, +\infty[$ *(ce qui assure que* f *est définie sur* I*), alors le résultat est encore vrai pour des exposants réels (possiblement négatifs)* $\alpha_{i,j}$, *c'est-à-dire* $Z_I(f) \leq 4ktm + 4\left(\mathrm{e}(1+t)\right)^{\frac{mk^2}{2}}$.

Démonstration. Soit N un entier tel que pour tout i et tout j nous ayons $\alpha_{i,j} + N > 0$. Considérons $\tilde{f} = \sum_{i=1}^{k} a_i g_i$ où $g_i = \prod_{j=1}^{m} f_j^{\alpha_{i,j}+N+k}$. Remarquons que $\tilde{f} = f \cdot \prod_{j=1}^{m} f_j^{N+k}$. Nous allons borner le nombre de zéros de $\tilde{f}$. Dans les deux cas (si les $\alpha_{i,j}$ sont entiers ou des nombres réels) les fonctions g_i sont analytiques sur I. De plus, nous pouvons supposer sans perdre de généralité que la famille (g_i) est linéairement indépendante. Effectivement, si ce n'est pas le cas, nous pouvons considérer une base de la famille (g_i) et écrire $\tilde{f}$ dans cette base. Ensuite, nous pouvons aussi supposer que tous les a_i sont non nuls, sinon, nous pouvons juste enlever ces termes de la somme. Nous voulons borner le nombre de zéros de $W(g_1, \ldots, g_s)$ pour tout $s \leq k$ pour pouvoir conclure en utilisant le théorème 5.9. Nous savons que pour $1 \leq u, v \leq s$

$$g_u^{(v-1)} = \sum_{\substack{r_1, r_2, \ldots, r_m \\ r_1 + \ldots + r_m = v-1}} \prod_{j=1}^{m} \left(f_j^{\alpha_{u,j}+N+k} \right)^{(r_j)}.$$

Utilisons maintenant le lemme 5.12 et simplifions les notations en écrivant $\beta_{u,j,s}$ au lieu de $\beta_{\alpha_{u,j}+N+k,s}$.

$$\begin{aligned} g_u^{(v-1)} &= \sum_{\substack{r_1, r_2, \ldots, r_m \\ r_1 + \ldots + r_m = v-1}} \prod_{j=1}^{m} \left[\sum_{s \in \mathscr{S}_{r_j}} \beta_{u,j,s} f_j^{\alpha_{u,j}+N+k-|s|} \prod_{k=1}^{r_j} \left(f_j^{(k)} \right)^{s_k} \right] \\ &= \left(\prod_{j=1}^{m} f_j^{\alpha_{u,j}+N} \right) \left(\prod_{j=1}^{m} f_j^{k-v+1} \right) T_{u,v}\left((f_p^{(q-1)})_{1 \leq p,q \leq s} \right). \end{aligned} \tag{5.4}$$

avec :

$$T_{u,v}\left((f_p^{(q-1)})_{1 \leq p,q \leq s} \right) = \sum_{\substack{r_1, r_2, \ldots, r_m \\ r_1 + \ldots + r_m = v-1}} \prod_{j=1}^{m} \left[\sum_{s \in \mathscr{S}_{r_j}} \beta_{u,j,s} f_j^{v-1-|s|} \prod_{k=1}^{r_j} \left(f_j^{(k)} \right)^{s_k} \right].$$

Le polynôme $T_{u,v}$ est homogène de degré total $(v-1)m$ par rapport aux s^2 variables $\left(f_p^{(q-1)} \right)_{1 \leq p,q \leq s}$ et chacun de ses termes est d'ordre de dérivation $v-1$.

Alors, nous remarquons que dans (5.4), la première parenthèse ne dépend pas de v et que la seconde ne dépend pas de u. Nous obtenons :

$$W(g_1, \ldots, g_s) = \left(\prod_{i=1}^{s} \prod_{j=1}^{m} f_j^{\alpha_{i,j}+N+k-i+1} \right) \det\left(\left(T_{u,v}\left((f_p^{(q-1)})_{1 \leq p,q \leq s} \right) \right)_{u,v \leq s} \right).$$

Donc,

$$Z(W(g_1,\dots,g_s)) \leq \left(\sum_{j=1}^{m} Z(f_j)\right) + Z\left(\det\left(T_{u,v}\left((f_p^{(q-1)})_{1\leq p,q\leq s}\right)\right)\right). \tag{5.5}$$

Bornons maintenant le nombre de monômes en x de $\det(\mathrm{T_{u,v}})$. Nous avons vu que $T_{u,v}$ est un polynôme homogène de degré $(v-1)m$ par rapport aux s^2 variables $\left(f_p^{(q-1)}\right)_{1\leq p,q\leq s}$ et d'ordre de dérivation $v-1$. De plus, comme la famille (g_i) est linéairement indépendante et comme ces fonctions sont analytiques, le wronskien n'est pas identiquement nul (lemme 5.4). D'où $\det(\mathrm{T_{u,v}})$ est une combinaison linéaire, par rapport aux variables $\left(f_p^{(q-1)}\right)_{1\leq p,q\leq s}$, de monômes de degré exactement $\sum_{v=1}^{s}(v-1)m = m\binom{s}{2}$ et d'ordre de dérivation $\binom{s}{2}$. D'après le lemme 5.13, les monômes en x sont dans l'ensemble $E_{\binom{s}{2}m,\binom{s}{2}}$. Par conséquent le nombre de monômes en x de $\det(\mathrm{T_{u,v}})$ est borné par le cardinal de $E_{\binom{s}{2}m,\binom{s}{2}}$, c'est-à-dire par $\binom{m\binom{s}{2}+mt-1}{mt-1}$. L'estimation de la règle de Descartes (Lemma 5.1) donne

$$Z\left(\det_{u,v\leq s}(T_{u,v})\right) \leq 2\binom{m\binom{s}{2}+mt-1}{mt-1} - 1. \tag{5.6}$$

Nous avons maintenant tous les outils nécessaires pour prouver le théorème. Nous savons :

$$Z(f) \leq Z(\sum_{i=1}^{k} a_i g_i).$$

Par le théorème 5.9 :

$$Z(f) \leq k - 1 + 2\sum_{s=1}^{k} Z(W(g_1,\dots,g_s)).$$

Utilisant la formule (5.5) :

$$Z(f) \leq k-1+2k\left(\sum_{j=1}^{m} Z(f_j)\right) + 2\sum_{s=1}^{k} Z\left(\det_{u,v\leq s}\left(T_{u,v}\left((f_p^{(q-1)})_{p,q\leq s}\right)\right)\right).$$

Puis par la règle de Descartes $\sum_{j=1}^{m} Z(f_j) \leq (2t-1)m$. Nous pouvons alors appliquer (5.6) pour obtenir l'inégalité

$$Z(f) \leq k-1+2k(2t-1)m + 2\sum_{s=1}^{k}\left(2\binom{m\binom{s}{2}+mt-1}{mt-1} - 1\right).$$

Finalement, nous utilisons la borne classique : $\binom{n}{k} \leq (en/k)^k$

$$\begin{aligned} Z(f) &\leq k-1+4ktm-2km-2k+4+4\sum_{s=2}^{k}\left(\mathrm{e}\left(1+\frac{mt-1}{m\binom{s}{2}}\right)\right)^{m\binom{s}{2}} \\ &\leq 4ktm + 4\left(\mathrm{e}(1+t)\right)^{\frac{mk^2}{2}}. \end{aligned}$$

□

En particulier nous avons déjà évoqué au chapitre 2 que dans le cas des circuits de profondeur bornée, des bornes inférieures exponentielles sont connues pour les circuits homogènes. Mais si on autorise les portes intermédiaires à calculer des polynômes de haut degrés, alors, à la connaissance de l'auteur, plus aucune borne non triviale n'est connue. Toutefois dans le cas du théorème précédent, si on choisit $m = 1$, on remarque que la borne obtenue ne dépend pas du degré entrant des portes d'exponentiation du niveau 3. En utilisant le corollaire 3.37, on obtient le résultat suivant :

Théorème 5.15. *Si* PERM_n *est calculé par un circuit de profondeur* 4 *de la forme*

$$\sum^{[k_n]} \bigwedge \sum^{[2^{n^{o(1)}}]} \prod$$

alors $k_n \geq n^{\Omega(1)}$.

Démonstration. D'après le corollaire 3.37, il existe un polynôme q et une projection D_n du circuit

$$\sum^{[k_{q(n)}]} \bigwedge \sum^{[2^{n^{o(1)}}]} \prod$$

tel que le polynôme $V_n(X)$ (défini au lemme 3.36) soit calculé par un circuit $D_n(Y_1, \ldots, Y_p)$ où les Y_i sont des puissances de X. Donc $V_n(X)$ est calculé par un circuit

$$\sum^{[k_{q(n)}]} \bigwedge \sum^{[2^{n^{o(1)}}]} \prod$$

Par le théorème 5.14,

$$Z_{\mathbb{R}}(V_n) = O\left(2^{\frac{n^{o(1)}k^2_{q(n)}}{2}}\right).$$

Or d'après le lemme 3.36, $Z_{\mathbb{R}}(V_n) = 2^n$. D'où, $k_n = n^{\Omega(1)}$. □

2.3 Applications à d'autres modèles

En utilisant des polynômes de petit degré au lieu des polynômes creux, le même argument implique une borne polynomiale.

Théorème 5.16. *Soit* $f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$ *où* f *est non nulle, les* f_j *sont de degré borné par* d *et telle que les* a_i *sont réels et les* $\alpha_{i,j}$ *sont des entiers. Alors* $Z_{\mathbb{R}}(f) \leq \frac{1}{3}k^3md + 2kmd + k \sim \frac{k^3md}{3}$.

De plus, si I *est un intervalle réel tel que pour tout* j, $f_j(I) \subseteq \mathbb{R}^{+\star\star}$ *(ce qui assure que* f *soit définie sur* I*), alors le résultat est encore avéré pour les exposants réels* $\alpha_{i,j}$, *i.e.* $Z_I(f) \leq \frac{1}{3}k^3md + 2kmd + k \sim \frac{k^3md}{3}$.

Démonstration. Dans la preuve du théorème 5.14, nous avons vu que $\det(T_{u,v})$ est un polynôme homogène de degré $m\binom{s}{2}$ en les s^2 variables $f_1, f_1', \ldots, f_s^{(s-1)}$. Donc, il est de degré $md\binom{s}{2}$ en la variable x. De plus, comme la famille (g_i) est linéairement indépendante et comme ces fonctions sont analytiques, le wronskien n'est pas identiquement nul (lemme 5.4). Dans l'équation (5.5), le premier terme est borné par md et le second par $md\binom{s}{2}$. D'après le théorème 5.9 [1], le nombre de zéros de $\sum_{i=1}^{k} a_i g_i$ est borné par $\left(\frac{1}{3}k^3md + 2kmd + k\right)$. □

Avendaño a étudié le cas $f = \sum_{i=1}^{k} x^{\alpha_i}(ax+b)^{\beta_i}$ où α_i et β_i sont des entiers [8]. Il a trouvé une borne supérieure linéaire en k pour le nombre de racines. Mais il a aussi montré que sa borne était fausse dans le cas des exposants réels. Nous obtenons ici une borne polynomiale qui marche aussi pour les puissances réelles.

Corollaire 5.17. *Soient $f = \sum_{i=1}^{k} c_i x^{\alpha_i}(ax+b)^{\beta_i}$ et I l'intervalle $\{x \in \mathbb{R} \mid x > 0 \wedge ax + b > 0\}$. Alors $Z_I(f) \leq \frac{2}{3}k^3 + 5k$.*

Li, Rojas et Wang [70] (Lemme 2) ont montré que les polynômes

$$f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m} (c_j X + d_j)^{\alpha_{i,j}}$$

où les coefficients a_i, b_j, c_j et les exposants $\alpha_{i,j}$ sont réels, ont au plus $m + m^2 + \ldots + m^{k-1}$ zéros. Notre résultat améliore cette borne :

Corollaire 5.18. *Soit $f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m}(c_j x + d_j)^{\alpha_{i,j}}$ où les coefficients a_i,c_j, d_j et les exposants $\alpha_{i,j}$ sont des nombres réels. Sur l'intervalle $I = \{x \in \mathbb{R} \mid \forall j, c_j x + d_j > 0\}$ nous avons $Z_I(f) = O(mk^3)$.*

Un autre corollaire a été suggéré par Maurice Rojas. Dans [70], Li, Rojas et Wang bornent, quand il est fini, le nombre d'intersections entre une courbe trinomiale et une courbe t-creuse par $2^t - 2$. Nous améliorons ici leur résultat. L'idée principale est d'effectuer un changement de variables et de se ramener au cas où f est affine. Cela pourrait introduire des exposants rationnels, même si le système original n'a que des coefficients entiers.

Corollaire 5.19. *Soient f un trinôme bivarié non nul et g un polynôme bivarié t-creux. Alors le nombre d'intersections dans le quadrant strictement positif entre ces deux courbes est infini ou borné par $\frac{2}{3}t^3 + 5t$.*

Finalement, le résultat tient encore si les exposants de f et de g sont réels.

Démonstration. Soient $f(X,Y) = c_1X^{\gamma_1}Y^{\delta_1} + c_2X^{\gamma_2}Y^{\delta_2} + c_3X^{\gamma_3}Y^{\delta_3}$ (avec $c_3 \neq 0$) et $g(X,Y) = \sum_{i=1}^{t} a_i X^{\alpha_i}Y^{\beta_i}$. Sur $(\mathbb{R}^{+\star})^2$, les zéros de f sont les mêmes que les zéros de $c_1 + c_2X^{\gamma_2-\gamma_1}Y^{\delta_2-\delta_1} + c_3X^{\gamma_3-\gamma_1}Y^{\delta_3-\delta_1}$. Alors, nous pouvons et nous supposerons que $\gamma_1 = \delta_1 = 0$.

— Premier cas : il existe $r \in \mathbb{R}^\star$ tel que $(\gamma_3, \delta_3) = r \cdot (\gamma_2, \delta_2)$. Dans ce cas, nous pouvons définir $A = X^{\gamma_2}Y^{\delta_2}$. Alors sur $\mathbb{R}^{+\star}$:

$$f = 0 \Leftrightarrow c_1 + c_2A + c_3A^r = 0.$$

1. Utiliser le théorème 5.7 au lieu du théorème 5.9 multiplierait notre borne par un facteur $O(k)$.

Par la règle des signes de Descartes (lemme 5.1) : la dernière équation a au plus deux racines réelles strictement positives que l'on notera s_1 et s_2. Donc le système est équivalent au système suivant :

$$\begin{cases} Y = \left(\frac{s_1}{X^{\gamma_2}}\right)^{\frac{1}{\delta_2}} \text{ ou } Y = \left(\frac{s_2}{X^{\gamma_2}}\right)^{\frac{1}{\delta_2}} \\ g(X,Y) = 0. \end{cases}$$

Nous obtenons

$$g(X,Y) = \sum_{i=1}^{t} a_i s_1^{\frac{\beta_i}{\delta_2}} X^{\alpha_i - \frac{\beta_i\gamma_2}{\delta_2}} \text{ ou } \sum_{i=1}^{t} a_i s_2^{\frac{\beta_i}{\delta_2}} X^{\alpha_i - \frac{\beta_i\gamma_2}{\delta_2}}.$$

De nouveau par le lemme 5.1, le nombre de solutions strictement positives est infini ou borné par $2t - 2 \leq \frac{2}{3}t^3 + 5t$.

— Second cas : la famille $((\gamma_2, \delta_2), (\gamma_3, \delta_3))$ est linéairement indépendante. Nous pouvons définir $A = X^{\gamma_2}Y^{\delta_2}$ et $B = X^{\gamma_3}Y^{\delta_3}$, alors sur $\mathbb{R}^{+\star}$:

$$\begin{aligned} f = 0 &\Leftrightarrow c_1 + c_2 A + c_3 B = 0 \\ &\Leftrightarrow B = -\frac{c_1}{c_3} - \frac{c_2}{c_3} A. \end{aligned}$$

Définissons $\Delta = \det \begin{vmatrix} \gamma_2 & \gamma_3 \\ \delta_2 & \delta_3 \end{vmatrix} \neq 0$. Alors $X = A^{\frac{\delta_3}{\Delta}} B^{-\frac{\delta_2}{\Delta}}$ et $Y = A^{-\frac{\gamma_3}{\Delta}} B^{\frac{\gamma_2}{\Delta}}$. Donc,

$$g(X,Y) = 0 \Leftrightarrow \sum_{i=1}^{t} a_i A^{\frac{\alpha_i\delta_3 - \beta_i\gamma_3}{\Delta}} B^{\frac{-\alpha_i\delta_2 + \beta_i\gamma_2}{\Delta}} = 0.$$

Le nombre de solutions correspond au nombre de racines du polynôme :

$$\sum_{i=1}^{t} a_i A^{\frac{\alpha_i\delta_3 - \beta_i\gamma_3}{\Delta}} \left(-\frac{c_1}{c_3} - \frac{c_2}{c_3} A\right)^{\frac{-\alpha_i\delta_2 + \beta_i\gamma_2}{\Delta}} = 0.$$

Par le corollaire 5.17, le nombre de racines strictement positives est infini (si le polynôme est identiquement nul) ou borné par $\frac{2}{3}t^3 + 5t$.

□

3 Algorithmes pour le test d'identité polynomiale

Un algorithme PIT (en anglais "Polynomial Identity Testing") prend un polynôme en entrée et décide si le polynôme est identiquement nul ou non. Il existe deux formes classiques de ces algorithmes : "à boîte noire" ou "à boîte blanche". Pour la première, l'entrée est donnée par une boîte noire, ie. un oracle d'évaluation du polynôme. Si on interroge l'oracle en un point x, l'oracle renvoie l'évaluation du polynôme en ce point x. Pour la deuxième version, l'entrée est donnée sous la forme d'un circuit calculant ce polynôme. Ces deux types d'algorithmes sont non comparables dans notre cas, car si nous avons un circuit, il n'est pas toujours possible d'évaluer facilement la

valeur du polynôme en un point puisque le circuit pourrait nécessiter des calculs d'évaluation de polynômes de très haut degré.

Le problème du PIT est un problème qui a été très étudié. Le lemme de Schwartz-Zippel [105] assure un algorithme probabiliste pour ce problème, mais l'existence d'un algorithme déterministe efficace est un problème ouvert célèbre. De nombreux liens entre les bornes inférieures pour les circuits et les algorithmes déterministes pour le PIT ont été découverts. Ce fut tout d'abord grâce aux travaux d'Heintz et Schnorr en 1980 [47], puis plus récemment par ceux de Kabanets et Impagliazzo [52], d'Aaronson et van Melkebeek [1] et d'Agrawal [2]. Aujourd'hui, de nombreux algorithmes ont été trouvé pour des familles particulières (cf. par exemple, les deux articles de synthèse [3, 90]). En particulier, un algorithme déterministe pour le PIT pour les polynômes de la forme (5.1) a déjà été donné dans [38]. Leur algorithme est polynomial en t, exponentiel en m et double-exponentiel en k tandis notre nouvel algorithme est seulement exponentiel en k.

3.1 Algorithmes PIT à boîte noire

En fait pour cette version du problème, la complexité des algorithmes est traditionnellement mesurée en nombre d'appels à l'oracle. L'idée étant que lorsqu'au cours de l'exécution, l'oracle retourne une valeur non nulle, celà signifie que le polynôme est non identiquement nul et l'algorithme principal peut terminer. De plus, tant que cela ne s'est pas passé, l'algorithme déterministe n'aura aucune information et effectuera les mêmes appels à toutes ses exécutions. L'algorithme se réduit alors à une liste de points pour lesquels il interroge l'oracle. L'algorithme retourne alors "vrai" (polynôme identiquement nul) si et seulement si l'oracle répond toujours "zéro" (l'évaluation du polynôme en chacun des points de la liste est nulle).

Les bornes sur les racines réelles du théorème 5.15 donnent immédiatement un algorithme PIT à boîte noire pour certaines familles de polynômes.

Corollaire 5.20. *Soit $f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$ une fonction telle que f_j est un polynôme avec au plus t monômes et telle que $a_i \in \mathbb{R}$ et $\alpha_{i,j} \in \mathbb{N}$. Alors, il existe un algorithme PIT à boîte noire utilisant seulement $1+4ktm+4\left(e(1+t)\right)^{\frac{mk^2}{2}}$ requêtes.*

Démonstration. Nous considérons l'algorithme qui teste si le polynôme retourne zéro sur les $1+4ktm+4\left(e(1+t)\right)^{\frac{mk^2}{2}}$ premiers entiers. Par le théorème 5.14, cet ensemble est un "hitting set", c'est-à-dire que si le polynôme est non nul, alors au moins un de ces entiers ne sera pas une racine du polynôme. □

Corollaire 5.21. *Soit $f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$ tel que les f_j sont de degré borné par d, les a_i sont des réels et tel que les $\alpha_{i,j}$ sont des entiers. Alors, il existe un algorithme PIT à boîte noire qui effectue seulement $1 + \frac{1}{3}k^3md + 2kmd + k$ appels à l'oracle.*

Démonstration. Le théorème 5.16 implique que tout ensemble de points de taille au moins $1 + \frac{1}{3}k^3md + 2kmd + k$ est un "hitting set" pour tout polynôme du type $\sum_{i=1}^{k} a_i \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$. □

3.2 Un algorithme PIT à boîte blanche

Les résultats pour les boîtes blanches sont plus compliqués. Ils sont basés sur le lien entre les wronskiens et la dépendance linéaire. Dans cette section, nous allons prouver la proposition suivante :

Proposition 5.22. *Soit $f = \sum_{i=1}^{k} a_i \prod_{j=1}^{m} f_j^{\alpha_{i,j}}$ où f_j est un polynôme avec au plus t monômes, les a_i sont des entiers et les $\alpha_{i,j}$ sont des entiers positifs. Soit C une borne supérieure sur les degrés des f_j, sur la taille en bits de leurs coefficients aussi bien que sur la taille en bits des coefficients a_i et des exposants $\alpha_{i,j}$. Alors, il existe un algorithme PIT à boîte blanche qui décide si f est nulle en temps $\tilde{O}\left(C2^{4mk^2 \log t}\right)$.*

Nous utiliserons effectivement dans la suite de cette section la notation $f(n) = \tilde{O}(g(n))$. C'est un raccourci pour $f(n) = O(g(n) \log^k g(n))$ avec k une constante.

Tout d'abord, nous aurons besoin d'un algorithme pour tester si des wronskiens sont identiquement nuls ou pas. Décrivons un algorithme qui prend comme entrée les fonctions $h_1 = \prod_{j=1}^{m} (f_j)^{\alpha_{1,j}}, \ldots, h_l = \prod_{j=1}^{m} (f_j)^{\alpha_{l,j}}$ (données par les suites $(f_j)_{1 \leq j \leq m}$ et $(\alpha_{i,j})_{1 \leq i \leq l, 1 \leq j \leq m}$) et qui renvoie le coefficient dominant du wronskien $W(h_1, \ldots, h_l)$ si le déterminant n'est pas identiquement nul, et qui renvoie zéro sinon.

Proposition 5.23. *Il existe un algorithme qui sur l'entrée $(f_j)_{j \leq m}$, $(\alpha_{i,j})_{i \leq l, j \leq m}$ renvoie le coefficient dominant du wronskien des fonctions*

$$\left(\prod_{j=1}^{m} (f_j)^{\alpha_{1,j}}, \ldots, \prod_{j=1}^{m} (f_j)^{\alpha_{l,j}} \right)$$

si le wronskien est non identiquement nul et qui renvoie zéro sinon. De plus, cet algorithme s'exécute en temps $\tilde{O}\left(C2^{4ml^2 \log t}\right)$.

Démonstration. Comme dans la preuve du théorème 5.14, nous calculons en fait le wronskien de $(g_1, \ldots, g_l)$ où $g_i = \prod_{j=1}^{m} (f_j)^{\alpha_{i,j}+l}$. Pour obtenir le coefficient dominant correct, il suffit de remarquer que

$$W(g_1, \ldots, g_l) = W(h_1, \ldots, h_l) \prod_{j=1}^{m} (f_j)^{l^2}.$$

Ainsi, nous voulons calculer le wronskien de $(g_1, \ldots, g_l)$. De nouveau comme dans la preuve du théorème 5.14, nous factorisons chaque colonne u par $\prod_{j=1}^{m} (f_j)^{\alpha_{u,j}}$ et chaque ligne v par $\prod_{j=1}^{m} (f_j)^{l-v+1}$. Nous noterons la matrice obtenue M. Les entrées de cette matrice sont des polynômes.

Selon le lemme 5.26 à la sous-section 3.3, nous pouvons calculer les polynômes développés dans une case (u, v) de la matrice M en temps $\tilde{O}\left(2^{vm} t^{mv} v^m C \log l\right)$.

Alors, calculer toutes les entrées de la matrice, qui est de taille $(l \times l)$ nécessite $\tilde{O}\left(2^{lm} t^{ml} l^m C\right)$ opérations. Ensuite, nous calculons le déterminant de cette matrice. Nous allons le calculer directement en le développant comme une somme de $l!$ produits. Ce calcul dure $\tilde{O}\left(C2^{4ml^2 \log t}\right)$ d'après le lemme 5.27 toujours en sous-section 3.3.

Si le déterminant est zéro, cela signifie que le déterminant est nul, et l'algorithme doit retourner zéro. Autrement, pour calculer le coefficient dominant, il suffit de multiplier le coefficient obtenu par le coefficient dominant de

$$\frac{\left(\prod_{u=1}^{l}\prod_{j=1}^{m}(f_j)^{\alpha_{u,j}}\right)\left(\prod_{v=1}^{l}\prod_{j=1}^{m}(f_j)^{l-v+1}\right)}{\prod_{j=1}^{m}(f_j)^{l^2}}.$$

Cette opération requiert seulement $\tilde{O}\left(Cml(C+l)\right)$ opérations puisqu'il est possible de calculer le produit de n entiers de taille s en temps $\tilde{O}(ns)$. □

Ensuite, nous aurons aussi besoin de l'algorithme suivant : si $W(h_1,\ldots,h_l)\neq 0$ et $W(h_1,\ldots,h_{l+1})=0$ alors l'algorithme trouve $a_1,\ldots,a_{l+1}$ tels que $a_1h_1+\ldots+a_lh_l=h_{l+1}$ (ces constantes existent d'après le lemme 5.4). Donc pour tout $i\in\mathbb{N}$, $a_1h_1^{(i)}+\ldots+a_lh_l^{(i)}=h_{l+1}^{(i)}$. Nous pouvons calculer les a_j en utilisant la formule de Cramer. Comme résultat, pour chaque $1\leq j\leq l$ nous avons :

$$\begin{aligned}a_j=&\frac{\begin{vmatrix} h_1 & \cdots & h_{j-1} & h_{l+1} & h_{j+1} & \cdots & h_l\\ h_1' & \cdots & h_{j-1}' & h_{l+1}' & h_{j+1}' & \cdots & h_l'\\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots\\ h_1^{(l-1)} & \cdots & h_{j-1}^{(l-1)} & h_{l+1}^{(l-1)} & h_{j+1}^{(l-1)} & \cdots & h_l^{(l-1)}\end{vmatrix}}{W(h_1,\ldots,h_l)}\\ =&\frac{lc\left(W(h_1,\ldots,h_{j-1},h_{l+1},h_{j+1},\ldots,h_l)\right)}{lc\left(W(h_1,\ldots,h_l)\right)}\end{aligned}$$

où $lc(W(h_1,\ldots,h_l))$ est le coefficient dominant du polynôme obtenu par le wronskien de la famille $(h_1,\ldots,h_l)$. Le précédent algorithme (Proposition 5.23) calcule ces coefficients, donc nous pouvons calculer les (a_j) en temps $\tilde{O}\left(C2^{4ml^2\log t}\right)$.

Finalement, à l'aide ces algorithmes, il suffit de considérer les fonctions allant de a_1h_1 jusqu'à $a_1h_1+\ldots+a_kh_k$. À chaque fois que l'on rajoute un h_i, soit il est linéairement indépendant et on l'ajoute à la base courante, soit il est linéairement dépendant, et nous pouvons l'exprimer dans la base actuelle. À la fin, $a_1h_1+\ldots+a_kh_k$ est exprimé comme une combinaison linéaire de fonctions de la base. Il suffit alors de vérifier si tous les coefficients sont identiquement nuls ou non. Cela complète la preuve de la proposition 5.22.

3.3 Deux lemmes techniques

Dans cette section, nous prouvons les deux lemmes (5.26 et 5.27) utilisés dans la preuve de la proposition 5.23. Ces preuves sont élémentaires mais quelque peu techniques.

Dans la suite, nous calculerons les additions de n entiers de taille s en temps $O(n(s+\log n))$ et les produits de n entiers de taille s en temps $\tilde{O}(ns)$.

Commençons par borner la complexité du développement des produits de polynômes creux.

Lemme 5.24. *Considérons un produit de μ polynômes τ-creux $P_1,\ldots,P_\mu$ où les degrés ainsi que la taille des coefficients en bits sont bornés par γ. Ce produit peut*

être développé en temps $\tilde{O}(\tau^\mu \gamma)$. *De plus, la taille des nouveaux coefficients est borné par* $\mu\gamma + \mu \log \tau$.

Démonstration. Pour développer un tel produit, nous allons calculer un par un, chaque monôme de la somme puis nous conserverons les coefficients des ces τ^μ nouveaux monômes. Pour calculer un coefficient, il y a trois choses à faire. Premièrement, il faut calculer son degré (somme de μ entiers de taille γ) en temps $O(\mu(\gamma + \log \mu))$, puis son coefficient (produit de μ entiers de taille γ) en temps $\tilde{O}(\mu\gamma)$ et enfin additioner le nouveau coefficient à la somme, enregistrée, de ceux correspondant aux monômes du même exposant. À la fin, au plus τ^μ coefficients seront ajoutés ensemble pour former un monôme particulier, donc la taille du coefficient est bornée par $\mu\gamma + \mu \log \tau$. Donc, comme nous ajoutons les coefficients un par un, à chaque étape, il faut additioner un entier de taille $\mu\gamma$ avec un de taille au plus $\mu\gamma + \mu \log \tau$. Chaque terme de la somme nécessite un temps

$$\begin{aligned}&\tilde{O}(\mu(\gamma + \log \mu) + \mu\gamma + (\mu\gamma + \mu \log \tau))\\ &= \tilde{O}(\mu\gamma + \mu \log(\mu\tau)).\end{aligned}$$

Donc, calculer tous les coefficients dure

$$\begin{aligned}&\tilde{O}(\tau^\mu(\mu\gamma + \mu \log(\mu\tau)))\\ &= \tilde{O}(\tau^\mu \gamma).\end{aligned}$$

□

Le théorème 5.14 utilise certaines constantes $\beta_{\alpha,s}$ qui ont été définies dans le lemme 5.12. Nous aurons besoin de les calculer.

Lemme 5.25. *Pour tout* p *dans* $\mathbb{N}$, *nous avons* $|\mathscr{S}_p| \leq 2^{p-1}$. *Pour tout* α, p *dans* $\mathbb{N}$ *et pour tout* s *dans* $\mathscr{S}_p$, $0 \leq \beta_{\alpha,s} \leq (p^2 + \alpha)^p$.

De plus, pour tous α, p *dans* $\mathbb{N}$ *nous pouvons calculer tous les* $\beta_{\alpha,s}$ *où* $s \in \mathscr{S}_q$ *et* $q \leq p$ *en temps* $\tilde{O}(2^p \log \alpha)$.

Démonstration. Nous avons montré dans la preuve du lemme 5.12 que $\beta_{\alpha,(1,0,0,\dots)} = \alpha$ et si $s \in \mathscr{S}_p$ avec $p \neq 1$, alors

$$\begin{aligned}\beta_{\alpha,s} = \mathbb{1}_{s_1 \neq 0}(\alpha - |s| + 1)\beta_{\alpha,(s_1-1,s_2,s_3,\dots)}\\ + \sum_{\substack{j\,:\,2\leq j\leq p\\ s_j \neq 0}} (s_{j-1} + 1)\beta_{\alpha,(s_1,\dots,s_{j-1},s_{j-1}+1,s_j-1,s_{j+1},\dots)}.\end{aligned} \tag{5.7}$$

Toutefois, dans la formule ci-dessus, les suites

$$(s_1 - 1, s_2, s_3, \dots) \text{ et } (s_1, \dots, s_{j-1}, s_{j-1} + 1, s_j - 1, s_{j+1}, \dots)$$

tombent dans $\mathscr{S}_{p-1}$. Notons $M_{\alpha,p} = \max_{s \in \mathscr{S}_p} |\beta_{\alpha,s}|$. Donc, si $p \neq 1$, (5.7) implique,

$$M_{\alpha,p} \leq (p^2 + \alpha) M_{\alpha,p-1}.$$

Comme, $M_{\alpha,1} = \alpha$, nous obtenons par récurrence $\beta_{\alpha,s} \leq (p^2 + \alpha)^{p-1}\alpha$.

Pour calculer ces constantes, remarquons que

$$\begin{aligned}|\mathscr{S}_{p+1}| &= |\{s \in \mathscr{S}_{p+1} \mid s_1 \neq 0\}| + |\{s \in \mathscr{S}_{p+1} \mid s_1 = 0\}| \\ &\leq 2|\mathscr{S}_p|.\end{aligned}$$

L'inégalité provient des deux fonctions surjectives :

$$\begin{aligned}\mathscr{S}_p &\to \{s \in \mathscr{S}_{p+1} \mid s_1 \neq 0\} \\ s &\mapsto (s_1 + 1, s_2, \ldots)\end{aligned} \qquad \text{et} \qquad \begin{aligned}\mathscr{S}_p &\to \{s \in \mathscr{S}_{p+1} \mid s_1 = 0\} \\ s &\mapsto (0, s_2, \ldots, s_{s_1}, s_{1+s_1} + 1, s_{2+s_1}, \ldots).\end{aligned}$$

Ainsi, par récurrence, $|\mathscr{S}_p| \leq 2^{p-1}$ et $|\bigcup_p \mathscr{S}_p| = O(2^p)$. Alors, si $s \in \mathscr{S}_p$ est fixé, pour calculer $\beta_{\alpha,s}$ avec (5.7), il nous faut calculer p produits d'un entier de taille $p\log(p^2+\alpha)$ par un entier de taille $\log p$ ou $\log \alpha$ (en temps $\tilde{O}\left(p\log(p^2+\alpha)\right)$) ainsi qu'une somme de tous ces produits en temps $\tilde{O}\left(p^2\log(p^2+\alpha)\right)$. Finalement calculer toutes ces constantes en temps $\beta_{\alpha,s}$ avec $s \in \mathscr{S}_q$ et $q \leq p$ nécessite un temps $\tilde{O}(2^p p^2 \log(p^2+\alpha))$. Ceci prouve le lemme. □

Nous pouvons désormais prouver les deux lemmes intermédiaires de la proposition 5.23. Pour la suite, nous conserverons les notations de la proposition 5.23.

Lemme 5.26. *Calculer le polynôme développé d'une case (v,u) de la matrice M nécessite un temps $\tilde{O}\left(2^{vm}t^{mv}v^mC\log l\right)$. La taille des coefficients est bornée par $\tilde{O}\left(mvC\log tl\right)$ et celle des degrés est bornée par Cmv.*

Démonstration. Nous utiliserons aussi les notations du théorème 5.14. Chaque case (v,u) correspond au polynôme

$$\begin{aligned}T_{u,v}\left((f_p^{(q-1)})_{1\leq p,q\leq l}\right) &= \sum_{\substack{r_1,r_2,\ldots,r_m \\ r_1+\ldots+r_m=v-1}} \prod_{j=1}^{m}\left[\sum_{s\in\mathscr{S}_{r_j}} \beta_{u,j,s} f_j^{v-1-|s|}\prod_{k=1}^{r_j}\left(f_j^{(k)}\right)^{s_k}\right] \\ &= \sum_{\substack{r_1,r_2,\ldots,r_m \\ r_1+\ldots+r_m=v-1}} \sum_{\substack{s^1,s^2,\ldots,s^m \\ s^i\in\mathscr{S}_{r_i}}} \left[\left(\prod_{j=1}^{m}\beta_{u,j,s^j}\right)\left(\prod_{j=1}^{m} f_j^{v-1-|s^j|}\prod_{k=1}^{r_j}\left(f_j^{(k)}\right)^{(s^j)_k}\right)\right].\end{aligned}$$

La première somme est de taille au plus v^m et la seconde est de taille bornée par 2^{vm} (lemme 5.25). Pour calculer un terme, nous devons tout d'abord calculer $\prod_{j=1}^m \beta_{u,j,s^j} = \prod_{j=1}^m \beta_{\alpha_{u,j}+l,s^j}$ qui est un produit de m entiers, chacun de taille $v\log(v^2+2^C+l)$ (car $\alpha \leq 2^C$). Cela peut être effectué en temps $\tilde{O}(mvC\log l)$.

Maintenant il ne reste plus qu'à développer la formule par rapport à x. Nous avons vu dans la preuve du théorème 5.14 que chaque monôme par rapport aux l^2 variables $\left(f_p^{(q-1)}\right)_{1\leq p,q\leq l}$ est de degré total $m(v-1)$. Considérons un monôme par rapport à $\left(f_p^{(q-1)}\right)_{1\leq p,q\leq l}$. Il s'agit d'un produit de $m(v-1)$ polynômes t-creux par rapport à la variable x. D'après le lemme 5.24, ce produit (la seconde parenthèse dans la formule) peut être développé en temps $\tilde{O}\left(t^{m(v-1)}C\right)$ et les coefficients sont de taille $Cm(v-1)+m(v-1)\log t$. Alors chaque coefficient est premièrement, multiplié par le coefficient correspondant $\prod_{j=1}^m \beta_{u,j,s^j}$ en temps

$$\begin{aligned}&\tilde{O}\left(\max\{Cm(v-1)+m(v-1)\log t, mv\log(v^2+2^C+l)\}\right) \\ &= \tilde{O}\left(mvC\log tl\right),\end{aligned}$$

ce qui donne un entier de taille au plus $\tilde{O}(mvC \log tl)$. Puis, il est additionné au coefficient préalablement enregistré correspondant au même monôme en temps

$$\begin{aligned}&\tilde{O}(mvC \log tl + \log(v^m 2^{vm}))\\ &= \tilde{O}(mvC \log tl).\end{aligned}$$

Pour conclure, calculer la case prend un temps

$$\begin{aligned}&\tilde{O}\left(v^m 2^{vm}\left(mvC \log l + \left(t^{m(v-1)}C + t^{m(v-1)}(mvC \log tl + mvC \log tl)\right)\right)\right)\\ &= \tilde{O}\left(2^{vm} v^m t^{m(v-1)} C \log l)\right).\end{aligned}$$

Ce qui complète la preuve du lemme. □

Lemme 5.27. *Supposons que les entrées de M sont données de manière développée (ie, comme une liste de monômes). Calculer le déterminant de M peut se faire en temps $\tilde{O}\left(C 2^{4ml^2 \log t}\right)$.*

Démonstration. Pour chacune des $(l!)$ permutations, nous développerons le polynôme correspondant. Chaque case a au plus $2^{ml} l^m t^{ml}$ monômes. Donc chaque permutation correspond à un produit de taille l de polynômes $\left(2^{ml} l^m t^{ml}\right)$-creux. Les exposants sont bornés par Cml et la taille des coefficients est bornée par $\tilde{O}(mlC \log t)$. D'après le lemme 5.24, chaque permutation peut être calculée en temps

$$\begin{aligned}&\tilde{O}\left(2^{ml^2} l^{ml} t^{ml^2} mlC \log t\right)\\ &= \tilde{O}\left(2^{3ml^2 \log t} C\right)\end{aligned}$$

et la taille des coefficients est bornée par

$$\begin{aligned}&\tilde{O}\left(ml^2 C \log t + l \log\left(2^{ml} l^m t^{ml}\right)\right)\\ &= \tilde{O}\left(ml^2 C \log t\right).\end{aligned}$$

Pour calculer le déterminant en entier, nous allons calculer les permutations une par une, rajoutant à chaque fois les nouveaux coefficients à celle calculée précédemment. Ce qui est fait en temps

$$\begin{aligned}&\tilde{O}\left(l^l\left(2^{3ml^2 \log t} C + 2^{ml^2} l^{ml} t^{ml^2} ml^2 C \log t\right)\right)\\ &= \tilde{O}\left(2^{4ml^2 \log t} C\right).\end{aligned}$$

□

4 Optimalité de la borne obtenue par les wronskiens

Rappelons que dans le théorème 5.7, il a été prouvé que

$$Z(a_1 f_1 + \ldots + a_k f_k) \leq (1 + |\Upsilon|)k$$

avec $\Upsilon = \bigcup_{1\leq i\leq k} Z\left(W(f_1,\ldots,f_i)\right)$. Il sera montré dans le théorème 5.31 que ce théorème est presque optimal dans le sens que pour des valeurs arbitrairement grandes de $|\Upsilon|$ et k, nous pouvons trouver des fonctions $f_1,\ldots,f_k$ et des coefficients $a_1,\ldots,a_k$ tels que

$$Z(a_1f_1+\ldots+a_kf_k)\geq(1+|\Upsilon|)(k-1).$$

Commençons avec un lemme technique.

Lemme 5.28. *Soit f un polynôme non-constant. Il existe pour $0\leq i\leq q$, des fonctions rationnelles $F_{i,q}$ telles qu'en notant $h_{p,i}$ les fonctions $\frac{p!}{(p-i)!}(f')^i f^{p-i}$ les propriétés suivantes sont vérifiées.*

1. *Pour tout $q\geq 0$, nous avons $F_{q,q}=1$.*
2. *Pour tout $0\leq i\leq q$, la fonction rationnelle $\left[(f')^q F_{i,q}\right]$ est un polynôme.*
3. *Pour tout $q\geq 0$ et pour tout $p\geq 1$ nous avons $(f^p)^{(q)}=\sum_{i=0}^{q} h_{p,i}F_{i,q}$.*

Le point principal est que les $F_{i,q}$ ne dépendent pas de p.

Démonstration. Nous définissons $F_{i,q}$ par récurrence sur q. Si $q=0$, posons $F_{0,0}=1$. Alors, nous avons bien $f^p=h_{p,0}$ et $\left[(f')^0F_{0,0}\right]=1$. Supposons maintenant que les $F_{i,q'}$ sont définis pour tous i, q' tels que $0\leq i\leq q'\leq q$. Posons $F_{i,q+1}$. Ainsi :

$$\begin{aligned}(h_{p,i})' &= \left[\frac{p!}{(p-i)!}(f')^i f^{p-i}\right]'\\ &= \frac{p!}{(p-i)!}\left[(p-i)(f')^{i+1}f^{p-i-1}+if''(f')^{i-1}f^{p-i}\right]\\ &= h_{p,i+1}+\left(i\frac{f''}{f'}\right)h_{p,i}.\end{aligned}$$

Donc,

$$\begin{aligned}(f^p)^{(q+1)} &= \left(\sum_{i=0}^{q} h_{p,i}F_{i,q}\right)'\\ &= \sum_{i=0}^{q}\left[h_{p,i}(F_{i,q})'+\left(h_{p,i+1}+\left(i\frac{f''}{f'}\right)h_{p,i}\right)F_{i,q}\right]\\ &= h_{p,0}(F_{0,q})'+\left[\sum_{i=1}^{q} h_{p,i}\left((F_{i,q})'+F_{i,q}\left(i\frac{f''}{f'}\right)+F_{i-1,q}\right)\right]\\ &\qquad\qquad +h_{p,q+1}F_{q,q}.\end{aligned}$$

Nous pouvons alors définir

$$\begin{aligned}&F_{0,q+1}=(F_{0,q})'\\ &\text{pour } 1\leq \mathrm{i}\leq \mathrm{q},\ \mathrm{F_{i,q+1}}=(\mathrm{F_{i,q}})'+\mathrm{F_{i,q}}\left(\mathrm{i}\frac{\mathrm{f''}}{\mathrm{f'}}\right)+\mathrm{F_{i-1,q}}\\ &\text{et } F_{q+1,q+1}=F_{q,q}=1.\end{aligned}$$

Par conséquent les propriétés (1) et (3) sont obtenues par construction. De plus, (2) est vérifiée car par hypothèse de récurrence :

$$(f')^{q+1}F'_{i,q} = [f'((f')^q F_{i,q})]' - (q+1)f'((f')^q F_{i,q})$$

est un polynôme. □

Nous allons montrer maintenant que les zéros de $W\left(f^{\alpha_1+k}, \ldots, f^{\alpha_s+k}(x)\right)$ sont soit les zéros de f, ou soit les zéros de f'.

Lemme 5.29. *Soient f une fonction analytique non constante sur un intervalle I et $\alpha_0, \ldots, \alpha_k$ k entiers deux-à-deux distincts (avec $k \geq 1$). Alors*

$$\left\{x \in I \mid \exists s \leq k,\, W\left(f^{\alpha_1+k}, \ldots, f^{\alpha_s+k}\right)(x) = 0\right\} \subseteq \{x \in I \mid (ff')(x) = 0\}.$$

Démonstration. Considérons $f^{\alpha_1+k}, \ldots, f^{\alpha_k+k}$. Pour commencer, nous pouvons supposer que cette famille est linéairement dépendante. Cela signifie qu'il existe des constantes

$$(a_1, \ldots, a_k) \in \mathbb{R}^k \setminus \{(0, 0, \ldots, 0)\}$$

telles que

$$\sum_{i=1}^{k} a_i f^{\alpha_i+k} = 0 \text{ sur } I. \tag{5.8}$$

Mais les entiers $(\alpha_i + k)$ sont tous distincts donc le polynôme $P(Y) = \sum_{i=1}^{k} a_i Y^{\alpha_i+k}$ n'est pas nul. Donc $P(Y)$ a un nombre fini de racines. Par (5.8), Im(f) est inclus dans l'ensemble (fini) de racines de P. Cependant, comme f est continue, par le théorème des valeurs intermédiaires, Im(f) est un intervalle réel. D'où Im(f) est un singleton. Ce qui contredit l'hypothèse que f n'est pas constante. Ainsi, la famille est en fait linéairement indépendante.

Soit Δ la matrice définie par $\Delta_{i,j} = \left(f^{\alpha_i+k}\right)^{(j-1)}$. D'après le lemme 5.28, nous savons que $\Delta_{i,j} = \sum_{l=0}^{j-1} h_{\alpha_i+k,l}\, F_{l,j-1}$, ce qui donne en terme de produit de matrices :

$$\Delta = [h_{\alpha_i+k,l-1}]_{1\leq i,l\leq s} \left[F_{l-1,j-1}\mathbb{1}_{l\leq j}\right]_{1\leq l,j\leq s}.$$

La deuxième matrice dans le produit est une matrice triangulaire supérieure dont les entrées sur la diagonale principale sont 1. Son déterminant vaut donc 1. Alors,

$$\det\left((\Delta_{i,j})_{1\leq i,j\leq s}\right) = \det\left((h_{\alpha_i+k,j-1})_{1\leq i,j\leq s}\right).$$

Finalement, $h_{\alpha_i+k,j-1} = \frac{(\alpha_i+k)!}{(\alpha_i+k-j+1)!}\left[f^{\alpha_i}\right]\left[(f')^{j-1} f^{k-j+1}\right]$. La première parenthèse ne dépend pas de j et la seconde ne dépend pas de i. Par conséquent,

$$\det\left(h_{\alpha_i+k,j-1}\right) = \left[f^{\sum_{l=1}^{s}\alpha_l}\right]\left[(f')^{\binom{s}{2}} f^{(k-s+1)s+\binom{s}{2}}\right] \det\left(\frac{(\alpha_i+k)!}{(\alpha_i+k-j+1)!}\right).$$

Alors, pour tout x dans I :

$$\begin{aligned} &W\left(f^{\alpha_1+k}, \ldots, f^{\alpha_s+k}\right)(x) = 0 \Leftrightarrow \det\left(h_{\alpha_i+k,j-1}\right)(x) = 0 \\ &\Rightarrow \left\{f(x) = 0 \text{ ou } f'(x) = 0 \text{ ou } \det\left(\frac{(\alpha_i+k)!}{(\alpha_i+k-j+1)!}\right) = 0\right\}. \end{aligned} \tag{5.9}$$

Si $\det\left(\frac{(\alpha_i+k)!}{(\alpha_i+k-j+1)!}\right) = 0$, comme cela ne dépend pas de x, la fonction $\det\left(h_{\alpha_i+k,j-1}\right)$ s'annule pour tout x et ainsi le wronskien est zéro sur tout I. Mais comme les fonctions f^{α_i+k} sont analytiques, elles pourraient être linéairement dépendantes d'après le lemme 5.4. Ce qui contredit l'hypothèse. Par conséquent,

$$\left\{x \in I \mid \exists s \leq k,\, W\left(f^{\alpha_1+k}, \ldots, f^{\alpha_s+k}\right) = 0\right\} \subseteq \left\{x \in I \mid (ff')(x) = 0\right\}.$$

□

Comme corollaire, cela permet de reprouver l'estimation de Descartes (lemme 5.1). Soit $g = \sum_{i=1}^{k} a_i x_i^{\alpha_i}$. Nous avons besoin de montrer que le nombre de racines réelles distinctes est borné par $2k-1$. Nous pouvons utiliser le résultat du lemme 5.29 avec $f(x) = x$. Dans ce cas $g = \sum_{i=1}^{k} a_i x^{\alpha_i}$. Nous obtenons

$$\begin{aligned}\Upsilon = \left\{x \in I \mid \exists s \leq k,\, W\left(f^{\alpha_1+k}, \ldots, f^{\alpha_s+k}\right) = \{0\}\right\} &\subseteq \left\{x \in I \mid (ff')(x) = 0\right\} \\ &\subseteq \{0\}\end{aligned}$$

Le théorème 5.7 implique $Z(f) \leq 2k-1$. Une preuve similaire du lemme 3.5 apparaît dans [85] (Partie V, exercice 90).

Au sujet du lemme 5.29, il est possible de remarquer que la réciproque de l'implication (5.9) est avérée dès que f' apparaît réellement comme un facteur de $\det\left(\left(h_{\alpha_i+k,j-1}\right)_{1\leq i,j\leq s}\right)$. C'est le cas quand $\binom{s}{2}$ est différent de zéro, c'est-à-dire quand $s \geq 2$. Cela implique le résultat suivant.

Lemme 5.30. *Soient f une fonction analytique non constante sur un intervalle I et $\alpha_0, \ldots, \alpha_k$ k entiers deux à deux distincts où $k \geq 2$. Alors,*

$$\left\{x \in I \mid \exists s \leq k,\, W\left(f^{\alpha_1+k}, \ldots, f^{\alpha_s+k}\right)(x) = 0\right\} = \left\{x \in I \mid (ff')(x) = 0\right\}.$$

Nous avons maintenant tous les outils nécessaires pour nous attaquer au principal résultat de cette section, l'optimalité du théorème 5.7. Nous sommes en train de montrer l'optimalité du théorème 5.7 alors que nous avons remarqué à la fin de la sous-section 1.1 que la borne du théorème 5.9 est généralement meilleure et que la conjecture 5.10 est aussi plus générale. En fait, le théorème 5.7 est optimal dans le cas où les $W(f_1, \ldots, f_i)$ ont les mêmes zéros. Effectivement, dans la preuve du théorème 5.31, les racines de tous les $W(f_1, \ldots, f_i)$ sont incluses dans les zéros de $W(f_1, \ldots, f_k)$.

Théorème 5.31. *Soit $\Upsilon = \{x \in I \mid \exists i \leq k, W(f_1, \ldots, f_i)(x) = 0\}$ défini comme dans le théorème 5.7. Pour tout k et tout p, il existe une fonction $g = \sum_{i=1}^{k} a_i f^{\alpha_i}$ telle que les α_i sont des entiers strictement positifs, f est un polynôme tel que $|\Upsilon| \geq p$ et telle que g a au moins $(1 + |\Upsilon|)(k-1) + Z(f)$ zéros.*

Démonstration. Soit $h = x\prod_{i=1}^{k-1}(x^2 - i^2)$. Ce polynôme est k-creux et a au plus $2k-1$ racines réelles distinctes : $-k+1 < \ldots < -1 < 0 < 1 < k-1$.

Soit $f = k\prod_{i=1}^{1+\left\lceil\frac{p+1}{2}\right\rceil}(x-2i)$. Alors, il suffit de vérifier que $g = h \circ f$ possède les propriétés désirées.

Or $g(x) = 0$ si et seulement si $f(x) \in [-k+1, k-1] \cap \mathbb{Z}$. Mais quand y est impair, nous obtenons $|f(y)| > k-1$, et quand y est un entier pair compris entre 2

```
def g(x): return 0.15*(x-2)*(x-4)*(x-6)*(x-8)*(x-10)
```

```
plot(g(x),xmin=0,xmax=20,ymin=-1.5*g(3),ymax=1.5*g(3))
```

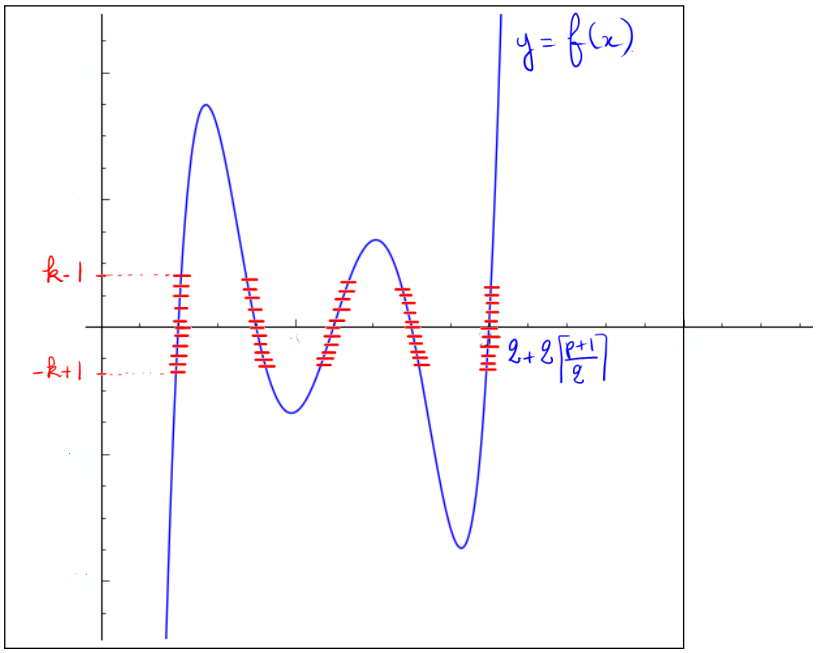


FIGURE 5.1 – racines de $g = h \circ f$ dans la preuve du théorème 5.31

et $2 + 2\left\lceil \frac{p+1}{2} \right\rceil$, nous obtenons $f(y) = 0$. Par le théorème des valeurs intermédiaires, g a au moins $k-1$ zéros sur chaque intervalle $(n, n+1)$ avec $1 \leq n \leq 2 + 2\left\lceil \frac{p+1}{2} \right\rceil$. Donc

$$\begin{aligned} Z(g) &= 2\left(1 + \left\lceil \frac{p+1}{2} \right\rceil\right)(k-1) + \left(1 + \left\lceil \frac{p+1}{2} \right\rceil\right) \\ &= (2k-1)\left(1 + \left\lceil \frac{p+1}{2} \right\rceil\right). \end{aligned} \tag{5.10}$$

1 sur 1 04/05/12 11:14

Le théorème de Rolle assure que pour deux racines de f, il existe une racine de f' qui soit strictement comprise entre les deux racines de f. Donc

$$Z(ff') \geq 2Z(f) - 1 = 1 + 2\left\lceil \frac{p+1}{2} \right\rceil.$$

Considérant le degré de ff', nous trouvons $Z(ff') = 1 + 2\left\lceil \frac{p+1}{2} \right\rceil$.

De plus, f n'est pas constante et donc par le lemme 5.30, $|\Upsilon| = Z(ff')$. D'où

$$|\Upsilon| = Z(ff') = 1 + 2\left\lceil \frac{p+1}{2} \right\rceil. \tag{5.11}$$

Nous pouvons vérifier que l'hypothèse $|\Upsilon| \geq p$ est vraie. Finalement, les équations (5.10) et (5.11) montrent que $Z(g) \geq (|\Upsilon| + 1)(k-1) + Z(f)$. □

Chapitre 6

Intersections entre une courbe creuse et une courbe de petit degré : le problème de Sevostyanov

La règle des signes de Descartes (lemme 3.5) assure que tout polynôme univarié réel avec $t \geq 1$ monômes a au plus $t-1$ racines réelles. En 1980, A. Khovanskiĭ [59] obtint une généralisation d'une portée considérable. Il montra qu'un système de n polynômes en n variables utilisant $l+n+1$ monômes distincts a moins que

$$2^{\binom{l+n}{2}}(n+1)^{l+n} \tag{6.1}$$

solutions non-dégénérées strictement positives. Comme celle de Descartes, cette borne ne dépend que du nombre de monômes des polynômes et pas de leurs degrés.

Dans cette théorie des "fewnomials" (l'expression a été introduite par Kushnirenko), Khovanskiĭ [59] obtint plusieurs résultats similaires, certains marchant pour des fonctions non-polynômiales. Dans le cas des polynômes, la borne de Khovanskiĭ a été améliorée par Bihan et Sottile [10]. Leur borne est

$$\frac{e^2+3}{4}2^{\binom{l}{2}}n^l. \tag{6.2}$$

Nous allons borner dans cette section (les résultats sont directement tirés de l'article [65]) le nombre de solutions réelles d'un système

$$F(X,Y) = G(X,Y) = 0 \tag{6.3}$$

de deux équations polynomiales en deux variables, où F est un polynôme de degré d et G a t monômes. Ce problème a une histoire intéressante [11, 69, 94]. Sevostyanov montra en 1978 que le nombre de solutions non-dégénérées peut être borné par une fonction $N(d,t)$ dépendant seulement de d et de t. Selon [94], ce résultat inspira Khovanskiĭ pour développer sa théorie des "fewnomials". Malheureusement Sevostyanov mourut jeune, et son résultat n'a jamais été publié. Aujourd'hui, il semblerait que la preuve de Sevostyanov ainsi même que la forme spécifique de sa borne aient disparues.

Les résultats de Khovanskiĭ (6.1), ou ceux de Bihan et Sottile (6.2), fournissent une borne sur $N(d,t)$ qui est exponentielle en d et t. La borne de Khovanskiĭ (6.1)

provient d'un résultat plus général sur des systèmes mixes (polynômes-exponentiels) (voir Section 1.2 de [59]). Ce dernier résultat permet d'obtenir une borne sur $N(d,t)$ qui est seulement exponentielle en t. Comme nous allons le voir, cette borne est loin d'être optimale.

Nous avons déjà évoqué au chapitre 5 que Li, Rojas et Wang [70] ont montré que le nombre de racines réelles est borné supérieurement par 2^t-2 quand F est un trinôme. Quand F est linéaire, Avendaño [8] obtint une meilleure borne $6t-4$. Le résultat de Li, Rojas et Wang [70] est en fait plus général : ils montrèrent que le nombre de solutions non-dégénérées strictement positives d'un système

$$F_1(X_1,\ldots,X_n)=F_2(X_1,\ldots,X_n)=\ldots=F_n(X_1,\ldots,X_n)=0$$

est au plus $n+n^2+\ldots+n^{t-1}$ lorsque chacun des polynômes $F_1,\ldots,F_{n-1}$ est un trinôme et que F_n a t termes.

Revenant au cas d'un système $F(X,Y)=G(X,Y)=0$ où F est un trinôme et G a t termes, nous avons montré au corollaire 5.19 une borne supérieure en $O(t^3)$ pour le nombre de racines réelles.

Dans ce chapitre tiré de l'article coécrit avec Koiran et Portier [65], nous allons nous intéresser au système de Sevostyanov (6.3). Le nombre de solutions réelles (s'il est fini) pour un tel système est borné par un polynôme en d et t. Plus précisément nous obtenons le théorème suivant :

Théorème 6.1. *Soit $F\in\mathbb{R}[X,Y]$ un polynôme bivarié non nul de degré d et soit $G\in\mathbb{R}[X,Y]$ un polynôme bivarié t-creux. L'ensemble des solutions réelles du système*

$$\begin{cases}F(X,Y)=0\\G(X,Y)=0\end{cases}$$

a un nombre de composantes connexes qui est $O(d^3t+d^2t^3)$.

Remarquons que notre borne fonctionne uniquement quand F est non nul. Comme mentionné à la section 2, le cas ou F est le polynôme nul est difficile. La raison est qu'un système de deux équations creuses peut être encodé dans un système à une seule équation creuse ! La question de savoir si, dans ce cas, le nombre de racines réelles peut être borné polynomialement est toujours ouverte.

Idée de la preuve

La preuve du théorème 6.1 est basée sur ce qui a été fait au chapitre 5. Il pourrait être utile de rappeler comment nous avons traité le cas $d=1$ (le corollaire 5.19 borne le nombre d'intersections réelles entre une courbe creuse et une ligne d'équation $Y=aX+b$). Pour cela, nous avons mis notre système sous la forme

$$\sum_{i=1}^{t}c_iX^{\alpha_i}(aX+b)^{\beta_i},$$

puis nous avons montré que pour borner le nombre de racines réelles d'une somme de fonctions analytiques, il suffisait de borner le nombre de racines des wronskiens de ces fonctions. Il s'agit du théorème 5.9 :

Théorème (Rappel du théorème 5.9)**.** *Soit I un intervalle ouvert de $\mathbb{R}$ et soient $f_1, \ldots, f_t : I \to \mathbb{R}$ une famille de fonctions analytiques qui sont linéairement indépendantes sur I. Pour $1 \leq i \leq t$, nous écrirons $W_i : I \to \mathbb{R}$ pour désigner le wronskien de $f_1, \ldots, f_i$. Alors,*

$$Z(f_1 + \ldots + f_t) \leq t - 1 + Z(W_t) + Z(W_{t-1}) + 2\sum_{j=1}^{t-2} Z(W_j)$$

où $Z(g)$ correspond au nombre de racines réelles distinctes d'une fonction $g : I \to \mathbb{R}$.

Supposons que pour un système $F(X, Y) = G(X, Y) = 0$, nous pouvons utiliser l'équation $F(X, Y) = 0$ pour exprimer Y comme une fonction (algébrique) de X. Alors, il suffit de borner le nombre de racines réelles d'un polynôme univarié de la forme

$$\sum_{i=1}^{t} c_i X^{\alpha_i} \phi(X)^{\beta_i},$$

ce qui correspond à une situation où l'on peut appliquer le théorème 5.9. Bien évidemment, transformer cette idée informelle en une véritable preuve nécessite un peu de soin. En particulier, la fonction algébrique ϕ n'est pas nécessairement définie sur la droite réelle entière et n'est pas non plus définie de manière unique. Pour résoudre ces problèmes, nous nous appuyerons sur la décomposition cylindrique algébrique introduite par Collins (voir Section 1.4). Nous aurons aussi besoin d'estimations quantitatives sur les dérivées de grand ordre d'une fonction algébrique ϕ car elles vont apparaître dans les wronskiens du théorème 5.9. Pour ces raisons, nous exprimons dans la section 1.2 les dérivées de ϕ en termes de ϕ et des dérivées partielles de F. Utilisant le théorème 5.9, nous pouvons finalement réduire le problème de Sevostyanov au cas d'un système où les deux polynômes ont un degré borné. Tous les ingrédients sont ensuite mis ensemble en section 2 pour obtenir la borne $O(d^3t+d^2t^3)$ sur le nombre de composantes connexes.

1 Outils techniques

Dans cette section, nous allons obtenir quelques résultats préliminaires nécessaires pour prouver le théorème 6.1.

1.1 Les dérivées d'une puissance

Nous rappelons brièvement, dans cette section, les résultats de la sous-section 2.1 du chapitre 5. Notons encore $\mathbb{N}^{(\mathbb{N})}$ l'ensemble des suites presque nulles d'entiers. Pour tout entier strictement positif p, posons $\mathcal{S}_p = \{(s_1, s_2, \ldots) \in \mathbb{N}^{(\mathbb{N})} \mid \sum_{i=1}^{\infty} i s_i = p\}$. De plus, pour tout p et tout $s = (s_1, s_2, \ldots) \in \mathbb{N}^{(\mathbb{N})}$, notons $|s| = \sum_{i=1}^{\infty} s_i$. Remémorrons-nous enfin le lemme 5.12.

Lemme 6.2 (Rappel du lemme 5.12)**.** *Soit p un entier strictement positif et $\alpha \geq p$ un nombre réel. Alors*

$$(f^\alpha)^{(p)} = \sum_{s \in \mathcal{S}_p} \left[\beta_{\alpha,s} f^{\alpha-|s|} \prod_{k=1}^{p} (f^{(k)})^{s_k} \right]$$

où les $(\beta_{\alpha,s})$ sont des constantes.

Ce lemme signifie juste que la dérivée p-ième d'une puissance α d'une fonction f est une combinaison linéaire de termes tels que chacun soit un produit de dérivées de f de degré total α et d'ordre total de dérivation p.

1.2 Les dérivées d'une fonction algébrique

Considérons un polynôme bivarié non-nul $F(X,Y) \in \mathbb{R}[X,Y]$ et un point (x_0, y_0) où $F(x_0, y^0) = 0$ et où la dérivée partielle $F_Y = \frac{\partial F}{\partial Y}$ ne s'annule pas. Par le théorème des fonctions implicites, dans un voisinage de (x_0, y_0), l'équation $F(X,Y) = 0$ est équivalente à une condition de la forme $y = \phi(x)$. La fonction implicite ϕ est définie sur un intervalle ouvert I contenant x_0, et est C^∞ (et même analytique). Dans cette section, nous exprimons les dérivées de ϕ en termes de ϕ et des dérivées partielles de F. Pour tous entiers a, b, nous noterons $F_{X^a Y^b} = \frac{\partial^{a+b}}{\partial X^a \partial Y^b} F(X,Y)$.

Lemme 6.3. *Pour tout $k \geq 1$, il existe un polynôme S_k de degré au plus $2k-1$ en $\binom{k+2}{2} - 1$ variables tel que*

$$\phi^{(k)}(x) = \frac{S_k(F_X(x,\phi(x)), \ldots, F_{X^a Y^b}(x,\phi(x)), \ldots)}{(F_Y(x,\phi(x)))^{2k-1}} \tag{6.4}$$

avec $1 \leq a+b \leq k$. Par conséquent le numérateur est un polynôme de degré total au plus $(2k-1)d$ en x et $\phi(x)$. De plus, S_k dépend seulement de k et F.

Démonstration. Pour tout k, posons $D_k(x) = \frac{\partial^k}{\partial x^k} F(x, \phi(x))$. Nous utiliserons un peu plus loin, le fait que $D_k(x)$ est la fonction identiquement nulle. Commençons par montrer par récurrence que pour tout $k \geq 1$,

$$D_k(x) = \phi^{(k)} F_Y + R_k(\phi'(x), \ldots, \phi^{(k-1)}(x), \ldots, F_{X^a Y^b}, \ldots)$$

où R_k est de degré total au plus 1 en $(F_{X^a Y^b})_{1 \leq a+b \leq k}$ et d'ordre de dérivation au plus k en les variables $(\phi^{(i)})_{1 \leq i \leq k}$.

Pour $k = 1$, nous obtenons immédiatement : $D_1 = \phi' F_Y + F_X$. Supposons maintenant que le résultat est vrai pour une certaine valeur de k, alors

$$\begin{aligned} D_{k+1} &= \phi^{(k+1)} F_Y + \phi^{(k)}(F_{XY} + F_{Y^2}\phi') + \frac{\partial}{\partial x} R_k\left(\phi', \ldots, \phi^{(k-1)}, F_{X^a Y^b}\right) \\ &= \phi^{(k+1)} F_Y + R_{k+1}\left(\phi', \ldots, \phi^{(k)}, F_{X^a Y^b}\right). \end{aligned}$$

De plus, R_{k+1} est de degré total au plus 1 en les variables $(F_{X^a Y^b})_{1 \leq a+b \leq k+1}$ et d'ordre de dérivation au plus $k+1$ en $\left(\phi^{(i)}\right)_{1 \leq i \leq k}$ (puisque R_k est d'ordre de dérivation au plus k en $\left(\phi^{(i)}\right)_{1 \leq i \leq k-1}$).

Comme $F(x, \phi(x))$ est la fonction nulle, on en déduit, pour tout $k \geq 1$, l'égalité $D_k(x) = \frac{\partial^k F(x,\phi(x))}{\partial x^k} = 0$. Donc

$$\phi^{(k)} = \frac{-R_k}{F_Y}.$$

Montrons maintenant pas récurrence sur k que pour tout $k \geq 1$, il existe un polynôme S_k de degré au plus $2k-1$ en $\left(\binom{k+2}{2} - 1\right)$ variables tel que l'équation (6.4) est vérifiée.

Le résultat est vrai pour $k = 1$ car $\phi' = \frac{-F_X}{F_Y}$. Soit $k \geq 1$ et supposons que le résultat est avéré pour tout i de sorte que $1 \leq i \leq k$. Nous savons $D_{k+1}(x) = \phi^{(k+1)} F_Y + R_{k+1}(\phi'(x), \ldots, \phi^{(k)}(x), \ldots, F_{X^a Y^b}, \ldots) = 0$. Donc,

$$\phi^{(k+1)} = \frac{-1}{F_Y} R_{k+1}(\phi'(x), \ldots, \phi^{(k)}(x), \ldots, F_{X^a Y^b}, \ldots).$$

Et, par hypothèse de récurrrence,

$$\phi^{(k+1)} = \frac{-1}{F_Y} R_{k+1}\left(\frac{S_1}{F_Y}, \ldots, \frac{S_k}{F_Y^{2k-1}}, \ldots, F_{X^a Y^b}, \ldots\right).$$

Comme $R_{k+1}(\phi'(x), \ldots, \phi^{(k)}(x), \ldots, F_{X^a Y^b}, \ldots)$ est d'ordre de dérivation $k+1$ sur ses k premières variables et est d'ordre total 1 sur ses $\left(\binom{k+2}{2} - 1\right)$ dernières variables, chaque monôme de la forme :

$$F_{X^a Y^b} \frac{S_{i_1}}{F_Y^{2i_1-1}} \cdots \frac{S_{i_p}}{F_Y^{2i_p-1}}$$

où $i_1 + \ldots + i_p \leq k+1$ et $p \geq 0$. Ainsi, nous obtenons :

$$\frac{F_{X^a Y^b} S_{i_1} \ldots S_{i_p}}{F_Y^{2i_1-1} \ldots F_Y^{2i_p-1}} = \frac{F_{X^a Y^b} S_{i_1} \ldots S_{i_p} F_Y^{2k-2i+p}}{F_Y^{2(k+1)-2}}$$

où $i = i_1 + \ldots + i_p \leq k+1$. Assurément, l'exposant $2k - 2i + p$ est un entier positif car si $p = 1$, alors $2i = 2i_1 \leq 2k$ et sinon, dans les autres cas $2i \leq 2(k+1) \leq 2k+p$. Le numérateur est un polynôme en les variables $F_{X^a Y^b}$ de degré

$$\begin{aligned}
&\leq 1 + d^\circ(S_{i_1}) + \ldots + d^\circ(S_{i_p}) + 2k - 2i + p \\
&\leq 1 + 2i_1 - 1 + \ldots + 2i_p - 1 + 2k - 2i + p \\
&\leq 1 + 2i - p + 2k - 2i + p \\
&\leq 2(k+1) - 1.
\end{aligned}$$

D'où, $\phi^{(k+1)}$ est de la forme :

$$\frac{S_{k+1}\left((F_{X^a Y^b})_{1 \leq a+b \leq k+1}\right)}{F_Y^{2(k+1)-1}}$$

avec S_{k+1} polynôme de degré au plus $2(k+1) - 1$. □

1.3 Versions réelles pour le théorème de Bézout

Le théorème de Bézout est un résultat fondamental en géométrie algébrique. On peut exprimer une version de ce résultat comme suit.

Théorème 6.4. *Considérons un corps algébriquement clos K et n polynômes $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$ de degrés $d_1, \ldots, d_n$. Si le système polynomial*

$$f_1 = f_2 = \cdots = f_n = 0$$

a un nombre fini de solutions dans K^n, ce nombre est borné supérieurement par $\prod_{i=1}^{n} d_i$.

La borne supérieure $\prod_{i=1}^{n} d_i$ peut ne pas marcher si K n'est pas algébriquement clos. En particulier, elle est incorrecte dans le cas du corps des nombres réels (voir e.g. chapitre 16 de [14] pour un contrexemple). Cependant, il existe beaucoup de travaux établissant des bornes similaires pour $K = \mathbb{R}$ (voir e.g. [9,14] et les références présentes). Par exemple, on peut trouver le résultat classique suivant.

Théorème 6.5 (Oleinik-Petrovski-Thom-Milnor)**.** *Soit $V \subseteq \mathbb{R}^n$ défini par un système $f_1 = 0, \ldots, f_p = 0$, où les f_i sont des polynômes réels de degré au plus d. Alors le nombre de composantes connexes de V est au plus $d(2d-1)^{n-1}$.*

Une preuve du théorème 6.5 peut être trouvée par exemple au chapitre 16 de l'article [14]. Dans la suite, nous utiliserons ce résultat aussi bien qu'une variation pour le cas $n = p = 2$ (voir le lemme 6.9 à la fin de cette sous-section). Le lemme 6.6 ci-dessous sera aussi utile dans la section 2. Voyons tout d'abord les preuves de ces deux lemmes.

Lemme 6.6. *Soit $g \in \mathbb{R}[X, Y]$ un polynôme non-nul de degré d. L'ensemble des zéros réels de g est l'union d'un ensemble d'au plus $d^2/4$ points et des ensembles des zéros des polynômes $g_1, \ldots, g_k \in \mathbb{R}[X, Y]$ qui divisent g et qui sont irréductibles dans $\mathbb{C}[X, Y]$.*

Démonstration. Factorisons g comme produit d'irréductibles dans $\mathbb{C}[X, Y]$. Ainsi

$$g = \lambda g_1^{\alpha_1} \cdots g_k^{\alpha_k} h_1^{\beta_1} \cdots h_l^{\beta_l} \overline{h_1}^{\beta_1} \cdots \overline{h_l}^{\beta_l}$$

où les polynômes g_j sont les facteurs dans $\mathbb{R}[X, Y]$, les polynômes $h_j, \overline{h_j}$ sont des conjugués complexes et λ est une constante réelle. Nous pouvons supposer qu'aucun des h_j n'est de la forme $h_j = \mu_j r_j$ avec $\mu_j \in \mathbb{C}$ et $r_j \in \mathbb{R}[X, Y]$: sinon, nous pouvons remplacer la paire $(h_j, \overline{h_j})$ par r_j^2 et la constante $\mu_j \overline{\mu_j}$ est absorbée par λ.

La supposition ci-dessus implique que les h_j (et leurs conjugués) ont un nombre fini de zéros. En fait, nommons p_j, q_j les parties réelles et imaginaires de h_j. Les solutions réelles de l'équation $h_j = 0$ sont les mêmes que celles du système $p_j = q_j = 0$. Ce système a un nombre fini de solutions car p_j et q_j sont non nuls et ne possèdent pas de facteur commun. Considérons un facteur présumé $f_j \in \mathbb{C}[X, Y]$ divisant p_j et q_j, de degré $\deg(f_j) \geq 1$. Comme f_j divise h_j et comme ce polynôme est irréductible, nous devons avoir $\deg(f_j) = \deg(h_j)$. Il en résulte que $\deg(p_j) = \deg(q_j) = \deg(f_j)$ et les deux premiers polynômes sont des multiples constants du troisième. En conlusion,

p_j ne diffère de q_j que d'un facteur multiplicatif constant, ce qui contredit notre supposition.

Par le théorème de Bézout, le système $p_j = q_j = 0$ a au plus $\deg(h_j)^2$ solutions complexes. Ce qui est aussi une borne supérieure pour le nombre de racines réelles du polynôme h_j. Le polynôme $\overline{h_j}$ a les mêmes racines réelles. Mis tous ensembles, les polynômes h_j et $\overline{h_j}$ ont au plus $\sum_{j=1}^{l} \deg(h_j)^2 \leq (d/2)^2$ racines réelles. □

Un intérêt de cette proposition est que comme chaque g_j est irréductible, l'ensemble des solutions singulières (ie., des solutions complexes du système $g = \partial g/\partial x = \partial g/\partial y = 0$) est fini et petit. Considérons en premier, le cas plus général obtenu par le système $g = \partial g/\partial x = 0$.

Lemme 6.7. *Si $g \in \mathbb{C}[X, Y]$ est un polynôme irréductible de degré $d \geq 1$, alors soit $g(X, Y)$ est de la forme $aY + b$ ou soit le nombre de solutions dans $\mathbb{C}^2$ de $g = \partial g/\partial x = 0$ est au plus $d(d-1)$.*

Démonstration. Nous considérons deux cas.

(i) Si le système $g = \partial g/\partial x = 0$ a un nombre fini de solutions, il en a au plus $d(d-1)$ d'après le théorème de Bézout.

(ii) Sinon, ce système a un nombre infini de solutions. Le polynôme $\partial g/\partial x$ doit s'annuler en tout point de l'ensemble des zéros de g comme g est irréductible. Pour la même raison, il en résulte que g divise $\partial g/\partial x$. Or ceci est impossible par les contraintes sur le degré à moins que $\partial g/\partial x \equiv 0$ sur $\mathbb{C}^2$. Donc g dépend seulement de la variable Y, et doit être de la forme $g(X, Y) = aY + b$ (encore par l'irréductibilité).

□

Comme la condition supplémentaire $\partial g/\partial y = 0$ implique $a = 0$ dans le lemme précédent, nous avons :

Corollaire 6.8. *Si $g \in \mathbb{C}[X, Y]$ est un polynôme irréductible de degré $d \geq 1$, il a au plus $d(d-1)$ zéros singuliers dans $\mathbb{C}^2$.*

Nous allons maintenant borner les nombre de racines d'un système réel de deux équations denses.

Lemme 6.9. *Soient $f, g \in \mathbb{R}[X, Y]$ deux polynômes non-nuls de degrés respectifs δ et d. Soit $\mathcal{U}$ un sous-ensemble ouvert de $\mathbb{R}^2$. Considérons le système suivant d'équations polynomiales :*

$$\begin{cases} f(X, Y) = 0 \\ g(X, Y) = 0. \end{cases} \tag{6.5}$$

Si le nombre de solutions dans $\mathcal{U}$ est fini, il est borné supérieurement par $d^2/4 + d\delta$.

De plus, si f est le polynôme nul, le nombre de solutions dans $\mathcal{U}$ de ce même système est infini ou borné par $\frac{d^2}{4} + d(d-1)$.

Démonstration. Supposons que le système a un nombre fini de solutions dans $\mathcal{U}$. Par le lemme 6.6, l'ensemble des racines de g est l'union d'un ensemble de taille au plus $d^2/4$ et de l'ensemble des racines des polynômes $g_1, \ldots, g_k$. Donc le nombre de solutions du système (6.5) est borné par $d^2/4$ plus la somme des nombres de solutions de chaque système $g_i(X, Y) = f(X, Y) = 0$. Posons d_i le degré de chaque g_i. Pour chaque i, il y a deux cas :

(i) Si g_i divise f alors soit le nombre de racines réelles de g_i est infini sur $\mathcal{U}$ et alors toutes ces racines sont des solutions du système (6.5) ou soit le nombre de ces racines est fini, et dans ce cas, chacune de ces racine est une racine singulière de g_i. Par le corollaire 6.8, le nombre de racines réelles est borné par $d_i(d_i - 1)$, et donc par $d_i\delta$ si f n'est pas identiquement nul car g_i divise f.

(ii) Autrement, g_i ne divise pas f et par conséquent, le système a un nombre fini de solutions dans $\mathbb{C}^2$ et ce nombre est borné par $d_i\delta$ selon le théorème de Bézout.

Ainsi, pour chaque i, le nombre de solutions du système $g_i(X, Y) = f(X, Y) = 0$ est au plus $d_i\delta$. □

On pourra remarquer que l'on peut obtenir la borne légèrement moins précise

$$\max(d, \delta).(2\max(d, \delta) - 1)$$

directement à partir du théorème 6.5.

1.4 Décomposition cylindrique algébrique pour un polynôme bivarié

Dans son article, Collins [25] a introduit la décomposition cylindrique algébrique. Le but était d'obtenir une preuve algorithmique de l'élimination des quantificateurs pour les corps réels clos. Plus de détails sur la décomposition cylindrique algébrique peuvent être trouvés dans [9]. Ici, nous utiliserons une décomposition similaire de $\mathbb{R}$ pour séparer les différents comportements des racines de notre système. Toutefois, dans notre cas la dimension est seulement deux, et nous souhaitons caractériser un seul polynôme. Pour ces raisons, nous utiliserons une décomposition un peu plus basique. Rappelons quelques définitions et propriétés tirées de [25].

Définition 6.10. *Soient $A(X, Y)$ un polynôme réel et S un sous-ensemble de $\mathbb{R}$. Nous dirons que les polynômes $f_1, \ldots, f_m$ (où $m \geq 1$)* décrivent les racines *de A sur S si les conditions suivantes sont toutes vérifiées :*

1. *$f_1, \ldots, f_m$ sont des fonctions continues distinctes de S vers $\mathbb{C}$.*
2. *Pour tout $1 \leq i \leq m$, il existe un entier strictement positif e_i tel que pour tout a dans S, $f_i(a)$ est une racine de $A(a, Y)$ de multiplicité e_i.*
3. *Si $a \in S$, $b \in \mathbb{C}$ et $A(a, b) = 0$ alors il existe $i \leq m$ tel que $b = f_i(a)$.*
4. *Il existe k où $0 \leq k \leq m$ et tel que les fonctions $f_1, \ldots, f_k$ sont à valeurs réelles avec $f_1 < f_2 < \ldots < f_k$ alors que les valeurs de $f_{k+1}, \ldots, f_m$ sont toutes non-réelles.*

La valeur e_i sera appelée la multiplicité *de f_i. Si $k \geq 1$, nous dirons que $f_1, \ldots, f_k$* décrivent les racines réelles *de A sur S. Les racines de A sont* descriptibles *sur S s'il existe des fonctions $f_1, \ldots, f_m$ qui décrivent les racines de A sur S.*

Collins prouva le théorème suivant.

Théorème 6.11 (Cas particulier du théorème 1 dans [25])**.** *Soit $A(X, Y)$ un polynôme de $\mathbb{R}[X][Y]$. Soit S un sous-ensemble connexe de $\mathbb{R}$. Si le coefficient dominant*

de A vu comme un polynôme en Y ne s'annule pas sur S, et si le nombre de racines distinctes de $A(X)$ sur $\mathbb{C}$ est invariant sur S alors les racines de A sont descriptibles sur S.

Des critères sont donnés dans la suite de l'article de Collins pour caractériser l'invariance du nombre de racines. En particulier, il utilise le résultant de deux polynômes.

Soit A et B deux polynômes dans $\mathbb{R}[X][Y]$ avec $\deg_Y(A) = m$ et $\deg_Y(B) = n$. La matrice de Sylvester de A et B est la matrice M de dimensions $m+n$ par $m+n$ dont les lignes successives contiennent les coefficients des polynômes $Y^{n-1}A(Y), \ldots, YA(Y), A(Y), Y^{m-1}B(Y), \ldots, B(Y)$, où le coefficient de Y^i apparait dans la colonne $m+n-i$. Le polynôme $\mathrm{Res(A, B)}$, résultant de A et B, est $\det(M)$, le déterminant de M. Si le coefficient dominant de A s'annule en un point particulier x_0, alors le résultant $\mathrm{Res(A, A_Y)}$ s'annule aussi en x_0. Nous remarquons, pour des applications prochaines, que si $A \in \mathbb{R}[X, Y]$, $\deg_X(A) \leq d$ et $\deg_Y(A) \leq d$, alors $\mathrm{Res(A, A_Y)}$ est un polynôme de $\mathbb{R}[X]$ de degré borné par $2d^2 - d$.

Un corollaire immédiat des théorèmes 1, 2 et 3 dans [25] est

Corollaire 6.12. *Soit $A(X, Y)$ un polynôme de $\mathbb{R}[X][Y]$. Soit S un sous-ensemble connexe de $\mathbb{R}$. Si $\mathrm{Res(A, A_Y)(X)}$ n'a pas de racines sur S, alors les racines de A sont descriptibles sur S.*

Ainsi, dans la suite, nous considérerons des sous-ensembles de $\mathbb{R}$ où le polynôme $\mathrm{Res(A, A_Y)}$ n'a pas de racines. En particulier, nous voulons que ce polynôme soit non nul. Nous montrons que c'est le cas lorsque A est irréductible dans $\mathbb{R}[X, Y]$.

Lemme 6.13. *Soit $A(X, Y)$ un polynôme irréductible de $\mathbb{R}[X][Y]$ avec $\deg_Y(A) \geq 1$. Alors $\mathrm{Res(A, A_Y)}$ n'est pas le polynôme nul.*

Démonstration. Par un résultat bien connu, l'irréductibilité de A dans $\mathbb{R}[X][Y]$ et la condition $\deg_Y(A) \geq 1$ impliquent que A est irréductible dans $\mathbb{R}(X)[Y]$. Supposons que $R(X) = \mathrm{Res(A, A_Y)(X)} = 0$. Cela implique que A et A_Y ont un facteur commun $B \in \mathbb{R}(X)[Y]$ de degré $\deg_Y(B) \geq 1$. Comme A est irréductible dans $\mathbb{R}(X)[Y]$, il existe C dans $\mathbb{R}(X)$ tel que $A = CB$. Nous avons donc $\deg_Y(A) = \deg_Y(B) \leq \deg_Y(A_Y)$. Ce qui est impossible car $\deg_Y(A) \geq 1$. □

Remarque 6.14. *Si (x_0, y_0) est une racine de A et de A_Y alors $Y - y_0$ divise les polynômes $A(x_0, Y)$ et $A_Y(x_0, Y)$. Ainsi $\mathrm{Res(A, A_Y)(x_0)} = 0$. Donc, si $\mathrm{Res(A, A_Y)}$ n'a aucun zéro sur le sous-ensemble S de $\mathbb{R}$, alors le système $A(X, Y) = A_Y(X, Y) = 0$ n'a aucune solution sur $S \times \mathbb{R}$. Cette remarque sera utile pour la preuve du lemme 6.18 dans la section suivante, et pour une application du théorème des fonctions implicites analytiques avant le lemme 6.17.*

2 Intersection d'une courbe creuse et d'une courbe de petit degré

Rappelons qu'un polynome est appelé t-creux s'il a au plus t monômes. Dans cette section, nous allons prouver le théorème 6.1 mentionné au début du chapitre.

Théorème (Rappel du théorème 6.1)**.** *Soit $F \in \mathbb{R}[X,Y]$ un polynôme bivarié non nul de degré d et soit $G \in \mathbb{R}[X,Y]$ un polynôme bivarié t-creux. L'ensemble des solutions réelles du système*

$$\begin{cases} F(X,Y) = 0 \\ G(X,Y) = 0 \end{cases} \tag{6.6}$$

a un nombre de composantes connexes qui est $O(d^3t + d^2t^3)$.

Nous allons prouver le résultat par réduction au cas où F est irréductible et où le système n'a qu'un nombre fini de solutions.

Proposition 6.15. *Considérons de nouveau un polynôme bivarié F de degré d ainsi qu'un polynôme bivarié G t-creux. Supposons de plus que F est irréductible dans $\mathbb{C}[X,Y]$ et que (6.6) n'a qu'un nombre fini de solutions réelles. Alors, ce système a $O(d^3t + d^2t^3)$ solutions réelles distinctes.*

Nous expliquerons tout d'abord pourquoi cette proposition implique le théorème 6.1. Commençons par enlever l'hypothèse que le système n'a qu'un nombre fini de solutions.

Corollaire 6.16 (Corollaire de la proposition 6.15)**.** *Considérons encore un polynôme bivarié F de degré d ainsi qu'un polynôme bivarié G t-creux. Supposons que F est irréductible dans $\mathbb{C}[X,Y]$. L'ensemble des solutions réelles de (6.6) a un nombre de composantes connexes borné par $O(d^3t + d^2t^3)$.*

Démonstration. Il y a deux cas :

1. Le système a un ensemble fini de solutions réelles. Dans ce cas, par la proposition 6.15, il y a au plus $O(d^3t + d^2t^3)$ solutions.
2. L'ensemble des solutions est infini. Cela implique que F et G partagent un facteur commun. Comme F est irréductible dans $\mathbb{C}$, F doit être un facteur de G. Mais dans ce cas, l'ensemble des solutions de (6.6) est exactement l'ensemble des zéros de F. Par le théorème 6.4, cet ensemble a au plus $2d(d-1)$ composantes connexes.

□

Preuve du théorème 6.1 à partir du corollaire 6.16. D'après le lemme 6.6, l'ensemble des zéros réels de F est l'union de l'ensemble des racines réelles des facteurs irréductibles réels $F_1, \ldots, F_k$ de F et d'un ensemble $\mathcal{U}$ de cardinalité au plus $d^2/4$. Par conséquent, le nombre de composantes connexes de l'ensemble des solutions de (6.6) est borné par la somme du nombre de composantes connexes des solutions des systèmes $F_i(x,y) = G(x,y) = 0$ pour $i \leq k$ et du système

$$\begin{cases} (X,Y) \in \mathcal{U} \\ G(X,Y) = 0. \end{cases}$$

Le dernier système a au plus $d^2/4$ solutions. Par le corollaire 6.16, chaque système $F_i(x,y) = G(x,y) = 0$ a au plus $O((\deg F_i)^3 t + (\deg F_i)^2 t^3)$ composantes connexes.

Pour conclure, observons que

$$\sum_{i=1}^{k}\left((\deg F_i)^3 t + (\deg F_i)^2 t^3\right) \leq \left(\sum_{i=1}^{k}\deg F_i\right)^3 t + \left(\sum_{i=1}^{k}\deg F_i\right)^2 t^3 \leq d^3 t + d^2 t^3.$$

□

Remarquons que la condition de non nullité pour F dans le théorème 6.1 et la proposition 6.15 est primordiale. Effectivement, l'existence d'un polynôme $P(t)$ qui borne supérieurement le nombre de solutions réelles de tout système de deux polynômes t-creux G et H quand ce nombre est fini, est un problème ouvert. Ainsi, si nous autorisons le polynôme F à être le polynôme nul dans le théorème 6.1, nous serions capable d'encoder le système de deux équations creuses dans le système suivant :

$$\begin{cases} F = 0 \\ G(X,Y)^2 + H(X,Y)^2 = 0. \end{cases}$$

Il reste à prouver maintenant la proposition 6.15. Dans la suite, nous supposerons que le système n'a qu'un nombre fini de solutions réelles. Nous commençons avec deux cas de base.

1. Si $F(X,Y) = cY$, alors comme $G(X,0) \neq 0$ (sinon $(x,0)$ est une solution de (6.6) pour tout x dans $\mathbb{R}$), par la règle de Descartes, le nombre de racines de la forme $(x,0)$ est borné par $2t-1$.
2. Si $F_Y(X,Y) = 0$, alors F ne dépend pas de Y et il y a au plus d valeurs $x_1,\ldots,x_p$ de X telles que $F(x_l,Y) = 0$. Pour chacune de ces valeurs, $G(x_l,Y)$ est un polynôme univarié t-creux donc a au plus $2t-1$ racines réelles distinctes. Dans ce cas, le système (6.6) a au plus $2td-d$ solutions.

Nous avons vérifié les bornes de la proposition 6.15 dans ces deux cas particuliers. Nous supposerons dans la suite que nous ne serons pas dans ces deux cas.

Considérons le polynôme univarié $\mathrm{Res}(\mathrm{F},\mathrm{F_Y})$, qui est de degré au plus $2d^2-d$ et qui est non nul d'après le lemme 6.13. Soit $x_1 < \ldots < x_q$ les racines réelles de ce polynôme où $q \leq 2d^2-d$ et soient $\mathcal{I} = \{(x_i, x_{i+1}) | 0 \leq i \leq q\}$ les intervalles ouverts correspondants où $x_0 = -\infty$ et $x_{q+1} = +\infty$. Nous remarquons que $|\mathcal{I}| \leq 2d^2-d+1$. Si I est dans $\mathcal{I}$, les racines de F sont descriptibles sur I par le corollaire 6.12.

Ainsi, pour chaque intervalle I dans $\mathcal{I}$, il y a $m_I \leq d$ fonctions continues à valeurs réelles $\phi_{I,1} < \ldots < \phi_{I,m_I} : I \to \mathbb{R}$ telles que $F(x,y) = 0$ sur $I \times \mathbb{R}$ si et seulement s'il existe $i \leq m_I$ tel que $y = \phi_{I,i}(x)$. De plus, $F_Y(x, \phi_{I,i}(x)) \neq 0$ car $\mathrm{Res}(\mathrm{F},\mathrm{F_Y})$ ne s'annule pas sur I (cf. Remarque 6.14). La version analytique du théorème des fonctions implicites montre que les fonctions $\phi_{I,i}$ sont analytiques sur I.

Nous noterons $\Omega = \bigcup_{I\in\mathcal{I}} I$. Bornons séparément le nombre s de solutions du système (6.6) sur $\Omega \times \mathbb{R}$ et le nombre s' de solutions sur $(\mathbb{R}\setminus\Omega)\times\mathbb{R}$.

Lemme 6.17. *Si $F_Y(X,Y)$ est un polynôme non nul, le nombre s' de solutions sur $(\mathbb{R}\setminus\Omega)\times\mathbb{R}$ du système (6.6) est au plus $2d^3-d^2$.*

Démonstration. Rappelons que $(\mathbb{R} \setminus \Omega) \times \mathbb{R} = \{x_1, \ldots, x_q\}$ est un ensemble fini de cardinalité au plus $2d^2 - d$. Pour chaque $i \leq q$, $X - x_i$ ne divise pas F car F est irréductible et $F_Y \neq 0$. Donc le nombre de racines de F sur $\{x_i\} \times \mathbb{R}$ est fini et borné par d. Par conséquent, $s' \leq 2d^3 - d^2$. □

Bornons maintenant le nombre s de solutions du système sur $\Omega \times \mathbb{R}$. Pour faire cela, nous allons borner le nombre s_j^I (avec $j \leq m_I$) de solutions du système suivant sur $I \times \mathbb{R}$:

$$\begin{cases} Y = \phi_j(X) \\ G(X, Y) = 0. \end{cases} \tag{6.7}$$

Ainsi, $\sum_I \sum_{0 \leq j \leq m_I} s_j^I = s$ et en particulier tous les s_j^I sont finis.

Le polynôme g est t-creux, d'où $G(X, Y) = \sum_{j=1}^t a_j X^{\alpha_j} Y^{\beta_j}$. Alors, si (x, y) est une racine de (6.7), nous avons $G(x, \phi_i(x)) = \sum_{j=1}^t a_j x^{\alpha_j} (\phi_i(x))^{\beta_j} = 0$.

Supposons qu'il existe des constantes réelles $c_1, \ldots, c_t$ (non toutes nulles) telles que $H(X, Y) = \sum_{j=1}^t c_j X^{\alpha_j} Y^{\beta_j}$ est un multiple de F. Dans ce cas, nous pouvons considérer le polynôme $\tilde{G}(X, Y) = G - \frac{a_u}{c_u} H$ qui est $t-1$-creux (où c_u est un coefficient non nul de H). Alors, les racines de (6.6) sont exactement les racines du système suivant :

$$\begin{cases} F(X, Y) = 0 \\ \tilde{G}(X, Y) = 0. \end{cases} \tag{6.8}$$

Dans ce système, le premier polynôme n'a pas changé et le nombre de termes du second polynôme a diminué. Nous pouvons donc supposer (par récurrence sur t) que la borne supérieure voulue, $O(d^3 t + d^2 t^3)$, sur le nombre de solutions réelles s'applique à (6.8). Par conséquent, nous supposerons dans la suite de la preuve que si $H(X, Y) = \sum_{j=1}^t c_j X^{\alpha_j} Y^{\beta_j}$ est un multiple de F alors toutes les constantes c_j sont nulles.

Avant d'énoncer le prochain lemme, nous rappelons que $\mathcal{I}$ est une liste finie d'intervalles ouverts définie avant le lemme 6.17.

Lemme 6.18. *Pour $s \leq t$, il existe un polynôme non nul $T_s(X, Y) \in \mathbb{R}[X, Y]$ de degré au plus $(1 + 2d)\binom{s}{2}$ en chaque variable tel que pour tout intervalle I dans $\mathcal{I}$ et tout $0 \leq i \leq m_I$, le wronskien des s fonctions $x^{\alpha_1}(\phi_i(x))^{\beta_1}, \ldots, x^{\alpha_s}(\phi_i(x))^{\beta_s}$ satisfait :*

$$W(x^{\alpha_1}(\phi_i(x))^{\beta_1}, \ldots, x^{\alpha_s}(\phi_i(x))^{\beta_s}) = \frac{x^{\alpha - \binom{s}{2}} \phi_i^{\beta - \binom{s}{2}}}{F_Y^{s(s-1)}(x, \phi_i)} T_s(x, \phi_i)$$

où $\alpha = \sum_{j=1}^s \alpha_j$ et $\beta = \sum_{j=1}^s \beta_j$. En outre, ce wronskien n'est pas identiquement nul sur I.

Démonstration. Soit I un intervalle de $\mathcal{I}$ et i un entier entre 0 et m_I. Si

$$\sum_{j=1}^t c_j x^{\alpha_j} \phi_i^{\beta_j} = H(x, \phi_i(x))$$

est le polynôme nul, alors F divise H par l'irréductibilité de F. Il en découle alors que $H \equiv 0$ par l'hypothèse précédent le lemme. La famille $x \mapsto x^{\alpha_j}(\phi_i(x))^{\beta_j}$ est donc linéairement indépendante. Comme les fonctions sont analytiques sur I, le wronskien $W(x^{\alpha_1}(\phi_i(x))^{\beta_1}, \dots, x^{\alpha_s}(\phi_i(x))^{\beta_s})$ n'est pas identiquement nul. Par la remarque 6.14, $F_Y(x, \phi_i(x))$ n'a pas de zéro sur I. Alors en utilisant les lemmes 5.12 et 6.3,

$$\begin{aligned}
\left(x^{\alpha_j}(\phi_i(x))^{\beta_j}\right)^{(p)} &= \sum_{k=0}^{p} \binom{p}{k} \left(x^{\alpha_j}\right)^{(k)} \left(\phi_i(x)^{\beta_j}\right)^{(p-k)} \\
&= \sum_{k=0}^{p} \binom{p}{k} \left(x^{\alpha_j}\right)^{(k)} \sum_{s \in \mathcal{S}_{p-k}} \left[c_{\beta_j,s} \phi_i^{\beta_j - |s|} \prod_{l=1}^{p-k} \left(\phi_i^{(l)}\right)^{s_l} \right] \\
&= x^{\alpha_j - p} \phi_i^{\beta_j - p} \sum_{k=0}^{p} \sum_{s \in \mathcal{S}_{p-k}} \left[c'_{\alpha_j,\beta_j,p,s} x^{p-k} \phi_i^{p-|s|} \prod_{l=1}^{p-k} \left(\frac{S_l}{F_Y^{2l-1}}\right)^{s_l} \right] \\
&= \frac{x^{\alpha_j - p} \phi_i^{\beta_j - p}}{F_Y^{2p}} \sum_{k=0}^{p} \sum_{s \in \mathcal{S}_{p-k}} \left[c'_{\alpha_j,\beta_j,p,s} x^{p-k} \phi_i^{p-|s|} F_Y^{2k+|s|} \prod_{l=1}^{p-k} S_l^{s_l} \right] \\
&= \frac{x^{\alpha_j - p} \phi_i^{\beta_j - p}}{F_Y^{2p}} T_{j,p}(x, \phi_i)
\end{aligned}$$

où $T_{j,p}(X, Y)$ est un polynôme de degré en X borné par

$$\begin{aligned}
\deg_X(T_{j,p}) &\leq \max_{k,s} \left(p - k + (2k + |s|)d + \sum_{l=1}^{p-k} s_l(2l-1)d \right) \\
&\leq \max_{k,s} \left(p - k + 2kd + |s|d + 2d(p-k) - d|s| \right) \\
&\leq 2dp + p
\end{aligned}$$

et de degré en Y borné par

$$\begin{aligned}
\deg_Y(T_{j,p}) &\leq \max_{k,s} \left(p - |s| + (2k + |s|)(d-1) + \sum_{l=1}^{p-k} s_l(2l-1)d \right) \\
&\leq \max_{k,s} \left(p - |s| + 2kd - 2k + |s|d - |s| + 2dp - 2dk - d|s| \right) \\
&\leq \max_{k,s} \left(p - 2|s| - 2k + 2dp \right) \\
&\leq p + 2dp.
\end{aligned}$$

De plus, $T_{j,p}$ ne dépend pas de ϕ_i par le lemme 6.3. Ainsi, le wronskien est une fonction rationnelle bivariée :

$$W\left(x^{\alpha_1}(\phi_i(x))^{\beta_1}, \dots, x^{\alpha_s}(\phi_i(x))^{\beta_s}\right) = \frac{x^{\alpha - \binom{s}{2}} \phi_i^{\beta - \binom{s}{2}}}{F_Y^{s(s-1)}(x, \phi_i)} T_s(x, \phi_i)$$

où $\alpha = \sum_{j=1}^{s} \alpha_j$, $\beta = \sum_{j=1}^{s} \beta_j$ et $T_s(X, Y)$ est un polynôme de degré borné par $(1 + 2d)\binom{s}{2}$ en chaque variable et qui ne dépend ni de I, ni de i. □

Comptons le nombre $v_{I,i}$ de racines de ϕ_i sur I. Nous avons supposé que Y ne divise pas F, donc le polynôme univarié $F(X,0)$ est non nul et est de degré au plus d. Si v_i désigne le nombre de racines de $F(X,0)$ sur I, nous avons $\left(\sum_{I\in\mathcal{I}} v_I\right) \leq d$. Comme chaque racine de ϕ_i est par définition une racine de $F(X,0)$, cela implique que ϕ_i a au plus v_I racines sur I.

Pour tout I et tout i, comptons le nombre $r^s_{I,i}$ de racines de $T_s(x,\phi_i(x))$. Ce nombre est fini car sinon le wronskien du lemme 6.18 serait identiquement nul. Enfin, appelons r_s le nombre de solutions sur $\Omega\times\mathbb{R}$ du système

$$\begin{cases} T_s\left(X,Y\right)=0 \\ F\left(X,Y\right)=0. \end{cases} \tag{6.9}$$

Donc, $r^s=\left(\sum_I\sum_i r^s_{I,i}\right)$ est fini.

Finalement, grâce au lemme 6.9 et comme le degré total de T_s est borné par $2(1+2d)\binom{s}{2}$, le nombre r^s de racines de (6.9) est borné par $d^2/4+2d(1+2d)\binom{s}{2}$.

Alors, en utilisant le lemme 6.18, pour tous I et i, $W\left(x^{\alpha_1}(\phi_i(x))^{\beta_1},\ldots,x^{\alpha_s}(\phi_i(x))^{\beta_s}\right)$ a au plus $\mathbb{1}_I(0)+v_I+r^s_{I,i}$ racines réelles et le théorème 5.9 implique que le nombre $s_{I,i}$ de racines réelles distinctes de $G(x,\phi_i(x))$ est borné par

$$t-1+2\sum_{s=1}^{t}\left(\mathbb{1}_I(0)+v_I+r^s_{I,i}\right)=t-1+2t\mathbb{1}_I(0)+2tv_I+2\sum_{s=1}^{t}r^s_{I,i}.$$

D'où,

$$\begin{aligned} s&=\sum_{I\in\mathcal{I}}\sum_{i\leq m_I}s_{I,i}\\ &\leq(2d^2-d+1)d(t-1)+2dt+2td^2+2\sum_{s=1}^{t}r^s\\ &\leq(2d^2-d+1)d(t-1)+2dt+2td^2+2\sum_{s=1}^{t}\left[d^2/4+2(1+2d)\binom{s}{2}d\right]\\ &=(2d^3t+4d^2t^3)(1+o(1)). \end{aligned}$$

Ceci complète la preuve de la proposition 6.15 et du théorème principal.

Bibliographie

[1] S. Aaronson et D. van Melkebeek. On circuit lower bounds from derandomization. *Theory of Computing*, 7(1):177–184, 2011.

[2] M. Agrawal. Proving lower bounds via pseudo-random generators. *Proceedings FSTTCS 2005*, 2005. Invited paper.

[3] M. Agrawal et R. Saptharishi. Classifying Polynomials and Identity Testing. *Current Trends in Science*, 2009.

[4] M. Agrawal et V. Vinay. Arithmetic circuits : A chasm at depth four. *Proceedings-Annual Symposium on Foundations of Computer Science*, pages 67–75, 2008.

[5] E. Allender, P. Bürgisser, J. Kjeldgaard-Pedersen et P. Bro Miltersen. On the complexity of numerical analysis. *SIAM Journal of Computing*, 38(5):1987–2006, 2009. Conference version in CCC 2006.

[6] E. Allender, J. Jiao, M. Mahajan, et V. Vinay. Non-commutative arithmetic circuits : depth reduction and size lower bounds. *Theoretical Computer Science*, 209(1–2):47 – 86, 1998.

[7] S. Arora et B. Barak. *Computational complexity : a modern approach*. Cambridge University Press, 2009.

[8] M. Avendaño. The number of roots of a lacunary bivariate polynomial on a line. *Journal of Symbolic Computation*, 44(9):1280–1284, 2009.

[9] S. Basu, R.D. Pollack, et M.F. Roy. *Algorithms in real algebraic geometry*, volume 10 de *Algorithms and Computation in Mathematics*, 2006.

[10] F. Bihan et F. Sottile. New fewnomial upper bounds from Gale dual polynomial systems. *Moscow Mathematical Journal*, 7(3):387–407, 2007.

[11] F. Bihan et F. Sottile. Fewnomial bounds for completely mixed polynomial systems. *Advances in Geometry*, 11(3):541–556, 2011.

[12] O. Bílka, K. Buchin, R. Fulek, M. Kiyomi, Y. Okamoto, S. Tanigawa et C.D. Tóth. A tight lower bound for convexly independent subsets of the Minkowski sums of planar point sets. *Electronic Journal of Combinatorics*, 17(1), 2010.

[13] L. Blum, F. Cucker, M. Shub et S. Smale. Algebraic settings for the problem "$\mathsf{P}\neq\mathsf{NP}$?". *The Mathematics of Numerical Analysis*, volume 32 de *Lectures in Applied Mathematics*, pages 125–144, 1996.

[14] L. Blum, F. Cucker, M. Shub et S. Smale. *Complexity and Real Computation*. Springer-Verlag, 1998.

[15] L. Blum, M. Shub et S. Smale. On a theory of computation and complexity over the real numbers : NP-completeness, recursive functions and universal machines. *Bulletin of the American Mathematical Society*, 21(1):1–46, 1989.

[16] M. Bôcher. On linear dependence of functions of one variable. *Bulletin of the American Mathematical Society*, 7(3):120–121, 1900.

[17] M. Bôcher. The theory of linear dependence. *The Annals of Mathematics*, 2(1/4):81–96, 1900.

[18] A. Borodin et S. Cook. On the number of additions to compute specific polynomials. *SIAM Journal on Computing*, 5(1):146–157, 1976.

[19] P. Bürgisser. *Completeness and Reduction in Algebraic Complexity Theory*. Volume 7 de *Algorithms and Computation in Mathematics*, 2000.

[20] P. Bürgisser. Cook's versus Valiant's Hypothesis. *Theoretical Computer Science*, 235:71–88, 2000.

[21] P. Bürgisser. On defining integers and proving arithmetic circuit lower bounds. *Computational Complexity*, 18:81–103, 2009. Conference version in STACS 2007.

[22] P. Bürgisser, M. Clausen et M.A. Shokrollahi. *Algebraic complexity theory*. Grundlehren der mathematischen Wissenschaften, 315, 1997.

[23] X. Chen, N. Kayal et A. Wigderson. Partial derivatives in arithmetic complexity and beyond. *Foundations and Trends in Theoretical Computer Science*, 6(1):1–138, 2011.

[24] S. Chillara et P. Mukhopadhyay. Depth-4 lower bounds, determinantal complexity : A unified approach. *Symposium on Theoretical Aspects of Computer Science*, 2014.

[25] G.E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. *Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20–23, 1975*, pages 134–183, 1975.

[26] D. Coppersmith et S. Winograd. Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251–280, 1990.

[27] W. De Melo et B.F. Svaiter. The cost of computing integers. *Proceedings American Mathematical Society*, 124 :1377–1378, 1996.

[28] S.M. Engdahl et A.E. Parker. Peano on Wronskians : A translation. *Mathematical Association of America*, 2011.
www.maa.org/publications/periodicals/convergence/peano-on-wronskians-a-translation-introduction.

[29] F. Eisenbrand, J. Pach, T. Rothvoß et N.B. Sopher. Convexly independent subsets of the Minkowski sum of planar point sets. *Electronic Journal of Combinatorics*, 15(1), 2008.

[30] I. Fischer. Sums of like powers of multivariate linear forms. *Mathematics Magazine*, 67(1):59–61, 1994.

[31] H. Fournier, N. Limaye, G. Malod et S. Srinivasan. Lower bounds for depth 4 formulas computing iterated matrix multiplication. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:100, 2013.

[32] G.F. Frobenius. Üeber die Determinante mehrerer Functionen einer Variabeln. *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, 1874:245–257, 1874.

[33] S. Gao. Absolute irreducibility of polynomials via Newton polytopes. *Journal of Algebra*, 237(2):501–520, 2001.

[34] M.R. Garey et D.S. Johnson. *Computers and intractability*. Freeman San Fransisco, volume 174, 1979.

[35] J. von zur Gathen. Feasible arithmetic computations : Valiant's hypothesis. *Journal of Symbolic Computation*, 4(2):137–172, 1987.

[36] D.G. Glynn. The permanent of a square matrix. *European Journal of Combinatorics*, 31(7):1887–1891, 2010.

[37] O. Goldreich. *Computational complexity : a conceptual perspective*. Cambridge University Press, 2008.

[38] B. Grenet, P. Koiran, N. Portier et Y. Strozecki. The limited power of powering : polynomial identity testing and a depth-four lower bound for the permanent. *Proceedings FSTTCS*, 2011.
arxiv.org/abs/1107.1434.

[39] D. Grigoriev. Lower bounds in algebraic complexity. *Notes of the Scientific Seminars of LOMI*, 118:25–82, 1982. En russe, traduction en anglais [40].

[40] D. Grigoriev. Lower Bounds in Algebraic Computational Complexity. *Journal Soviet Math.*, 29:1388–1425, 1985.

[41] D. Grigoriev et M. Karpinski. A zero-test and an interpolation algorithm for the shifted sparse polynomials. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, 162–169, 1993.

[42] D. Grigoriev, M. Karpinski et M.F. Singer. The interpolation problem for k-sparse sums of eigenfunctions of operators. *Advances in Applied Mathematics*, 12(1):76–81, 1991.

[43] D. Grigoriev, M. Karpinski et M.F. Singer. Computational complexity of sparse rational interpolation. *SIAM Journal on Computing*, 23(1):1–11, 1994.

[44] A. Gupta, P. Kamath, N. Kayal et R. Saptharishi. Approaching the chasm at depth four. *Proceedings of the Conference on Computational Complexity (CCC)*, 2013.

[45] A. Gupta, P. Kamath, N. Kayal et R. Saptharishi. Arithmetic circuits : A chasm at depth three. *Electronic Colloquium on Computational Complexity*, 20, 2013.

[46] G. Hajós. Solution to problem 41. *Mat. Lapok*, 4:40–41, 1953.

[47] J. Heintz et C.P. Schnorr. Testing polynomials which are easy to compute (extended abstract). *Proceedings of the Symposium on Theory of Computing (STOC)*, 262–272, 1980.

[48] P. Hrubeš. On the Real τ-Conjecture and the Distribution of Complex Roots. *Theory of Computing*, 9(10):403–411, 2013.

[49] P. Hrubeš et A. Yehudayoff. Arithmetic complexity in ring extensions. *Theory of Computing*, 7:119-129, 2011.

[50] W. Hurewicz. *Lectures on ordinary differential equations*. Dover edition, 1990.

[51] J.I. Hutchinson. On a remarkable class of entire functions. *Transactions of the American Mathematical Society*, 25(3):325–332, 1923.

[52] V. Kabanets et R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[53] E. Kaltofen et G. Villard. On the complexity of computing determinants. *Computational complexity*, 13(3-4):91–130, 2005.

[54] R. Karp et R. Lipton. Turing machines that take advice. *L'Enseignement Mathématique*, 28:191–209, 1982.

[55] N. Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 19, 2012.

[56] N. Kayal, N. Limaye, C. Saha et S. Srinivasan. An exponential lower bound for homogeneous depth four arithmetic formulas. *Electronic Colloquium on Computational Complexity (ECCC)*, 2014.

[57] N. Kayal, C. Saha et R. Saptharishi. A super-polynomial lower bound for regular arithmetic formulas. *Electronic Colloquium on Computational Complexity (ECCC)*, 20, 2013.

[58] N. Kayal et R. Saptharishi. A selection of lower bounds for arithmetic circuits, 2014.

[59] A.G. Khovanskiĭ. *Fewnomials*. Translations of mathematical monographs. American Mathematical Society, 1991.

[60] P. Koiran. Arithmetic circuits : the chasm at depth four gets wider. *Theoretical Computer Science*, (448):56–65, 2012.

[61] P. Koiran. Shallow circuits with high-powered inputs. *Proceedings of Second Symposium on Innovations in Computer Science (ICS 2011)*, 2011.
arxiv.org/abs/1004.4960.

[62] P. Koiran. Valiant's model and the cost of computing integers. *Computational Complexity*, 13:131–146, 2004.

[63] P. Koiran et S. Périfel. VPSPACE and a transfer theorem over the reals. *Computational Complexity*, 18:551–575, 2009. Conference version in STACS 2007.

[64] P. Koiran, N. Portier et S. Tavenas. A Wronskian approach to the real τ-conjecture. *Effective Methods in Algebraic Geometry (MEGA 2013)*, 2013.
arxiv.org/abs/1205.1015.

[65] P. Koiran, N. Portier et S. Tavenas. On the intersection of a sparse curve and a low-degree curve : A polynomial version of the lost theorem. ArXiv preprint, 2013.
arxiv.org/abs/1310.2447.

[66] P. Koiran, N. Portier, S. Tavenas et S. Thomassé. A tau-conjecture for Newton polygons. ArXiv preprint, 2013.
arxiv.org/abs/1308.2286.

[67] M. Kumar et S. Saraf. Superpolynomial lower bounds for general homogeneous depth 4 arithmetic circuits. ArXiv preprint, 2013.
arxiv.org/abs/1312.5978.

[68] D.C. Kurtz. A Sufficient Condition for All the Roots of a Polynomial To Be Real. *The American Mathematical Monthly*, 99(3):259–263, 1992.

[69] A. Kushnirenko. Letter to Frank Sottile, 2008. www.mat.tamu.edu/ sottile/research/pdf/Kushnirenko.pdf.

[70] T.Y. Li, J.M. Rojas et X. Wang. Counting real connected components of trinomial curve intersections and m-nomial hypersurfaces. *Discrete & Computational Geometry*, 30(3):379–414, 2003.

[71] G. Malod. Polynômes et coefficients. *Thèse de doctorat, Université Claude Bernard, Lyon*, 2003.

[72] G. Malod et N. Portier. Characterizing valiant's algebraic complexity classes. *Journal of Complexity*, 24(1):16–38, 2008.

[73] G.L. Miller, V. Ramachandran et E. Kaltofen. Efficient parallel evaluation of straight-line code and arithmetic circuits. *SIAM Journal on Computing*, 17(4):687–695, 1988.

[74] T. Muir. *A treatise on the Theory of Determinants*. Courier Dover Publications, 1960.

[75] N. Nisan. Lower bounds for non-commutative computation. *Proceedings of the twenty-third Annual ACM Symposium on Theory of Computing*, 410–418, 1991.

[76] N. Nisan et A. Wigderson. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity*, 6(3):217–234, 1996.

[77] D. Novikov et S. Yakovenko. Simple exponential estimate for the number of real zeros of complete Abelian integrals. *Annales de l'institut Fourier*, 45(4):897–927, 1995.

[78] A.M. Ostrowski. Über die Bedeutung der Theorie der konvexen Polyeder für die formale Algebra. *Jahresberichte Deutsche Math. Verein*, 20:98–99, 1921.

[79] C.H. Papadimitriou. *Computational complexity*. John Wiley and Sons Ltd., 2003.

[80] G. Peano. Sur le déterminant wronskien. *Mathesis*, 9:75–76, 1889.

[81] G. Peano. Sur les wronskiens. *Mathesis*, 9:110–112, 1889.

[82] S. Périfel. *Complexité Algorithmique*. Ellipses, 2014.

[83] K. Phillipson et J.M. Rojas. Fewnomial Systems with Many Roots, and an Adelic Tau Conjecture. ArXiv preprint, 2010. arxiv.org/abs/1011.4128.

[84] G. Pólya. On the mean-value theorem corresponding to a given linear homogeneous differential equation. *Transactions of the American Mathematical Society*, 24:312–324, 1922.

[85] G. Pólya et G. Szegő. *Problems and Theorems in Analysis. Volume II*, 1976.

[86] K. Ranestad et F.O. Schreyer. On the rank of a symmetric form. *Journal of Algebra*, 346(1):340–342, 2011.

[87] J.J. Risler. Additive complexity and zeros of real polynomials. *SIAM Journal on Computing*, 14:178–183, 1985.

[88] H.J. Ryser. Combinatorial mathematics. *The carus mathematical monographs*, 1963.

[89] N. Saxena. Diagonal circuit identity testing and lower bounds. *Automata, Languages and Programming*, volume 5125 de *Lecture Notes in Computer Science*, 60–71, 2008.

[90] N. Saxena. Progress on Polynomial Identity Testing. *Bulletin EATCS*, 99:49–79, 2009.

[91] A. Shpilka et A. Yehudayoff. Arithmetic circuits : A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4), 2010.

[92] M. Shub et S. Smale. On the intractability of Hilbert's Nullstellensatz and an algebraic version of $\mathsf{P} = \mathsf{NP}$. *Duke Mathematical Journal*, 81(1):47–54, 1995.

[93] S. Smale. Mathematical problems for the next century. *Mathematical Intelligencer*, 20(2):7–15, 1998.

[94] F. Sottile. *Real Solutions to Equations from Geometry*. University lecture series. American Mathematical Society, 2011.

[95] V. Strassen. Vermeidung von Divisionen. *Journal für die reine und angewandte Mathematik*, 264:184–202, 1973.

[96] B. Sturmfels. Polynomial equations and convex polytopes. *The American Mathematical Monthly*, 105(10):907–922, 1998.

[97] K.J. Swanepoel et P. Valtr. Large convexly independent subsets of Minkowski sums. *Electronic Journal of Combinatorics*, 17(1), 2010.

[98] S. Tavenas. Improved bounds for reduction to depth 4 and depth 3. *Proceedings 38th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, 2013.

[99] L.G. Valiant. Completeness classes in algebra. *Proceedings 11th ACM Symposium on Theory of Computing*, pages 249–261, 1979.

[100] L.G. Valiant. Reducibility by algebraic projections. *Logic and Algorithmic (an International Symposium held in honour of Ernst Specker)*, pages 365–380. Monographie n^o 30 de L'Enseignement Mathématique, 1982.

[101] L. Valiant, S. Skyum, S. Berkowitz et C. Rackoff. Fast parallel computation of polynomials using few processors. *SIAM Journal on Computing*, 12(4):641–644, 1983.

[102] M. Voorhoeve et A.J. van der Poorten. Wronskian determinants and the zeros of certain functions. *Indagationes Mathematicae (Proceedings)*, 78(5):417–424, 1975.

[103] K.W. Wagner. The complexity of combinatorial problems with succinct input representation. *Acta Informatica*, 23(3):325–356, 1986.

[104] V.V. Williams. Multiplying matrices faster than Coppersmith-Winograd. *Proceedings of the 44th Symposium on Theory of Computing*, 887–898, 2012.

[105] R. Zippel. Probabilistic algorithms for sparse polynomials. *Proceedings EUROSAM*, 216–226, 1979.