Bornes inférieures sur le calcul de polynômes

Sylvain Perifel

Lyon, le 10 et 11 février 2011

Question centrale : bornes inférieures sur la taille des circuits arithmétiques pour le calcul de polynômes. Par exemple, le permanent peut-il être calculé par une famille de circuits de taille polynomiale ?

Malheureusement, la meilleure borne qu'on connaisse pour des polynômes "explicites" (permanent, déterminant, etc.) est $\Omega(n \log n)\ldots$ Ce résultat est dû à Baur et Strassen (1983) et constituera notre première partie.

Lorsqu'on relâche la contrainte "explicite", on peut constuire pour tout k un polynôme ad-hoc n'ayant pas de circuits de taille n^k : ce résultat de Lipton puis Schnorr (1978) sera l'objet de notre deuxième partie.

Enfin, dans la troisième partie nous verrons des liens avec la complexité booléenne : dérandomiser le test d'identité de polynômes implique que NEXP n'a pas de circuits booléens de taille polynomiale ou que le permanent n'a pas de circuits arithmétiques de taille polynomiale (résultat de Kabanets et Impagliazzo, 2004). Nous verrons également à cette occasion quelques résultats sur les problèmes de test d'identité de polynômes et d'entiers calculés par circuits arithmétiques.

Rappels Circuit arithmétique sur $\mathbb{C}$ = graphe orienté sans cycle, portes $+$ et $\times$, entrées $x_1, \ldots, x_n$ et constantes arbitraires de $\mathbb{C}$. La taille est le nombre de sommets (y compris les entrées et les constantes). À la partie 1, nous considérerons aussi des circuits à plusieurs sorties.

1 Baur et Strassen

Nous allons d'abord voir la "degree bound" de Strassen (1973) par une démonstration de Schönage (1976). Il s'agit de donner une borne inférieure sur la taille d'un circuit calculant plusieurs polynômes. Puis nous verrons comment le calcul des dérivées partielles (par une démonstration de Morgenstern, 1984) nous permettra de revenir au calcul d'un seul polynôme.

1.1 Borne du degré

Dans cette section, K désigne un corps infini quelconque. Avant de prouver le résultat principal, nous avons besoin de plusieurs lemmes sur l'existence de relations polynomiales entre des polynômes calculés par circuit. En guise d'échauffement, nous rappelons le nombre de monômes d'un certain degré.

A. Lemme – Le nombre de monômes de degré $\leq d$ en $x_1, \ldots, x_n$ est $\binom{n+d}{d}$.

Démonstration. Il s'agit de placer n délimiteurs dans un tableau de $(n+d)$ cases : le nombre de cases libres entre le délimiteur i et le délimiteur $i+1$ est le degré de x_i. □

Le lemme suivant montre l'existence d'un polynôme annulateur : remarquer que le degré en y_0 ne dépend pas de celui de p_0.

B. Lemme – Si $p_0, p_1, \ldots, p_m \in K[x_1, \ldots, x_m]$ sont des polynômes de degré $\deg(p_i) = d_i$, alors il existe un polynôme non nul $H \in K[y_0, \ldots, y_m]$ tel que $\deg_{y_0}(H) \leq D = d_1 \times \ldots \times d_m$ et $H(p_0, \ldots, p_m) = 0$.

Démonstration. Soit d un entier que nous fixerons plus tard (une borne sur le degré total de $H(p_0, \ldots, p_n)$). Écrivons un polynôme $H(y_0, \ldots, y_m) = \sum_{\bar{v}} c_{\bar{v}} y_0^{v_0} \ldots y_m^{v_m}$, où $\bar{v} = (v_0, \ldots, v_m) \in \mathbb{N}^{m+1}$ vérifient :

$$(\star) \qquad v_0 \leq D \qquad \text{et} \qquad v_0 d_0 + \ldots + v_m d_m \leq d.$$

Comptons le nombre de tels $\bar{v}$.

Tout d'abord, dénombrons les solutions de $v_1 d_1 + \ldots + v_m d_m \leq q$ (Eq. 1) pour un certain $q \leq d$. À une solution $\bar{u}$ de l'équation $u_1 + \ldots + u_m \leq q$ (Eq. 2) on associe la solution $\bar{v}$ de l'équation 1 définie par $v_i = \lfloor u_i / d_i \rfloor$. Tout $\bar{v}$ a au plus D antécédents (choix des restes $0 \leq r_i < d_i$). Puisqu'il y a $\binom{q+m}{m}$ solutions à l'équation 2 par le lemme A, il y en a au moins $\binom{q+m}{m}/D$ à l'équation 1.

Pour notre application, $q = d - v_0 d_0$. Or $\binom{m+(d-v_0 d_0)}{m} \sim d^m/m!$ quand d tend vers l'infini (ici, m, d_0, v_0 et D sont des constantes). Puisqu'on peut choisir v_0 entre 0 et D, on en déduit que le nombre de solutions de $(\star)$ est au moins

$$\sum_{v_0=0}^{D} \binom{m + (d - v_0 d_0)}{m} / D \sim \frac{(D+1) d^m}{D m!}.$$

Pour d grand, le polynôme H a donc plus de $(1 + 1/(2D)) d^m/m!$ monômes.

Soit maintenant $G(x_1, \ldots, x_m) = H(p_0, \ldots, p_m)$: le degré de G est au plus d puisque $v_0 d_0 + \ldots + v_m d_m \leq d$, donc G a $\leq \binom{d+m}{m} \sim d^m/m!$ coefficients par le lemme A. Pour d grand, le nombre de coefficients de G est donc moins de $(1 + 1/(2D)) d^m/m!$.

Chaque coefficient de G est une combinaison linéaire des coefficients $c_{\bar{v}}$. La contrainte $H(p_0, \ldots, p_m) = 0$ se traduit donc en moins de $(1 + 1/(2D)) d^m/m!$ équations linéaires en les coefficients $c_{\bar{v}}$ (le coefficient de chaque monôme doit être nul). Ce système a une solution non nulle car le nombre d'inconnues est plus grand que le nombre d'équations. □

En appliquant le lemme précédent au cas de polynômes calculés par un circuit, on peut maîtriser le degré du polynôme annulateur en fonction de la taille du circuit.

C. Lemme – Soit C un circuit arithmétique de taille t, calculant n polynômes $p_1, \ldots, p_n \in K[x_1, \ldots, x_n]$. Alors pour tout polynôme $p_0 \in K[x_1, \ldots, x_n]$, il existe un polynôme non nul $H \in K[y_0, \ldots, y_n]$ tel que $\deg_{y_0}(H) \leq 2^t$ et $H(p_0, \ldots, p_n) = 0$.

Démonstration. On numérote les portes de C de 1 à t de sorte que les $n + k$ premières portes soient les variables $x_1, \ldots, x_n$ et les constantes $\alpha_1, \ldots, \alpha_k$, et on introduit t nouvelles variables $z_1, \ldots, z_t$. Pour tout i entre 1 et $(t + n)$, on définit un polynôme $f_i \in K[x_1, \ldots, x_n, z_1, \ldots, z_t]$ de la manière suivante :

- pour $1 \leq i \leq n$ (portes correspondant aux variables $x_1, \ldots, x_n$), $f_i = z_i - x_i$;
- pour $n + 1 \leq i \leq n + k$ (portes correspondant aux constantes $\alpha_1, \ldots, \alpha_k$), $f_i = z_i - \alpha_{i-n}$;
- pour $n + k + 1 \leq i \leq t$, si la porte i est une opération $\circ \in \{+, \times\}$ d'arguments j et j', alors $f_i = z_i - (z_j \circ z_{j'})$;
- enfin, pour $i > t$, soit j_{i-t} la porte calculant p_{i-t} : on définit alors $f_i = z_{j_{i-t}}$.

Au plus t de ces polynômes ont un degré 2, les autres ayant un degré ≤ 1. Par le lemme B, il existe donc un polynôme non nul $G \in K[y_0, \ldots, y_{t+n}]$ tel que $\deg_{y_0}(G) \leq 2^t$ et $G(p_0, f_1, \ldots, f_{t+n}) = 0$.

On peut voir $G(p_0, f_1, \ldots, f_{t+n})$ comme un polynôme de $(K[x_1, \ldots, x_n])[z_1, \ldots, z_t]$. Alors, par définition des polynômes f_i, remarquons que, si $g_i(\bar{x})$ est le polynôme calculé par la porte i, on a :

$$[G(p_0, f_1, \ldots, f_t, f_{t+1}, \ldots, f_{t+n})](g_1, \ldots, g_t) = G(p_0, 0, \ldots, 0, p_1, \ldots, p_n) = 0,$$

l'égalité portant sur des polynômes de $K[x_1, \ldots, x_n]$ (puisque $g_i \in K[x_1, \ldots, x_n]$). Ainsi, $H(y_0, \ldots, y_n) = G(y_0, 0, \ldots, 0, y_1, \ldots, y_n)$ est le polynôme recherché. □

Rappel On dit que *presque tout* point $x \in K^n$ vérifie une propriété s'il existe un polynôme non nul $f \in K[x_1, \ldots, x_n]$ tel que x vérifie la propriété dès que $f(x) \neq 0$ (c'est-à-dire que la propriété est vraie partout sauf éventuellement sur une hypersurface).

Voici le résultat principal de cette section : la "degree bound" de Strassen.
D. Théorème – Soient des polynômes $p_1, \ldots, p_n \in \mathbb{C}[x_1, \ldots, x_n]$ et un entier $d \geq 1$ tels que pour presque tout point $\bar{v} = (v_1, \ldots, v_n) \in \mathbb{C}^n$, le système d'équations $(p_i(\bar{x}) = v_i)_{1 \leq i \leq n}$ a au moins d solutions distinctes sur $\mathbb{C}^n$ (propriété $(\star)$). Alors tout circuit calculant les n polynômes $p_1, \ldots, p_n$ a une taille au moins $\log_2(d)$.

Démonstration. Soit C un circuit de taille minimale t calculant $p_1, \ldots, p_n$. On introduit n nouvelles variables $z_1, \ldots, z_n$ et on considère le calcul de C sur le corps $K = \mathbb{C}(z_1, \ldots, z_n)$. Soit $p_0 = z_1 x_1 + \ldots + z_n x_n \in K[x_1, \ldots, x_n]$: le lemme C fournit un polynôme $H \in K[y_0, \ldots, y_n]$ tel que $\deg_{y_0}(H) \leq 2^t$ et $H(p_0, \ldots, p_n) = 0$, qu'on peut écrire

$$H(y_0, \ldots, y_n) = \sum_{i=0}^{M} q_i(y_1, \ldots, y_n) y_0^i,$$

où $M \leq 2^t$ et $q_M \neq 0$. Ainsi, le polynôme P défini par $P(\bar{x}) = H(p_0, \ldots, p_n)(\bar{x})$ est nul ; en d'autres termes :

$$P(\bar{x}) = \sum_{i=0}^{M} q_i(p_1(\bar{x}), \ldots, p_n(\bar{x}))(\sum_{j=1}^{n} z_j x_j)^i = 0.$$

Soit $f \in \mathbb{C}[x_1, \ldots, x_n]$ un polynôme tel que $(\star)$ soit vérifiée pour tout point $\bar{v} \in \mathbb{C}^n$ dès lors que $f(\bar{v}) \neq 0$, et soit $\bar{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ tel que $f(\bar{\alpha}) \neq 0$ et $q_M(\bar{\alpha}) \neq 0$. Par hypothèse, le système d'équations $(p_i(\bar{x}) = \alpha_i)_i$ a au moins d solutions $\bar{a}^{(1)}, \ldots, \bar{a}^{(d)} \in \mathbb{C}^n$: pour tout i, j, $p_i(\bar{a}^{(j)}) = \alpha_i$. Soit $b^{(i)} = p_0(\bar{a}^{(i)}) = \sum_j z_j a_j^{(i)} \in K$: on a, pour tout k,

$$P(\bar{a}^{(k)}) = \sum_{i=0}^{M} q_i(p_1(\bar{a}^{(j)}), \ldots, p_n(\bar{a}^{(j)}))(\sum_{j=1}^{n} z_j a_j^{(k)})^i = \sum_{i=0}^{M} q_i(\alpha_1, \ldots, \alpha_n)(b^{(k)})^i = 0.$$

Ainsi, les $b^{(i)}$ sont d racines distinctes du polynôme non nul

$$h(x) = \sum_{j=0}^{M} q_j(\bar{\alpha}) x^j \in K[x],$$

donc $2^t \geq M \geq d$, c'est-à-dire $t \geq \log_2 d$. □

1.2 Dérivées partielles

Nous avons vu comment montrer une borne inférieure pour plusieurs polynômes calculés simultanément ; nous allons maintenant voir comment se ramener au calcul d'un seul polynôme, en utilisant ses dérivées partielles. On appellera *porte d'opération* toute porte qui n'est pas une entrée dans un circuit arithmétique (c'est-à-dire ni une variable ni une constante).

E. Lemme – Soit $p(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ un polynôme calculé par un circuit arithmétique ayant t portes d'opération. Alors il existe un circuit arithmétique à n sorties ayant $\leq 5t$ portes d'opération, les mêmes entrées et les constantes 0 et 1, calculant toutes les dérivées partielles $\frac{\partial p}{\partial x_i}(x_1, \ldots, x_n)$.

Démonstration. Par récurrence sur t. Soit $C(x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_k)$ un circuit arithmétique à t portes d'opérations calculant p, où les α_i sont des constantes. Pour $t = 0$, soit $p = x_i$ soit $p = \alpha_i$ et dans les deux cas on calcule ses dérivées partielles par un circuit ayant 0 porte d'opération (puisqu'il s'agit des constantes 0 et 1).

Pour $t \geq 1$: soit g une porte dont les deux arguments sont des entrées (constantes ou variables). Sans perte de généralité, on peut considérer qu'au moins l'un des arguments est une variable : en effet, si les deux arguments sont des constantes α, β, on peut remplacer la porte g par une nouvelle constante $g(\alpha, \beta)$ sans changer la taille du circuit.

On considère le circuit C' ayant $(t-1)$ portes d'opérations et dont les entrées sont $x_1, \ldots, x_n, \alpha_1, \ldots, \alpha_k, g$. Ce circuit calcule un polynôme $q(x_1, \ldots, x_n, y)$ (où y est la nouvelle variable créée par la nouvelle entrée g). On a : $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n, g)$ et donc

$$\frac{\partial p}{\partial x_i}(x_1, \ldots, x_n) = \frac{\partial q}{\partial x_i}(x_1, \ldots, x_n, g) + \frac{\partial q}{\partial y}(x_1, \ldots, x_n, g)\frac{\partial g}{\partial x_i}.$$

Par induction, il existe un circuit D' à $(n+1)$ sorties, ayant $\leq 5t-5$ portes d'opérations, calculant $\frac{\partial q}{\partial x_i}$ (pour $1 \leq i \leq n$) et $\frac{\partial q}{\partial y}$. Nous allons maintenant considérer les différents cas possibles pour la porte g pour construire un circuit D calculant toutes les dérivées partielles de p.

1. Addition d'une constante et d'une variable, $g(x_a, \alpha_b) = \alpha_b + x_a$: pour tout $i \neq a$, $\frac{\partial g}{\partial x_i} = 0$ et donc $\frac{\partial p}{\partial x_i} = \frac{\partial q}{\partial x_i}$. Pour $i = a$: $\frac{\partial p}{\partial x_a} = \frac{\partial q}{\partial x_a} + \frac{\partial q}{\partial y}$. Pour calculer toutes les dérivées partielles de p, il suffit donc d'ajouter une porte (une addition) ; par ailleurs, il faut également calculer g, ce qui ajoute une porte. La taille de D est donc $\leq 5t-3$.
2. Multiplication d'une constante et d'une variable, $g(x_a, \alpha_b) = \alpha_b x_a$: pour tout $i \neq a$, $\frac{\partial g}{\partial x_i} = 0$ et donc $\frac{\partial p}{\partial x_i} = \frac{\partial q}{\partial x_i}$. Pour $i = a$: $\frac{\partial p}{\partial x_a} = \frac{\partial q}{\partial x_a} + \alpha_b \frac{\partial q}{\partial y}$. Pour calculer toutes les dérivées partielles de p, il suffit donc d'ajouter 2 portes (une multiplication et une addition) ; par ailleurs, il faut également calculer g, ce qui ajoute une porte. La taille de D est donc $\leq 5t-2$.
3. Addition de deux variables, $g(x_a, x_b) = x_a + x_b$: pour tout $i \neq a, b$, $\frac{\partial g}{\partial x_i} = 0$ et donc $\frac{\partial p}{\partial x_i} = \frac{\partial q}{\partial x_i}$. Pour $i = a$: $\frac{\partial p}{\partial x_a} = \frac{\partial q}{\partial x_a} + \frac{\partial q}{\partial y}$, de même pour $i = b$. Pour calculer toutes les dérivées partielles de p, il suffit donc d'ajouter 2 portes (deux additions) ; par ailleurs, il faut également calculer g, ce qui ajoute une porte. La taille de D est donc $\leq 5t-2$.
4. Multiplication de deux variables, $g(x_a, x_b) = x_a x_b$: pour tout $i \neq a, b$, $\frac{\partial g}{\partial x_i} = 0$ et donc $\frac{\partial p}{\partial x_i} = \frac{\partial q}{\partial x_i}$. Pour $i = a$: $\frac{\partial p}{\partial x_a} = \frac{\partial q}{\partial x_a} + x_b \frac{\partial q}{\partial y}$, de même pour $i = b$. Pour calculer toutes les dérivées partielles de p, il suffit donc d'ajouter 4 portes (deux multiplications et deux additions) ; par ailleurs, il faut également calculer g, ce qui ajoute une porte. La taille de D est donc $\leq 5t$.

Dans tous les cas, il existe un circuit D ayant $\leq 5t$ portes d'opération, les mêmes entrées que C et les constantes 0 et 1, et calculant toutes les dérivées partielles de p. □

En comptant cette fois les entrées, on obtient le corollaire suivant.

F. Corollaire – Soit $p(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_N]$ un polynôme calculé par un circuit arithmétique de taille t. Alors il existe un circuit arithmétique de taille $\leq 5t$ à n sorties calculant toutes les dérivées partielles $\frac{\partial p}{\partial x_i}(x_1, \ldots, x_n)$.

Démonstration. Soit C un circuit de taille t pour $p(\bar{x})$ et soit $m \geq 1$ le nombre d'entrées (variables et constantes). Alors le nombre de portes d'opérations est $t - m$, donc en comptant les constantes 0 et 1, le lemme E fournit un circuit de taille $\leq 2 + m + 5(t - m) = 5t - 4m + 2 \leq 5t$ pour les dérivées partielles. □

Le calcul des dérivées partielles combiné à la borne du degré permet de déduire des bornes inférieures sur le calcul d'un polynôme seul.

G. Corollaire – Tout circuit arithmétique calculant le polynôme $p(x_1, \ldots, x_n) = \sum_i x_i^d$ a une taille $\Omega(n \log d)$.

Démonstration. Soit t la taille d'un plus petit circuit pour p. Par le corollaire F, il existe un circuit de taille $\leq 5t$ calculant toutes les dérivées partielles de p, c'est-à-dire calculant dx_i^{d-1} pour tout i.

Or $dx^{d-1} = \alpha \in \mathbb{C}$ a exactement $(d-1)$ racines distinctes, sauf pour $\alpha = 0$. Ainsi, pour presque tout $\bar{v} \in \mathbb{C}^n$ (tous sauf les racines du polynôme $\prod_i x_i$), le système $(dx_i^{d-1} = v_i)_{i=1..n}$ a $(d-1)^n$ solutions distinctes. Par le théorème D, $5t \geq \log_2((d-1)^n)$. Ainsi, $t = \Omega(n \log d)$. □

2 Lipton et Schnorr

Nous allons maintenant voir une meilleure borne inférieure mais pour un polynôme construit pour cela ("non naturel"). La difficulté ici est la présence de constantes arbitraires de $\mathbb{C}$, ce qui empêche d'utiliser un argument de comptage. Mais commençons par spécifier sur quel genre de polynôme doit porter la borne inférieure.

2.1 Bornes inférieures triviales

Les bornes inférieures suivantes ne sont pas intéressantes.

- Le polynôme $p(x) = x^{2^t}$ ne peut pas être calculé par des circuits de taille $< t$.
- Le polynôme $p(x_1, \ldots, x_t) = \sum_i x_i$ ne peut pas être calculé par des circuits de taille $< t$.
- Si $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$ sont algébriquement indépendants, alors le polynôme $p(x) = \sum_i \alpha_i x^i$ ne peut pas être calculé par des circuits de taille $< t$.

Pour obtenir un résultat intéressant, pour tout k nous voulons une borne inférieure $\Omega(n^k)$ sur un polynôme p à une variable, de degré polynomial en n et à coefficients dans $\{0, 1\}$. Remarquons qu'un tel polynôme est toujours calculable par un circuit arithmétique de taille polynomiale.

2.2 Borne inférieure en n^k

Nous travaillons donc maintenant sur des polynômes univariés. Nous nous intéressons encore une fois à des relations polynomiales, mais cette fois entre les coefficients d'un polynôme calculé par un circuit.

H. Lemme – Pour tout t, il existe une famille de polynômes $g_j \in \mathbb{Z}[y_1, \ldots, y_{t^2+2t}]$, $j \in \mathbb{N}$, $\deg(g_j) \leq 3tj + 1$, satisfaisant la propriété suivante.

Si $f(x)$ est calculé par un circuit C de taille $\leq t$ alors $\exists \alpha_1, \ldots, \alpha_{t^2+2t} \in \mathbb{C}$ tels que pour tout j le coefficient de x^j dans $f(x)$ est $g_j(\alpha_1, \ldots, \alpha_{t^2+2t})$.

Démonstration. On numérote à partir de 1 les portes non constantes de C de manière compatible avec leur profondeur. On va définir des polynômes $h_i \in \mathbb{C}[x, \bar{y}, \bar{y}']$ pouvant simuler le calcul de la porte i, et $h_{i,j} \in \mathbb{C}[\bar{y}, \bar{y}', \bar{z}]$ sera le coefficient de x^j dans h_i. On prendra alors $g_j = h_{t,j}$. De plus, on définit $h_0 = 1$. Afin de maîtriser le degré, on traite les coefficients constants à part : pour tout i on pose $h_{i,0} = z_i$ (z_i représente donc le coefficient constant de la porte i).

On pose $h_1 = x$, polynôme calculé par la porte 1, donc $h_{1,1} = 1$ et $h_{1,j} = 0$ pour $j \neq 1$. Puis par récurrence on définit pour $i > 1$

$$h_i = (\sum_{k=0}^{i-1} y_{k,i} h_k)(\sum_{k=0}^{i-1} y'_{k,i} h_k),$$

et donc pour $j > 0$:

$$h_{i,j} = \sum_{j_1+j_2=j} \sum_{k_1,k_2<i} y_{k_1,i} y'_{k_2,i} h_{k_1,j_1} h_{k_2,j_2}.$$

On a $h_i \in \mathbb{Z}[x, \bar{y}, \bar{y}']$ et $h_{i,j} \in \mathbb{Z}[\bar{y}, \bar{y}', \bar{z}]$ (les variables z_k représentant les coefficients constants).

Il existe des valeurs $\bar{\alpha}$ et $\bar{\alpha}' \in \mathbb{C}$ pour les $\bar{y}$ et $\bar{y}'$ telles que $h_i(x, \bar{\alpha}, \bar{\alpha}')$ soit le polynôme calculé par la porte i :

- si la porte i est une addition $h_{i_1} + h_{i_2}$, il suffit de prendre $\alpha_{i_1,i} = \alpha_{i_2,i} = 1$, $\alpha'_{0,i} = 1$ et le reste à 0 ;
- si la porte i est une multiplication $h_{i_1} h_{i_2}$, il suffit de prendre $\alpha_{i_1,i} = \alpha'_{i_2,i} = 1$ et le reste à 0 ;
- si la porte i est une multiplication par une constante γh_{i_1}, il suffit de prendre $\alpha_{i_1,i} = \gamma$, $\alpha'_{0,i} = 1$ et le reste à 0 ;
- enfin, si la porte i est une addition avec une constante $\gamma + h_{i_1}$, il suffit de prendre $\alpha_{0,i} = \gamma$, $\alpha_{i_1,i} = 1$, $\alpha'_{0,i} = 1$ et le reste à 0.

Si par ailleurs on donne aux variables z_i la valeur β_i du coefficient constant de la porte i, alors $h_{i,j}(\bar{\alpha}, \bar{\alpha}', \bar{\beta})$ est le coefficient de x^j de la porte i.

Les variables de $h_{t,j}$ sont $y_{i,k}$ et $y'_{i,k}$ pour $1 \leq i \leq t$ et $0 \leq k < i$, ainsi que z_i pour $1 \leq i \leq t$, donc $h_{t,j}$ a $t(t+1) + t = t^2 + 2t$ variables.

En outre, on montre par récurrence sur i que $\deg(h_{i,j}) \leq 3ij + 1$: c'est vrai pour $i = 1$ et, $\forall i$, pour $j = 0$. Pour $i > 1$ et $j > 0$: $\deg(h_{i,j}) \leq 2 + \max_{j_1+j_2=j; k_1,k_2<i}(\deg(h_{k_1,j_1}) + \deg(h_{k_2,j_2})) \leq 2 + 3(i-1)j + 2 = 3ij + 4 - 3j \leq 3ij + 1$.

Ainsi, $g_j = h_{t,j}$ vérifie la propriété demandée. □

I. Lemme – Si $g_1, \ldots, g_{t^3} \in \mathbb{Z}[x_1, \ldots, x_{t^2+2t}]$, $\deg(g_i) \leq 3t^4+1$, alors il existe un polynôme non nul $H \in \mathbb{Z}[y_1, \ldots, y_{t^3}]$, $\deg(H) \leq t^4$, tel que $H(g_1, \ldots, g_{t^3}) = 0$.

Démonstration. On écrit le système que doivent vérifier les coefficients du polynôme $H = \sum_{i_1,\ldots,i_{t^3}} \alpha_{i_1,\ldots,i_{t^3}} y_1^{i_1} \ldots y_{t^3}^{i_{t^3}}$: on doit avoir $H = \sum_{i_1,\ldots,i_{t^3}} \alpha_{i_1,\ldots,i_{t^3}} g_1(\bar{x})^{i_1} \ldots g_{t^3}(\bar{x})^{i_{t^3}} = 0$. Le coefficient de chaque monôme est une combinaison linéaire des α, donc on a un système linéaire en α. Le nombre d'inconnues est au moins t^{t^3} puisque chaque i_j peut prendre n'importe quelle valeur entre 0 et t.

Par ailleurs, le nombre d'équations est égal au nombre de monômes en $\bar{x}$: puisqu'il y a $t^2 + 2t$ variables x_i et que le degré de chaque monôme est $\leq \sum_{j=1}^{t^3} i_j \deg(g_j) \leq t^3 \times t^4 \times (3t^4 + 1) < t^{12}$, il y a au plus $t^{12(t^2+2t)}$ monômes.

Il y a donc plus d'inconnues que d'équations, donc le système admet une solution non nulle. □

Les deux lemmes précédents nous donnent le résultat suivant.

J. Corollaire – Pour tout t, il existe un polynôme non nul $H \in \mathbb{Z}[y_1, \ldots, y_{t^3}]$, $\deg(H) \leq t^4$, tel que pour tout $f(x) = \sum_{i=1}^{t^3} \gamma_i x^i$ calculé par un circuit de taille t, $H(\gamma_1, \ldots, \gamma_{t^3}) = 0$.

Démonstration. Par le lemme H, il existe $\bar{\alpha} \in \mathbb{C}$ tel que $\gamma_i = g_i(\bar{\alpha})$, et $\deg(g_i) \leq 3t^4 + 1$ pour $1 \leq i \leq t^3$. Par le lemme I, il existe H tel que $H(g_1, \ldots, g_{t^3}) = 0$. En évaluant $H(g_1, \ldots, g_{t^3})$ en $\bar{\alpha}$, on obtient $H(\gamma_1, \ldots, \gamma_{t^3}) = 0$. □

Enfin, le lemme suivant montre qu'un polynôme non nul ne peut pas s'annuler en tous les points de petite valeur.

K. Lemme – Soit un polynôme non nul $H \in \mathbb{Z}[y_1, \ldots, y_{t^3}]$ tel que $\deg(H) \leq n^4$. Alors il existe $a_1, \ldots, a_{t^3} \in \{0, \ldots, t^4\}$ tel que $H(a_1, \ldots, a_{t^3}) \neq 0$.

Démonstration. Il s'agit d'un résultat classique (voir par exemple Schwartz-Zippel). Montrons par récurrence sur le nombre n de variables que si p est un polynôme non nul de degré d à n variables, alors il existe $\bar{a} \in \{0, \ldots, d\}$ tel que $p(\bar{a}) \neq 0$.

Pour $n = 1$, le nombre de racines ne peut être plus grand que le degré.

Pour $n > 1$: on peut écrire p sous la forme $p(x_1, \ldots, x_n) = \sum_i p_i(x_2, \ldots, x_n) x_1^i$ où les x_i sont des polynômes à $(n-1)$ variables de degré $\leq d - i$. Puisque p est non nul, il existe i_0 tel que p_{i_0} est non nul. Le degré de p_{i_0} est $\leq d$. Par hypothèse de récurrence, il existe $a_2, \ldots, a_n \in \{0, \ldots, d\}$ tel que $p_{i_0}(a_2, \ldots, a_n) \neq 0$. Ainsi, le polynôme à une variable $q(x_1) = p(x_1, a_2, \ldots, a_n)$ est non nul et de degré $\leq d$: il existe donc $a_1 \in \{0, \ldots, d\}$ tel que $q(a_1) = p(a_1, \ldots, a_n) \neq 0$. □

Nous sommes maintenant prêts pour la borne inférieure : en effet, du corollaire J et du lemme K on déduit le résultat suivant.

L. Corollaire – Pour tout t, il existe $a_1, \ldots, a_{t^3} \in \{0, \ldots, t^4\}$ tel que le polynôme $\sum_{i=1}^{t^3} a_i x^i$ n'a pas de circuits de taille t.

Enfin, on peut ramener les coefficients dans $\{0, 1\}$.

M. Corollaire – Pour tout t, il existe $b_1, \ldots, b_{t^3} \in \{0, 1\}$ tel que le polynôme $\sum_{i=1}^{t^3} b_i x^i$ n'a pas de circuits de taille $t/(4 \log t)$.

En particulier (choisir $t = n^{k+1}$) : pour tout k, il existe $b_1, \ldots, b_{n^{3(k+1)}} \in \{0, 1\}$ tel que le polynôme $\sum_{i=1}^{n^{3(k+1)}} a_i x^i$ n'a pas de circuits de taille n^k.

Démonstration. Soient $a_1, \ldots, a_{t^3}$ les coefficients donnés par le corollaire L : soit $a_i = \sum_{j=0}^{m} a_{i,j} 2^j$ leur décomposition en base 2, avec $m = \log(t^4) = 4 \log t$ et $a_{i,j} \in \{0, 1\}$. Alors

$$p(x) = \sum_{j=0}^{m} 2^j \sum_i a_{i,j} x^i$$

donc l'un des polynômes $\sum_i a_{i,j} x^i$ n'a pas de circuits de taille $t/(4 \log t)$. □

Remarque – En menant des calculs plus précis, on peut obtenir t^2 plutôt que t^3 pour le degré de notre polynôme.

Question ouverte – Peut-on calculer ces coefficients b_i efficacement ? Existe-t-il un polynôme de "VNP^0 uniforme" qui n'a pas de circuits de taille n^k ?

3 Kabanets et Impagliazzo

Cette partie est dédiée au résultat de Kabanets et Impagliazzo (2004) : dérandomiser le test d'identité de polynômes implique une borne inférieure non uniforme. Commençons par la définition du problème d'identité de polynômes et d'une variante sur les entiers.

N. Définition – Le problème PIT (polynomial identity testing) est le problème de décision suivant :

- entrée : un circuit arithmétique, avec pour seule constante -1, calculant un polynôme $p \in \mathbb{Z}[x_1, \ldots, x_m]$;
- question : p est-il identiquement nul ?

On définit également une restriction IIT (integer identity testing) aux circuits calculant des entiers :

- entrée : un circuit arithmétique sans variable et avec pour seule constante -1, calculant un entier $N \in \mathbb{Z}$;
- question : $N = 0$?

En réalité, ces deux problèmes sont équivalents ; pour le montrer, nous avons besoin du lemme suivant.

O. Lemme – Si $p \in \mathbb{Z}[x_1, \ldots, x_n]$ est un polynôme de degré d et dont les coefficients sont majorés en valeur absolue par M, alors pour tout $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ vérifiant $\alpha_1 \geq M + 1$ et $\alpha_{i+1} \geq 1 + M(d+1)^i \alpha_i^d$, on a : $p = 0$ ssi $p(\alpha) = 0$.

Démonstration. Par récurrence sur le nombre de variables n. Si $n = 1$: si $p \neq 0$ alors p s'écrit $p(x) = \sum_{i=0}^{m} a_i x^i$ avec $a_m \neq 0$. Alors $|p(\alpha_1)| \geq \alpha_1^m - |\sum_{i<m} a_i \alpha_1^i|$; or $|\sum_{i<m} a_i \alpha_1^i| \leq M \sum_{i=0}^{m-1} \alpha_1^i = M(\alpha_i^m - 1)/(\alpha_1 - 1) < \alpha_1^m$ car $\alpha_1 \geq M + 1$: donc $p(\alpha_1) \neq 0$.

Pour $n > 1$: soient p_i tels que $p(x_1, \ldots, x_n) = \sum_{i=0}^{d} p_i(x_1, \ldots, x_{n-1}) x_n^i$; si $p \neq 0$ alors il existe i_0 tel que p_{i_0} est non nul. Puisque p_{i_0} est de degré $\leq d$ et a ses coefficients majorés en valeur asbolue par M, par récurrence $p_{i_0}(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Ainsi, $q(x_n) = p(\alpha_1, \ldots, \alpha_{n-1}, x_n)$ est un polynôme non nul à une variable et ses coefficients sont les $p_i(\alpha_1, \ldots, \alpha_{n-1})$: ils sont donc majorés en valeur absolue par $M(d+1)^{n-1}\alpha_{n-1}^d$ puisque p_i a $\leq (d+1)^{n-1}$ monômes et ses coefficients sont $\leq M$. Par le cas $n = 1$, si $\alpha_n \geq 1 + M(d+1)^{n-1}\alpha_{n-1}^d$, alors $q(\alpha_n) \neq 0$. Ainsi, $p(\alpha_1, \ldots, \alpha_n) \neq 0$. □

On a également besoin d'un lemme sur la valeur maximale des coefficients d'un polynôme calculé par un circuit.

P. Lemme – Si $p \in \mathbb{Z}[x_1, \ldots, x_n]$ est calculé par un circuit de taille t (sans autre constante que (-1)), alors les coefficients de p sont majorés en valeur absolue par $2^{2^{2t}}$.

Démonstration. Un polynôme en n variables calculé par un circuit de taille t a un degré $\leq 2^t$. Ainsi, il a au plus $(1 + 2^t)^n$ monômes.

On montre le résultat par récurrence sur t. Pour $t = 1$, le résultat est clair puisque le polynôme calculé est soit la constante -1 soit une variable x_i. Pour $t > 1$, soit C un circuit de taille t et $g = g_1 \circ g_2$ sa porte de sortie, où $\circ \in \{\times, +\}$. Par hypothèse de récurrence, les coefficients de g_1 et g_2 ont tous leur valeur absolue majorée par $\alpha_{t-1} = 2^{2^{2(t-1)}}$.

Si $g = g_1 + g_2$ alors les coefficients de g sont tous la somme d'un coefficient de g_1 et d'un coefficient de g_2 donc ils sont majorés en valeur absolue par $2\alpha_{t-1}$.

Si $g = g_1 g_2$ alors les coefficients de g sont la somme d'au plus $(1 + 2^t)^n$ produits d'un coefficient de g_1 et d'un coefficient de g_2 donc ils sont majorés en valeur absolue par $(1 + 2^t)^n \alpha_{t-1}^2$.

Puisque $n \leq t$ on a donc dans les deux cas : $\alpha_t \leq (1 + 2^t)^t \alpha_{t-1}^2 \leq 2^{2t^2} 2^{2 \times 2^{2(t-1)}} \leq 2^{2^{2t}}$.
□

Nous pouvons enfin voir que PIT et IIT sont équivalents. Puisque IIT est une restriction de PIT, il est clair que IIT se réduit à PIT ; le lemme suivant montre la réciproque.
Q. Lemme – Le problème PIT se réduit au problème IIT pour les réduction many-one polynomiales : PIT $\leq_m^p$ IIT.

Démonstration. Soit C une instance de PIT de taille t et $p \in \mathbb{Z}[x_1, \ldots, x_n]$ le polynôme calculé par C. Les coefficients de p sont majorés en valeur absolue par $2^{2^{2^t}}$ et son degré par 2^t.

Par le lemme O, $p = 0$ ssi $p(\alpha_1, \ldots, \alpha_n) = 0$ dès que $\alpha_1 > 2^{2^{2^t}}$ et $\alpha_{i+1} > 2^{2^{2^t}}(1 + 2^t)^i \alpha_i^{2^t}$. On peut prendre $\alpha_i = 2^{2^{2(i+1)t}}$, qui est calculable par $2(i+1)t$ élévations au carré successives. Ainsi, notre instance de IIT est $C(\alpha_1, \ldots, \alpha_n)$, calculable en temps polynomial à partir de C. □

Nous donnons maintenant un algorithme probabiliste polynomial pour IIT (et donc pour PIT par le lemme Q).
R. Lemme – IIT $\in$ coRP, c'est-à-dire qu'il existe un algorithme probabiliste polynomial tel que si $C \in$ IIT alors C est accepté avec probabilité 1, et si $C \notin$ IIT alors C est rejeté avec probabilité $\geq 2/3$.

Démonstration. Soit N l'entier calculé par une instance C de IIT de taille n. On ne peut pas calculer N en temps polynomial car il est potentiellement trop grand mais on peut l'évaluer modulo des entiers aléatoires. Voici l'algorithme probabiliste.
- Répéter $O(n^2)$ fois :
  - choisir $m \in \{2, \ldots, 2^{n^2}\}$ au hasard,
  - évaluer N mod m.
- Rejeter ssi au moins l'une des évaluations est non nulle.

Si $N = 0$ alors l'algorithme accepte C.

Si $N \neq 0$: puisque $N \leq 2^{2^n}$, il a au plus 2^n diviseurs premiers. Or, par le théorème des nombres premiers, il existe une constante $c > 0$ telle que le nombre de nombres premiers dans l'intervalle $[2, 2^{n^2}]$ est $\geq c2^{n^2}/n^2$. Ainsi, si k est choisi au hasard dans $\{2, \ldots, 2^{n^2}\}$, $\Pr(k \text{ ne divise pas } N) \geq \Pr(k \text{ ne divise pas } N | k \text{ premier}) \Pr(k \text{ premier}) \geq (1 - 2^n/(c2^{n^2}/n^2))c/n^2 \geq c/(2n^2)$. En choisissant $O(n^2)$ moduli k, on a donc une probabilité $\geq 2/3$ que l'un des k ne divise pas N : l'algorithme rejette donc C avec probabilité $\geq 2/3$.

Ainsi, IIT $\in$ coRP. □

Remarque – C'est une question ouverte de savoir si IIT $\in$ P (et donc, bien sûr, de même pour PIT).

Pour cette partie, nous admettrons le résultat le plus difficile… Il est dû à Babai, Fortnow, Lund 1990 pour EXP puis Impagliazzo, Kabanets et Wigderson 2001 pour NEXP. Ici, PH désigne la hiérarchie polynomiale (en fait le résultat est vrai pour la classe MA (Merlin-Arthur) à la place de PH).
S. Lemme – Si NEXP $\subset$ P/poly alors NEXP = PH.

(Idée de la preuve – On montre d'abord que EXP $\subset$ P/poly $\Rightarrow$ EXP = MA : par Karp-Lipton et Meyer, EXP $\subset$ P/poly implique EXP = Σ_2^p = PSPACE = IP, donc pour EXP on peut utiliser le protocole IP de QBF. Dans ce protocole, le prouveur est lui-même dans PSPACE, donc a des circuits de taille polynomiale. Merlin peut alors donner à Arthur le circuit correspondant et Arthur peut simuler le protocole en un seul tour.

Puis on montre que NEXP $\subset$ P/poly $\Rightarrow$ NEXP = EXP : si $L \in$ NEXP $\setminus$ EXP alors pour certains mots $x \in L$, les témoins pour x n'ont pas de circuits de taille polynomiale (sinon

on énumère les circuits). Dans NEXP on peut alors deviner un témoin et l'utiliser pour dérandomiser les protocoles MA pour EXP (en utilisant un générateur pseudo-aléatoire). Ainsi, $\mathsf{EXP} = \mathsf{MA} \subseteq \mathsf{NTIME}(2^{n^k})$ pour un k fixé et donc, si $\mathsf{NEXP} \subset \mathsf{P/poly}$, EXP a des circuits de taille $n^{k'}$ pour k' fixé, ce qui n'est pas possible.)

Rappel Le permanent est le polynôme à n^2 variables $(x_{i,j})_{1 \leq i,j \leq n}$ défini comme suit :

$$\mathrm{per}_n(x_{1,1}, \ldots, x_{1,n}, x_{2,1}, \ldots, x_{n,n}) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} x_{i,\sigma(i)}.$$

Dans la notation $\mathsf{P}^{\mathrm{per}}$, l'oracle permet de calculer en temps unitaire le permanent d'une matrice à coefficients entiers écrite sur le ruban.
T. Lemme – Si PIT $\in$ P et le permanent a des circuits arithmétiques de taille polynomiale ayant pour seule constante -1, alors $\mathsf{P}^{\mathrm{per}} \subseteq \mathsf{NP}$.

Démonstration. Supposons que (per_n) a des circuits arithmétiques de taille n^c. On va simuler le fonctionnement d'une machine $M(x)$ fonctionnant en temps n^d avec oracle per par une machine NP. Remarquons que les requêtes de M à per ne portent pas sur des matrices de taille supérieure à n^d.

Pour cela, on devine des circuits arithmétiques $C_1, C_2, \ldots, C_{n^d}$, où $|C_i| = i^c$, on vérifie que C_i calcule per_i et on simule $M(x)$ en remplaçant les requêtes à l'oracle par l'évaluation d'un circuit C_i. Il suffit donc de voir comment vérifier que les circuits C_i calculent le permanent.

On commence par vérifier que C_1 calcule $\mathrm{per}_1 = x_{1,1}$ en utilisant l'algorithme pour PIT. Puis nous vérifions les circuits suivants les uns après les autres : si $C_1, \ldots, C_{i-1}$ calculent respectivement $\mathrm{per}_1, \ldots, \mathrm{per}_{i-1}$, on vérifie que C_i calcule per_i en vérifiant l'égalité

$$C_i(x_{1,1}, \ldots, x_{i,i}) = \sum_{j=1}^{i} x_{1,j} C_{i-1}(x_{2,1} \ldots, x_{2,j-1}, x_{2,j+1}, \ldots, x_{2,i}, x_{3,1}, \ldots, x_{3,j-1}, x_{3,j+1}, \ldots, x_{i,i})$$

(calcul du permanent en développant selon la première ligne), ce qui se fait en utilisant l'algorithme pour PIT. □

Cela nous permet de montrer le résultat principal de cette partie.
U. Théorème – Si PIT $\in$ P alors soit $\mathsf{NEXP} \not\subset \mathsf{P/poly}$, soit le permanent n'a pas de circuits arithmétiques de taille polynomiale ayant pour seule constante -1.

Démonstration. Supposons que l'on ait à la fois PIT $\in$ P, $\mathsf{NEXP} \subset \mathsf{P/poly}$ et le permanent a des circuits arithmétiques de taille polynomiale ayant pour seule constante -1. Alors par le lemme S, $\mathsf{NEXP} \subseteq \mathsf{PH}$. Le théorème de Toda ($\mathsf{PH} \subseteq \mathsf{P}^{\mathrm{per}}$) implique donc $\mathsf{NEXP} \subseteq \mathsf{P}^{\mathrm{per}}$. Mais par le lemme T, $\mathsf{P}^{\mathrm{per}} \subseteq \mathsf{NP}$, donc $\mathsf{NEXP} \subseteq \mathsf{NP}$, ce qui est contraire au théorème de hiérarchie en temps non déterministe. □

Remarque – En calculant le numérateur et le dénominateur séparément, on peut de la même manière permettre les constantes rationnelles arbitraires dans nos circuits pour le permanent, pour peu qu'elles soient données explicitement en bits.