Straight-Line Computations over Semirings

Loïck Magnin

12 décembre 2006

Résumé

Nous étudions la complexité pour calculer certains polynômes dans des semi-anneaux puis la comparons avec celle des mêmes polynômes mais dans un modèle de calcul moins limitatif (anneau par exemple). Un *gap* exponentiel peut être obtenu. Pour montrer cela, nous allons dans une première partie définir un modèle de calcul, dans la seconde partie, nous allons donner des bornes inférieures dans ce modèle de calcul. Dans la troisième partie, nous allons les appliquer dans différents cas. Enfin nous discuterons des performances de ce modèle de calcul.

1 Modèle de calcul

Comme nous ne savons toujours pas si $\mathcal{P} = \#\mathcal{P}$ (ou non) car cette question est difficile, il est souvent utile, et surtout beaucoup plus simple de se placer dans le cadre de modèles de calculs simples.

Nous nous plaçons dans un semi-anneau. C'est à dire que l'on munit un ensemble $\mathcal{S}$ d'une opération $\oplus$ associative et commutative (son neutre est noté 0) et d'une opération $\otimes$ commutative et distributive sur $\oplus$ (son neutre est noté 1) et tel que $\forall s \in \mathcal{S}, s \otimes 0 = 0$. Nous avons donc un anneau sans soustraction ni division ni nombres strictement négatifs.

Exemples Les systèmes suivants sont des semi-anneaux :
- $(0, 1, \vee, \wedge, 0, 1)$
- $\mathcal{R} = (\mathbb{R}^+, +, \cdot, 0, 1)$
- $\mathcal{M} = (\mathbb{R}^{+*}, \min, +, +\infty, 0)$

Voici maintenant un ensemble de définitions concernant les polynômes

Définition 1
- *Soient* $X = \{x_1, \ldots, x_n\}$ *un ensemble d'inderterminées. On appelle monôme un objet de la forme* $m = x_1^{i_1} \cdot x_2^{i_2} \cdot \cdots \cdot x_n^{i_n}$ *et un polynôme* $p = \oplus_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)} x_1^{i_1} \cdot x_2^{i_2} \cdot \cdots \cdot x_n^{i_n}$. *Cette écriture définit un unique polynôme.*
- $mon(p)$ *est l'ensemble des monômes de* p *tels que* $a_m \neq 0$
- $deg(m) = \sum_{j=1}^{n} i_j$ *et* $deg(p) = \max_{m\in mon(p)} deg(m)$
- p *est homogène si tous ces monômes ont le même degré.*
- p *est linéaire si chaque monôme est linéraire en ses indéterminées* ($i_j \in \{0, 1\}$)
- $\nu p : \mathcal{S}^n \longrightarrow \mathcal{S}$ *est la fonction associée au polynôme* p

Remarque ν n'est pas nécessairement injective, il peut exister deux polynômes p et p' tels que $\nu p = \nu p'$. C'est ce qui est utilisé en abondance dans l'article présenté il y a deux semaines : "A lower bound for monotone arithmetic circuits computing 0-1 permanent".

Le modèle de calcul est celui des circuits arithmétiques de degré entrant de chaque nœud (autre que ceux d'entrée) égal à 2 et de degré sortant égal à 1. On note génériquement ρ le nœd de sortie et Γ le circuit. On note $nodes(\Xi)$ l'ensmble des nœds de Ξ un sous-ensemble connexe de Γ.

À chaque nœud, il est possible d'associer le polynôme "calculé" par le sous-circuit ayant pour sortie ce nœud. On confondra sans se priver un nœud et son polynôme associé afin de ne pas surcharger les notations.

Définition 2
Pour tout α, nœud de Γ, on peut définir
- *complement*(α) *l'ensemble* $\{m \quad \text{tq} \quad \forall m' \in mon(\alpha), mm' \in mon(\rho)\}$
- *content*(α) *l'ensemble* $\{mm' \quad \text{tq} \quad m \in complemen(\alpha), m' \in mon(\alpha)\}$

Dans toute la suite on se place dans le cas de polynômes linéaires. Ils sont donc nécessairement calculés par des circuits multiplicativement disjoints. Pour chaque noeud α et $m \in mon(\alpha)$ on peut définir le développement $PT(\alpha, m)$ de Γ qui calcule m et qui a pour porte de sortie α.

Remarque Un des théorèmes important de l'article sur les 0-1 permanents donne la forme général des circuits qui les calculent. Ils ne sont pas mutltiplicatevement disjoints. Toute la suite diffère donc un peu.

Définition 3
La $\otimes$-complexité d'un circuit Γ est simplement le nombre de portes $\otimes$ dans Γ.

Remarque Il y a là encore une différence avec l'article calculant le 0-1 permanent. Dans toutes la suite nous allons nous intéresser uniquement à la $\otimes$-complexité alors que dans l'article du 0-1 permanent s'intéressait à la complexité totale en nombre de portes et pour cela utilise un circuit alterné : les portes $\oplus$ et $\otimes$ sont alternées. Il est précisé que cela, au pire, multiplie la complexité par 2. Il est ici possible d'avoir des résultats qui diffèrent entre les deux articles. En effet, imaginons un circuit qui a $\mathcal{O}(n)$ portes $\otimes$ et $\mathcal{O}(2^n)$ portes $\oplus$, alors cet article donnera une complexité en $\mathcal{O}(n)$ alors que l'article du 0-1 permanent donnerait $\mathcal{O}(2^n)$.

2 Théorèmes de bornes inférieures

Dans toute cette section, je vais énoncer les théorèmes donnés par l'article sans donner leur preuves dans le détail. Je ne donne que l'idée principale.

Théorème 1
Soit m un élément de $mon(\rho)$. Si $\alpha \in nodes[PT(\rho, m)]$ alors $m \in content(\alpha)$

Preuve On note m_α le monôme calculé par α dans $PT(\rho, m)$. On montre ensuite par induction sur les noeuds de $PT(\rho, m)$ qu'il existe m'_α tel que $m_\alpha m'_\alpha = m$ et $\forall n \in mon(\alpha), m'_\alpha n \in mon(\alpha)$. Cela signifie que $m'_\alpha \in complement(\alpha)$ et $m \in mon(\alpha)$, d'où le résultat $m = m_\alpha m'_\alpha \in content(\alpha)$.

Et dans la "vraie vie", qu'est ce que cela dit ? En substance, cela veut dire qu'un noeud ne peut pas appartenir à beaucoup de développements de Γ ; et c'est justement ce "pas beaucoup" qui va devenir une borne inférieure par la suite.

Définition 4
Soit T un développement de Γ. Le ***poids*** *de T est défini par :*

$$w(T) = \sum_{\alpha \in \otimes - noeuds(T)} |content(\alpha)|^{-1}$$

Théorème 2

$$\sum_{m \in mon(\rho)} w(PT(\rho, m)) \leq |\otimes - noeuds(\Gamma)|$$

Preuve

$$\begin{aligned} \sum_{m \in mon(\rho)} w(PT(\rho, m)) &= \sum_{\alpha \in \otimes - noeuds(\Gamma)} \frac{|\{m \quad \text{tq} \quad \alpha \in \otimes - noeuds(PT(\rho, m))\}|}{|content(\alpha)} \\ &\leq \sum_{\alpha \in \otimes - noeuds(\Gamma)} \frac{|\{m \quad \text{tq} \quad m \in content(\alpha)\}|}{|content(\alpha)} \end{aligned}$$

L'inégalité est obtenue grâce au théorème 1.

Voilà, nous avons une borne inférieure sur le nombre de noeuds $\otimes$. Il nous reste maintenant à lier le poids des développements de Γ avec le polynôme qu'il calcule. Et maintenant, il y a un gros truc pas naturel du tout que l'auteur sort de son chapeau, et on ne voit pas trop ce qui fait marcher le truc, mais bon, ça marche.

Supposons qu'il existe une fonction $c(r, d)$ avec $2 \leq r \leq deg(p)$ et $1 \leq d \leq \lfloor r/2 \rfloor$ qui satisfasse :

$$c(r, d) \geq \max \{|content(\alpha)| \quad \text{tq} \quad \alpha \in \otimes - noeud(\Gamma), deg(\alpha) = r, deg(pred(\alpha)) = \{d, r - d\}\}$$

Théorème 3
Si W est défini par
- $W(1) \leq 0$
- $W(r) \leq min\left\{W(d) + W(r - d) + (c(r, d))^{-1}, 1 \leq d \leq \lfloor r/2 \rfloor\right\}$

alors $\forall \alpha \in nodes(\Gamma), m \in mon(\alpha), w(PT(\alpha, m)) \geq W(deg(\alpha))$

Preuve Par induction sur l'arbre.

Mais ce qui est important, c'est surtout le corollaire suivant :

Corollaire 1
Pour un polynôme p, linéaire et homogène, $|mon(p)| \cdot W(deg(p)) \leq \otimes$-complexité de p.

Voilà la partie pénible est finie, maintenant, nous allons appliquer ce résultat dans 3 cas concrets.

3 Applications

Il y a deux autres applications dans le papier original, mais elle sont moins intéressantes en terme d'étude de complexité. La bonne nouvelle, c'est donc que toute la machinerie mise en place dans la partie précédente ne sert pas uniquement à calculer une borne inférieure du permanent.

3.1 Multiplication de matrices

Ce premier exemple est le plus simple. Nous allons calculer une borne inférieure pour la multiplication d'une chaîne de t matrices $n \times n$,

$$[X]_{ij} = [X^{(1)}X^{(2)} \cdots X^{(T)}]_{ij} = \bigoplus_{1 \leq i_k \leq n} x^{(1)}_{ii_2} x^{(2)}_{i_2 i_3} \cdots x^{(t)}_{i_t j}$$

Nous avons alors n^2 polynômes à calculer, ce qui n'est pas très pratique. Voici donc comment nous nous ramenons à un seul polynôme[1]. Nous allons d'abord définir un polynôme $\tilde{p} = \bigoplus_{1 \leq i,j \leq n} X_{ij}$ ce qui nous donne

$$\tilde{p} = \bigoplus_{1 \leq i_k \leq n} x^{(1)}_{i_1 i_2} x^{(2)}_{i_2 i_3} \cdots x^{(t)}_{i_t i_{t+1}}$$

. Nous remarquons que ce polynôme est potentiellement moins $\otimes$-complexe que de calculer chacun des coéfficients séparément. Une petite astuce nécessaire pour la suite, fait que nous allons en fait considérer le polynôme p suivant :

$$p = \bigoplus_{1 \leq i_k \leq n} x^{(1)}_{i_1 i_2} x^{(2)}_{i_2 i_3} \cdots x^{(t)}_{i_t i_{t+1}} x^{(t+1)}_{i_{t+1} i_1}$$

Nous avons alors

$$\otimes\text{-complexité}(p) - n^2 \leq \otimes\text{-complexité}(\tilde{p}) \leq \otimes\text{-complexité}$$

Nous alons donc maintenant chercher une fonction c qui satisfasse aux hypothèses du théorème 3. Pour faire cela, la démarche est dans la même dans les 3 applications. Nous allons considérer trois polynômes u, v, w de degrés $d, r-d, deg(p)-r$ tels que $mon(uvw) \subseteq mon(p)$ et leur associer trois ensembles I_u, I_v et I_w qui partitionnent $\{1, 2, \ldots, deg(p)\}$, ce qui nous permettra de calculer une fonction c en minorant $|mon(uvw)|$.

Pour la multiplication d'une chaîne de matrices, nous choisisson I_q l'ensemble des exposants des indéterminées qui sont dans q. Nous avons donc triviallement I_u, I_v et I_w disjoints et ils partitionnent comme voulu $\{1, 2, \ldots, t+1\}$.

Considérons maintenant l'ensemble $\mathcal{A}$ des articulations défini par $\mathcal{A} = \{k \in \{1, t+1\}$ tel que k et $k-1 mod(t+1)$ soient dans deux ensembles différents $\}$.

Nous avons alors $|mon(uvw)| \leq n^{t+1-|\mathcal{A}|}$. Si $r < t+1$ alors $|\mathcal{A}| \geq 3$ et si $r = t+1, |\mathcal{A}| \geq 2$. Nous posons donc

$$c(r,d) = \begin{cases} n^{t-2} & (r < t+1) \\ n^{t-1} & (r = t+1) \end{cases}$$

La fonction c est presque constante et satisfait aux hypothèse du théorème 3 (Les inégalités sont en fait des égalités dans ce cas précis), ce qui donne après calculs $W(t+1) = (t-1)n^{2-t} + n^{1-t}$ donc en appliquant le corollaire 1, il vient :

[1] Pas clair du tout dans le papier, d'autant plus qu'il y a plusieurs typos dans les indices.

$$\otimes\text{-complexité(p)} \geq \left((t-1)n^{2-t} + n^{1-t}\right) |mon(p)| = (t-1)n^3 + n^2$$

d'où

$$\otimes\text{-complexité}(\tilde{p}) \geq (t-1)n^3$$

Et donc, là, évidement nous sommes contents, car la borne que l'on trouve avec cette méthodologie n'est pas triviale, mais en plus, c'est un *min* et pas seulement un inf.

3.2 Calcul du permanent

Nous allons faire à peu près la même chose, mais le polynôme est le permanent. Nous rappellons sa définition :

$$per(X) = p = \bigoplus_{\pi \in S(n)} x_{1,\pi(1)} x_{2,\pi(2)} \cdots x_{n,\pi(n)}$$

Nous construisons ici les ensembles $I_q = \{i \quad \text{tq} \quad x_{ij} \text{ soit une indéterminée de } q\}$, et les ensembles "duaux" $J_q = \{j \quad \text{tq} \quad x_{ij} \text{ soit une indéterminée de } q\}$. Les ensembles I_u, I_v et I_w sont triviallement disjoints et nous avons même $|I_u| = d, |I_v| = r - d, |I_w| = n - r$. Ils partitionnent donc $\{1, 2, \ldots, t+1\}$.

De même en considérant que π est une permutation, les mêmes propriétés sont valables pour les J_q.

Les éléments de $mon(uvw)$ sont les permutations de π tels que $\pi(I_q) = J_q$. Il est facile de dénombrer ces permutations, ce qui nous donne

$$c(r, d) = d!(r-d)!(n-r)!$$

La preuve que c vérifie toutes les hypothèses est calculatoire, et le lecteur soucieux de comprendre se rapportera à l'article original. Le calcul de W n'est pas trivial non plus. La seule remarque qui mérite d'être faite est le fait que là encore il y a égalité dans la définition de W dans les hypothèses du théorème 3. Nous trouvons $W(n) = \frac{2^{n-1}-1}{(n-1)!}$. En appliquant le corollaire 1, et puisque p est la somme de $n!$ monômes, il vient :

$$\otimes\text{-complexité}(permanent) \geq n(2^{n-1} - 1)$$

Ici encore la borne est très forte puisqu'il s'agit d'un *min*. L'algorithme est celui de l'expansion de Laplace, qui est une formule à peu près équivalente au développement d'un déterminant, mais dans le cas du permanent.

Remarque L'article du 0-1 permanent donne cette même borne.

3.3 Polynôme d'arbre couvrant

Pour un graphe à n sommets, nous associons à chaque arête dirigiée $i \to j$ l'indéterminée x_{ij}. Soit $T(n) = \{t : \{2, 3, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\} \quad \text{tq} \quad \forall i \, \exists k, \, t^k(i) = 1$. Alors pour tout t de $T(n)$, $x_{2,t(2)} x_{3,t(3)} \cdots x_{n,t(N)}$ représente un arbre couvrant dont sa racine est le sommet 1.

On définit alors le polynôme d'arbre couvrant par

$$p = \bigoplus_{t \in T(n)} x_{2,t(2)} x_{3,t(3)} \cdots x_{n,t(N)}$$

Ce polynôme peut avoir deux interprétations différentes

1. Si on se place dans le semi-anneau $\mathcal{M} = (\mathbb{R}^{+*}, \min, +, +\infty, 0)$ où les $x_{i,j}$ représentent le poids de l'arête, alors ce polynôme correspond au poids de l'arbre couvrant de poids minimal.
2. Si on se place dans le semi-anneau $\mathcal{R} = (\mathbb{R}^{+}, +, \cdot, 0, 1)$ où $(X) = (x_{ij})_{1 \leq i,j \leq n}$ est la matrice d'adjacence du graphe, alors le polynôme correspond au nombre d'arbres couvrants.

Et c'est parti pour le calcul de la borne. Posons $I_q = \{i \quad \text{tq} \quad x_{ij} \text{ soit une indéterminée de } q\}$. ($I_u, I_v$ et I_w forment une partition de $\{1, 2, \ldots, t+1\}$). Nous ne pouvons pas faire comme pour le permanent en posant les ensembles J_q puisqu'ils ne formeraient pas la bonne partition.

Posons $X_i = \{x_{ij} \quad \text{tq} \quad x_{ij} \text{ soit une indéterminée de } u, v \text{ ou } w\}$. On remarque que s'il existe i_1 et i_2 tels que $x_{i_1 i_2}$ soit dans X_{i_1} alors, $x_{i_2 i_1}$ n'est pas dans X_{i_2}. Donc :

$$\sum_{i=2}^{n} |X_i| \leq (n-1)^2 - d(r-d) - r(n-r-1)$$

Le nombre de monômes dans l'ensemble $mon(uvw)$ est clairement borné par le nombre de fonctions de $T(n)$ qui vérifient $x_{i,t(i)} \in X_i$ qui vaut $\Pi_{i=2}^{n} |X_i|$, ce qui donne

$$c(r,d) = \left(\frac{(n-1)^2 - d(r-d) - r(n-r-1)}{n-1} \right)^{n-1}$$

On calcule, on calcule, on remarque que cette fois-ci nous n'avons pas l'égalité dans la définition de W et l'on trouve :

$$\otimes\text{-complexité}(p) \geq \tfrac{1}{n} \left(\tfrac{3}{4}\right)^{n-1}$$

En 1982, quand l'article a été écrit, cette borne n'était pas atteinte. Je n'ai pas trouvé d'article en faisant mention. Cela vient certainement du fait que la borne n'est pas atteignable. En effet, il y a une différence conceptuelle ici par rapport aux deux exemples précédents : lorsqu'on applique le théorème 3, nous avons une inégalité, ce qui nous fait perdre de la précision. Mais cette borne est suffisante cependant pour avoir un *gap* exponentiel avec d'autres modèles de calcul. Nous discutons cela dans la partie suivante.

4 De la validité de ce modèle de calcul

Du pouvoir de la soustraction Nous savons tous que la borne que nous avons trouvée pour la multiplication de matrices n'est pas optimal dans le cas om l'on s'autorise les soustractions : il suffit d'appliquer la méthode de Schonage. Nous améliorons la complexité, mais pas tant que ça (dans le meilleur des cas d'un facteur n). Il est bien plus intéressant de regarder l'exemple des arbres couvrants. Dans ce cas-là, la matrice (X) peut être remaniée et le polynôme peut alors s'exprmier comme un déterminant d'une matrice $n \times n$, ce qui se fait en complexité $\mathcal{O}(n^3)$. Nous pouvons donc avoir un *gap* exponentiel. Pour le permanent, il est possible de faire mieux que notre borne, mais pas beaucoup, puisqu'il existe un algorithme en $(n-1)2^{n-1} + 3$ multiplications. Il serait surprenant d'avoir un *gap* exponentiel ici puisque le permanent est $\#\mathcal{P}$-complet.

Du pouvoir des branchements Ce modèle de calcul est une restriction des SLPs puisque l'on ne peut pas utiliser plusieurs fois un résultat. De toute manière, il était prouvé que les branchements ne pouvaient pas améliorer la complexité dans $\mathcal{R}$, oui, mais pas dans $\mathcal{M}$! Et c'est encore le polynôme d'arbre couvrant qui est le contre exemple. En utilisant les opérations min et $+$, le polynôme peut être calculé en $\mathcal{O}(n^2 \log n)$ si on s'authorise les branchements en plus. Et le permanent s'y met aussi : il peut être calculé en $\mathcal{O}(n^3)$. Moralité : Les branchements peuvent être exponentiellement puissants.

5 Conclusion

Dans ce papier relativement long où les auteurs se perdent parfois un peu dans les détails, ils une méthode pour obtenir une borne inférieure de la complexité en multiplications de polynômes homogènes dans des semi-anneaux. Les auteurs expliquent aussi comment lever la condition d'homogenéité. Les bornes sont souvent très fortes et permettent de montrer que la soustraction et les branchements peuvent améliorer exponentiellement des algorithmes. Le papier souligne aussi le fait que tous les semi-anneaux n'ont pas vraiment le même statut puisqu'avec branchement le calcul du permanent est exponentiellement moins complexe dans $\mathcal{M}$ que dans $\mathcal{R}$. On sent aussi que les auteurs ont éssayé de développer un outil similaire dans le cas de la complexité en nombre d'addition (partie 2, où ils introduisent $le(p)$) mais sans y être parvenus. Il y a donc là, comme je déjà souligné, une différence notable avec l'article sur le 0-1 permanent. L'analyse d'algorithmes dans la "vraie vie" est difficile, c'est pourquoi les auteurs se sont limités ici à un modèle de calcul limité pour dire en substance : "*La vraie vie est plus accomodante que les SLPs*"