Annexe :
La multiplication de matrice rapide

Yann Strozecki

25 décembre 2007

Table des matières

Résumé

Nous allons ici donner une méthode pour borner la complexité (appelée ω) de la multiplication de deux matrices sur un corps de caractéristiques zéro, utilisant la théorie des représentations . Cette méthode ne donne pas encore de résultats aussi bon que ceux de la LASER méthode donnant une borne de 2,38 et due à Coppersmith et Vinograd (on peut trouver toute cette théorie dans Algebraic Complexity Theory de P. Bürgisser, M. Clausen, et M.A. Shokrollahi). Néanmoins elle paraît prometteuse pour enfin prouver $\omega = 2$.

1 Présentation du problème

On peut multiplier de manière rapide deux polynômes grâce à la transformée de Fourier, c'est en fait la même technique qui est utilisée ici. On va expliquer comment réaliser cela dans cette section.

Définition 1. Soit S un sous-ensemble du groupe G, on pose

$$Q(S) = \{ss'^{-1} | s, s' \in S\} = SS^{-1}$$

On dit que $Q(S)$ est le quotient à droite de S.

Définition 2. Soit trois sous-ensembles S, T, U d'un groupe G, on dit que S, T, U vérifie la condition du triple produit (triple product condition) si

$$\forall u, s, t \in Q(U), Q(S), Q(T), (ust = 1) \Leftrightarrow (u = s = t = 1)$$

On dit aussi que G réalise $< |S|, |T|, |U| >$.

On considère l'algèbre du groupe G noté $\mathbb{C}[G]$ dont les éléments sont des sommes formelles d'éléments de G à coefficient dans $\mathbb{C}$, $\sum_{g \in G} a_g g$. On considère les éléments de la forme suivante (où U,S et T sont trois sous-ensembles de G) :

$$A = \sum_{s \in S, t \in T} a_{s,t} s^{-1} t$$

$$B = \sum_{t \in T, u \in U} b_{t,u} t^{-1} u$$

On fait correspondre bijectivement à ces deux éléments de $\mathbb{C}[G]$ les matrices $\overline{A} = (a_{s,t})_{s \in S, t \in T}$ et $\overline{B} = (b_{t,u})_{t \in T, u \in U}$ (bien définies si S, T, U vérifie la condition du triple produit). Si on multiplie l'élément A par l'élément B on obtient l'égalité suivante :

$$A * B = \sum_{f \in G} (\sum_{s^{-1} t t'^{-1} u = f} a_{s,t} b_{t',u}) f$$

Donc si S, T, U vérifie la condition du triple produit, on a comme coefficient devant $s^{-1}u$ dans le produit :

$$\sum_t a_{s,t} b_{t,u}$$

Donc les coefficients devant les $s^{-1}u$ dans AB sont les entrées de la matrice $(\overline{AB})_{s,u}$. On réalise ainsi une multiplication d'une matrice de $M_{|S|,|T|}(\mathbb{C})$ par une autre de $M_{|T|,|U|}(\mathbb{C})$ en multipliant deux éléments de l'algèbre $\mathbb{C}[G]$.

Théorème 1. *On sait représenter l'algèbre d'un groupe fini comme un produit d'espaces matriciels, de la manière suivante :*

$$\mathbb{C}[G] \cong \prod \mathbb{C}^{d_i * d_i}$$

où les d_i sont les degrés des représentations irréductibles de $\mathbb{C}[G]$.

Ce résultat permet de définir un algorithme récursif pour calculer le produit de deux matrices. On associe aux deux matrices qu'on veut multiplier deux éléments de l'algèbre d'un groupe fini comme expliqué précédemment. On sait représenter l'algèbre de groupe par la remarque précédente comme un produit d'espace matriciels. Donc la multiplication des deux matrices de départ correspond à la multiplication d'un certain nombre de matrice (la multiplication dans l'algèbre de groupe correspond à la multiplication composante à composante). On rapplique récursivement l'algorithme aux matrices obtenues.
Le passage d'un élément de l'algèbre de groupe à sa représentation dans le produit d'espace matriciel se fait par une transformée de Fourier dont la complexité est linéaire, cela n'a donc pas d'impact sur la complexité globale de l'algorithme. Bien entendu pour réaliser ce résultat il faut que le groupe contiennent 3 sous-ensembles vérifiant la condition de triple produit et de taille correspondant aux deux matrices qu'on veut multiplier.

2 Résultats élémentaires

Je donne ici toute une série de résultats intéressants sur la condition de triple produit et sur les bornes sur ω qu'on peut en déduire.

Lemme 1. *Si un sous-groupe normal N de G réalise $< n_1, m_1, p_1 >$ et que G/N réalise $< n_2, m_2, p_2 >$, alors G réalise $< n_1 n_2, m_1 m_2, p_1 p_2 >$. En particulier si G_1 réalise $< n_1, m_1, p_1 >$ et G_2 réalise $< n_2, m_2, p_2 >$, alors $G_1 \times G_2$ réalise $< n_1 n_2, m_1 m_2, p_1 p_2 >$.*

Définition 3. Le pseudo-exposant $\alpha(G)$ d'un groupe fini non trivial est le minimum de

$$\frac{3log|G|}{\log(nmp)}$$

sur tout les n, m, p tels que G réalise $< n, m, p >$.

Lemme 2. *Le pseudo-exposant d'un groupe est compris entre 2 et 3 et c'est exactement 3 si le groupe est abélien.*

Théorème 2. *Soit G un groupe de pseudo exposant α et dont les degrés des caractères sont les d_i, on a l'inégalité suivante :*

$$|G|^{\omega/\alpha} \leq \sum_i d_i^{\omega}$$

Ce théorème nous permet de borner ω simplement en trouvant un groupe qui a les bonnes propriétés. L'inégalité provient de l'algorithme que j'ai décrit précédemment.

Corollaire 1. *Soit* $\gamma = \frac{log|G|}{log\, d}$ *où* $d = max\ d_i$. *On obtient, à partir de l'inégalité précédente, en bornant tous les* d_i *par* d, *si* $\alpha(G) < \gamma(G)$ *:*

$$\omega \leq \alpha(\frac{\gamma - 2}{\gamma - \alpha})$$

On a donc une borne un peu moins précise mais qui ne dépends que du degré maximum des caractères de G. On peut donner encore un corollaire qui nous éclaire sur la possibilité de trouver $\omega = 2$.

Corollaire 2. *Si il existe une famille de groupes finis* $G_1, G_2 \ldots$ *tels que* $\alpha(G_i) = 2 + o(1)$ *et* $\alpha(G_i) - 2 = o(\gamma(G_i) - 2)$, *alors* $\omega = 2$.

Bien sur, pour l'instant aucune telle famille n'a été trouvée. Même si elle n'existait pas il y aurait encore un espoir que cela soit seulement la majoration due à l'introduction de γ qui est trop butale.

Lemme 3. *Soit un groupe* G, *et trois sous groupes qui vérifient la condition du triple produit alors si deux de ces sous groupes commutent entre eux, il ne donne pas de meilleure borne sur* $\alpha(G)$ *que 3. De même si ce sont trois ensembles quelconques qui vérifient la condition du triple produit, que l'un d'entre eux est commutatif et que les deux autres commutent entre eux, cela ne donne pas de meilleure borne que 3.*

Ce lemme est intéressant car pour trouver une bonne borne à ω on cherche des sous-groupes et des sous-ensembles qui vérifient le triple produit, ce qui permet de borner $\alpha(G)$ et ensuite on étudie les caractères du groupe pour pouvoir appliquer les inégalités précédentes.
Dans la pratique on remarque qu'il est simple de trouver des sous-groupes qui vérifient ces conditions, mais qu'ils donnent de mauvaises bornes sur α, et dans le cas ou deux commutent entre eux, pas de borne du tout.
Cela souligne qu'il faut chercher plutôt des sous-ensembles, de préférence non commutatifs. C'est d'ailleurs ce qui motive la construction de groupes à partir de produit semi-direct, c'est à dire introduire de la non commutativité dans des structures que l'on connaît bien.

3 Exemples

Définition 4 (Produit semi-direct)**.** Soit deux groupes G, H et une action à gauche de G sur H, alors on définit le produit semi-direct de G et H, $G \ltimes H$, comme les paire $(g \in G, h \in H)$ avec la loi de groupe suivante :

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, (g_2.h_1)h_2)$$

Exemple 1. Il existe des familles de groupe tel que α tende vers 2.
La famille $S_{n(n+1)/2}$ a un pseudo exposant borné par $2+\frac{2-\log 2}{\log n}+0(\frac{1}{(\log n)^2})$.
L'exemple qu'on a donné ici est utile pour les résultats les plus récents évoqués à la fin. Les sous-ensembles utilisés pour réaliser cela sont les suivants : on considère les triplets (a,b,c) tels que $a+b+c=n-1$ et on fait agir $S_{n(n+1)/2}$ dessus comme le groupe des permutations de cet ensemble.
On considère les trois sous groupes qui laisse fixe une des coordonnées, ils vérifient la condition du triple produit et donnent la borne ci-dessus. Néanmoins, malgré la bonne connaissance des caractères de S_n, cela ne donne aucune borne sur ω.

Exemple 2. Voici le premier exemple qui a confirmé la possibilité de trouver par cette méthode un borne inférieure stricte à 3, alors que cela n'était pas sur lors de la parution du premier article sur le sujet en 2003. On considère le produit semi-direct d'un groupe abélien quelconque élevé à la puissance 6 avec $\mathbb{Z}/2\mathbb{Z}$. $G=\mathbb{Z}/2\mathbb{Z}\ltimes A^6$ et l'action de $\mathbb{Z}/2\mathbb{Z}$ est tout simplement la permutation des 3 premières coordonnées de A^6 avec les 3 suivantes.
On introduit alors les ensembles suivants, avec z générateur de $\mathbb{Z}/2\mathbb{Z}$:

$$S_i=\{(a_1,\ldots,a_6)z^j | a_i, a_{4+i} \text{ sont les seuls non nuls et} j\in\{0,1\}\}$$

Ces 3 ensembles vérifient la condition du triple produit et on obtient l'inégalité suivante :

$$\omega\leq\frac{6\log|A|-1}{\log A+\log(|A|-1)}$$

On utilise pour cela l'inégalité obtenue dans la partie précédente, en majorant le degré des caractères par 2. En effet A est abélien et donc de caractère 1 et on peut montrer facilement que les degrés des caractères du produit direct sont au plus le cardinal du groupe non abélien.
Cela donne au mieux $w<2,9088$, en choisissant $|A|=17$.
Néanmoins on peut généraliser un peu cette construction en considérant le groupe $G=\mathbb{Z}/k\mathbb{Z}\ltimes A^{3k}$, l'action est toujours la même c'est à dire la permutation des blocs de 3 coordonnées. On peut étendre les S_i de la même manière et on a alors l'inégalité :

$$\omega\leq\frac{3k\log|A|-\log k}{(k-1)\log A+\log(|A|-1)}$$

dont le minimum est atteint pour $|A|=7$ et $k=4$, ce qui permet d'obtenir $\omega<2,8790$. Dans les deux cas j'ai aussi calculé précisément les caractères, mais cela n'apporte qu'une amélioration inférieure à 10^{-4} aux résultats précédents.
Il est satisfaisant de voir que la méthode marche mais les résultats sont cependant moins bon que ceux qu'a obtenu Strassen avec son premier algorithme de multiplication de complexité inférieure à 3.

Exemple 3. Soit D_m le groupe diédral à $m = 2n$ éléments, c'est à dire engendré par deux éléments x, y d'ordre n et 2 tels que $yxy = x^{-1}$. Si on prends n premier il est facile de trouver tous les sous-groupes. On peut montrer alors que tout triplet de sous-groupe vérifiant la condition du triple produit ne donne rien de mieux que $\alpha \leq 3$. Cela souligne encore une fois que les sous-groupes ne donnent pas de bons résultats. Si la borne n'est pas meilleure, c'est que $\mathbb{C}[D_m] = \prod \mathbb{C}^{2*2}$, en fait on ne divise le produit qu'en produits de matrices de taille $2 * 2$.
Par ailleurs on a un phénomène intéressant, $\alpha(D_8) = 3$ mais $\alpha(D_8^k)$ est borné par une fonction qui tend vers $3\log_{12}(8) = 2,51\ldots$ quand k tend vers l'infini. Comme γ reste constant quand on fait augmenter k (remarque générale), on voit qu'il peut être bon de considérer des puissances de groupe, comme famille de groupe, car la borne obtenue ne peut que s'améliorer.

4 Perspectives

D'abord on a essayé de tester le maximum de groupes à l'aide d'un programme informatique, mais cela n'a pas donné de résultat intéressant, il faut donc réfléchir !
On a remarqué que les ensembles non commutatifs donnaient de bons résultats, on a donc étudié le Wreath Product qui est le produit semi-direct d'un groupe cyclique à la puissance n avec le groupe des permutations de taille n qui agit en permutant les coordonnées. On prend comme sous-ensemble vérifiant la condition du triple produit $H_1 = \{(\pi, 0) | \pi \in S_n\}$, $H_2 = \{(\pi, \pi u - u) | \pi \in S_n\}$, $H_2 = \{(\pi, \pi v - v) | \pi \in S_n\}$ où $u = (1, 2, \ldots, n)$ et $v = (n, n-1, \ldots, 1)$. Cela donne une famille de groupe dont α tends vers 2, et les constructions plus sophistiquées s'inspirent de celle-ci.
On pourrait aussi penser à construire un groupe à partir des conditions de triple produit sur trois sous-groupes ou sous-ensembles, en maximisant α, c'est à dire en construisant un goupe aussi petit que possible pour des sous-ensembles de taille fixée.
La notion la plus importante, pour les résultats intéressants est celle de triple produit simultané :
les ensembles A_i, B_i, C_i vérifient le triple produit simultané si
pour tout i, A_i, B_i, C_i vérifient la condition du triple produit
pour tout $i, j, k, a_i(a'_j)^{-1} b_j (b'_k)^{-1} c_k (ci')^{-1} = 1 \Rightarrow i = j = k$.
Elle est utilisée avec des familles de Wreath Product, l'astuce qui sert dans l'exemple 1 et avec des notions combinatoires comme celle des USP ou 'Uniquely Solvable Puzzle'. On obtient au mieux pour l'instant $\omega < 2,41$.
Les résultats trouvés ont des liens clairs avec les démonstrations des mêmes bornes dans un autre cadre, mais cette nouvelle méthode a l'aventage d'être plus claire et de se faire dans un cadre bien défini. On obtient d'ailleurs deux jolies conjectures qui nous amènerait si elles étaient prouvées à $w = 2$.

Dernière remarque, avec cette méthode, on peut déterminer w pour des corps de caractéristique non nulle simplement en prenant des algébres de groupe dans un corps fini (la complexité ne dépends pas du corps mais de sa caractéristique seulement).

Crédits :

Cet aperçu rapide de la multiplication rapide de matrices par l'utilisation de la théorie des représentations est principalement inspirée de

- H.Cohn et C.Umans, A Group Theoritic Approach to Fast Matrix Multiplication
- H.Cohn, R.Kleinberg, B.Szegedy et C.Umans, Group Theoritic Algorithms for Matrix Multiplication
- mes propres réflexions sur le sujet