Multiplication rapide d'entiers et de polynômes

Joris van der Hoeven

Laboratoire d'informatique, UMR 7161 CNRS
Campus de l'École polytechnique
1, rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing, CS35003
91120 Palaiseau

Email: vdhoeven@lix.polytechnique.fr

1 octobre 2014

Travail en commun avec David Harvey et Grégoire Lecerf

Résumé

Un problème fondamental en algorithmique est la multiplication rapide de deux entiers de n bits. Soit $\mathsf{I}(n)$ cette complexité, en supposant le modèle des machines de Turing avec un nombre fini de bandes. Jusqu'à récemment, la meilleure borne asymptotique pour $\mathsf{I}(n)$ était due à Fürer [1, 2]. Plus précisément, il a montré qu'il existe une constante $K > 1$ avec

$$\mathsf{I}(n) \;=\; O(n \log n \, K^{\log^* n}), \tag{1}$$

où $\log^* x$ (pour $x \in \mathbb{R}$) désigne l'itérateur du logarithme, c.à.d.,

$$\begin{aligned} \log^* x &:= \min \{k \in \mathbb{N} : \log^{\circ k} x \leqslant 1\}, \\ \log^{\circ k} &:= \log \circ \underset{k \times}{\cdots} \circ \log. \end{aligned} \tag{2}$$

Dans un travail récent [3], nous avons amélioré cette borne. Utilisant un nouveau type d'algorithme, nous avons montré que $K = 8$ (et même $K = 4$ si une certaine conjecture en théorie des nombres est valide). En optimisant l'approche originale de Fürer, il semble que l'on ne peut pas obtenir mieux que $K = 16$.

Dans un deuxième travail [4], nous avons également montré comment adapter notre méthode à la multiplication de polynômes de degré $\leqslant n$ à coefficients dans un corps fini $\mathbb{F}_q$. Plus précisément, désignant par $\mathsf{M}_q(n)$ cette complexité, nous montrons que

$$\mathsf{M}_q(n) \;=\; O\big((n \log q) \log (n \log q) \, K^{\log^* (n \log q)}\big),$$

uniformément en q. Ici encore, on peut prendre $K = 8$ (et même $K = 4$ si certaines conjectures en théorie des nombres sont valides). Auparavant, pour q fixé, la meilleure borne connue était $\mathsf{M}_q(n) = O(n \log n \log \log n)$.

Dans notre exposé, nous survolerons les idées principales derrière ces résultats.

Bibliographie

[1] M. Fürer. Faster integer multiplication. In *Proceedings of the Thirty-Ninth ACM Symposium on Theory of Computing, STOC 2007*, pages 57–66, New York, NY, USA, 2007. ACM Press.

[2] M. Fürer. Faster integer multiplication. *SIAM J. Comput.*, 39(3):979–1005, 2009.

[3] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. Technical report, HAL, 2014. http://hal.archives-ouvertes.fr.

[4] D. Harvey, J. van der Hoeven, and G. Lecerf. Faster polynomial multiplication over finite fields. Technical report, HAL, 2014. http://hal.archives-ouvertes.fr.