Une implémentation de la multiplication rapide des polynômes binaires

Robin Larrieu
Travail en commun avec Joris van der Hoeven et Grégoire Lecerf
Laboratoire d'informatique de l'École polytechnique (LIX)

La multiplication efficace des polynômes dans le corps fini $\mathbb{F}_2$ est un problème fondamental en informatique, avec plusieurs applications pour les codes correcteurs et en cryptographie. Le but de cet exposé est de présenter une solution efficace en pratique pour de grands degrés [5].

Notre implémentation se base sur l'arithmétique efficace dans le corps $\mathbb{F}_{2^{60}}$ [3], mais améliore la librairie précédente grâce à un nouvel algorithme ; plus précisément une variante du *Frobenius FFT* [4]. Ceci permet d'éviter presque entièrement le surcoût lié au travail dans une extension de corps. On arrive ainsi à gagner un facteur 2 par rapport aux librairies de référence [1, 2, 3].

Article détaillé : `https://hal.archives-ouvertes.fr/hal-01579863`

Code source : Disponible sur le serveur SVN `https://gforge.inria.fr/projects/mmx/` (révision 10681), dans la librairie JUSTINLINE

Références

[1] R. P. Brent, P. Gaudry, E. Thomé, et P. Zimmermann. Faster multiplication in GF(2)[x]. In A. van der Poorten and A. Stein, editors, *Algorithmic Number Theory*, volume 5011 of *Lect. Notes Comput. Sci.*, pages 153–166. Springer Berlin Heidelberg, 2008.

[2] Ming-Shing Chen, Chen-Mou Cheng, Po-Chun Kuo, Wen-Ding Li, et Bo-Yin Yang. Faster multiplication for long binary polynomials. `https://arxiv.org/abs/1708.09746`, 2017.

[3] D. Harvey, J. van der Hoeven, et G. Lecerf. Fast polynomial multiplication over $\mathbb{F}_{2^{60}}$. In M. Rosenkranz, editor, *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 255–262. ACM, 2016.

[4] J. van der Hoeven et R. Larrieu. The Frobenius FFT. In M. Burr, editor, *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 437–444. ACM, 2017.

[5] J. van der Hoeven, R. Larrieu et G. Lecerf. Implementing fast carryless multiplication.. `https://hal.archives-ouvertes.fr/hal-01579863`. Accepté à MACIS 2017.