Calcul de racines sur un corps fini à l'aide de transformées de Graeffe

B. Grenet[(a)], J. van der Hoeven[(b)], G. Lecerf[(b)]
[(a)] LIRMM, Université de Montpellier
[(b)] LIX, CNRS – École Polytechnique
bruno.grenet@lirmm.fr
lecerf@lix.polytechnique.fr
vdhoeven@lix.polytechnique.fr

Soit $\mathbb{F}_q$ un corps fini. Nous nous intéressons au calcul des racines de polynômes scindés à racines simples sur $\mathbb{F}_q$. Nous proposons une nouvelle approche pour ce problème, basée sur des transformées de Graeffe généralisées, qui donne lieu à plusieurs algorithmes.

Le calcul des racines d'un polynôme $f \in \mathbb{F}_q[X]$ est un problème important du calcul formel qui sert de brique de base à de nombreux algorithmes du domaine (factorisation, interpolation, ...). Il s'agit également de l'un des rares problèmes que l'on sait résoudre en temps polynomial probabiliste mais pas en temps polynomial déterministe. Une motivation de notre travail vient de l'observation que dans les algorithmes d'interpolation creuse, le calcul de racines de polynômes $f \in \mathbb{F}_q[X]$ représente une part importante du temps de calcul [6]. Dans ces algorithmes, on peut choisir pour q un nombre premier *de type FFT*, c'est-à-dire de la forme $q = M \cdot 2^m + 1$ avec $M = O(\log q)$.

D'une part, nous décrivons un algorithme déterministe. Cet algorithme suppose donnés la factorisation de $(q-1)$ et un élément primitif de $\mathbb{F}_q^\times$. Nous obtenons ainsi une nouvelle borne de complexité déterministe en fonction de $\sqrt{S_1(q-1)}$ où $S_1(q-1)$ est le plus grand diviseur premier de $(q-1)$. Celle-ci améliore légèrement un résultat de VON ZUR GATHEN [2]. Dans le cas favorable $S_1(q-1) = O(\log q)$, la complexité de notre algorithme déterministe est équivalente à celle de l'algorithme (probabiliste) de CANTOR et ZASSENHAUS [1], à des facteurs logarithmiques près.

D'autre part, nous donnons des algorithmes probabiliste et heuristique. Ceux-ci sont particulièrement efficaces lorsque le cardinal $(q-1)$ de $\mathbb{F}_q^\times$ est friable, par exemple si q est un nombre premier de type FFT. Pour de telles

valeurs de q, notre algorithme probabiliste a une complexité moyenne similaire à celle de l'algorithme de CANTOR et ZASSENHAUS, et l'implantation d'une variante heuristique dans le logiciel libre MATHEMAGIX [5] permet d'obtenir des gains significatifs en pratique. Ces gains permettent une accélération des algorithmes d'interpolation creuse.

Cette exposé est basé sur les deux articles [3, 4].

Bibliographie

[1] D. G. CANTOR, H. ZASSENHAUS, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. 36(154), pp. 587–592, 1981.

[2] J. VON ZUR GATHEN, *Factoring polynomials and primitive elements for special primes*, Theoret. Comput. Sci. 52(1-2), pp. 77–89, 1987.

[3] B. GRENET, J. VAN DER HOEVEN, G. LECERF, *Randomized Root Finding over Finite FFT-fields using Tangent Graeffe Transforms*, Proc. ISSAC, pp. 197–204, 2015.

[4] B. GRENET, J. VAN DER HOEVEN, G. LECERF, *Deterministic root finding over finite fields using Graeffe transforms*, Manuscript (submitted), 2015.

[5] J. VAN DER HOEVEN, ET AL, *Mathemagix*, from 2002. `http://www.mathemagix.org`.

[6] J. VAN DER HOEVEN, G. LECERF, *Sparse Polynomial Interpolation in Practice*, ACM Commun. Comput. Algebra 48(3-4), pp 187–191, 2014.