Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields

Adrien Poteaux[⋆] & Marc Rybowicz[†]
[⋆] CRIStAL-CFHP, université de Lille
adrien.poteaux@univ-lille1.fr
[†] XLIM-DMI, université de Limoges
marc.rybowicz@unilim.fr

Let L be a field of characteristic p with $\mathfrak{q}$ elements and $F \in L[X,Y]$ be a polynomial with $p > \deg_Y(F)$ and total degree d. In [2], we showed that rational Puiseux series of F above $X = 0$ could be computed with an expected number of $O^{\sim}(d^5 + d^3 \log \mathfrak{q})$ arithmetic operations in L. In this paper, we reduce this bound to $O^{\sim}(d^4 + d^2 \log \mathfrak{q})$ using Hensel lifting and changes of variables in the Newton-Puiseux algorithm that give a better control of the number of steps. The only asymptotically fast algorithm required is polynomial multiplication over finite fields. This approach also allows to test the irreducibility of F in $\overline{L}[[X]][Y]$ with $O^{\sim}(d^3)$ operations in L. Finally, we describe a method based on structured bivariate multiplication [1] that may speed up computations for some input.

This work has been presented at ISSAC'15 [3].

Bibliographie

[1] J. Lebreton, E. Schost, and J. V. der Hoeven. Structured FFT and TFT : symmetric and lattice polynomials. In ACM, editor, *Proc. ISSAC '13*, pages 355–362, 2013.

[2] A. Poteaux and M. Rybowicz. Complexity Bounds for the Rational Newton-Puiseux Algorithm over Finite Fields. *Applicable Algebra in Engineering, Communication and Computing*, 22(3) :187–217, 2011.

[3] Adrien Poteaux, Marc Rybowicz. *Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields.* In Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic

Computation, ISSAC '15, pages 299–306, New York, NY, USA, 2015. ACM.