Factoring polynomials over discrete valuation rings

Adrien Poteaux Martin Weimann

Consider a discrete valuation ring $\mathbb{A}$ - we have in mind $\mathbb{A} = \mathbb{Q}_p$ or $\mathbb{A} = \mathbb{K}((x))$. Factorisation in $\mathbb{A}[y]$ is a well studied topic [2, 3, 6, 7, 10]. Denoting $F \in \mathbb{A}[y]$ monic and separable, and δ the valuation of its discriminant, the complexity given in [2] is $\mathcal{O}\tilde{}(d^2 + d\,\delta^2)$, and $\mathcal{O}\tilde{}(d^2 + \delta^2)$ if we only want to test irreducibility.

In this talk, we will provide an algorithm that provides an irreducibility test in $\mathcal{O}\tilde{}(\delta)$, and a factorisation in $\mathcal{O}\tilde{}(d\,\rho\,\delta)$, where ρ is the number of factors. In particular, following [11], we can get half of the factors (counted with degrees) in $\mathcal{O}\tilde{}(\rho\,\delta)$, improving the $\mathcal{O}\tilde{}(d\,\delta)$ bound of [11].

We have been interested in this topic to avoid the costly blowing up while, in the case $\mathbb{A} = \mathbb{K}[[x]]$, computing Puiseux series via any Newton-Puiseux like algorithm (which make an irreduciblity test in $\Omega(d\,\delta)$ via [11]). This made us study the *approximate roots* of Abhyankhar-Moh [1] (irreducibility test in $\mathbb{C}[[x, y]]$ without any blow-up) and generalise it to $\mathbb{K}[[x]][y]$. Our contributions are :

- we establish a bridge between the Newton-Puiseux algorithm, the Montes algorithm (i.e. extended valuations and *key* polynomials *à la* MacLane [8, 9, 12]) and Abhyankar's irreducibility criterion :
  - → we prove that *well chosen* approximate roots $\Psi = (\psi_0, \cdots, \psi_g)$ are key polynomials (this is well known for $\mathbb{A} = \mathbb{K}[[x]]$ [1, 4]), and that they can be computed via Newton iteration,
  - → we compute essential terms of Puiseux series via Ψ-expansions (i.e. successive generalised Taylor expansions) of the input.

  Following this strategy, and using dynamic evaluation, we get an irreducibily test for $F \in \mathbb{A}[y]$ in an expected $\mathcal{O}\tilde{}(\delta)$ arithmetic operations.
- Inspired by [3], we show that, given an extended valuation υ, the quadratic Hensel lifting [5, section 14.4] works fine (i.e. we get $\upsilon(F - G_i\,H_i) \geq \upsilon(F) + 2^i$) as long as we start with well chosen initialisation (G_0, H_0), that can be read on the Ψ-adic expansion of F. We get a quasi-linear time algorithm to factorise $F = G\,H$ in $\mathbb{A}[y]$ *without any initial change of variables*, as in [3].

A main interest of these algorithms is that the "complicated" computations (dealing with field extensions, gcd computations...) are made only with univariate polynomials (with coefficients in a finite extension of the residue field of $\mathbb{A}$), while computations above $\mathbb{A}[y]$ are only Newton iterations and generalised Taylor expansions (i.e. successive euclidean division with monic polynomials). This should make the implementation far easier than the algorithm presented in [11].

This is a work in progress with Martin Weimann. Some partial implementations have been made in Sage. Several assumptions are not discussed in this abstract.

Références

[1] S. Abhyankar. *Algebraic Geometry for Scientists and Engineers*, volume 35 of *Mathematical surveys and monographs*. Amer. Math. Soc., 1990.

[2] J.-D. Bauch, E. Nart, and H. Stainsby. Complexity of the OM factorizations of polynomials over local fields. *LMS Journal of Computation and Mathematics*, 16 :139–171, 2013.

[3] X. Caruso, D. Roe, and T. Vaccon. Division and slope factorization of p-adic polynomials. In ISSAC '16, pages 159–166.

[4] V. Cossart and G. Moreno-Socías. Irreducibility criterion : a geometric point of view. *Fields Inst. Commun.*, (33) :27–42, 2003.

[5] J. v. z. Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 3rd edition, 2013.

[6] J. Guàrdia, J. Montes, and E. Nart. Newton polygons of higher order in algebraic number theory. *Transsactions of the American Mathematical Society*, 364 :361–416, 2012.

[7] J. Guàrdia, E. Nart, and S. Pauli. Single-factor lifting and factorization of polynomials over local fields. *Journal of Symbolic Computation*, 47(11) :1318 – 1346, 2012.

[8] S. MacLane. A construction for absolute values in polynomial rings. *Trans. Amer. Math. Soc.*, 40(3) :363–395, 1936.

[9] S. Mac Lane. A construction for prime ideals as absolute values of an algebraic field. *Duke Math. J.*, 2(3) :492–510, 1936.

[10] J. Montes Peral. *Polígonos de newton de orden superior y aplicaciones aritméticas*. PhD thesis, Universitat de Barcelona, 1999.

[11] A. Poteaux and M. Weimann. Computing Puiseux series : a fast divide and conquer algorithm. submitted to publication, 2018.

[12] J. Rüth. *Models of curves and valuations*. PhD thesis, Universität Ulm, 2014.