Applications of Computer Algebra – ACA 2019
Montréal, Canada | July 16-20, 2019
École de technologie supérieure

Computing the genus of plane curves with cubic complexity in the degree

A. Poteaux, M. Weimann martin.weimann@upf.pf

CRIstal, University of Lilles, France
GAATI, University of French Polynesia

In this presentation, we report on new complexity results about the resolution of singularities of plane curves, obtained in collaboration with Adrien Poteaux in [9] and [10]. Let C be an absolutely irreducible algebraic plane curve defined over a perfect field $\mathbb{K}$ of characteristic 0 or greater than $d = \deg(C)$. We will sketch the proof of the following result [9, Cor. 1] :

Theorem 1. *There exists an algorithm which computes the geometric genus of C with an expected $\tilde{\mathcal{O}}(d^3)$ arithmetic operations over $\mathbb{K}$.*

If $\mathbb{K} = \mathbb{Q}$, we can use a criterion of good reduction modulo p [7] and derive a Las Vegas algorithm for the genus running with an expected *bit* complexity $\tilde{\mathcal{O}}(d^3(h+1))$ where h stands for the logarithmic height of a polynomial equation of C over $\mathbb{Q}$ (similar results stand over arbitrary number fields, see [9]). Our approach uses Puiseux series. There exist other algorithms for the genus, using for instance linear differential operators [2, 3] or topological methods [5] (for complex curves). To our knowledge, none of these methods have been proved to provide a better complexity than that of Theorem 1.

The proof of Theorem 1 is based on a fast Newton-Puiseux type algorithm. If $F \in \mathbb{K}[[x]][y]$ is a square-free polynomial defined over a perfect field $\mathbb{K}$ of characteristic 0 or greater than $d = \deg(F)$, the roots of F in $\overline{\mathbb{K}((x))}$ may be represented as fractional Puiseux series. Computing these Puiseux series is an important algorithmic issue related to algebraic curves with various applications (resolution of singularities, integral basis of function fields, Riemann-Roch spaces, monodromy, factorization, geometric modeling, etc). An important fact in our context is that the singular parts of the Puiseux series (obtained after truncation up to a suitable power of x) contain the classical numerical invariants attached to the singular germs of plane curve defined by F along the line $x = 0$. In particular, they determine their equisingularity type, which is the main notion of equivalence for plane curve singularities introduced by Zariski in the 60's. Denoting δ the x-valuation of the discriminant of F, we prove [9, Thm.1]:

Theorem 2. *There exists an algorithm which computes the singular parts of the Puiseux series of F with an expected $\tilde{\mathcal{O}}(d\delta)$ arithmetic operations over $\mathbb{K}$.*

When compared to the Newton-Puiseux type algorithms of Duval [4] and Poteaux-Rybowicz [7, 8], the new idea behind the proof of Theorem 2 is to use a divide and conquer strategy. To this aim, we use suitable sharp truncation bounds (updated at each step of the algorithm) combined with a generalization of the classical Hensel lifting. Also, we need to rely on dynamic evaluation in order to avoid to perform too many univariate irreducibility tests (this task is too costly over characteristic zero fields and might be too costly also for finite fields when computing the Puiseux series above critical points with high algebraic degree over $\mathbb{K}$). Theorem 1 then follows from Theorem 2 by computing the singular parts of the Puiseux series of the polynomial defining C above all critical points of a suitable projection $C \to \mathbb{P}^1$, and by applying eventually the Riemann-Hurwitz formula. We can derive also from Theorem 2 a quasi-optimal factorization algorithm in $\mathbb{K}[[x]][y]$, which has a special interest with regards to the irreducible decomposition of algebraic plane curves [11].

Theorem 2 leads in particular to an irreducibility test in $\mathbb{K}[[x]][y]$ running with complexity $\tilde{\mathcal{O}}(d\delta)$. If time permits, I will present an algorithm which allows to get rid of the d factor. Keeping hypothesis of Theorem 2, we prove the following result [10, Thm.1]:

Theorem 3. *We can test if F is irreducible in $\mathbb{K}[[x]][y]$ with $\tilde{\mathcal{O}}(\delta + d)$ operations over $\mathbb{K}$ and at most two degree d univariate irreducibility tests over $\mathbb{K}$.*

If F is Weirestrass, the complexity drops to $\tilde{\mathcal{O}}(\delta)$ and one univariate irreducibility test. If F is given as a dense bivariate polynomial in $\mathbb{K}[x, y]$, the complexity is quasi-linear with respect to the arithmetic size of the input. This algorithm is of a different nature than the algorithm of Theorem 2, as we do not use here the usual monomial transforms (blow-ups) and shifts inherent to the Newton-Puiseux type algorithms. We rather generalize Abhyankhar's irreducibility criterion [1] to the case of non algebraically closed residue fields. The main idea is to detect the irreducibility of F on its Ψ-adic expansion, where $\Psi = (\psi_0, \ldots, \psi_k)$ is the collection of some well chosen *approximate roots* of F that we update at each step of the algorithm.

Remark. The three algorithms described above are purely symbolic. They are completely deterministic except for the use of a Las Vegas subroutine for computing primitive elements in the various residue fields extensions, thus avoiding to deal with towers of algebraic extensions of $\mathbb{K}$. However, thanks to the recent preprint [6], we expect that they become deterministic up to substituting d by $d^{1+o(1)}$ in our complexity estimates. Theorem 1 provides a worst-case complexity bound which is equivalent (up to a logarithmic factor) to the computation of the discriminant of a degree d bivariate polynomial, and improving this complexity would be a major breakthrough in Computer Algebra. However, this provides for the moment only a theoretical result : our algorithm is a combination of many subroutines, and the implementation of a fast efficient version would require a huge amount of work, especially due to the dynamic evaluation part. We are currently investigating alternative algorithms based on approximate roots which are easier to implement.

References

[1] S.S. Abhyankar, Irreducibility criterion for germs of analytic functions of two complex variables. *Adv. Mathematics* **35**:190–257 (1989).

[2] A. Bostan; F. Chyzak; B. Salvy; G. Lecerf; E. Schost, Differential equations for algebraic functions, in *Proceedings of ISSAC'07*, 25–32 (2007).

[3] O. Cormier; M.F. Singer; F. Ulmer, Linear differential operators for polynomial equations, *J. of Symb. Comp.*, **34**(5):355–398 (2002).

[4] D. Duval, Rational Puiseux expansions, *Compos. Math.* **70**(2):119–154 (1989).

[5] M. Hodorog; B. Mourrain; J. Schicho, GENOM3CK: a library for genus computation of plane complex algebraic curves using knot theory, in *Comm. in Comp. Alg.*, **44**, ACM (2010).

[6] G. Lecerf; J. Van Der Hoeven, Accelerated tower arithmetic, *Preprint* hal-01788403 (2018).

[7] A. Poteaux; M. Rybowicz, Good reduction of puiseux series and applications, *J. of Symb. Comp.*, **47**(1):32 – 63 (2012).

[8] A. Poteaux; M. Rybowicz, Improving complexity bounds for the computation of puiseux series over finite fields, in *Proceedings of ISSAC'15*, 299–306, ACM (2015).

[9] A. Poteaux; M. Weimann, Computing Puiseux series: a fast divide and conquer algorithm, *Preprint* arXiv:1708.09067v2 (2018).

[10] A. Poteaux; M. Weimann, A quasi-linear irreducibility test in $\mathbb{K}[[x]][y]$, *Preprint* arXiv:1904.00286v1 (2019).

[11] M. Weimann, Bivariate factorization using a critical fiber, *J. Found. of Comp. Math.*, **17**(5):1219–1263 (2016).