Effective algorithm for factoring polynomials in the ring of multivariable formal power series in zero–characteristic

Alexander L. Chistov

Let k be a ground field of zero–characteristic with algebraic closure $\overline{k}$. We assume that k is finitely generated over its primitive subfield. Let $k[[X_1, \dots, X_n]]$ (respectively $\overline{k}[[X_1, \dots, X_n]]$) the ring of formal power series in the variables $X_1, \dots, X_n$ with coefficients from the field k (respectively $\overline{k}$). By definition an algorithm constructs a polynomial with coefficients in the ring of formal power series if and only if it can construct arbitrary approximations of all the coefficients of this polynomial.

Let $f \in k[X_1, \dots, X_n, Z]$ be a polynomial of degree $\deg_{Z,X_1,\dots,X_n} \leqslant d$, $d \geqslant 2$, and the leading coefficient with respect to Z of f is equal to 1. We suggest algorithms for factorization such a polynomial f in the rings $k[[X_1, \dots, X_n]][Z]$ and $\overline{k}[[X_1, \dots, X_n]][Z]$. To our knowledge so far nobody has described such algorithms for the case $n \geqslant 2$ (may be only particular cases has been considered). As a direct consequence of the suggested algorithms we get algorithms for factorization of polynomials from $k[X_1, \dots, X_n]$ in the rings of formal power series $k[[X_1, \dots, X_n]]$ and $\overline{k}[[X_1, \dots, X_n]]$. Again as far as we know no such algorithms have been obtained for $n \geqslant 3$ (the case $n = 1$ is trivial and the case $n = 2$ can be treated using the method of Newton's broken lines, cf. [6]).

For any $j \geqslant 1$ the suggested algorithms can construct the j-th approximation of all the objects at their output. We give explicit complexity bounds for the running time of the described algorithms. These complexity bounds are polynomial in j and the size of the input data if the number n of variables is fixed, say $n = 2, 3, 4, \dots$.

There is no easy solution of the considered problem of factorization of a polynomial $f \in k[X_1, \dots, X_n, Z]$ using only Newton polygons or polyhedrons for $n \geqslant 2$. Of course the roots of the polynomial f belong to the field of multiple formal fractional power series in $X_1, \dots, X_n$, i.e. to the union by all integers $\nu_1, \dots, \nu_n \geqslant 1$ of the fields of multiple formal power series

$$\overline{k}((X_1^{1/\nu_1}))((X_2^{1/\nu_2}))\dots((X_n^{1/\nu_2})).$$

For example, it is difficult to decide whether a root z of the polynomial f from this field actually belongs to $k[[X_1,\dots,X_n]]$.

Our method is based on the results on normalization of algebraic varieties and completions of their local rings. First of all it is an effective normalization of algebraic varieties in zero–characteristic with the explicit complexity bound. It was described by the author erlier, see [3], [4], [5]. Secondly we use the theorems related to analytical irreducibility and analytical normality of normal algebraic varieties, see [9] v.II, Chapter 8 §13 Theorems 31–33. Of course we use also the results from [2].

We don't consider the case of nonzero characteristic mainly since no results similar to [3] have been obtained so far in this case. But, of course, one can use another algorithms for normalization of algebraic varieties in nonzero characteristic (there are no explicit estimates of complexity for these algorithms in literature) and get an analog of our result in nonzero characteristic but without a bound for the complexity of algorithms.

For more details, see Theorem 1 [7]. Actually the complexity of the algorithm from this theorem is polynomial in $d^{2^{n^c}}$ and j^n for a constant $c>0$. At present we have analysed the construction of this algorithm thoroughly. We hope to improve it using the result of [8]. The complexity bound of the new version of this algorithm will be polynomial in d^{n^c} and j^n (the constant c will be specified).

Note also that in [7] we refer to Theorem 1 §3 Chapter IV [1] about factroring polynomials over a field complete with respect to a discrete valuation (although factually one can manage without this theorem in [7]). Recently we have found that it is not quite obvious that the construction from the proof of this theorem in [1] gives a polynomial time algorithm in our situation. Still it is true. Only minor modifications are required in this construction. We are going to clarify this question in the next paper.

References

[1] Z. I. Borevich, I. R. Shafarevich *Number theory*, New York Academic Press 1966.

[2] A.L. Chistov, *Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 137 (1984), p. 124–188 (in Russian) [English transl.: J. Sov. Math. 34 (4) (1986)].

[3] A.L. Chistov, *Effective Construction of a Nonsingular in Codimension One Algebraic Variety over a Zero-Characteristic Ground Field*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 387 (2011), p. 167–188 [English transl.: Journal of Mathematical Sciences v. 179 (2011), p. 729–740].

[4] A.L. Chistov, *An overview of effective normalization of a nonsingular in codimension one projective algebraic variety'*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 373 (2009), p. 295–317 [English transl.: Journal of Mathematical Sciences v. 168 (2010), p. 478–490].

[5] A.L. Chistov, *Effective normalization of a nonsingular in codimension one projective algebraic variety*, Doklady Academii Nauk 427, no. 5 (2009), p. 605–608 (in Russian) [English transl.: Doklady Mathematics, 80:1 2009, p. 577–580].

[6] A.L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm*, In: International Symposium on Mathematical Foundations of Computer Science 1986. Lecture Notes in Computer Science Vol. 233 Springer (1986) p. 247–255.

[7] A.L. Chistov *An algorithm for factoring polynomials in the ring of multivariable formal power series in zero–characteristic*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 517 (2022), p. 268–290 (in Russian) [English transl.: to appear in Journal of Mathematical Sciences].

[8] W.-L. Chow *On the theorem of Bertini for local domains*, Proceedings of the National Academy of Sciences, (1958) v.44, #6 p. 580–584.

[9] O. Zariski, P. Samuel P. *Commutative algebra*, v.I-II, Berlin New York Springer–Verlag, 1958–1960.

Alexander L. Chistov
St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia
e-mail: `alch@pdmi.ras.ru`