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

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

Our talk is devoted to the problem of factoring polynomials in the rings of formal power series over a field. It is well–known that the rings of formal power series over a field and the rings of polynomials over such rings of formal power series are factorial

We suggest algorithms for factoring polynomials in the rings of multivariables formal power series over the ground field of zero–characteristic and over an algebraic closure of this ground field. Also we construct algorithms for factoring monic polynomials in one variable over these formal power series rings. We give explicit estimates for the complexity of suggested algorithms. These results are important for local investigation of algebraic varieties from the algorithmic point of view.

More precisely, let be given a system of polynomial equations $f_1 = \ldots = f_m = 0$, where the polynomials $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$, k is a ground field of zero–characteristic. Then one can decompose $\mathcal{Z}(f_1, \ldots, f_m)$ near the point $(0, \ldots, 0)$ into the union of algebroid varieties.

Namely, at first we decompose the set of zeroes $\mathcal{Z}(f_1, \ldots, f_m) \subset \mathbb{A}^n(\overline{k})$ into the union of irreducible over k components. After that it is sufficient to represent each constructed irreducible component as a union of algebroid varieties. So we shall suppose without loss of generality that $\mathcal{Z}(f_1, \ldots, f_m)$ is an irreducible over k variety of dimension r. Then we construct a finite dominant separable and birational morphism $\mathcal{Z}(f_1, \ldots, f_m) \to \mathcal{Z}(F(L_1, \ldots, L_{r+1}))$, where $L_1, \ldots, L_{r+1} \in k[X_1, \ldots, X_n]$ are linearly independent linear forms and F is a polynomial. Now to get the required algebroid components defined over k (or $\overline{k}$) it is sufficient to factor F in the rings of formal power series $k[[X_1, \ldots, X_n]]$ (or $\overline{k}[[X_1, \ldots, X_n]]$).

Now let $f \in k[X_1, \dots, X_n, Z]$ be a polynomial and the leading coefficient with respect to Z of f is equal to 1. Our aim is to 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 $n \geqslant 2$. 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. [4]).

[4] **Chistov A. L.:** *"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.

For any $j \geqslant 1$ the suggested algorithms can construct the j-th approximation of all the objects at their output, see below for details. 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 $n = 2, 3, 4, \ldots$.

There is no easy solution of the considered problem of factorization of a polynomial $f \in k[X_1, \ldots, X_n, Z]$ 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 $X_1, \ldots, X_n$, i.e. to the union by all integers $\nu_1, \ldots, \nu_n \geqslant 1$ of the fields of multiple formal power series

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

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

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 [5], [6], [7].

[5] **Chistov A. L.:** *“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].

[6] **Chistov A. L.:** *“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].

[7] **Chistov A. L.:** *“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].

Secondly we use the theorems related to analytical irreducibility and analytical normality of normal algebraic varieties, see [10] v.II, Chapter 8 §13 Theorems 31–33.

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

Of course applying the algorithm from [3] we can assume in what follows without loss of generality that f is irreducible in the ring $k[X_1, \ldots, X_n, Z]$.

[3] **Chistov A. L.:** *"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)].

We don't consider the case of nonzero characteristic mainly since no results similar to [5] 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.

Denote by $\mathfrak{m}$ the maximal ideal of the local ring $\widehat{A}$. So the ideal $\mathfrak{m}$ is generated by the elements $X_1, \ldots, X_n$. Let $z \in \widehat{A}$ and $N \geqslant 0$ be an integer. Then there is a unique polynomial $z' \in \overline{k}[X_1, \ldots, X_n]$ of degree $\deg_{X_1,\ldots,X_n} z' \leqslant N$ such that $z - z' \in \mathfrak{m}^{N+1}$. By definition put $z_{\#,N} = z'$. We shall identify the set of elements of the factor ring $\widehat{A}/\mathfrak{m}^{N+1}$ with the linear space of polynomials of degree at most N from $\overline{k}[X_1, \ldots, X_n]$. Hence now $z_{\#,N} = z \bmod \mathfrak{m}^{N+1}$ for any $z \in \widehat{A}$.

For a polynomial $g \in \widehat{A}[Z]$ one can define in a similar way the element $g_{\#,N} = g \bmod \mathfrak{m}^{N+1} \in \overline{k}[X_1, \ldots, X_n, Z]$. Hence $\deg_{X_1,\ldots,X_n} g \leqslant N$.

DEFINITION 1 *We shall say that an algorithm constructs an element $z \in \widehat{A}$ (respectively a polynomial $g \in \widehat{A}[Z]$) if and only if for any given integer $N \geqslant 0$ this algorithm can constructs the polynomial $z_{\#,N}$ (respectively $g_{\#,N}$).*

Let us proceed to exact statements, for details see [8] **Chistov A. L.:** *"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].

The field k is finitely generated over the field of rational numbers $\mathbb{Q}$. We suppose that $k = \mathbb{Q}(T_1, \dots, T_l)[\eta]$, the elements $T_1, \dots, T_l$ are algebraically independent over $\mathbb{Q}$ and the element η is algebraic (and separable) over the field $\mathbb{Q}(T_1, \dots, T_l)$, and the minimal polynomial $\varphi \in \mathbb{Q}(T_1, \dots, T_l)[Z]$ of the element η over the field $\mathbb{Q}(T_1, \dots, T_l)$ is given.

We shall suppose that $\deg_{T_1,\dots,T_l,Z} \varphi < d_1, \quad \deg_{T_1,\dots,T_l} f < d_2$, $\deg_{X_1,\dots,X_n,Z} f \leqslant d, \quad \mathrm{l}(\varphi) \leqslant M_1, \quad \mathrm{l}(f) \leqslant M_2$ for some positive integers $d \geqslant 2$, d_1, d_2, M_1, M_2. These degrees are defined in natural way.

Fo simplicity we assume l to be fixed, i.e. regard l as a constant.

THEOREM 1 *Let $f \in k[X_1, \dots, X_n, Z]$ be an irreducible polynomial (in this ring) with the leading coefficient $\mathrm{lc}_Z f = 1$. Then one can factor the polynomial f in the ring $k[[X_1, \dots, X_n]][Z]$ (respectively $\overline{k}[[X_1, \dots, X_n]][Z]$). More precisely, the following assertions hold true.*

(i) One constructs the decomposition $f = \prod_{i \in I} f_i$ where all f_i are irreducible elements from the ring $k[[X_1, \dots, X_n]][Z]$ and all leading coefficients $\mathrm{lc}_Z f_i = 1$.

(ii) For every $i \in I$ one construct an irreducible polynomial $\varphi_i \in k[Y]$ of degree $\deg_Y \varphi_i \leqslant d$. Denote by $\{\eta_w\}_{w \in J_i}$ the family of all the roots from the algebraic closure $\overline{k}$ of the polynomial φ_i (these roots are conjugated over the field k).

(iii) For every $i \in I$ one constructs the decomposition $f_i = \prod_{w \in J_i} f_w$ where all $f_w \in k[\eta_w][[X_1, \dots, X_n]][Z]$ and all f_w are irreducible elements from

the ring $\overline{k}[[X_1, \ldots, X_n]][Z]$ *and the leading coefficients* $\mathrm{lc}_Z\, f_w = 1$. *In what follows we assume that for all* $i_1, i_2 \in I$ *if* $i_1 \neq i_2$ *then* $J_{i_1} \cap J_{i_2} = \varnothing$.

(iv) For every integer $j \geqslant 1$ *the running time of the algorithm for constructing all the polynomials* $f_i \bmod \mathfrak{m}^j$, $f_w \bmod \mathfrak{m}^j$ *is polynomial in* j^n, $d^{2^{n^c}}$, d_1, d_2, M_1, M_2 *for an absolute constant* $c > 0$.

Note that for any fixed n, say for $n = 2, 3, 4, \ldots$, the running time of the algorithms from Theorem 1, see (iv), is polynomial in j, d, d_1, d_2, M_1, M_2, i.e. this running time is polynomial in j and the size of the input data.

REMARK 1 Denote by δ the discriminant of the polynomial f with respect to Z. Put $r = \mathrm{ord}_X(\delta)$. One can use Theorem 1 §3 Chapter IV [1] about factroring polynomials over a field complete with respect to a discrete valuation

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

To prove Theorem 1 it is sufficient to construct all the polynomials $\overline{f}_i = f_i \bmod \mathfrak{m}^{r+1}$ and $\overline{f}_w = f_w \bmod \mathfrak{m}^{r+1}$ and after that applying the cited theorem from [1] obtain f_i and f_w, see Lemma 1 [8] for details.

Note also that 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 and after that it becomes much more similar to the lifting in the standard Hensel lemma. We are going to clarify this question in the next paper.

But factually the proof of Theorem 1 is self–contained and one can manage also without Theorem 1 §3 Chapter IV [1].

COROLLARY 1 *Under conditions of Theorem 1 put* $I'' = \{i \in I : f_i(0,\ldots,0,0) \neq 0\}$ *and* $I' = I \setminus I''$. *Set* $a = \prod_{i \in I''} f_i$ *(so* a *is invertible in* $\widehat{A}[[Z]]$*). Then for every* $i \in I'$ *the polynomial* f_i *is an irreducible element in the ring* $k[[X_1,\ldots,X_n,Z]]$. *For every* $i \in I'$, $w \in J_i$ *the polynomial* f_w *is an irreducible element in the ring* $\overline{k}[[X_1,\ldots,X_n,Z]]$. *Hence* $f = a \prod_{i \in I'} f_i$ *(respectively* $f = a \prod_{i \in I',\, w \in J_i} f_w$*) is a decomposition into irreducibles of the polynomial* f *in the ring* $k[[X_1,\ldots,X_n,Z]]$ *(respectively* $\overline{k}[[X_1,\ldots,X_n,Z]]$*).*

PROOF This follows immediately from Corollary of Proposition 7 §3 Chapter VII [2] (it is related to the Weierstrass preparation theorem).

[2] **Bourbaki N.:**, *"Algèbre commutative"*, Paris 1961, 1964, 1965.

COROLLARY 2 *Using Corollary 1 one can obtain an algorithm for factoring any polynomial* $g \in k[X_1,\ldots,X_n]$ *(here we assume that* $n \geqslant 2$*) in the rings of formal power series* $k[[X_1,\ldots,X_n]]$ *and* $\overline{k}[[X_1,\ldots,X_n]]$.

REMARK 2 *Notice that rings of formal power series over a field are integrally closed. Denote by* $k((X_1,\dots,X_n))$ *(respectively* $\overline{k}((X_1,\dots,X_n))$*) the field of fractions of the ring* $k[[X_1,\dots,X_n]]$ *(respectively* $\overline{k}[[X_1,\dots,X_n]]$*). Then in the case of arbitrary leading coefficient* $\mathrm{lc}_Z\, f \in k[X_0,\dots,X_n]$ *using the standard changing of variables* $Y = (\mathrm{lc}_Z\, f)Z$ *and applying Theorem 1 one can factor* f *over the field* $k((X_1,\dots,X_n))$ *(respectively* $\overline{k}((X_1,\dots,X_n))$*). But if* $\mathrm{lc}_Z\, f \notin k$ *this does not give an algorithm for factoring* f *in the ring* $k[[X_1,\dots,X_n]]$ *(respectively* $\overline{k}[[X_1,\dots,X_n]]$*).*

About the proof of Theorem 1.

Denote by $V \subset \mathbb{P}^{n+1}(\overline{k})$ the affine algebraic variety defined over k over k with the ring of regular functions $k[X_1, \ldots, X_n, Z]/(f) = B$. Put $z = Z \bmod f$. We shall suppose without loss of generality that the polynomial f is irreducible in the ring $\overline{k}[X_1, \ldots, X_n, Z]$. Denote by V' the normalization of the affine algebraic variety V. So V' is an affine algebraic variety. We construct using our results about the normalization the generic point tyhe integral closure B' of the ring B. Namely, $B' = k[y_1, \ldots, y_N]$ where each $y_v = (1/\delta) \sum_{0 \leqslant i < \deg_Z f} y_{v,i} z^i$ for some $y_{v,i} \in k[X_1, \ldots, X_n]$. Additionally assume that $y_v = X_v$, $0 \leqslant v \leqslant n$, and $y_{n+1} = z$ (so $N \geqslant n + 1$).

Denote by $\pi : V' \to \mathbb{A}^n(\overline{k})$ the morphism of affine algebraic varieties corresponding the inclusion $k[X_1, \ldots, X_n] \subset B'$ of ring of regular functions defined over k. Put $x = (0, \ldots, 0) \in \mathbb{A}^n(\overline{k})$.

At first we construct an element $\xi \in B'$ such that $\xi = \sum_{n+1\leqslant i\leqslant N} a_i y_i$ for some $a_i \in k$, the field of fractions $k(X_1,\dots,X_n)[\xi] = k(X_1,\dots,X_n)[z]$ and the number of elements $\#\xi(\pi^{-1}(x)) = \#\pi^{-1}(x)$. We find also a minimal polynomial $F \in k[X_1,\dots,X_n,Q]$, $\mathrm{lc}_Q F = 1$, of the element ξ over the field $k(X_1,\dots,X_n)$. Solving a linear system we represent $z = (1/\Delta)\sum_{0\leqslant i<\deg_Q F} z_{j,i}\xi^i$, where all $z_{j,i} \in k[X_1,\dots,X_n]$ and Δ. is the discriminant of the polynomial F with respect to Q.

After that we factor the polynomial $F(0, \dots, 0, Q) \in k[Q]$ into the product of pairwise relatively prime factors ψ_j, $\mathrm{lc}_Q\, \psi_j = 1$, over the field $\overline{k}$. Now using the standard Hensel lemma we can lift these factors till the factors Ψ_j, $\mathrm{lc}_Q\, \Psi_j = 1$, of the polynomial F in the ring $\overline{k}[[X_1, \dots, X_n]][Q]$. By the properties of ξ and the results from [10] these factors Ψ_j are irreducible elements of the ring $\overline{k}[[X_1, \dots, X_n]][Q]$. Put $\alpha_j = \deg_Q \Psi_j$.

Now for every $w \in J_i$, $i \in I$, there is a unique j such that

$$\Delta^{\alpha_j} f_w = \mathrm{Res}_Q\Big(\Psi_j,\, \Delta Z - \sum_{0 \leqslant j < \deg_Q F} z_{j,i} Q^i\Big), \tag{1}$$

where $\mathrm{Res}_Q(\dots)$ denotes the resultant of the considered polynomials from $\overline{k}[[X_1, \dots, X_n]][Z, Q]$ with respect to Q. So we can compute the polynomials $\Delta^{\alpha_j} f_w$ and after that f_w with arbitrary precision, the details see in [8]. The case of factors f_i irreducible in the ring $k[[X_1, \dots, X_n]][Z]$ is similar.

For more details, see Theorem 1 [8]. The complexity of the algorithm from Theorem 1 is polynomial in the size of the input data, $d^{2^{n^c}}$ and j^n for a constant $c > 0$. At present we have analyzed the construction of this algorithm thoroughly. We hope to improve it using the result of [9].

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

The complexity bound of the new version of this algorithm will be polynomial in the size of the input data, d^{n^c} and j^n (the constant c will be specified).

Also we are going to prove other interesting results related to the subject of this talk.

References

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

[2] **Bourbaki N.:**, *“Algèbre commutative”, Chap. 1–7* Actualités Sci. Indust., nos. 1290, 1293, 1308, 1314, Paris 1961, 1964, 1965.

[3] **Chistov A. L.:** *“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)].

[4] **Chistov A. L.:** *“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.

[5] **Chistov A. L.:** *“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].

[6] **Chistov A. L.:** *“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].

[7] **Chistov A. L.:** *“Effective normalization of a nonsingular in codi-*

mension 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].

[8] **Chistov A. L.:** *"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].

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

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