Записки научных
семинаров ПОМИ
Том 387, 2011 г.

A. L. Chistov

EFFECTIVE CONSTRUCTION OF A NONSINGULAR IN CODIMENSION ONE ALGEBRAIC VARIETY OVER A ZERO–CHARACTERISTIC GROUND FIELD

Abstract. Let k be a field of zero-characteristic finitely generated over a primitive subfield. Let f be a polynomial of degree at most d in n variables with coefficients from k and irreducible over an algebraic closure $\overline{k}$. Then we construct a nonsingular in codimension one algebraic variety V and a finite birational isomorphism $V \to \mathcal{Z}(f)$ where $\mathcal{Z}(f)$ is the hypersurface of all common zeroes of the polynomial f in the affine space. The working time of the algorithm for constructing V is polynomial in the size of the input.

Let f be a polynomial of degree less than d in n variables with coefficients from a field k finitely generated over a primitive subfield and irreducible over an algebraic closure $\overline{k}$ of k. Then we construct an affine nonsingular in codimension one algebraic variety V (i.e., the set of singular points $\mathrm{Sing}(V)$ of V has codimension at least one in V) which is birationally equivalent to the hypersuface $\mathcal{Z}(f)$ of all common zeroes of the polynomial f. Moreover, the constructed birational isomorphism $V \to \mathcal{Z}(f)$ is finite. The working time of the algorithm for constructing V is polynomial in the size of the input. The degree of the variety V is $(\deg \mathcal{Z}(f))^{O(1)}$ with an absolute constant in $O(1)$. This algorithm is based on the polynomial-time bounds for the complexity of the Newton-Puiseux algorithm [1] and important additional constructions from [2].

In the case of a nonzero characteristic ground field to obtain a similar algorithm with the same (or similar) working time is an open problem. Still the results analogous to those obtained in [1] and [2] also valid for a finite constant field. They can be obtained on the basis of the author's papers [4] and [5]. However, the fundamental problem here is not in estimating the sizes of the coefficients (as in [1], [2]), but in the presence of a higher-order ramification for extensions of fields of formal power series of

Key words and phrases: algebraic varieties, nonsingular in codimension one, effective algorithms, reduction to the case of algebraic curves.

nonzero characteristic, where it becomes impossible to select in advance a uniformizing element in the extension (in the case of local and global fields of zero–characteristic we have here similar difficulties and even more of them). I would like also to notice that in the English translation of [4] two pages are given in the wrong order: one must permute pages 1913 and 1914. The detailed version of [5] was planned for publication in one of the volumes of Zapiski Nauchn. Semin. LOMI in the series "Complexity Theory of Computation"(as all the other my results of the of that time) but not appeared by the reasons independent of the author.

The problem considered in this paper is the first part of our algorithm for effective normalization of an algebraic variety in zero–characteristic. If we got V then the normalization of $\mathcal{Z}(f)$ can be constructed using the algorithm from [3] (it can be applied in arbitrary characteristic) and all is reduced to solving a linear equation $aX + bY + cZ = 0$ over a ring of polynomials.

As far as I know so far there have not been obtained or published other algorithms of polynomial complexity similar to the one from [2] (probably the main difficulty here is to estimate the size of coefficients from the ground field of the obtained objects). In spite of their importance we have not presented the results of [2] at any conference in detail. So it is a high time to do it in a slightly new situation. In [2] we present also at length with the proofs all the estimates for the result of [1]. Recently I have looked through [2] and found minor corrections. In the Introduction there must be $F = \mathbb{Q}(T_1, \dots, T_l)[\eta]$ in place of $F = \mathbb{Q}(T_1, \dots, T_l)$ as it is seen from the context. In the assertion of Lemma 2.1 one must add $\xi_i \neq \xi_j$ (notice that in [1] in the same lemma this condition is not absent, everything is correct). Further, one should delete in [2] one wrong sentence on page 147, line 18 from below (respectively in English translation of [2] on page 866, line 18 from below): "If elements ω_j and $\widetilde{\omega}_j$ coincide...". Actually all these and several other corrections are straightforward if one reads the paper attentively (and to understand the paper one needs to do it). Due to the importance of Lemma 2.1 [2] we formulate it in the Appendix at the end of the paper for the convenience of the reader.

At present we would like to apply the results from [2] but we have an $(n-1)$-dimensional variety $\mathcal{Z}(f)$ at the input of the algorithm in place of a curve in [2]. Still we can replace our variety $\mathcal{Z}(f)$ by the curve considering, say, the first $n-2$ variables as elements of the new ground field and after that apply the results of [2]. If we apply the results of [2] directly we get slightly less strong estimates than the ones from Theorem 1, see below.

So one need at present following the method of [2] carefully analyze all the estimations again.

Now we proceed to exact statements. Let the field $k = \mathbb{Q}(t_1, \dots, t_l)[\theta]$ where $t_1, \dots, t_l$ are algebraically independent over the field $\mathbb{Q}$, $l \geqslant 0$, and θ is algebraic over $\mathbb{Q}(t_1, \dots, t_l)$ with the minimal polynomial $F \in \mathbb{Q}[t_1, \dots, t_l, Z]$, and leading coefficient $\mathrm{lc}_Z F$ of F is equal to 1. Let $f \in k[X_1, \dots, X_n]$, $n \geqslant 2$, be a polynomial irreducible over the algebraic closure $\overline{k}$. Denote by $\mathrm{lc}_{X_n}(f)$ the leading coefficient of the polynomial f with respect to X_n. We shall suppose additionally that $\mathrm{lc}_{X_n}(f) = 1$. This is a condition of general position which can be easily satisfied performing a nondegenerate linear transformation of the coordinate functions with coefficients from $\mathbb{Z}$ (but notice that after a linear transformation of the coordinates one can get a polynomial with the upper bound for the degree nd; so, may be, it is more natural to consider in a statement a polynomial of total degree at most d, see Corollary 1). The ring of regular functions defined over k of the algebraic variety $V_0 = \mathcal{Z}(f)$ is $k[V_0] = k[X_1, \dots, X_n]/(f)$. The field $k(V_0)$ of rational functions defined over k of the variety V_0 is the field of fractions of the ring $k[X_1, \dots, X_n]/(f)$. Put $x_n = X_n \bmod f \in k[V_0]$. Denote by $\Delta = \mathrm{Res}_{X_n}(f, \partial f/\partial X_n)$ the discriminant of the polynomial f with respect to X_n.

We shall represent the polynomial f in the form

$$f = \frac{1}{a_0} \sum_{i_1, \dots, i_n} \sum_{0 \le j < \deg_Z F} a_{i_1, \dots, i_n, j} \theta^j X_1^{i_1} \cdots X_n^{i_n}, \tag{1}$$

where $a_0, a_{i_1, \dots, i_n, j} \in \mathbb{Z}[t_1, \dots, t_l]$, $\mathrm{GCD}_{i_1, \dots, i_n, j}(a_0, a_{i_1, \dots, i_n, j}) = 1$. Define the length $\mathrm{l}(a)$ of an integer a by the formula $\mathrm{l}(a) = \min\{s \in \mathbb{Z} :: |a| < 2^{s-1}\}$. The length of coefficients $\mathrm{l}(f)$ of the polynomial f is defined to be the maximum of lengths of coefficients from $\mathbb{Z}$ of polynomials $a_0, a_{i_1, \dots, i_n, j}$ and the degree

$$\deg_{t_\gamma}(f) = \max_{i_1, \dots, i_n, j} \{\deg_{t_\gamma}(a_0), \deg_{t_\gamma}(a_{i_1, \dots, i_n, j})\},$$

where $1 \le \gamma \le l$. In the similar way we shall define degrees and lengths of integer coefficients of other polynomials, in particular $\deg_{t_\gamma} F$ and $\mathrm{l}(F)$ are defined.

We shall suppose that we have the following bounds

$$\begin{gathered}\deg_{X_i}(f) < d,\ \deg_{t_\gamma}(f) < d_2, \mathrm{l}(f) < M, \\ \deg_Z(F) < d_1,\ \deg_{t_\gamma}(F) < d_1,\ \mathrm{l}(F) < M_1\end{gathered} \tag{2}$$

for all $1 \le i \le n$, $1 \le \gamma \le l$. The size $\mathrm{L}(f)$ of the polynomial f is defined to be the product of $\mathrm{l}(f)$ to the number of all the coefficients from $\mathbb{Z}$ of f in the dense representation. We have

$$\mathrm{L}(f) < (d^n d_1 + 1) d_2^l M$$

Similarly $\mathrm{L}(F) < d_1^{l+1} M_1$.

Theorem 1. *Under previous conditions one can construct an element $z \in k(V_0)$ integral over the subalgebra $k[X_1, \dots, X_{n-1}]$ and satisfying the following properties.*

(i) *z is a primitive element of the extension $k(V_0) \supset k(X_1, \dots, X_{n-1})$.*

(ii) *Let us represent $z = (\sum_{0 \le i < \deg_{X_n} f} z_i x_n^i)/\Delta$ where all $z_i \in k[X_1, \dots, X_{n-1}]$. Then the degrees and the lengths of integer coefficients*

$$\deg_{X_m} z_i = d^{O(1)}, \quad \deg_{t_\alpha} z_i = d_2 (d_1 d)^{O(1)},$$
$$\mathrm{l}(z_i) = (M_1 + M_2 + l + n) d_2 (d_1 d)^{O(1)}$$

for all i and $1 \le m \le n-1$, $1 \le \alpha \le l$ with absolute constants in $O(1)$.

(iii) *Suppose that $\deg_{X_1, \dots, X_{n-1}} f < d'$. Then $\deg_{X_1, \dots, X_{n-1}} z_i = d' d^{O(1)}$ for all $1 \leqslant i < \deg_{X_n} f$.*

(iv) *The working time of the algorithm for constructing elements z_1, z_2 is polynomial in M_1, M_2, $(d_1 d_2 d)^{l+1}$, d^n. Hence it is polynomial in $\mathrm{L}(f)$, $\mathrm{L}(F)$ if l is fixed (i.e., if l is considered as a constant; notice that it is general situation for all our algorithms). Denote by V the defined over k affine algebraic variety with the ring of defined over k regular functions $k[X_1, \dots, X_{n-1}][x_n, z]$. Hence $V \subset \mathbb{A}^{n+1}(\overline{k})$ and there is a finite birational isomorphism of defined over k affine algebraic varieties $V \to V_0$ induced by the inclusions of the rings of regular functions. Denote by D the degree of the affine algebraic variety $V_0 = \mathcal{Z}(f)$ (by definition the degree of an affine algebraic variety is the degree of its closure with respect to the Zariski topology in the corresponding projective space), hence $D < nd$. Finally, we have*

(v) *the degrees of the algebraic variety $\deg V = D^{O(1)}$ with an absolute constant in $O(1)$.*

All the constants $O(1)$ in this theorem can be computed explicitly. It would be interesting to find the minimal values of the constants $O(1)$ in this theorem, especially in assertion (v) related to degrees of algebraic varieties. In (ii) using [2] one can obtain more precise bounds.

Corollary 1. *Let us replace the conditions* $\deg_{X_m} f < d$, $1 \leqslant m \leqslant n$ *by* $\deg_{X_1,\dots,X_n} f < d$. *Then a new version of Theorem 1 holds true. Namely, to obtain this version one must replace in* (ii) $\deg_{X_m} z_i = d^{O(1)}$ *for all* $1 \leqslant i \leqslant n-1$ *by* $\deg_{X_1,\dots,X_{n-1}} z_i = d^{O(1)}$ *and in* (iv) d^n *by* $\binom{n+d^{O(1)}}{n}$ *with an absolute constant in* $O(1)$.

Sketch of the proof. Let us replace n by $n+1$, $X_1,\dots,X_n$ by $X_0,\dots,X_n$, the polynomial f by its homogenization

$$\overline{f} = X_0^{\deg_{X_1,\dots,X_n} f} f(X_1/X_0,\dots,X_n/X_0)$$

and apply Theorem 1 to the polynomial $\overline{f}$. Since $\overline{f}$ is homogeneous all the elements appearing in the proof of Theorem 1, see Section 1, can be chosen to be homogeneous and they have the degrees $d^{O(1)}$ with respect to $X_0,\dots,X_n$. Using, e.g., the criterion of irreducibility from [6] one can suggest a version of the algorithm for factoring homogeneous polynomials of degree d' in $n+1$ variables with the complexity polynomial in $\binom{n+(d')^{O(1)}}{n}$ and the maximum of lengths of its coefficients from the ground field. All the other algorithms applied in the proof of Theorem 1 are also have the similar bounds for complexity for homogeneous polynomials at the input. Thus by Theorem 1 with $\overline{f}$ in place of f we get an element $\overline{z}$ within the required working time. Now it is sufficient to put $z = \overline{z}|_{X_0=1}$. □

Corollary 2. *Let us replace in the statement of Corollary 1* n *by* $n+1$, $X_1,\dots,X_n$ *by* $X_0,\dots,X_n$ *and assume that* f *is homogeneous. Then the assertion of Corollary 1 holds and all the elements* z_i *and* z *(i.e., the polynomial* $\sum_{0\leqslant i<\deg f} z_i X_n^i$*) are homogeneous. Let* $\nu = \deg(\sum\limits_{0\leqslant i<\deg f} z_i X_n^i) - \deg\Delta$ *be the homogeneous degree of* z*, hence* $\nu = d^{O(1)}$. *Denote by* B *the subring of* $k[V]$ *generated by all the homogeneous elements of degree* ν *of* $k[V]$. *So* B *is a graded ring. Put the new homogeneous degree of a homogeneous element* $b \in B$ *to be* $(\deg b)/\nu$ *where* $\deg b$ *is the (old) homogeneous degree of* b. *Thus, we introduce the new graduation on* B*, and* B *becomes a homogeneous ring of a projective algebraic variety* $V_1 \subset \mathbb{P}^N(\overline{k})$, $N = \binom{\nu+n}{n}$. *The variety* V_1 *is nonsingular in codimension one and there is a finite birational isomorphism of projective algebraic varieties* $V_1 \to \mathcal{Z}(f)$ *(here* $\mathcal{Z}(f) \subset \mathbb{P}^n(\overline{k})$*) induced by the inclusions of rings* $B \subset k[V]$ *and* $k[V_0] \subset k[V]$. *By the Bézout theorem the degree* $\deg V_1 = d^{O(n)}$. *Further, one can construct a linear projection* $\pi : \mathbb{P}^N(\overline{k}) \to \mathbb{P}^{n+2}(\overline{k})$ *inducing the finite birational isomorphism* $V_1 \to \pi(V_1) = V_2$ *of projective algebraic* *varieties and the variety V_2 is nonsingular in codimension one, the degree* $\deg V_2 = d^{O(n)}$. *The working time of the algorithm for constructing the variety V_2 is polynomial in d^{n^2} and the size of the input, i.e., in d^{n^2} and* M_1, M_2, $(d_1 d_2 d)^{l+1}$.

Proof. It is not difficult to construct a linear projection $\pi' : \mathbb{P}^N(\overline{k}) \to \mathbb{P}^{n+1}(\overline{k})$ inducing the finite birational isomorphism $V_1 \to \pi'(V_1) = V_3$. Now $V_3 = \mathcal{Z}(f_3) \subset \mathbb{P}^{n+1}(\overline{k})$ is a hypersurface. Let $\mathbb{P}^{n+1}(\overline{k})$ have homogeneous coordinate functions $X_0, \dots, X_n$. We compute the polynomial f_3. We can suppose without loss of generality performing if necessary a nondegenerate linear transformation of the coordinates that the leading coefficient $\mathrm{lc}_{X_n} f_3 = 1$. Let us replace in the construction of Section 1 $(f, k[V'])$ by $(f_3, k[V_1])$ where $k[V_1]$ is a homogeneous ring of the projective algebraic variety V_1. Then we obtain at the output of this construction the homogeneous ring of some projective algebraic variety in place of $k[X_1, \dots, X_{n-1}][x_n, z]$. By definition V_2 is the last projective algebraic variety. The estimation of the working time for constructing V_2 now follows immediately from Theorem 1 (and the construction of Section 1). □

I would like also to note that one can suggest a version of the algorithm for Theorem 1 which does not use factoring polynomials over $\mathbb{Q}$ (or over any finitely generated extension of $\mathbb{Q}$). Finding square-free parts of polynomials over such fields is sufficient. Even the condition that f is irreducible over $\overline{k}$ can be omitted and then at the output we get equidimensional algebraic varieties (i.e., all the irreducible components of the varieties at the output have the same dimension) nonsingular in codimension one.

Remark 1. Theorem 1 slightly strengthen Theorem 1 from [7]. To get the last theorem it is sufficient to take $z_1 = x_n$, $z_2 = z$ and $V_1 = V$ where V and z are from Theorem 1.

In Remark 1 of [7] we wrote that in the homogeneous case the degree of the obtained projective algebraic variety is the same as in the affine case. It is not true in general. Actually we meant there the degree of the affine algebraic variety with the ring of regular functions $k[X_1, \dots, X_{n-1}][x_n, z]$ which is a graded ring if f is homogeneous. The required projective algebraic variety can be glued using affine algebraic variety of degrees $d^{O(1)}$ but to obtain an embedding into the projective space in the case $\deg z > 1$ we need a kind of the Veronese mapping and get the degree $d^{O(n)}$, see Corollary 2.

Reduction to the case of a curve

The aim of this section is to prove Theorem 1 reducing everything to the case of a curve which will be considered in Section 3.

Let $1 \leqslant i \leqslant n-1$ be an integer. Put the multiplicatively closed set

$$S_i = k[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_{n-1}] \setminus \{0\},$$

the field

$$k_i = S_i^{-1} k[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_{n-1}].$$

Let $\mathbb{A}^2(\overline{k_i})$ have coordinate functions X_i, X_n Denote by $C_i \subset \mathbb{A}^2(\overline{k_i})$ the affine curve defined over the field k_i with the ring of regular functions $k_i[C_i] = S_i^{-1}k[V_0] = k_i[X_i, X_n]/(f)$. Notice that the curve C_i is irreducible over k_i by the Gauss lemma since f is irreducible over k.

Denote by B_i the integral closure of $k_i[C_i]$ in its field of fractions, i.e., in the ring of rational functions $k(V_0)$. For every $1 \leqslant i \leqslant n-1$ let us apply Theorem 3, see Section 3 replacing $T_1, \dots, T_m$ by $X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_{n-1}$, and construct a system of generators $y_{i,1}, \dots, y_{i,m_i}$ of the $k_i[C_i]$-module B_i. We shall suppose without loss of generality in what follows that

$$y_{i,j} = \Big(\sum_{0 \leqslant q < \deg_{X_n} f} y_{i,j,q} x_n^q \Big) / \Delta \tag{3}$$

where $y_{i,j,q} \in k[X_1, \dots, X_{n-1}]$ for all i, j, q.

Denote by $y_1, \dots, y_m$ the family consisting of all the elements $y_{i,j}$, $1 \leqslant j \leqslant m_i$, $1 \leqslant i \leqslant n-1$, and the element x_n. From Theorem 3 we get immediately $m = nd^{O(1)}$. Put $A' = k[X_1, \dots, X_{n-1}, y_1, \dots, y_m] \subset k(V_0)$. Denote by V' the algebraic variety with the ring of defined over k regular functions A'. From the described construction and the Zariski main theorem we get immediately.

Lemma 1. *The algebraic variety $V' \subset \mathbb{A}^{n-1+m}(\overline{k})$ is nonsingular in codimension one, and the inclusion of rings of regular functions induces the finite birational morphism $V' \to V_0$.* □

Let us compute the discriminant $\Delta \in k[X_1, \dots, X_{n-1}]$ of the polynomial f with respect to X_n. Using the algorithm for factoring polynomials from [8] we decompose $\Delta = \lambda_0 \prod_{j \in J} \delta_j^{c_j}$ where all $\delta_j \in k[X_1, \dots, X_{n-1}]$ are irreducible, pairwise distinct, $c_j \geqslant 1$ are integers and $\lambda_0 \in k$.

Notice that for every irreducible factor $\delta = \delta_j$ dividing Δ there is i such that $S_i \subset k[X_1, \dots, X_{n-1}] \backslash (\delta)$ and hence the localization $k[V]_{(\delta)} \supset k_i[C_i]$. We choose such an index $i = i(j)$ for every $j \in J$. Applying Theorem 3 from Section 3 we construct all the maximal ideals $\mathfrak{m}_\gamma \subset k_i[C_i]$, $\gamma \in \Gamma_j$ such that $\mathfrak{m}_\gamma \supset (\delta_j)$. Moreover, $\mathfrak{m}_\gamma = (\delta_j, \pi_\gamma)$ for an element $\pi_\gamma \in B_i$ which is constructed.

Denote by $p : V' \to \mathbb{A}^{n-1}(\overline{k})$ the finite projection induced by the inclusion of ring of defined over k functions $k[V'] \supset k[X_1, \dots, X_{n-1}]$. Notice that the irreducible over k components of the algebraic variety $p^{-1}(\mathcal{Z}(\delta_j))$ are in the one–to–one correspondence with the maximal ideals $\mathfrak{m}_\gamma$, $\gamma \in \Gamma_j$. More precisely, denote by W_γ the irreducible over k component of $p^{-1}(\mathcal{Z}(\delta_j))$ corresponding to $\mathfrak{m}_\gamma$ and by $k(W_\gamma)$ the field of rational functions defined over k of this algebraic variety. Then the natural homomorphism $k[V'] \to B_{i(j)}/\mathfrak{m}_\gamma$ induces the isomorphism $k(W_\gamma) \to B_{i(j)}/\mathfrak{m}_\gamma$. In the other words the last isomorphism defines a generic point defined over k of the algebraic variety W_γ. We shall denote it by w_γ.

Let us represent $W_\gamma = \bigcup_{\iota \in I_\gamma} E_\iota$ where E_ι are the irreducible over $\overline{k}$ components of W_γ. They are conjugated over the field k and hence have the same dimension. We shall suppose without loss of generality that $I_{\gamma_1} \cap I_{\gamma_2} = \varnothing$ for all distinct $\gamma_1, \gamma_2 \in \Gamma_j$ for every $j \in J$. Put $I_j = \bigcup_{\gamma \in \Gamma_j} I_\gamma$ for every $j \in J$.

Notice that each component E_ι contains a smooth point of V' since V' is nonsingular in codimension one. It is known that in this case any generic point e_ι of E_ι is a smooth point of the variety V'. We choose and fix the generic points e_ι such that the zero-dimensional algebraic variety corresponding to each w_γ contains only the points e_ι.

Let $Y_1, \dots, Y_m$ be new variables and $L \in k[Y_1, \dots, Y_m]$ be a linear form. Let us define the morphism

$$p_L : V' \to \mathbb{A}^n(\overline{k}), \quad z \mapsto (X_1(z), \dots, X_{n-1}(z), L(y_1, \dots, y_m)(z)).$$

Since p is finite dominant we have $p_L(V') = \mathcal{Z}(f_L)$ for the uniquely defined irreducible polynomial $f_L \in k[X_1, \dots, X_n]$ with the leading coefficient $\mathrm{lc}_{X_n} f_L = 1$. Denote by $p'_L : V' \to p_L(V')$ the finite dominant morphism induced by p_L.

Let $j \in J$. Consider the following conditions:

1) The fields $k(X_1, \dots, X_{n-1}, L(y_1, \dots, y_m)) = k(V)$ coincide.
2) The differential $d_{e_\iota} p_L$ is a monomorphism for every $\iota \in I_j$.
3) For all distinct $\iota_1, \iota_2 \in I_j$ we have $p_L(e_{\iota_1}) \neq p_L(e_{\iota_2})$.

Lemma 2. *Let $L \in k[Y_1, \dots, Y_m]$ be a linear form and $j \in J$. Then the following conditions are equivalent.*

(a) *For the linear form L all conditions* 1), 2), 3) *hold true.*

(b) *The morphism p'_L is finite birational and $p'_L(e_\iota)$ is a smooth point of the hypersurface $\mathcal{Z}(f_L)$ for every $\iota \in I_j$.*

(c) *The degree $\deg_{X_n} f_L = \deg_{X_n} f$ and for every $\gamma \in \Gamma_j$ at least one of n elements*

$$\frac{\partial f_L}{\partial X_i}(X_1, \dots, X_{n-1}, L(y_1, \dots, y_m)), \quad 1 \leqslant i \leqslant n,$$

does not belong to the ideal $\mathfrak{m}_\gamma \subset B_{i(j)}$.

Moreover, (b) implies by the Zariski main theorem that the differential $d_{e_\iota} p'_L$ is an isomorphism for every $\iota \in I_j$.

Proof. To deduce (b) from (a) one can apply the implicit function theorem for formal power series (we leave the details to the reader here). The inverse implication follows from the Zariski main theorem. The equivalence of (b) and (c) is straightforward from the definitions. □

Further, we get immediately the following two lemmas.

Lemma 3. *There are at most $(nd)^{O(1)}$ integers c satisfying the following property. For the linear form $L = \sum_{1 \leqslant i \leqslant m} c^i Y_i$ there is $j \in J$ such that at least one of conditions* 1), 2), 3) *does not hold.* □

Lemma 4. *Let $L, L' \in k[Y_1, \dots, Y_m]$ be linear forms. Suppose that for all $j \in J$ conditions* 1), 2), 3) *are satisfied for the linear form L. Then for all $t \in k$, except at most a polynomial in $(nd)^{O(1)}$ number, conditions* 1), 2), 3) *are satisfied for the linear form $L + tL'$ (in place of L).* □

Now we are going to describe how to construct an element z from the statement of Theorem 1. Let us enumerate integer $c = 0, 1, 2, \dots$. For the considered c put $L = \sum_{1 \leqslant i \leqslant m} c^i Y_i$. Using representations (3) and solving a linear system over the field $k(X_1, \dots, X_{n-1})$ we construct the polynomial f_L. Applying Theorem 3 from Section 3 we decide whether

($*$) assertion (c) of Lemma 3 holds for every $\gamma \in \Gamma_j$ for every $j \in J$.

If ($*$) is not fulfilled then we proceed to the next c. By Lemma 2 and Lemma 3 there is $c = (nd)^{O(1)}$ such that ($*$) holds true. We shall find such an integer c and stop the enumeration at this $c = c_0$.

Now we describe a new recursion on (L,α) where L is a linear form and $1 \leqslant \alpha \leqslant m$ is an integer. At the beginning of this recursion $\alpha = 1$ and $L = \sum_{1\leqslant i\leqslant m} c_0^i Y_i$. Let us describe the step of this recursion with the input (L,α). Let $L = \sum_{1\leqslant i\leqslant m} l_i Y_i$, where all l_i are integers. By Lemma 4 with $L' = Y_\alpha$ applying Theorem 3 from Section 3 (only its assertion related to $\varphi \in \mathfrak{m}_g$) we construct a new linear form $L'' = \sum_{1\leqslant i\leqslant m,\, i\neq\alpha} l_i Y_i + t_\alpha Y_\alpha$ satisfying property $(*)$ with L'' in place of L and an integer $t_\alpha = (nd)^{O(1)}$. Put the new linear form L to be L''. If $\alpha+1 \leqslant m$ we proceed to the next step with the input $(L, \alpha+1)$. If $\alpha = m$ then we stop, i.e., the step with $\alpha = m$ is final.

Put $z = L(y_1,\dots,y_m)$ for the constructed linear form L. Now assertions (i)-(iv) of Theorem 1 hold true by the Zariski main theorem and Theorem 3 from Section 3.

It remains to prove (v). Let $u = \{u_{i,j}\}$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n+1$, and $k(u)$ be the extension of k by all the elements $u_{i,j}$ from the family u. Hence the transcendency degree of the field $k(u)$ over k is $n(n+1)$. Put $u_i = \sum_{1\leqslant j\leqslant n-1} u_{i,j}X_j + u_{i,n}x_n + u_{i,n+1}z$, $1 \leqslant i \leqslant n$. Then there is an irreducible over $k(u)$ polynomial $\Phi \in k(u)[X_1,\dots,X_n]$ such that $\Phi(u_1,\dots,u_n) = 0$. The polynomial Φ is uniquely defined up to a nonzero factor from $k(u)$. From the Bézout theorem we deduce that the degree $\deg V = \deg_{X_1,\dots,X_n}\Phi$.

There is a nondegenerate $k(u)$-linear transformation of the elements u_i, $1 \leqslant i \leqslant n$, such that the transformed elements

$$u'_v = \sum_{1\leqslant i\leqslant n} \lambda_{v,i}u_i = X_v + \mu_v x_n, \quad 1 \leqslant v \leqslant n-1,$$

$$u'_n = \sum_{1\leqslant i\leqslant n} \lambda_{n,i}u_i = z + \mu_n x_n,$$

where all $\lambda_{v,i}, \mu_v \in k(u)$, $1 \leqslant i, v \leqslant n$, and the transcendency degree of the field $k(\mu_1,\dots,\mu_n)$ over k is n. Hence there is a polynomial Φ' such that $\Phi'(u'_1,\dots,u'_n) = 0$ and $\deg\Phi = \deg\Phi'$.

Put $f' = f(X_1 - \mu_1 X_n, \dots, X_{n-1} - \mu_{n-1}X_n, X_n)$. Then

$$f'(u'_1,\dots,u'_{n-1},x_n) = 0,$$

the polynomial f' is irreducible in $k(u)(X_1,\dots,X_{n-1})[X_n]$ and $\deg_{X_n} f' = \deg_{X_1,\dots,X_n} f = \deg V_0$. Set the fields $K = k(u)(X_1,\dots,X_{n-1})$ and

$K' = K[T]/(f'(X_1, \dots, X_{n-1}, T))$ where T is a new variable. Put

$$t = T \bmod f'(X_1, \dots, X_{n-1}, T) \in K'.$$

Recall that $z = (\sum_{0 \leqslant i < \deg_{X_n} f} z_i x_n^i)/\Delta$ where all $z_i \in k[X_1, \dots, X_{n-1}]$. Put

$$\begin{aligned} z_i' &= z_i(X_1 - \mu_1 t, \dots, X_{n-1} - \mu_{n-1} t), \quad 0 \leqslant i < \deg_{X_n} f, \\ \Delta' &= \Delta(X_1 - \mu_1 t, \dots, X_{n-1} - \mu_{n-1} t), \end{aligned}$$

and $z' = \sum_{0 \leqslant i < \deg_{X_n} f} z_i' t^i$. We have $0 \neq \Delta' \in K'$ since, otherwise, by the Gauss lemma f' divides $\Delta(X_1 - \mu_1 X_n, \dots, X_{n-1} - \mu_{n-1} X_n)$ in the ring $k(u)[X_1, \dots, X_n]$ and this implies a contradiction: f divides Δ.

Consider the mapping of the norm $\mathcal{N} : K'(X_n) \to K(X_n)$. Now $0 \neq \Phi'' = \mathcal{N}(\Delta' X_n - (z' + \mu_n \Delta' t)) \in k(u)[X_1, \dots, X_n]$ since $\mathrm{lc}_{X_n} f' \in k(u)$. Further, according to our definitions Φ' divides Φ''. Hence, $\deg \Phi' \leqslant \deg \Phi''$. Therefore, it is sufficient to prove $\deg \Phi'' = D^{O(1)}$.

We can compute Φ'' as the determinant of the matrix corresponding to the $K(X_n)$-linear mapping

$$K'(X_n) \to K'(X_n), \quad a \mapsto (\Delta' X_n - (z' + \mu_n \Delta' t))a$$

taking t^i, $0 \leqslant i < \deg f$ as a basis of $K'(X_n)$ over $K(X_n)$. Now the required bound $\deg \Phi'' = D^{O(1)}$ follows from (ii) and (iii). The theorem is proved (modulo Theorem 3).

2. A version of the theorem on factoring polynomials over fields of formal power series

In [2] we describe polynomial–time algorithms for factoring polynomials over the fields $k((X))$, $\overline{k}((X))$ and $\Omega = \overline{k((X))} = \bigcup_{\nu \geqslant 1} \overline{k}((X^{1/\nu}))$ (now k plays the role of the field F from [2]) with estimations of sizes of all the objects from these algorithms. In the case of Ω we get also explicit upper bounds for all degrees and lengths of integer coefficients of these objects (for $k((X))$ and $\overline{k}((X))$ one can also get them analogously but we just omit the details in [2] in these cases). Now for the proof of Theorem 3 from Section 3 we need to obtain similar algorithms and estimations for a more general field of coefficients K in place of k. We refer explicitly only to the case of the field $K((X))$ in Section 3. So we formulate our result only over the field $K((X))$, see Theorem 2 below.

Namely, let k be the field from the Introduction, $T_1, \dots, T_m$ be new variables, $m \geqslant 0$, and the field $K = k(T_1, \dots, T_m)$. Let $f \in K[X, Y]$ be a polynomial. Set $X_1 = X$, $X_2 = Y$. We represent f it in the form (1) with $n = 2$ but now all $a_0, a_{i_1,i_2,j} \in \mathbb{Z}[t_1, \dots, t_l, T_1, \dots, T_m]$, $\mathrm{GCD}_{i_1,i_2,j}(a_0, a_{i_1,i_2,j}) = 1$ in this ring. We define

$$\deg_{T_\beta}(f) = \max_{i_1,i_2,j}\{\deg_{T_\beta}(a_0), \deg_{T_\beta}(a_{i_1,i_2,j})\}, \quad 1 \leqslant \beta \leqslant m,$$
$$\deg_{T_1,\dots,T_m}(f) = \max_{i_1,i_2,j}\{\deg_{T_1,\dots,T_m}(a_0), \deg_{T_1,\dots,T_m}(a_{i_1,i_2,j})\}.$$

The degrees $\deg_{t_\gamma} f$, $1 \leqslant \gamma \leqslant l$, the length of integer coefficients $l(f)$ are defined in the same way as in the Introduction. Similarly are defined the degrees $\deg_{T_\beta}$, $1 \leqslant \beta \leqslant m$, $\deg_{T_1,\dots,T_m}$, $\deg_{t_\gamma}$, $1 \leqslant \gamma \leqslant l$, and the length of integer coefficients of other elements (e.g., of the polynomials $g_{\#}(N)$, $f_{i\,\#}(N)$, see below).

We shall suppose that (1), (2) hold, see the Introduction, and additionally

$$\deg_{T_1,\dots,T_m}(f) < d_4, \quad \deg_{T_\beta}(f) < d_3, \quad 1 \leqslant \beta \leqslant m.$$

We shall assume that the leading coefficient $\mathrm{lc}_Y f = 1$ and hence $\deg f = \deg_Y f$. Consider the decomposition into the irreducible factors

$$f = \prod_{i \in I} f_i^{e_i} \tag{4}$$

over the field $K((X))$. Additionally suppose that $\mathrm{lc}_Y f_i = 1$ for all $i \in J$. Recall that $K[[X]]$ denotes the ring of formal power series of X over K. Let $g = f_i$ be an arbitrary factor. Then it is represented in the form $g = \sum_{0 \leqslant j < \deg_Y g} g_j Y^j$ where all $g_j \in K[[X]]$ since the coefficients g_j are integral over $K[X]$. Hence $g_j = \sum_{i \geqslant 0} g_{j,i} X^i$ where all $g_{j,i} \in K$. For a real number N by definition put

$$g_{\#}(N) = \sum_{0 \leqslant j < \deg_Y g} Y^j \sum_{0 \leqslant i \leqslant N} g_{j,i} X^i \in k[X, Y],$$

hence if $N \geqslant 0$ is an integer then X^{N+1} divides $g - g_{\#}(N)$ in the ring $K[[X]]$ and $\deg_X g_{\#}(N) \leqslant N$. So $g_{\#}(N) \in K[X, Y]$ is the N-th approximation of the polynomial $g \in K[[X]][Y]$. We shall say, cf. [2], that the decomposition (4) is constructed by an algorithm within the time polynomial in $A_1, \dots, A_\alpha$ (here A_i depends on the input data) if for every integer $N \geqslant 0$ using this algorithm one can construct within the time polynomial in $A_1, \dots, A_m$ and N^{l+m+1} the set of indices I and for all $i \in I$ the polynomials $f_{i\,\#}(N)$ and integers e_i.

Theorem 2. *One can construct decomposition (4) within the time polynomial in $(d_1d_2d)^{l+1}$, $(d_3d)^m$, d, M_1, M_2. Moreover, for every integer $N \geqslant 0$ for all $i \in I$ we have the following estimations for degrees and lengths of integer coefficients*

$$\deg_{t_\gamma} f_{i\,\#}(N) = Nd_2(d_1d)^{O(1)}, \quad 1 \leqslant \gamma \leqslant l,$$
$$\deg_{T_\beta} f_{i\,\#}(N) = Nd_3d^{O(1)}, \quad 1 \leqslant \beta \leqslant m,$$
$$\mathrm{l}(f_{i\,\#}(N)) = N\log(N+1)(M_1+M_2+l+m)(d_2+d_3)(d_1d)^{O(1)},$$
$$\deg_{T_1,\dots,T_m} f_{i\,\#}(N) = Nd_4d^{O(1)}.$$

PLAN FOR THE PROOF. At first one needs to consider the estimations for the algorithm for factoring polynomials over the field $\Omega_1 = \bigcup_{\nu\geqslant 1}\overline{K}((X^{1/\nu}))$. They are similar to the ones from Theorem 2 [2] and the required bounds for degrees and lengths of integer coefficients for the field K in place of k are obtained analogously to Section 2 of [2] where the complexity of the Newton–Puiseux algorithm is estimated. After that it is sufficient to collect together factors conjugated over the field $K((X))$, cf. Section 3 of [2]. To estimate the complexity notice that actually everything is reduced to factoring polynomials over the field K (and its finite extensions) and solving linear systems of size $d^{O(1)}$. From here the bounds from the statement of the theorem follow directly, cf. [2]. □

Note that the estimates for degrees and lengths of integer coefficients from the statement of the theorem are not sharp (but they are sufficient for our aims), one can obtain here more fine bounds, cf. the statement of Theorem 2 [2].

3. Constructing a smooth affine curve

In Section 4 of [2] we prove Theorem 3 [2] and suggest an algorithm for constructing the normalization of the affine curve $\mathcal{Z}(f) \subset \mathbb{A}^2(\overline{F})$ for a polynomial $f \in F[X,Y]$ irreducible over $\overline{F}$. The field F is similar to the field k from the Introduction. Now our aim is to obtain in Theorem 3 the analogous result for the field K in place of F and a polynomial

$f \in K[X,Y]$ irreducible over K (it is not necessarily irreducible over $\overline{K}$ but actually it does not change anything). Since the situation now is slightly different in comparison with [2] we repeat the required part of the construction from [2] in the proof of Theorem 3 below for this more general situation of the field K (in place of k). Simultaneously we would like to correct minor inexactitudes from Section 4 of [2] (factually it can be easily done by the reader from the context).

Let $f \in K[X,Y]$ be the polynomial from Section 2. Hence the leading coefficient $\mathrm{lc}_Y f = 1$ and f satisfies the same estimates for all the degrees and length of integer coefficients. Now additionally we shall suppose that the polynomial f is irreducible over K. Let $V_0 = \mathcal{Z}(f) \subset \mathbb{A}^2(\overline{K})$ be the affine curve defined over K with the ring of defined over K regular functions $K[V_0] = K[X,Y]/(f)$. Denote $y = Y \bmod f \in K[X,Y]/(f)$. The field of defined over K rational functions of the algebraic variety V_0 is $K(V_0) = K(X)[y]$.

Denote by V_1 the normalization of V_0. It is a defined over K affine curve irreducible over K and the ring of defined over K regular functions $K[V_1]$ is the integral closure of the ring $K[V_0]$ in $K(V_0)$.

Let us compute the discriminant $\Delta \in K[X]$ of the polynomial f with respect to Y and using the algorithm from [8] decompose $\Delta = \lambda_0 \prod_{j\in J} \delta_j^{c_j}$ into irreducible over K factors with integers $c_j \geqslant 1$ and $\lambda_0 \in K$. Hence the number of elements $\#J = O(d^2)$.

Let us find an integer $\lambda = d^{O(1)}$ such that for every $j \in J$ the element $y + \lambda X$ is a primitive element of the extension of fields $K(V_0) \supset K(\delta_j)$. Replacing y by $y + cX$ we shall suppose in what follows without loss of generality that $c = 0$.

Let $j \in J$. Denote $d'_j = \deg_X \delta_j$. Denote for brevity $\delta = \delta_j$. For an arbitrary $K[\delta]$-module E denote by $E_{(\delta)}$ the localization of E with respect to the multiplicatively closed set $K[\delta] \setminus (\delta)$.

Now $K[V_1]_{(\delta)}$ is a free $K[\delta]_{(\delta)}$-module and $K[V_1]_{(\delta)}$ has a basis over $K[\delta]_{(\delta)}$ of the form

$$\omega_i^{(j)} = \Big(\sum_{0\leqslant i<\deg_Y f} \omega_{i,v}^{(j)} y^v \Big)/\Delta, \quad 0 \leqslant i < d'_j \deg_Y f, \tag{5}$$

where all $\omega_{i,v}^{(j)} \in K[X]$. Now $\omega_i^{(j)} \in K[V_1]$ for all i,j and, cf. the proof of Theorem 3 [2], we get immediately.

Lemma 5. *The family consisting of all the elements* $\omega_i^{(j)}$, $0 \leqslant i < d'_j \deg_Y f$, $j \in J$, *and* y^i, $0 \leqslant i < \deg_Y f$, *is a system of generators of the* $K[X]$*-module* $K[V_1]$. □

Denote by $\mathfrak{m}_g$, $g \in G_j$ the family of all the maximal ideals of the ring $K[V_1]_{(\delta)}$ (recall that $\delta = \delta_j$) such that $\mathfrak{m}_g \cap K[\delta]_{(\delta)} = (\delta)$. For every $g \in G_j$ there is an element $\pi_g \in \mathfrak{m}_g \cap K[V_1]$ such that $\pi_g \notin \mathfrak{m}_{g_1}$ for every $g \neq g_1 \in G_j$ and $\pi_g \notin \mathfrak{m}_g^2$. Then obviously the ideal $\mathfrak{m}_g = (\delta_j, \pi_g)$. One can represent

$$\pi_g = \Big(\sum_{0 \leqslant i < \deg_Y f} \pi_{g,v} y^v \Big) / \Delta, \tag{6}$$

where all $\pi_{g,v} \in K[\delta_j]$.

Finally let be given an element

$$\varphi = \left(\sum_{0 \leqslant i < \deg_Y f} \varphi_v y^v \right) / \Delta \in K[V_1].$$

Suppose that the estimations

$$\begin{aligned} \deg_{t_\gamma} \varphi_v &= d_2 (d_1 d)^{O(1)}, \quad 1 \leqslant \gamma \leqslant l, \\ \deg_{T_\beta} \varphi_v &= d_3 d^{O(1)}, \quad 1 \leqslant \beta \leqslant m, \\ \mathrm{l}(\varphi_v) &= (M_1 + M_2 + l + m)(d_2 + d_3)(d_1 d)^{O(1)}, \\ \deg_{T_1, \dots, T_m} \varphi_v &= d_4 d^{O(1)}. \end{aligned}$$

hold true.

Theorem 3. *Under previous conditions one can construct all the elements* $\omega_i^{(j)}$, π_g *and their representations* (5), (6) *within the time polynomial in* $(d_1 d_2 d)^{l+1}$, $(d_3 d)^m$, d, M_1, M_2. *One can decide within the same time whether* $\varphi \in \mathfrak{m}_g$ *for every* $g \in G_j$, $j \in J$. *Moreover, the following estimations for degrees and lengths of integer coefficients hold*

$$\begin{aligned} &\deg_{t_\gamma} \omega_{i,v}^{(j)} = d_2 (d_1 d)^{O(1)}, \quad 1 \leqslant \gamma \leqslant l, \\ &\deg_{T_\beta} \omega_{i,v}^{(j)} = d_3 d^{O(1)}, \quad 1 \leqslant \beta \leqslant m, \\ &\mathrm{l}(\omega_{i,v}^{(j)}) = (M_1 + M_2 + l + m)(d_2 + d_3)(d_1 d)^{O(1)}, \\ &\deg_{T_1, \dots, T_m} \omega_{i,v}^{(j)} = d_4 d^{O(1)}, \\ &\deg_{t_\gamma} \pi_{g,v} = d_2 (d_1 d)^{O(1)}, \quad 1 \leqslant \gamma \leqslant l, \end{aligned}$$

$$
\begin{aligned}
&\deg_{T_\beta} \pi_{g,v} = d_3 d^{O(1)}, \quad 1 \leqslant \beta \leqslant m,\\
&\mathrm{l}(\pi_{g,v}) = (M_1 + M_2 + l + m)(d_2 + d_3)(d_1 d)^{O(1)},\\
&\deg_{T_1,\dots,T_m} \pi_{g,v} = d_4 d^{O(1)}.
\end{aligned}
$$

for all $0 \leqslant i, v < dd'_j$, $g \in G_j$, $j \in J$ *with absolute constants in* $O(1)$.

Proof. We shall enumerate $j \in J$ and for every j perform the following construction. Let us fix $j \in J$, as previously denote $\delta = \delta_j$, $d' = d'_j = \deg_X \delta_j$, $c = c_j$ and for convenience of notation denote by $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ the ideals from the family $\mathfrak{m}_g$, $g \in G_j$ (hence now the number of elements $\#G_j = r$). Set $\mathcal{O}_i = (K[V_1]_{(\delta)} \setminus \mathfrak{m}_i)^{-1} K[V_1]_{(\delta)}$ to be the localization of the ring $K[V_1]_{(\delta)}$ with respect to the maximal ideal $\mathfrak{m}_i$. Let $\widehat{\mathcal{O}}_i$ be the completion of the local ring $\mathcal{O}_i$ with respect to $\mathfrak{m}_i\mathcal{O}_i$-adic topology. Denote by $\widehat{K}_i$ the field of rational functions of the ring $\widehat{\mathcal{O}}_i$.

We have $K(X)[Y] \supset k(\delta)[Y]$. Let $\mathcal{N} : K(X)[Y] \to k(\delta)[Y]$ be the mapping of the norm (the field $K(X) = K(X)[Z]/(\delta(X) - Z) \supset K(Z) \simeq K(\delta)$, $Z \mapsto \delta$ under the last isomorphism, and hence one can compute this norm). Denote $\widetilde{f} = \mathcal{N}(f) \in K[\delta, Y]$. The polynomial $\widetilde{f}$ is irreducible over K since y is a primitive element of the extension $K(V_0) \supset K(\delta)$ and the degree of this extension is $d'_j \deg_Y f = \deg_Y \widetilde{f}$. Besides that, we have the isomorphisms of fields

$$
K(V_1) \simeq K(Z)[X,Y]/(\delta(X){-}Z, f) \simeq K(Z)[Y]/(\widetilde{f}(Z,Y)) \simeq K(\delta)[Y]/(\widetilde{f}), \tag{7}
$$

where the isomorphism in the middle takes place since f divides $\widetilde{f}(Z,Y)$ and the degrees of the both algebras over the field $K(Z)$ coincide.

Using Theorem 2 we get the decomposition $\widetilde{f} = \prod\limits_{1 \leqslant i \leqslant r} \widetilde{f}_i$ into the irreducible over $K((\delta))$ factors. The polynomials $\widetilde{f}_i$ are in the one–to–one correspondence with the maximal ideals $\mathfrak{m}_i$, $1 \leqslant i \leqslant r$. More precisely, we have the commutative diagram

$$
\begin{tikzcd}
K[V_1]_{(\delta)} \arrow[r, phantom, "="] \arrow[d, phantom, "\cap"] & K[V_1]_{(\delta)} \arrow[r, phantom, "\supset"] \arrow[d, phantom, "\cap"] & K[\delta]_{(\delta)} \arrow[d, phantom, "\cap"] \\
K[V_1] \otimes_{K[\delta]} K[[\delta]] \arrow[r, phantom, "\simeq"] \arrow[d, phantom, "\cap"] & \prod_{1 \leqslant i \leqslant r} \widehat{\mathcal{O}}_i \arrow[r, phantom, "\supset"] \arrow[d, phantom, "\cap"] & K[[\delta]] \arrow[d, phantom, "\cap"] \\
K(V_1) \otimes_{K(\delta)} K((\delta)) \arrow[r, "q"] & \prod\limits_{1 \leqslant i \leqslant r} K((\delta))[Y]/(\widetilde{f}_i(Y)) \arrow[r, phantom, "\supset"] & K((\delta)).
\end{tikzcd}
\tag{8}
$$

By (7) and the Chinese remainder theorem the construction of the N-th approximation of the isomorphism q^{-1} from the low row of diagram (8) is reduced to finding polynomials $A_\alpha, B_\alpha \in K(\delta)$, $1 \leqslant \alpha \leqslant r$, such that

$$A_\alpha \prod_{i\neq\alpha} \widetilde{f}_i + B_\alpha \widetilde{f}_\alpha = 1 \bmod \delta^N \tag{9}$$

Actually $A_\alpha, B_\alpha \in (1/\delta^c)K[\delta]$, $1 \leqslant \lambda \leqslant r$. The polynomials $\widetilde{f}_i \in K[[\delta]][Y]$ for all i since $\widetilde{f} \in K[\delta, Y]$ and $\mathrm{lc}_Y\, \widetilde{f} = 1$. Denote $A'_\alpha = \delta^c A_\alpha$, $B'_\alpha = \delta^c B_\alpha$. Then (9) is equal to

$$A'_\alpha \prod_{i\neq\alpha} \widetilde{f}_{i,\#}(N+c-1) + B'_\alpha \widetilde{f}_{\alpha,\#}(N+c-1) = \delta^c \bmod \delta^{N+c}$$

(here and below we replace X, see Section 2, by δ in the definition of the approximation $a_\#(N')$, $N' \in \mathbb{R}$, of a polynomial a with coefficients from $\overline{K}((\delta)))$. Hence one can find A'_α, B'_α solving a linear system of the size $(Nd)^{O(1)}$ over the field K.

Denote for brevity $\nu = \deg_Y \widetilde{f}_i$. Denote

$$y_i = Y \bmod \widetilde{f}_i \in K((\delta))[Y]/(\widetilde{f}_i(Y)).$$

Let

$$\mathcal{N}_i \,:\, K((\delta))[Y]/(\widetilde{f}_i(Y))[Z] \to K((\delta))[Z]$$

be the mapping of the norm.

Let us show how to construct a uniformizing element $\widetilde{\pi}_i \in K(\delta)[y_i]$ of the ring $\widehat{\mathcal{O}}_i$ for every $1 \leqslant i \leqslant r$. For every element $0 \neq z \in \widehat{K}_i$ the order $\mathrm{ord}_\delta\, z$ is defined. Namely, the uniformizing element has the least possible positive order $1/e_i$ where the integer $e_i \geqslant 1$, and $\mathrm{ord}_\delta\, z = \mu/e_i$ if and only if $z^{e_i}/\delta^\mu \in \widehat{\mathcal{O}}_i \setminus \mathfrak{m}_i\widehat{\mathcal{O}}_i$.

Let $\Phi \in \widehat{K}_i[Z]$ be the minimal polynomial of the element z over the complete field $\widehat{K}_i$ with $\mathrm{lc}_Z\, \Phi = 1$. It is known that the orders of all the roots of Φ coincide. Hence if $z \neq 0$ then the Newton broken line of the polynomial Φ has only one edge.

Lemma 6. *Assume that a polynomial $Q \in K(\delta)[Y]$ is given such that $z = Q(y_i, \delta)$ and the bound is known: $\mathrm{ord}_\delta\, z = d^{O(1)}$. Then the following assertions hold.*

(i) *One can compute the order* $\operatorname{ord}_\delta(z)$ *within the time polynomial in* $(d_1d_2d)^{l+1}$, $(d_3d)^m$, d, M_1, M_2 *and the size* $\mathrm{L}(Q)$ *(of the polynomial* Q*). In particular, one can decide whether* $\operatorname{ord}_\delta z \geqslant 0$ *or which is the same whether* $z \in \mathcal{O}_i$.

(ii) *If* $\operatorname{ord}_\delta z = 0$ *then within the same time one can find the minimal polynomial* $H \in K[Z]$ *of the element* $\overline{z} = z \bmod \mathcal{O}_i\mathfrak{m}_i \in \mathcal{O}_i/\mathfrak{m}_i\mathcal{O}_i$ *over the field* K.

(iii) *Let us represent* $z^{-1} = \sum\limits_{0\leqslant j<\nu-1} a_j y_i^j$ *where all* $a_j \in K((\delta))$. *Then for every integer* $N \geqslant 0$ *one can compute the* $a_{j\,\#}(N)$ *within the time polynomial in* $(d_1d_2d)^{l+1}$, $(d_3d)^m$, d, M_1, M_2 *and the size* $\mathrm{L}(Q)$ *and* N^{l+m+1}.

Proof. (i). It is sufficient to compute the coefficient of the slope of the Newton broken line of the minimal polynomial $\Phi \in K((\delta))[Z]$ of the element z over the field $K((\delta))$. We have $\Psi = \mathcal{N}_i(Z - z) = \Phi^a$ for an integer $a \geqslant 1$. Hence it is sufficient to compute $\Psi_\#(N)$ for $N = d^{O(1)}$. The polynomial $\Psi_\#(N)$ is calculated as an approximation of the determinant of the matrix of the $K((\delta))$-linear mapping. It can be done within the required time (we leave the details to the reader).

(ii). Suppose that $\operatorname{ord}_Z \delta = 0$. Then $\Psi(0, Z) = H^a$ for a separable polynomial $H \in K[Z]$ and an integer $a \geqslant 1$. Now the minimal polynomial of the element $\overline{z}$ over the field K is H. Thus, we can compute this minimal polynomial.

(iii) Let $\Psi = Z^\nu + \sum\limits_{0\leqslant i<\nu-1} \Psi_i Z^i$ where all $\Psi_i \in K((\delta))$. We have $z^{-1} = -(z^{\nu-1} + \sum_{0<i<\nu-1} \Psi_i z^{i-1})/\Psi_0$ and $\operatorname{ord}_\delta \Psi_0 = d^{O(1)}$, see the proof of (i). By the proof of (i) we can construct the approximations of all the coefficients Ψ_i. This implies (iii). □

Remark 2. Assume that we don't now in advance the estimate $\operatorname{ord}_\delta z = d^{O(1)}$. Then within the time from the statement of assertion (i) constructing Ψ from the proof of assertion (i) one can decide simultaneously whether $\operatorname{ord}_\delta z = d^{O(1)}$ and stop the computation if $\operatorname{ord}_\delta z = d^{O(1)}$ is not true (with a fixed constant in $O(1)$).

For every $1 \leqslant s < \nu$ put $z_s = (\partial^s \widetilde{f}_i/\partial Y^s)_\#(c/2)(y_i, \delta)$ if

$$\operatorname{ord}_\delta(\partial^s \widetilde{f}_i/\partial Y^s)(y_i, \delta) \leqslant c/2 \tag{10}$$

(recall that $c = c_j$ for $\delta = \delta_j$) and $z_s = 1$ if (10) is not true. We introduce condition (10) since we are interested principally in the partial derivatives corresponding to the points $(-s+\nu, \varepsilon_s)$ which belong to the Newton broken line with respect to (Y, δ) of the polynomial $\widetilde{f}_i(Y+y_i, \delta) \in \widehat{K}_i[Y, \delta]$ (but some other points may also satisfy this condition). Notice that $\mathrm{ord}_\delta(\partial \widetilde{f}_i/\partial Y)(y_i, \delta) \leqslant c/2$.

For all $1 \leqslant s < \nu$ let us compute using Lemma 6 (i) the orders ε_s of all the elements z_s.

Lemma 7. *The least common denominator of all ε_s, $1 \leqslant s \leqslant \nu-1$, is e_i.*

Proof. Let $a = \sum_{j \geqslant j_0} a_j \delta^{j/e_i} \in \overline{K((\delta))}$, $a_j \in \overline{K}$, be a root of the polynomial $\widetilde{f}_i$ and $\zeta^{e_i} = 1$, $\zeta \in \overline{K}$. Then $a' = \sum_{j \geqslant j_0} a_j \zeta^j \delta^{j/e_i} \in \overline{K((\delta))}$ is also the root of $\widetilde{f}_i$. From here the required assertion follows by Lemma 2.1 [2], see Lemma 9 from the Appendix, using the characteristic pairs or directly. Applying Lemma 2.1 note that at present δ plays the role of X. Further, this lemma can be applied to polynomials from $K[[\delta]][Y]$ separable with respect to Y in place of separable polynomials from $K[\delta, Y]$; the proof is without changes (it is sufficient to replace f from the formulation of the Lemma 2.1 by its appropriate approximation from the ring $K[\delta, Y]$). We leave the details to the reader. □

Let us find integers $1 \leqslant \mu_s, \mu \leqslant d^{O(1)}$ such that $\sum_{1 \leqslant s < \nu} \mu_s \varepsilon_s - \mu = 1/e_i$ and $\mu_s = 0$ whenever $z_s = 1$. Put $\widetilde{\pi}_i = (\prod_{1 \leqslant s < \nu} z_s^{\mu_s})/\delta^\mu$. Now $\widetilde{\pi}_i$ is a uniformizing element in the field $\widehat{K}_i$.

Put $u_s = z_s/\widetilde{\pi}_i^{e_i \varepsilon_s}$, $1 \leqslant s < \nu$, and $u_0 = \widetilde{\pi}_i^{e_i}/\delta$ and $\overline{u}_s = u_s \bmod \mathfrak{m}_i \in \mathcal{O}_i/\mathcal{O}_i\mathfrak{m}_i$, $0 \leqslant s < \nu$.

Lemma 8. *The field $K[\overline{u}_0, \dots, \overline{u}_{\nu-1}]$ coincides the residue field $\mathcal{O}_i/\mathfrak{m}_i\mathcal{O}_i$.*

Proof. Let $\widetilde{u}_s$ be the elements of the maximal unramified extension K' of the field $K((\delta))$ contained in $\widehat{K}_i$ such that $\widetilde{u}_s = u_s \bmod \widetilde{\pi}_i$ for all s.

Put $K'' = K((\delta))[\widetilde{u}_0, \dots, \widetilde{u}_{\nu-1}] \subset K'$. Let us show that there are at most e_i distinct K''-embeddings $\sigma : \widehat{K}_i \to \overline{K((\delta))}$. Indeed, suppose contrary. Let us choose such an embedding σ_0 and identify $\sigma_0(\widetilde{\pi}_i) = \widetilde{\pi}_i$.

Since $\sigma(\widetilde{u}_0) = \widetilde{u}_0$ we have $\sigma(\widetilde{\pi}_i) = \zeta\widetilde{\pi}_i \bmod \delta^{2/e_i}$ where $\zeta^{e_i} = 1$, and hence $\sigma(\widetilde{u}_s \pi^{e_i\varepsilon_i}) = \zeta^{e_i\varepsilon_i}\pi^{e_i\varepsilon_i}\widetilde{u}_s \bmod \delta^{\varepsilon_i+1/e_i}$, $1 \leqslant s < \nu$.

Therefore, there are two embeddings $\sigma_1 \neq \sigma_2$ such that the corresponding ζ is the same. Then we have $\sigma_1(z_s) = \sigma_2(z_s) \bmod \delta^{\varepsilon_i+1/e_i}$ for all $1 \leqslant s < \nu$. Thus, the partial derivatives (corresponding to the points $(-s+\nu, \varepsilon_s)$ which belong to the Newton broken line with respect to (Y, δ)

of the polynomial $\widetilde{f}_i(Y+y_i,\delta) \in \widehat{K}_i[Y,\delta]$) do not separate the roots $\sigma_1(y_i)$ and $\sigma_2(y_i)$ of the polynomial $\widetilde{f}_i$. This contradicts to Lemma 2.1 [2]. Thus, $K'' = K'$ and hence $K[\overline{u}_0,\dots,\overline{u}_{\nu-1}] = \mathcal{O}_i/\mathfrak{m}_i\mathcal{O}_i$. □

Using Lemma 6 (iii) and (ii) one can construct an element $\widetilde{\eta}_i$ such that $\widetilde{\eta}_i \bmod \mathcal{O}_i\mathfrak{m}_i$ is a primitive element of the extension $\mathcal{O}_i/\mathcal{O}_i\mathfrak{m}_i \supset K$. Namely, using Lemma 6 (iii) we find approximations u_i' of the elements u_i such that u_i' are represented in the form from the statement of Lemma 6, i.e., similarly to z, and $u_i' = u_i \bmod \mathcal{O}_i\mathfrak{m}_i$ (we leave the details to the reader). Further, applying Lemma 6 (ii) we choose $\widetilde{\eta}_i = u_0' + \sum_{1\leqslant a\leqslant \nu-1} \lambda_a u_s'$ where $0 \leqslant \lambda_a \leqslant \nu$ and for every $1 \leqslant s \leqslant \nu-1$ the degree of the minimal polynomial over K of the element $\widetilde{\eta}_{i,s} = (u_0' + \sum_{1\leqslant a\leqslant s} \lambda_a u_a') \bmod \mathcal{O}_i\mathfrak{m}_i$ is maximal possible (we construct subsequently $\widetilde{\eta}_{i,1}, \widetilde{\eta}_{i,2}, \dots, \widetilde{\eta}_{i,\nu-1} = \widetilde{\eta}_i$).

Now the elements

$$(0,\dots,0,\widetilde{\pi}_i^{m_1}\widetilde{\eta}_i^{m_2},0,\dots,0) \in \prod_{1\leqslant i\leqslant r} K((\delta))[Y]/(\widetilde{f}_i) = \Lambda, \qquad (11)$$

$0 \leqslant m_1 < e_i$, $0 \leqslant m_2 < (\deg_Y \widetilde{f}_i)/e_i$, $1 \leqslant i \leqslant r$, (here the nonzero entry is at the place number i) form a basis of the ring $\prod_{1\leqslant i\leqslant r} \widehat{\mathcal{O}}_i$ (as a free module) over $K[[\delta]]$. Denote elements (11) by $\widetilde{\omega}_w$, $0 \leqslant w < \deg_Y \widetilde{f}$ (recall that at present $d' = d_j'$, and $d' \deg_Y f = \deg_Y \widetilde{f}$).

Let $\widetilde{\omega}_w = \sum_{0\leqslant v<\deg_Y \widetilde{f}} \widetilde{\omega}_{w,v} y^v$ where all $\widetilde{\omega}_{w,v} \in K((\delta))$. Using Lemma 6 (iii) and isomorphisms (7) and q^{-1} from (8) we compute the approximations

$$\omega_w = \sum_{0\leqslant v<\deg_Y \widetilde{f}} \widetilde{\omega}_{w,v\,\#}(c) y^v, \quad 0 \leqslant w < \deg_Y \widetilde{f}.$$

As it is known (this follows, e.g., from the Nakayama lemma) the family ω_w, $0 \leqslant w < \deg_Y \widetilde{f}$, is also a basis of the ring $\prod_{1\leqslant i\leqslant r} \widehat{\mathcal{O}}_i$ as a free module over $K[[\delta]]$ and simultaneously it is a basis of the semilocal ring $K[V_1]_{(\delta)}$ as a free module over $K[\delta]_{(\delta)}$.

Now for every $1 \leqslant i \leqslant r$ we are going to construct an element $\pi_i \in \mathfrak{m}_i$ which is a uniformizing element of $\mathfrak{m}_i$ but $\pi_i \notin \mathfrak{m}_{i_1}$ for every $1 \leqslant i_1 \neq i \leqslant r$. We find the element π_i as a sum of some ω_v. This sum is an approximation of the element $(1,\dots,1,\widetilde{\pi}_i,1,\dots,1)\in\prod_{1\leqslant i\leqslant r}\widehat{\mathcal{O}}_i\subset\Lambda$, see (11). Recall that i corresponds to $g\in G_j$. Set $\pi_g=\lambda\pi_i$ where $0\neq\lambda\in K[X]$ is chosen of the minimal possible degree such that (6) holds and $\mathrm{lc}_X\,\lambda=1$. The elements π_g, $g\in G_j$, are constructed.

It remains to show how to decide whether $\varphi\in\mathfrak{m}_i$. We apply Lemma 6 (iii) to the element $\widetilde{\pi}_i$ and find an approximation of the element $\varphi/\widetilde{\pi}_i\in K(\delta)[y_i]$. Finally applying Lemma 6 (i) (and if necessary Remark 2) we decide whether $\mathrm{ord}_\delta(\varphi/\widetilde{\pi}_i)>0$ in the field $\widehat{K}_i$, i.e., $\varphi\in\mathfrak{m}_i$.

The estimations for the working time, degrees and lengths of integer coefficients follow immediately from the described construction and Theorem 2 from Section 2. The theorem is proved. □

Appendix: The statement of Lemma 2.1 from [2]

Here we formulate a version of Lemma 2.1 from [1] and [2]. We slightly changed the notation and give the statement for a separable polynomial f in place of an irreducible polynomial f, but the proof is without changes.

Let k be a field of zero-characteristic and $\Omega=\overline{k((X))}=\bigcup_{\nu\geqslant1}\overline{k}((X^{1/\nu}))$ be the field of fractional-power series over an algebraically closed field $\overline{k}$.

Lemma 9. *Let $f\in k[X,Y]$ be a separable polynomial with the leading coefficient $\mathrm{lc}_Y\,f=1$. Denote by $\Delta\in k[X]$ the discriminant of the polynomial f with respect to Y. Let $y_i,y_j\in\Omega$ be two distinct roots of f considered as a polynomial from $k(X)[Y]$. Then there is an integer $1\leqslant\gamma<\deg_Y f$ and the elements $\xi_i,\xi_j\in\overline{k}$ and the number $\mu(i,j)\in\mathbb{Q}$ such that $\xi_i\neq\xi_j$ and $\mathrm{ord}_X((\partial^\gamma f/\partial Y^\gamma)(X,y_s)-\xi_s X^{\mu(i,j)})>\mu(i,j)$ for $s=i,j$. Besides that, $0\leqslant\mu(i,j)\leqslant\mathrm{ord}_X(\Delta)/2$ and $\mu(i,j)=\mu_1(i,j)/\nu(i)$ where $\mu_1(i,j)$, $\nu(i)$ are integers, $1\leqslant\nu(i)\leqslant\deg_Y f$, and $\nu(i)$ depends only on the root y_i.* □

References

1. A. L. Chistov, *Polynomial complexity of the Newton–Puiseux algorithm.* — in: Lecture Notes in Computer Science, Vol. 233, Springer, 1986, p. 247–255.
2. A. L. Chistov, *Polynomial-time algorithms for computational problems in the theory of algebraic curves.* — Zap. nauchn. semin. POMI **176** (1989), 127–150.
3. A. L. Chistov, *An overview of effective normalization of a nonsingular in codimension one projective algebraic variety.* — Zap. nauchn. semin. POMI **373** (2009), 295–317.

4. A. L. Chistov, *Polynomial-time factoring polynomials over local fields.* — Zap. nuchn. semin. (POMI) **192** (1991), 112–148.
5. A. L. Chistov, *The complexity of constructing the ring of integers of a global field.* — Dokl. Akad. Nauk SSSR **306** (1989), 1063–1067.
6. A. L. Chistov, *A deterministic polynomial–time algorithm for the first Bertini theorem.* — Preprint of St.Petersburg Mathematical Society (2004), http://www.MathSoc.spb.ru.
7. A. L. Chistov, *Effective Construction of a Nonsingular in Codimension One Algebraic Variety.* in: Polynomial Computer Algebra 2010, Theses of Talks, 15–18.
8. A. L. Chistov, *Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time.* — Zap. nauchn. semin. (POMI) **137** (1984), 124–188.

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

Поступило 2010 г.