Estimates for roots of a polynomial in the field of multiple formal fractional 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 estimating and constructing the roots of a polynomial in the field multiple fractional power series in zero characteristic.

More precisely,let k be a ground field of zero–characteristic with algebraic closure $\overline{k}$. We assume that $k = \mathbb{Q}(T_1, \dots, T_l)[\theta]$ is finitely generated over the field of rational numbers $\mathbb{Q}$. Here the elements $T_1, \dots, T_l$ are algebraically independent over $\mathbb{Q}$ and the element θ is algebraic over $T_1, \dots, T_l$, the minimal polynomial for θ over $\mathbb{Q}(T_1, \dots, T_l)$ is given.

Let $f \in k[X_1, \dots, X_n, Z]$ be a polynomial of degree $\deg_{Z, X_1, \dots, X_n} \leqslant d$ for an integer $d \geqslant 2$. Consider $f \in k(X_1, \dots, X_n)[Z]$ as a polynomial in one variable Z with coefficients in $k(X_1, \dots, X_n)$. We assume that the degree $\deg_Z f \geqslant 1$. Then the roots $Z = z_\alpha$ 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 fractional power series:

$$\bigcup_{\nu_1, \dots, \nu_n \geqslant 1} \overline{k}((X_1^{1/\nu_1}))((X_2^{1/\nu_2})) \dots ((X_n^{1/\nu_2})). \quad (1)$$

This field is algebraically closed.

The aim of this talk is to attract the atention to the problem of estimating and constructing the roots z_α in the field (1). Of course one needs to estimate the sizes of coefficients from $\overline{k}$ of z_α in the field (1).

Example. Let $f = Z^2 - 2X_1X_2 - X_2^2 - X_3^2$. Then one of the roots of f

$$z_\alpha = \sqrt{2}X_1^{1/2}X_2^{1/2}(1 + X_2/(2X_1) + X_3^2/(2X_1X_2))^{1/2} \in \mathbb{Q}[\sqrt{2}][[X_1^{1/2}, X_2^{1/2}/X_1^{1/2}, X_3/(X_1^{1/2}X_2^{1/2})]].$$

So in the general case one needs to construct the similar representation for z_α (and estimate all its parameters), i.e., to construct the field k_α which is a finite extension of k and represent z_α as a formal power series with coefficients from k_α in the quotients of fractional power monomials in $X_1, \ldots, X_n$.

This problem is solved for $n = 1$ in

[1] **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.

To our knowledge for the case case $n > 1$ no estimates have been obtained so far.

Let us proceed to details. The problem for an arbitrary n is reduced to the case $\nu_1 = \ldots = \nu_n = 1$. Indeed, if $\nu_1, \ldots, \nu_n$ are the least possible in the representation of z_α then there are at least $\nu = \mathrm{LCM}\{\nu_1, \ldots, \nu_n\}$ pairwise distinct roots z_α of the polynomial f. Hence $\nu \leqslant d$ and one can replace the initial polynomial f by the new one $f(X_1^\nu, \ldots, X_n^\nu, Z)$. For this new polynomial f the corresponding root $z_\alpha \in \overline{k}((X_1))((X_2))\ldots((X_n))$. So now we get $\nu_1 = \ldots = \nu_n = 1$ and the degree of this new polynomial f if bounded by d^2.

Further, for all $1 \leqslant j \leqslant n$ put $X'_j = X_j/(X_1^{\mu_{j,1}} \cdot \ldots \cdot X_{j-1}^{\mu_{j,j-1}})$ for some integers $\mu_{j,i} \geqslant 0$ (so $X'_1 = X_1$). Then one can choose integers $\mu_{j,i}$ such that

$$z_\alpha \in \overline{k}[[X'_1, \ldots, X'_n]], \tag{2}$$

i.e., z_α are formal power series in $X'_1, \ldots, X'_n$ with coefficients from $\overline{k}$. This follows from the construction described in the cited paper [1] applied recursively.

If $\mu_{j,i}$ are known then one can construct the polynomial $\tilde{f}$ such that $\tilde{f}(X'_1, \ldots, X'_n, Z) = f$. Assume that we have some upper bounds for integers $\mu_{j,i}$. Then upper bounds for the coefficients of formal power series in (2) can be obtained applying the results of [2], [3] to the polynomial $\tilde{f}$.

[2] **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)

[3] **Chistov A. L.:** *“An algorithm for factoring polynomials in the ring of multivariable formal power series in zero–characteristic. II”*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 529 (2023), p. 261–290 (in Russian).

Last year on the conference PCA’2023 I told about the results of [2]. In [3] they are strengthened: in brief, the complexity of the algorithms from [2] is polynomial in $d^{2^{n^c}}$ for a constant $c > 0$ and in [3] it is polynomial in d^n (of course, the complexity depends also on other parameters).

Now it remains to estimate the least possible $\mu_{j,i}$. This can be done applying the results of [1] or [3] recursively. The direct application of [1] or [3] gives double–exponential in n upper bounds for $\mu_{j,i}$. But we hope to improve the estimates from [3] and obtain upper bounds for $\mu_{j,i}$ which are subexponential in the number of coefficients of the polynomial f, i.e., upper bounds polynomial in $d^{n^{O(1)}}$.

Let us outline how it can be done (still one need check the details). First of all we assume that the degree $\deg_{X_1,\ldots,X_n} f \leqslant D$ for an integer $D \geqslant d$ (this assumption is convenient for the recursion in our construction). Then we are going to prove applying the result of [1] recursively (and with some improvements and modifications) that for all j, i the integers $\mu_{j,i} \leqslant Dd^{(n+1-j)c}$ for an absolute constant $c > 0$.

Now we can describe one step of the recursion.

We can suppose without loss of generality that the polynomial f is separable and the leading coefficient $\mathrm{lc}_Z f = 1$. Put the separable algebra $\Lambda = k(X_1, \dots, X_n)[Z]/(f)$ and $z = Z \bmod f \in \Lambda$. Modifying the construction from [1] with partial derivatives $\partial^\gamma f/\partial Z^\gamma$ one can find an element $q \in k[X_1, \dots, X_n, Z]$ satisfying the following properties. Denote by $\Phi \in k(X_1, \dots, X_n)[Q]$ (Q is a variable) the minimal polynomial of the element $q(z)$ over $k(X_1, \dots, X_n)$. Then $\deg_Q \Phi = \deg_Z f$, $\mathrm{lc}_Z \Phi = 1$, for every root z_β of f the order $\mathrm{ord}_{X_n} q(z_\beta) \geqslant 0$, $\mathrm{ord}_{X_n} q(z_\alpha) = 0$ and $\eta = q(z_\alpha|_{X_n=0}) \in k(X_1, \dots, X_{n-1})$ is a root of the polynomial $\Phi(X_1, \dots, X_{n-1}, 0, Q)$ of multiplicity 1. Denote by Ψ the minimal polynomial of the element η. So Ψ divides Φ.

Using the Hensel lemma one can represent

$$q(z_\alpha) = \eta + \sum_{v\geqslant 1,\, 0\leqslant v<\deg_Q \Psi} q_{v,w}\eta^v X_n^w/\delta^{2w-1} \tag{3}$$

where all $q_{v,w}, \delta \in k[X_1, \dots, X_{n-1}]$.

Further one can represent in the algebra Λ

$$z = 1/a \sum_{0\leqslant v<\deg_Q \Phi} z_v q^v \tag{4}$$

where all $a, z_v \in k[X_1, \dots, X_{n-1}]$.

Note that the degrees with respect to $X_1, \ldots, X_n$ of the elements $q, \Phi, \Psi, \delta, a, q_v$ are bounded from above by Dd^c for a constant $c > 0$ (one needs to check it).

On the other hand, one can represent $z_\alpha = z_{\alpha,0} + \sum_{w \geqslant 1} z_{\alpha,w} X_n^w$ where all $z_{\alpha,0}, z_{\alpha,w} \in \overline{k}((X_1))((X_2)) \ldots ((X_{n-1}))$.

Now $\mu_{j,i}$ corresponding to $z_{\alpha,0}$ and η (in place of z_α and with $n-1$ in place of n) can be estimated recursively. Finally using (3) and (4) one can estimate $\mu_{j,i}$ corresponding to $\sum_{w \geqslant 1} z_{\alpha,w} X_n^w$ and hence to z_α.

Notice that there is a minor inacuracy in the statement of Lemma 2.1 of [1]. One of the assertions of this lemma is that $\mu(i,j) = \mu_1(i,j)/\nu(i)$ for some integers $\mu_1(i,j)$ and $\nu(i)$, where $\nu(i)$ depends only on i. But recently we have found that in the general case it is true only if $\xi_i \neq 0$ (in the notation from this lemma).

This inacuracy is not essential for the main result of [1] and its proof. Only small modifications in the definitions of the elements $Q_{i,j}$ and q in Lemma 2.2 [1] are required (we are going to give the details in the next paper).

References

[1] **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.

[2] **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)

[3] **Chistov A. L.:** *"An algorithm for factoring polynomials in the ring of multivariable formal power series in zero–characteristic. II"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 529 (2023), p. 261–290 (in Russian).