Записки научных
семинаров ПОМИ
Том 390, 2011 г.

A. L. Chistov

AN IMPROVEMENT OF THE COMPLEXITY BOUND FOR SOLVING SYSTEMS OF POLYNOMIAL EQUATIONS

Abstract. In 1984 the author suggested an algorithm for solving systems of polynomial equations. At present we modify it and improve bounds for its complexity, degrees and lengths of coefficients from the ground field of the elements constructed by this algorithm.

§1. Statement of the theorem

Let F be a field finitely generated over the field H, where $H = \mathbb{Q}$ or the finite field $\mathbb{F}_{q^\kappa}$ of q^κ elements for a prime number q. If the characteristic $\mathrm{char}(F) > 0$ then $q = \mathrm{char}(F)$, if $\mathrm{char}(F) = 0$ put $q = 1$. Suppose that the field $F = H(T_1, \dots, T_l)[\eta]$, the element $T_1, \dots, T_l$ are algebraically independent over H and the element η is algebraic separable over the field $H(T_1, \dots, T_l)$, the minimal polynomial $\varphi \in H(T_1, \dots, T_l)[Z]$ of the element η over the field $H(T_1, \dots, T_l)$ is given. The degree $\deg_{T_1,\dots,T_l,Z} < d_1$, and the maximum of lengths of coefficients from H of the polynomial φ is bounded from above by M_1, see below the exact definitions. Let $f_0, \dots, f_{k-1} \in F[X_0, \dots, X_n]$ be linearly independent over F homogeneous polynomials with $\deg_{X_0,\dots,X_n} f_i < d$, $\deg_{T_1,\dots,T_l} f_i < d_2$ and the maximum of lengths of coefficients from H of the polynomials f_i is bounded from above by M_2 for all $0 \leqslant i \leqslant k-1$, see below.

In [1] an algorithm is suggested for solving the system $f_0 = \ldots = f_{k-1} = 0$ in $\mathbb{P}^n(\overline{F})$. In the general case the complexity of this algorithm is polynomial in $(d^n d_1 d_2)^{n+l}$, M_1, M_2, k, and q. Till the present time this algorithm has had the best known complexity bound in the general case. But now we discovered that this bound can be improved. Namely one can obtain the analogous algorithm with the complexity polynomial in d^{n^2}, $(d^n d_1 d_2)^{l+1}$, M_1, M_2, k, and q. This estimate does not depend on $(d_1 d_2)^n$ and it is more natural and understandable since there are only

Key words and phrases: polynomial systems, efficient algorithm, algebraic varieties, irreducible components.

l transcendental elements $T_1, \dots, T_l$. Similar improvements are obtained for degrees and lengths of coefficients from the ground field of all the elements constructed by this algorithm. More precise bounds are given in the formulation of Theorem 1. It is of importance. We use this algorithm in many papers. The algorithm itself remains almost without changes. To achieve our goal it is sufficient only to introduce two steps factoring over finitely generated fields arising in the computation. We discuss it below.

Now we proceed to exact statements. We represent the polynomial $\varphi = \sum_{0\leqslant i\leqslant \deg_Z \varphi} \varphi_i^{(1)}/\varphi^{(2)} Z^i$ where all $\varphi_i^{(1)}, \varphi^{(2)} \in \widetilde{H}[T_1, \dots, T_l]$, $\widetilde{H} = \mathbb{Z}$ if the characteristic $\mathrm{char}(F) = 0$, $\widetilde{H} = H$ if $\mathrm{char}(F) = q > 0$ and $\mathrm{GCD}_i\{\varphi_i^{(1)}, \varphi^{(2)}\} = 1$ in $\widetilde{H}[T_1, \dots, T_l]$. Each element $f \in F[X_0, \dots, X_n]$ is represented in the form

$$f = \frac{1}{b} \sum_{0\leqslant i\leqslant \deg_Z \varphi, i_0, \dots, i_n} a_{i,i_0,\dots,i_n} \eta^i X_0^{i_0} \cdot \ldots \cdot X_n^{i_n},$$

where all $a_{i,i_0,\dots,i_n}, b \in \widetilde{H}[T_1, \dots, T_l]$, $\mathrm{GCD}_{i,i_0,\dots,i_n}\{a_{i,i_0,\dots,i_n}, b\} = 1$ in the last ring. Put

$$\deg_{T_1,\dots,T_l} f = \max\{\deg_{T_1,\dots,T_l} a_{i,i_0,\dots,i_n}, \deg_{T_1,\dots,T_l} b\}. \tag{1}$$

The length $\mathrm{l}(h)$ of an element $h \in \mathbb{Z}$ is its bitwise length. The length $\mathrm{l}(h)$ of an element $h \in \mathbb{F}_{q^\kappa}$ is $\kappa \log_2 q$. Denote by $\mathrm{l}(f)$ the maximum of lengths of coefficients from H (actually from $\widetilde{H}$) at the monomials in $T_1, \dots, T_l$ of the polynomials $a_{i,i_0,\dots,i_n}, b$. In the similar way the degree $\deg_{T_1,\dots,T_l,Z} \varphi$ and the length of coefficients $\mathrm{l}(\varphi)$ are defined. We shall suppose that for all $0 \leqslant i \leqslant k-1$

$$\deg_{T_1,\dots,T_l,Z} \varphi < d_1, \quad \deg_{T_1,\dots,T_l} f_i < d_2, \quad \deg_{X_0,\dots,X_n} f_i < d,$$
$$\mathrm{l}(\varphi) \leqslant M_1, \quad \mathrm{l}(f_i) \leqslant M_2$$

for some integers d, d_1, d_2. By definition put the sizes $\mathrm{L}_2(f_i) = \binom{d+n}{n} d_1 d_2^l M_2$, $\mathrm{L}_2(\varphi) = d_1^{l+1} M_1$ (here $\mathrm{L}_2(\dots)$ is the notation from [1]; $\mathrm{L}_1(\dots)$ is used in [1] but not in this paper).

The projective algebraic variety $\mathcal{Z}(f_0, \dots, f_{k-1}) \subset \mathbb{P}^n(\overline{F})$ of the roots of the system $f_0 = \ldots = f_{k-1} = 0$ is decomposed $\mathcal{Z}(f_0, \dots, f_{k-1}) = \cup_\alpha W_\alpha \subset \mathbb{P}^n(\overline{F})$ where each component W_α is defined and irreducible over the perfect closure $F^{q^{-\infty}}$ of the field F. Further, $W_\alpha = \cup_\beta W_{\alpha,\beta}$ where (absolutely irreducible) components $W_{\alpha,\beta}$ are defined and irreducible over the algebraic closure $\overline{F}$ of the field F. The algorithm from Theorem 1, see below, constructs all the components W_α and after that all $W_{\alpha,\beta}$ (actually W_α and $W_{\alpha,\beta}$ are defined over some finite extensions of the field F which also are constructed by the algorithm). Each component W_α (respectively $W_{\alpha,\beta}$) is represented by the algorithm in two ways: by its generic point, see (2), and a system of polynomial equations such that the set of its roots coincides with the component W_α (respectively $W_{\alpha,\beta}$). We shall say that this system gives (or define) the considered component.

Remark 1. Notice also that if $q > 1$ then we suppose that the field H contains sufficiently many elements extending the field H if necessary, see the description of the algorithm from [1]. We choose some linear forms with coefficients from H in the algorithm from [1]. If $l > 0$ then alternatively one can choose these linear forms from $H[T_1, \dots, T_l]$ and don't extend H. In any case using the Frobenius automorphism within the time bounds from Theorem 1, see below, one can easily find the maximal separable subfield of the minimal field of definition over the initial field F (when H is not extended) of each constructed component W_α or $W_{\alpha,\beta}$.

Now we need to formulate the definition of the generic point used in this paper and [1]. Let $W \subset \mathbb{P}^n(\overline{F})$ be a projective algebraic variety, $\operatorname{codim}_{\mathbb{P}^n} W = m$. Suppose that W is defined and irreducible over the field F_1 which is a finite extension of F. Let F_2 be the maximal separable extension of F such that the field $F_2 \subset F_1$. Let $t_1, \dots, t_{n-m}$ be algebraically independent elements over the field F. The generic point of the algebraic variety W is given by the F_2-isomorphism of the field:

$$\begin{aligned} &F_2(t_1, \dots, t_{n-m})[\theta] \\ &\simeq F_2\left(\frac{X_{j_1}}{X_{j_0}}, \dots, \frac{X_{j_{n-m}}}{X_{j_0}}, \left(\frac{X_0}{X_{j_0}}\right)^{q^\nu}, \dots, \left(\frac{X_n}{X_{j_0}}\right)^{q^\nu}\right) \subset F_1(W), \end{aligned} \tag{2}$$

where θ is an algebraic separable element over the field $K = F_2(t_1, \dots, t_{n-m})$ with the minimal polynomial $\Phi \in K[Z]$, the leading coefficient $\mathrm{lc}_Z \Phi = 1$; the elements X_j/X_{j_0} are considered here as the rational functions on W and the variety $W \not\subset \mathcal{Z}(X_{j_0})$ for some $0 \leqslant j_0 \leqslant n$, every element $t_i \mapsto X_{j_i}/X_{j_0}$ under isomorphism (2); if $q > 1$ then $\nu \geqslant 0$ is an integer, if $q = 1$ then $\nu = 0$.

The field $F_2 = H(T_1, \dots, T_l)[\eta_2]$ where η_2 is an algebraic separable over the field $H(T_1, \dots, T_l)$ with the minimal polynomial $\varphi_2 \in H(T_1, \dots, T_l)[Z]$. We suppose that φ_2 is given for the generic point (2). We represent each element from the field $z \in K[\theta][Z]$ in the form

$$z = (1/z_0) \sum_{i,j,w} z_{i,j,v} \eta_2^i \theta^j Z^w, \tag{3}$$

where all $z_0, z_{i,j,v} \in \widetilde{H}[T_1, \ldots, T_l, t_1, \ldots, t_{n-m}]$ are relatively prime elements, $0 \leqslant i < \deg_Z \varphi_2$, $0 \leqslant j < \deg_Z \Phi$. Now the degrees $\deg_{T_1,\ldots,T_l} z$, and $\deg_{t_1,\ldots,t_{n-m}} z$ are defined in the natural way similarly to (1) and also the length $\mathrm{l}(z)$ of coefficients from H is defined (here we leave to give the exact definitions to the reader). If $\deg_{T_1,\ldots,T_l} z < d_3$, $\deg_{t_1,\ldots,t_{n-m}} z < d_4$, $\deg_Z \varphi_2 < d_5$, $\deg_Z \Phi < d_6$, $\mathrm{l}(z) < M_3$ then the size $\mathrm{L}_2(z) < d_3^l d_4^{n-m}(d_5 d_6 + 1)M_3$.

In what follows we shall write $a < \mathcal{P}(b, c)$ if and only if there is a polynomial $\mathcal{P}$ with integer coefficients such that the last inequality holds. We shall use also other similar notations.

Theorem 1. (a) *An algorithm is suggested for finding the decomposition $\mathcal{Z}(f_0, \ldots, f_{k-1}) = \cup_\alpha W_\alpha$. For every $W_\alpha = W$ the algorithm constructs its generic point (2) (with $F_2 = F$, $\varphi_2 = \varphi$) and polynomials $\Psi_1^{(\alpha)}, \ldots, \Psi_N^{(\alpha)} \in F[X_0, \ldots, X_n]$ such that $W_\alpha = \mathcal{Z}(\Psi_1^{(\alpha)}, \ldots, \Psi_N^{(\alpha)})$. Put $m = \mathrm{codim}_{\mathbb{P}^n} W_\alpha$, $\theta_\alpha = \theta$, $\Phi_\alpha = \Phi$, $M = M_1 + M_2 + ld_2 + (n-m)$. Then $q^\nu < d^{2m}$, $\deg_Z \Phi_\alpha \leqslant \deg W_\alpha \leqslant (d-1)^m$. For all j the degrees, lengths of coefficients and the sizes*

$$\begin{aligned}
&\deg_{t_1,\ldots,t_{n-m}} \Phi_\alpha < \mathcal{P}(d^m), \quad \deg_{t_1,\ldots,t_{n-m}}((X_j/X_{j_0})^{q^\nu}) < \mathcal{P}(d^m),\\
&\deg_{T_1,\ldots,T_l} \Phi_\alpha < d_2\mathcal{P}(d_1, d^m), \quad \deg_{T_1,\ldots,T_l}((X_j/X_{j_0})^{q^\nu}) < d_2\mathcal{P}(d_1, d^m),\\
&\mathrm{l}(\Phi_\alpha) \quad \text{and} \quad \mathrm{l}((X_j/X_{j_0})^{q^\nu}) < M\mathcal{P}(d_1, d^m),\\
&\mathrm{L}_2(\Phi_\alpha) \quad \text{and} \quad \mathrm{L}_2((X_j/X_{j_0})^{q^\nu}) < M d_2^l \mathcal{P}(d_1^{l+1}, d^{m(l+n-m+1)}).
\end{aligned}$$

The number of equations $N \leqslant m^2 d^{4m}$, the degrees $\deg_{X_0,\ldots,X_n} \Psi_s^{(\alpha)} < d^{2m}$, $\deg_{T_1,\ldots,T_l} \Psi_s^{(\alpha)} < d_2\mathcal{P}(d_1, d^m)$. Further, every $\Psi_s^{(\alpha)}$ is represented by the algorithm in the form $\Psi_s^{(\alpha)} = \overline{\Psi}_s^{(\alpha)}(Z_{s,0}, \ldots, Z_{s,n-m+2})$ where all $Z_{s,j}$ are linear forms in $X_0, \ldots, X_n$ with coefficients from $\widetilde{H}$. The length of coefficients of all linear forms $\mathrm{l}(Z_{s,j}) < \mathcal{P}(m) \log d$, for all s the degrees $\deg_{Z_{s,0},\ldots,Z_{s,n-m+2}} \overline{\Psi}_s^{(\alpha)} < d^{2m}$, the degrees, lengths of coefficients and the *sizes*

$$\deg_{T_1,\dots,T_l} \overline{\Psi}_s^{(\alpha)} < d_2\mathcal{P}(d_1, d^m), \quad \mathrm{l}(\overline{\Psi}_s^{(\alpha)}) < M\mathcal{P}(d_1, d^m),$$
$$\mathrm{L}_2(\overline{\Psi}_s^{(\alpha)}) < Md_2^l\mathcal{P}(d_1^{l+1}, d^{m(l+n-m+1)}).$$

Put $c = 1 + \max_\alpha \dim W_\alpha$. *Then the working time of the algorithm for constructing all* W_α *with their generic points and defining them systems is polynomial in* $d^{n(c+l)}$, $(d_1d_2)^{l+1}$, M_1, M_2 *and* q.

(b) *An algorithm is suggested for constructing the decomposition* $W = \cup_{\alpha,\beta}W_{\alpha,\beta}$. *For every absolutely irreducible component* $W_{\alpha,\beta}$ *this algorithm finds the maximal separable subfield* F_2 *of the minimal field of definition* $F_1 \supset F$ *of the variety* $W_{\alpha,\beta}$. *The algorithm construct the minimal polynomial* $\varphi_\alpha = \varphi_2$, *of the primitive element* $\eta_{\alpha,\beta} = \eta_2$ *of the field* F_2 *over* $H(T_1,\dots,T_l)$. *Let us replace in assertion (a) the quadruple* $(F,\eta,\varphi,W_\alpha)$ *by* $(F_2,\eta_{\alpha,\beta},\varphi_\alpha,W_{\alpha,\beta})$. *Then similarly to (a) the algorithm constructs a generic point of the variety* $W_{\alpha,\beta}$ *and a system of equations defining this component. For all the parameters of the generic point of* $W_{\alpha,\beta}$ *and the system of equations defining* $W_{\alpha,\beta}$ *the same estimates as the ones from (a) hold true. Besides that, the algorithm represents* $F_2 = F[\xi_{\alpha,\beta}]$, *finds the minimal polynomial* $\psi_\alpha \in F[Z]$ *of* $\xi_{\alpha,\beta}$, *and the representation* $\xi_{\alpha,\beta} \in H(T_1,\dots,T_l)[\eta_{\alpha,\beta}]$ *in form (3). The following estimates for degrees, lengths of coefficients and sizes hold:*

$$\deg_{T_1,\dots,T_l}\varphi_\alpha, \quad \deg_{T_1,\dots,T_l}\xi_{\alpha,\beta} \quad \textit{and} \quad \deg_{T_1,\dots,T_l}\psi_\alpha < d_2\mathcal{P}(d_1,d^m),$$
$$\mathrm{l}(\varphi_\alpha), \quad \mathrm{l}(\xi_{\alpha,\beta}) \quad \textit{and} \quad \mathrm{l}(\psi_\alpha) < M\mathcal{P}(d_1,d^m),$$
$$\mathrm{L}_2(\varphi_\alpha), \quad \mathrm{L}_2(\xi_{\alpha,\beta}) \quad \textit{and} \quad \mathrm{L}_2(\psi_\alpha) < Md_2^l\mathcal{P}(d_1^{l+1},d^{m(l+1)}).$$

The upper bound for the working time of this algorithm is the same as the one from assertion (a).

Now we discuss how to prove this theorem. In [1] we factor using Proposition 1.1 and Theorem 1.2 of [1] polynomials in one variable (or homogeneous polynomials in two variables) with coefficients from the field $K[\theta] = F(t_1,\dots,t_{n-m})[\theta]$. According to [1] these polynomials satisfy the estimates to the degrees and length of coefficients similar to the ones for the polynomial Φ_α from the statement of Theorem 1. In [1] we consider the field $K[\theta]$ as finitely generated over H with the transcendency basis $T_1,\dots,T_l,t_1,\dots,t_{n-m}$ and get the bound for the working time (of the decomposition into irreducible of each considered polynomial) depending on $(d^md_1d_2)^{n-m+l+1}$.

This factoring is modified in the algorithm from Theorem 1. Suppose, e.g., that we need to factor a polynomial $G \in K[Z]$. At first using Proposition 1.1 (or Theorem 1.1) [1] we reduce this problem to factoring some polynomials G_i in the ring $F[t_1, \dots, t_{n-m}, Z]$. After that we construct an extension $H_1 = H[\eta_1]$ such that the fields F and $H_1(T_1, \dots, T_l)$ are linearly disjoint over the field $H(T_1, \dots, T_l)$ and the degree of the extension $H_1 \supset H$ is the least possible satisfying the inequality

$$[H_1 : H] \geqslant (2 \max_i \{\deg_{t_1,\dots,t_{n-m},Z} G_i\} + 1)^{n-m+1}.$$

Hence $[H_1 : H] < \mathcal{P}(d^{m(n-m+1)})$. Put F_1 to be the composite of the fields H_1 and F over H. Theorem 1.2 [1] (we replace in its statement θ by η_1) reduces factoring the polynomials G_i, to the decomposition into the irreducible factors of some polynomials $\widetilde{G}_i \in F_1[X, U]$, where X, U are new variables. Next, again applying Theorem 1.1 [1] and the remark at the end of **§**1, Chap. I [1] to the polynomials in two variables X, U and the extension of fields $F_1 \supset H_1(T_1, \dots, T_l)$ we reduce factoring $\widetilde{G}_i$ to the decomposition into irreducible factors of some polynomials $Q_{i,j} \in H_1(T_1, \dots, T_l)[X, U]$. We shall suppose without loss of generality that $Q_{i,j} \in H_1[T_1, \dots, T_l, X, U]$. Assume at first that $l \geqslant 2$. By the Gauss lemma everything is reduced to factoring $Q_{i,j} \in H_1(X, U)[T_1, \dots, T_l]$ in the last ring and some polynomials $P_{i,j} \in H_1[X, U]$. After that we construct an extension $H_2 = H[\eta_2] \supset H_1$ such that its degree $[H_2 : H_1] = (2 \max_{i,j}\{\deg_{T_1,\dots,T_l} Q_{i,j}\} + 1)^l$. We have $[H_2 : H_1] < d_2^l \mathcal{P}(d_1^l, d^{ml})$. Theorem 1.2 [1] (we replace in its statement (F, θ) by $(H_1(X, U), \eta_2)$) reduces factoring the polynomials $Q_{i,j}$, to the decomposition into the irreducible factors of some polynomials $\widetilde{Q}_{i,j} \in H_2[X, U, X', U']$, where X', U' are new variables. The polynomials $\widetilde{Q}_{i,j}$ and $P_{i,j}$ are factored directly using the algorithm from Chap. I [1]. If $l < 2$ then similarly all $Q_{i,j}$ are decomposed directly. Thus, we have described the required modification of the algorithm. It is known that the extensions of fields $H_i \supset H$, $i = 1, 2$, can be constructed within the time polynomial in $[H_i : H]$ and q (this is not quite trivial if $q > 1$). Now a simple analysis of the complexity using the results from [1] proves Theorem 1.

§2. Application to the estimation of sizes of coefficients of the effective smooth cover and smooth stratification of an algebraic variety

Let the field $k = F$, the integer $m = k - 1$, $f_1, \dots, f_m$ be polynomials from the Introduction. We consider l as a constant in this section. In [2] we prove the existence of a smooth cover and a smooth stratification of an algebraic variety $\mathcal{Z}(f_1, \dots, f_m)$ with degrees of all strata polynomial in $2^{2^{n^C}} d^n$ for a constant $C > 0$ and suggested the an algorithm for constructing these smooth cover and smooth stratification in [4]. In [3] we obtained the similar result about the existence of a smooth cover and a smooth stratification in the case of nonzero characteristic. These results are difficult, strong and important. In [2, 3] we were concentrated on the estimation of degrees of strata but did not pay sufficient attention to the sizes of coefficients from the ground field of the equations giving the strata. Actually the estimates for sizes coefficients are straightforward and we did not estimate them explicitly. There are minor inexactidudes related to the sizes of coefficients from the ground field of the polynomials giving the strata.

Now using the explicit estimates for lengths of coefficients and degrees of the elements at the output of the algorithm from Theorem 1 we give bounds for sizes of coefficients of the equations defining strata in the constructions of [2–4]. The estimations for the degrees and sizes of coefficients from the ground field from Theorem 1 are applied recursively in the constructions of [2, 3].

Assertion (vi) of Theorem 2 from [2] must be corrected as follows:

(vi) *For all* $\alpha \in A$, $1 \leqslant j \leqslant s(\alpha)$ *the lengths of coefficients from* k *of polynomials* $h_{\alpha,j}$ *are bounded from above by a polynomial in* $n^{2^{s(\alpha)^C}} d^{s(\alpha)^2}$, $d_1^{s(\alpha)}$, d_2, M, M_1, m *for an absolute constant* $0 < C \in \mathbb{R}$. *Further, in the case of smooth stratification the lengths of coefficients from* k *of all polynomials of the family* f *are bounded from above by a polynomial in* $2^{2^{n^C}} d^{n^2}$, d_1^n, d_2, M, M_1, m *for an absolute constant* $0 < C \in \mathbb{R}$.

Thus, one needs to replace d^n, d_1 by $d^{s(\alpha)^2}$, $d_1^{s(\alpha)}$ for the case of the smooth cover (respectively by d^{n^2}, d_1^n for the case of the smooth stratification) in (vi) Theorem 2 [2]. All the other assertions of this theorem and its proof are without changes. In particular, the degrees of all the strata are bounded from above by $2^{2^{n^C}} d^n$. The proof is the same since actually we did not estimate the lengths of coefficients from k of these polynomials explicitly. The bound from (vi) is obtained straightforwardly by the recursive application of Theorem 1 [2] and the estimates from Theorem 1, see the proof Theorem 2 [2].

In the similar assertions (vi) of Theorem 3 [3] and (vi) of Theorem 4 [4] one needs to replace $d^{ns(\alpha)}$, d_1 by $d^{s(\alpha)^2}$, $d_1^{s(\alpha)}$ for the case of smooth cover (respectively by d^{n^2}, d_1^n for the case of the smooth stratification). Here we improve the results of [3] and [4] replacing $d^{ns(\alpha)}$ by $d^{s(\alpha)^2}$ and correct them replacing d_1 by $d_1^{s(\alpha)}$ (respectively d_1^n).

The working time of the algorithm from Theorem 4 [4] for constructing the smooth cover and the smooth stratification is polynomial in the size of the output and $2^{2^{n^C}} d^{n^2}$, d_1^n, d_2, M, M_1, m, where $0 < C \in \mathbb{R}$ is an absolute constant.

Notice that the proof of Theorem 3 [2] about computing the dimension of a real algebraic variety is the same. It uses only the fact that the degrees of the strata from Theorem 2 [2] are bounded from above by $2^{2^{n^C}} d^n$. But now one can not use immediately Theorem 4 [4] to deduce Theorem 3 [2]. So I know only one proof of Theorem 3 [2] using the original construction from [2].

References

1. A. L. Chistov, *Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time.* — Zap. Nauchn. Semin. LOMI **137** (1984), 124–188.
2. A. L. Chistov, *Efficient smooth stratification of an algebraic variety in zero–characteristic and its applications.* — Zap. Nauchn. Semin. POMI **266** (2000), 254–311.
3. A. L. Chistov, *Efficient construction of local parameters of irreducible components of an algebraic variety in nonzero characteristic.* — Zap. Nauchn. Semin. POMI **326** (2005), 248–278.
4. A. L. Chistov, *Polynomial-time algorithms for a new model of representation of algebraic varieties (in characteristic zero).* — Zap. Nauchn. Semin. POMI **378** (2010), 133–170.

St. Petersburg Department
of Steklov Mathematical Institute,
Fontanka 27, St. Petersburg 191023, Russia
E-mail: alch@pdmi.ras.ru

Поступило 21 сентября 2011 г.