Proceedings of the International Congress of Mathematicians
Berkeley, California, USA, 1986

Computational Complexity in Polynomial Algebra

D. YU. GRIGOR'EV

In recent years a number of algorithms have been designed for the "inverse" computational problems of polynomial algebra—factoring polynomials, solving systems of polynomial equations, or systems of polynomial inequalities, and related problems—with running time considerably less than that of the algorithms which were previously known. (For the computational complexity of the "direct" problems such as polynomial multiplication or determination of g.c.d.'s see [**1**, **16**] and also [**9**].) It should be remarked that as a result a hierarchical relationship between the computational problems of polynomial algebra, from the point of view of computational complexity, has been elucidated. The successful design of these algorithms depended to a large degree on developing them in the correct order: first the algorithms for the problems which are easier in the sense of this hierarchy were designed, which were then applied as subroutines in the solutions of more difficult problems. So far problems of the type discussed here have been considered easier only when they are special cases of the more difficult ones; e.g., the solution of a system of polynomial equations is considered as a particular case of quantifier elimination.

A powerful impetus for this development came initially from the development of polynomial-time algorithms for factoring polynomials. On the other hand, a major role has been played by a new insight from the computational point of view: treating the solution of systems of polynomial equations in the framework of the determination of the irreducible components of an algebraic variety. This has made it possible to apply the polynomial factorization algorithm to this problem. In addition a successful reduction of the problem of solving systems of polynomial inequalities to the "nonspecial" case of this problem was achieved by means of an explicit use of infinitesimals in the calculations, and the "nonspecial" case was in turn reduced to the solution of a suitable system of polynomial equations. Finally, for the design of decision procedures for the first order theories of algebraically closed or real closed fields, appropriate solvability criteria for the corresponding systems with variable coefficients were produced which are "uniform" in the set of auxiliary parameters.

Since all the bounds on time complexity given in the present paper are only specified up to a polynomial, while on the other hand all reasonable models of computation (such as Turing machines or RAM's) are equivalent in the sense of polynomial time complexity, the choice of a particular model of computation is irrelevant to this paper. One may take the complexity measure below to be the number of bit operations executed. As usual, complexity is considered as a function of the size of the input data in the worst case. The terms "polynomial time" and "exponential time" will be used in this sense (see, e.g., [1]).

1. Factoring polynomials. Attempts to design procedures for factoring polynomials go back to Newton (for a historical survey see [16]). The Kronecker-Schubert algorithm for factoring polynomials from the ring $\mathbf{Q}[X_1, \dots, X_n]$ is well known (see, e.g., [25]). This and similar algorithms have exponential running time, however. Thus the question arose as to whether a polynomial time algorithm for factoring polynomials exists.

In the case of polynomials $f \in F_p[X]$ in one variable over a finite field of characteristic p, a positive answer to this question was given by Berlekamp's algorithm (see, e.g., [16]), whose running time is polynomial in p, s and the degree $\deg_X(f)$. For a long time there was no significant progress in attempts to design fast algorithms for factoring polynomials, until finally in [18] an ingenious polynomial-time algorithm for factoring polynomials from the ring $\mathbf{Q}[X]$ was produced. In [18] the problem of factoring polynomials was reduced to one of finding a sufficiently short vector in a lattice, and in addition for the latter problem a polynomial-time algorithm was designed. The result of [18] was then generalized in [3] (see also [4, 5, 8]), where a polynomial-time algorithm for factoring polynomials $f \in F[X_1, \dots, X_n]$ in many variables over a fairly large class of fields F was produced. We mention also that in [12, 13] an algorithm for factoring polynomials from the ring $\mathbf{Q}[X_1, \dots, X_n]$ was designed, whose complexity is polynomial for a fixed number n of variables.

Before proceeding to an exact formulation of the result from [3], we need to describe how a ground field F and a polynomial $f \in F[X_1, \dots, X_n]$ are presented. Thus, we consider a field of the form $F = H(T_1, \dots, T_e)[\eta]$, where $H = \mathbf{Q}$ or $H = \mathbf{F}_p$ (in other words H is a prime field), the elements $T_1, \dots, T_e$ are algebraically independent over H, the element η is separably algebraic over the field $H(T_1, \dots, T_e)$. Let $\varphi(Z) = \sum_{0 \le i < \deg_Z(\varphi)} (\varphi_i^{(1)}/\varphi^{(2)}) Z^i \in H(T_1, \dots, T_e)[Z]$ be the minimal polynomial of η over the field $H(T_1, \dots, T_e)$ with the leading coefficient $\mathrm{lc}_Z(\varphi) = 1$, where the polynomials $\varphi_i^{(1)}, \varphi^{(2)} \in H[T_1, \dots, T_e]$ and the degree $\deg(\varphi^{(2)})$ is the least possible. Any polynomial $f \in F[X_1, \dots, X_n]$ can be uniquely represented in the form

$$f = \sum_{0 \le i < \deg_Z(\varphi); i_1, \dots, i_n} (a_{i, i_1, \dots, i_n}/b) \eta^i X_1^{i_1} \cdots X_n^{i_n}$$

where the polynomials $a_{i, i_1, \dots, i_n}$, $b \in H[T_1, \dots, T_e]$ and the degree $\deg(b)$ is the

least possible. Define the degree

$$\deg_{T_j}(f) = \max_{i,i_1,\dots,i_n} \{\deg_{T_j}(a_{i,i_1,\dots,i_n}), \deg_{T_j}(b)\}.$$

Another measure of the size of a representation of a polynomial is the (bit) length of its coefficients (from the field H). Namely, if $H = \mathbf{Q}$ and $\alpha/\beta \in \mathbf{Q}$, where α, β are relatively prime integers, then the length $l(\alpha/\beta)$ is defined by $\log_2(|\alpha\beta| + 2)$; if $H = \mathbf{F}_p$ then the length $l(\alpha)$ for any element $\alpha \in \mathbf{F}_p$ is defined as $\log_2 p$. The length $l(f)$ of the coefficients of a polynomial f is defined as the maximal length of the coefficients from H of the monomials in the variables $T_1, \dots, T_e$ occurring in the polynomials $a_{i,i_1,\dots,i_n}, b$. Finally, as the size $L_1(f)$ of a polynomial f we take here the value

$$\left(\max_{1\le i\le n} \deg_{X_i}(f) + 1\right)^{n+e} \left(\max_{1\le j\le e} \deg_{T_j}(f) + 1\right)^{e} (\deg_Z(\varphi) + 1) l(f),$$

analogously

$$L_1(\varphi) = \left(\max_{1\le j\le e} \deg_{T_j}(\varphi) + 1\right)^{e} (\deg_Z(\varphi) + 1) l(\varphi).$$

The size of a polynomial provides an estimate for the sum of the bit lengths of all its coefficients.

We use the notation $g_1 \le g_2 P(g_3, \dots, g_s)$ for functions $g_1, \dots, g_s$ to mean that for a suitable polynomial P the following inequality holds:

$$|g_1| \le |g_2| P(|g_3|, \dots, |g_s|).$$

THEOREM 1. *One can factor a polynomial f over the field F within time polynomial in $L_1(f)$, $L_1(\varphi)$, p. Moreover for any normalized divisor $f_1 \in F[X_1, \dots, X_n]$ of the polynomial f the following bounds are valid:*

$$\deg_{T_j}(f_1) \le \deg_{T_j}(f) P\left(\max_{1\le i\le n} \deg_{X_i}(f), \max_{1\le j\le e} \deg_{T_j}(\varphi), \deg_Z(\varphi)\right),$$

$$l(f_1) \le (l(f) + l(\varphi) + e \max_{1\le j\le e} \deg_{T_j}(f) + n) \cdot P\left(\max_{1\le i\le n} \deg_{X_i}(f), \max_{1\le j\le e} \deg_{T_j}(\varphi), \deg_Z(\varphi)\right).$$

First Theorem 1 was proved in [3] for finite fields F, where in order to reduce the multivariable case to the case of two variables an effective version of Hilbert's Irreducibility Theorem was given.

Theorem 1 has various applications (see, e.g., [4]) to absolute polynomial factorization, to constructing a primitive element in a field extension, and to finding the Galois group of a polynomial.

2. Solving a system of polynomial equations. Let the polynomials

$$f_1, \dots, f_\kappa \in F[X_1, \dots, X_n]$$

be given for a field of the same form as in §1. Assume for the present section that the following bounds are fulfilled:

$$\deg_{X_1,\dots,X_n}(f_i) < d, \qquad \deg_{T_1,\dots,T_s,Z}(\varphi) < d_1, \qquad \deg_{T_1,\dots,T_s}(f_i) < d_2,$$
$$l(\varphi) \le M_1, \qquad l(f_i) \le M_2, \qquad 1 \le i \le \kappa.$$

A way to decide the solvability of a system of the form $f_1 = \dots = f_\kappa = 0$ over the algebraic closure $\overline{F}$ of a field F was given in the nineteenth century relying on elimination theory (see, e.g., [**25**]). The time complexity of this procedure, however, is nonelementary (in particular, it grows faster than any tower of a fixed number of exponential functions). In [**22**] (see also [**11**]) a method was devised with the help of which one can solve systems within time $(M_2\kappa d)^{2^{O(n)}}$ when either $F = \mathbf{Q}$ or F is finite. In [**17**] an algorithm was produced for solving a system of homogeneous equations in the case when the projective variety of all its roots (defined over the field $\overline{F}$) consists of a finite number of points, and the running time of this algorithm is polynomial in M_2, κ, d^n, p if the ground field F is finite of characteristic p. In [**4**] (see also [**5, 8**]) an algorithm for solving systems of polynomial equations was designed, whose running time can be bounded by a polynomial in M_2, κ, d^{n^2}, p in the case when either the field $F = \mathbf{Q}$ or F is finite.

Actually, the algorithm from [**4**] finds the irreducible components V_i of the variety $V = \bigcup_i V_i \subset \overline{F}^n$ of all the roots of the system $f_1 = \dots = f_\kappa = 0$. Furthermore, the algorithm represents each component in two ways: by a generic point, and secondly by a certain system of polynomials, whose associated variety coincides with the component.

In this connection, a generic point of a variety $W \subset \overline{F}^n$ of dimension $\dim(W) = n - m$ which is both defined and irreducible over the perfect closure $F^{p^{-\infty}}$ of the field F [**27**] is an effective version of the usual notion of generic point in algebraic geometry (an embedding of the field of rational functions on the variety). Thus we now define a generic point to be a field isomorphism of the following form:

$$F(t_1, \dots, t_{n-m})[\theta] \simeq F(X_{j_1}, \dots, X_{j_{n-m}}, X_1^{p^\nu}, \dots, X_n^{p^\nu}) \subset F^{p^{-\infty}}(W) \qquad (1)$$

where $t_1, \dots, t_{n-m}$ are algebraically independent over the field F, and in addition $F^{p^{-\infty}}(W)$ is a field of rational functions on the variety W over the field $F^{p^{-\infty}}$, and the exponent $\nu \ge 0$ (we adopt the convention that $p^\nu = 1$ when $\operatorname{char}(F) = 0$); furthermore the element θ is the image under the isomorphism (1) of a linear function $\sum_{1 \le j \le n} c_j X_j$ for certain natural numbers $c_1, \dots, c_n$. Under the isomorphism (1) the coordinate function X_{j_i} is mapped into t_i, for $1 \le i \le n-m$. The algorithm represents a generic point by specifying the coefficients $c_1, \dots, c_n$, the exponent p^ν, the minimal polynomial $\Phi(Z) \in F(t_1, \dots, t_{n-m})[Z]$ of the element θ, and the images under the isomorphism (1) of the functions $X_j^{p^\nu}$ in the field $F(t_1, \dots, t_{n-m})[\theta]$. In the formulations of the theorems below we use

the notations introduced in (1), and we define the degrees and the lengths of the coefficients of the functions $X_j^{p^\nu}$ as the degrees and the lengths of the coefficients of their images.

THEOREM 2. *For given polynomials $f_1, \dots, f_\kappa$ one can find all irreudcible components V_i of the variety $V \subset \overline{F}^n$ of all the roots of the system $f_1 = \dots = f_\kappa = 0$ within time polynomial in $M_1, M_2, (d^n d_1 d_2)^{n+e}, \kappa, p$.*

Moreover, for each component V_i the algorithm yields a generic point for it (see (1)) and a family of polynomials $\Psi_1^{(i)}, \dots, \Psi_N^{(i)} \in F[X_1, \dots, X_n]$ such that V_i coincides with the variety of all roots of the system $\Psi_1^{(i)} = \dots = \Psi_N^{(i)} = 0$. Denote $m = \operatorname{codim} V_i$, $\theta_i = \theta$, $\Phi_i = \Phi$. Then the following bounds hold:

$$p^\nu \le d^{2m}, \qquad c_j \le \deg_Z(\Phi_i) \le \deg V_i \le (d-1)^m, \qquad N \le m^2 d^{4m};$$

$$\deg_{T_1,\dots,T_e,t_1,\dots,t_{n-m}}(\Phi_i), \deg_{T_1,\dots,T_e,t_1,\dots,t_{n-m}}(X_j^{p^\nu}) \le d_2 P(d^m, d_1);$$

$$l(\Phi_i), l(X_j^{p^\nu}), l(\Psi_s^{(i)}) \le (M_1 + M_2 + (e+n-m)d_2) P(d^m, d_1);$$

$$\deg_{X_1,\dots,X_n}(\Psi_s^{(i)}) \le d^{2m}; \qquad \deg_{T_1,\dots,T_e}(\Psi_s^{(i)}) \le d_2 P(d^m, d_1).$$

Theorem 2 allows us to answer the principal questions about the variety of roots of a system of polynomial equations, namely, whether the variety is empty, and what its dimension is. Provided that the variety consists of a finite number of points, the algorithm enumerates all of them; otherwise if the variety is not zero-dimensional then the algorithm allows us to pick out any desired number of roots of the system.

Evidently, the time-bound in Theorem 2 cannot be considerably improved in general, if one desires to find all the irreducible components of a variety, since the size of a presentation of a component with dimension near $n/2$ is of the order $M_2 d^{n^2}$ in the case when either $F = \mathbf{Q}$ or F is finite.

The algorithm from Theorem 1 is involved essentially in the proof of Theorem 2. On the other hand, polynomial factorization is a particular case (when $\kappa = 1$) of the problem of finding all the irreducible components of a variety.

As a corollary of Theorem 2 one can find all the absolutely irreducible components of a variety within the same time-bound as in Theorem 2 [4].

Note that the methods discussed do not allow us to recognize within the same time-bound, whether a polynomial f belongs to an ideal $(f_1, \dots, f_\kappa) \subset F[X_1, \dots, X_n]$ (by means of Theorem 2 one can test, however, whether a polynomial f belongs to the radical $\operatorname{rad}(f_1, \dots, f_\kappa)$).

3. Quantifier elimination in the first-order theory of algebraically closed fields. Quantifier elimination in the first-order theory of algebraically closed fields is a generalization of the problem of solving systems of polynomial equations. Thus, consider a formula of this theory of the form

$$\exists X_{1,1} \cdots \exists X_{1,s_1} \forall X_{2,1} \cdots \forall X_{2,s_2} \cdots \exists X_{a,1} \cdots \exists X_{a,s_a} (\Pi) \tag{2}$$

where Π is a quantifier-free formula of the theory containing κ atomic subformulas of the sort $(f_i = 0)$, $1 \le i \le \kappa$, here the polynomials

$$f_i \in F[X_1, \dots, X_{s_0}, X_{1,1}, \dots, X_{a,s_a}]$$

(we assume the field F and the polynomials f_i satisfy the same bounds as in the beginning of the previous section). Denote by $n = s_0 + s_1 + \cdots + s_a$ the total number of variables (including free ones $X_1, \dots, X_{s_0}$), and by a the number of quantifier alternations in the formula (in the presentation of the formula (2) a is odd, but this is not essential).

In [**23**] (see also [**21**]) a quantifier elimination procedure was described, which for a given formula of the form (2) yields an equivalent quantifier-free formula. The time-bounds of these procedures, however, were nonelementary. In [**11**] a quantifier elimination method is described, having time-bound $(M_2 \kappa d)^{2^{O(n)}}$ in the case when either the field $F = \mathbf{Q}$ or F is finite (when $F = \mathbf{Q}$ the same time-bound follows from the methods of [**6**, **26**]). In [**5**] a quantifier elimination algorithm is produced with time-bound polynomial in $M_2, (\kappa d)^{(O(n))^{2a}}$ in the case when either $F = \mathbf{Q}$ or F is finite, more exactly the following is valid.

THEOREM 3. *For a given formula of the form* (2) *one can construct an equivalent quantifier-free formula of the first-order theory of algebraically closed fields*

$$\bigvee_{1 \le i \le \mathcal{N}} \left(\&_{1 \le j \le \mathcal{K}} (g_{ij} = 0) \,\&\, (g_{i,0} \ne 0) \right)$$

within time polynomial in $M_1, M_2, (\kappa d)^{(O(n))^{2a} e}, (d_1^a d_2)^{n+e}, p$. *Moreover the polynomials* $g_{ij} \in F[X_1, \dots, X_{s_0}]$ *satisfy the following bounds:*

$$\deg_{X_1, \dots, X_{s_0}}(g_{ij}) \le (\kappa d^n)^{(82(n+3)(n+2a)/a)^a} = \mathcal{M};$$

$$\deg_{T_1, \dots, T_e}(g_{ij}) \le d_2 \mathcal{P}(\mathcal{M}, d_1^a);$$

$$l(g_{ij}) \le (M_1 + M_2 + e d_2) \mathcal{P}(\mathcal{M}, d_1^a); \qquad \mathcal{N}, \mathcal{K} \le \mathcal{M}.$$

The main auxiliary subroutine for proving the theorem is the projection (with respect to many variables) of a quasiprojective variety, based on Theorem 2. Furthermore, a bound on the degree of a projection of a constructible set is obtained. For a constructible set $\mathcal{W} \subset \overline{F}^n$ we say that its degree $\deg(\mathcal{W}) \le \mathcal{D}$, provided that there is a representation $\mathcal{W} = \bigcup_i (\mathcal{V}_i \backslash \mathcal{U}_i)$, where $\mathcal{V}_i$, $\mathcal{U}_i$ are closed sets (in the Zariski topology [**26**]) such that $\sum_i (\deg(\mathcal{V}_i) + \deg(\mathcal{U}_i)) \le \mathcal{D}$. The method from [**5**] entails the following bound. If $\pi \colon \overline{F}^n \to \overline{F}^{n-m}$ is a linear projection, then $\deg(\pi(\mathcal{W})) \le (\deg(\mathcal{W}))^{O(nm+1)}$.

The time-bound in Theorem 3 is significantly lower than time-bounds from [**6**, **26**, **20**, **11**] for small a. We remark, on the other hand, that an exponential lower bound for the complexity of a decision procedure for the first-order theory of algebraically closed fields was obtained in [**7**] (see also [**2**]) for a succession of formulas in which the number a of quantifier alternations grows linearly with the number n of variables. From this remark and from Theorem 3 one can conclude

that the parameter a gives the most significant contribution to the complexity of quantifier elimination in a formula of the theory.

4. Solving system of polynomial inequalities. Let a system of polynomial inequalities

$$f_1 > 0, \ldots, f_m > 0, f_{m+1} \geq 0, \ldots, f_\kappa \geq 0 \tag{3}$$

be given, where the polynomials $f_i \in \mathbf{Q}[X_1, \ldots, X_n]$ satisfy the bounds

$$\deg_{X_1,\ldots,X_n}(f_i) < d, \quad l(f_i) \leq M, \qquad 1 \leq i \leq \kappa.$$

Decidability (over the field $\mathbf{R}$) of systems of the form (3) was proved in [**23**] (see also [**21**]). The time-bounds of the procedures from [**23**, **21**], however, were nonelementary. In [**6**, **26**] the algorithms for solving systems of inequalities were designed with time-bound $(M\kappa d)^{2^{O(n)}}$ (also, an algorithm with a worse elementary time-bound was described in [**20**]). In [**24**] an algorithm for this problem was produced with time-bound polynomial in $M(\kappa d)^{n^2}$.

We mention that in the case when $\deg(f_i) = 1$ for $1 \leq i \leq \kappa$ (linear programming) a polynomial time algorithm was described for the first time in [**15**] (a more practical polynomial time method was described in [**14**]).

For the exact formulation of the result [**24**] we introduce the notion of a representative set for a semialgebraic set. The set consisting of all real points satisfying a system of inequalities of the form (3), is a semialgebraic set $S \subset \mathbf{R}^n$, which can be represented as a union $S = \bigcup_i S_i$ of its connected components (in the euclidean topology), each S_i being in its turn a semialgebraic set [**23**]. We say that a finite family of points $\mathcal{T} \subset S \subset \mathbf{R}^n$ is a representative set for the system of inequalities (3) (or for the semialgebraic set S) if $\mathcal{T} \cap S_i \neq \varnothing$ for every i.

Observe that unlike §2, where an algebraic point from $\overline{F}^n$ was given by the algorithm actually as an element of a class of points conjugate over the field F, to represent a real algebraic point $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{R}^n$ one needs to specify an interval containing a unique root of the minimal polynomial of a primitive element of the field $\mathbf{Q}(\alpha_1, \ldots, \alpha_n)$. Namely, $\alpha_i = \sum_j \alpha_i^{(j)} \theta^j$ where $\alpha_i^{(j)} \in \mathbf{Q}$ and $\theta \in \mathbf{R}$ is a root of a polynomial $\Phi(Z) \in \mathbf{Q}[Z]$ which is irreducible over $\mathbf{Q}$, furthermore $\theta = \sum_{1 \leq i \leq n} c_i \alpha_i$ for some natural numbers $c_1, \ldots, c_n$; the algorithm gives $\Phi, \alpha_i^{(j)}, c_i$ and in addition an interval $(\beta_1, \beta_2) \subset \mathbf{R}$ with rational endpoints $\beta_1 < \beta_2$, containing only one root θ of the polynomial Φ. Below in the formulation of Theorem 4 we utilize the same notation.

THEOREM 4. *For a given system of inequalities of the kind* (3) *one can construct a representative set* $\mathcal{T}$ *containing* $(\kappa d)^{O(n^2)}$ *points within time polynomial in* $M(\kappa d)^{n^2}$. *Moreover, for any point* $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathcal{T}$ *the following bounds are valid*:

$$c_i \leq \deg(\Phi) \leq (\kappa d)^{O(n)}; \qquad l(\Phi), l(\alpha_j^{(i)}), l(\beta_1), l(\beta_2) \leq M(\kappa d)^{O(n)}.$$

We remark that the number of connected components S_i of a semialgebraic set S does not exceed $(\kappa d)^{O(n)}$ (see, e.g., [**19**]).

The proof of Theorem 4 involves essentially Theorem 2.

5. Deciding Tarski algebra. Similarly to the case of algebraically closed fields (§3) we now consider the first-order theory of real closed fields (or in other words, Tarski algebra). Namely, consider a formula of the form

$$\exists X_{1,1} \cdots \exists X_{1,s_1} \forall X_{2,1} \cdots \forall X_{2,s_2} \cdots \exists X_{a,1} \cdots \exists X_{a,s_a} (\Omega) \tag{4}$$

where Ω is a quantifier-free formula of Tarski algebra, containing κ atomic subformulas of the kind $(f_i \geq 0)$, $1 \leq i \leq \kappa$; here the polynomials $f_i \in \mathbf{Q}[X_{1,1}, \ldots, X_{a,s_a}]$. As in §3 a is the number of quantifier alternations. Unlike §3 we consider only closed formulas (without free variables) in the present section; denote by $n = s_1 + \cdots + s_a$ the number of all variables. As in §4 assume that $\deg(f_i) < d$, $l(f_i) \leq M$, $1 \leq i \leq \kappa$.

In [**23**] (see also [**21**]) a quantifier elimination procedure for Tarski algebra was described, which implies its decidability. The time-bounds for these procedures, however, were nonelementary. In [**6**, **26**] quantifier elimination methods for Tarski algebra were described with running time $(M\kappa d)^{2^{O(n)}}$. (Also in [**20**] a certain method was described having an elementary, but worse time-bound.) In [**10**] the following theorem is claimed.

THEOREM 5. *There is a decision algorithm for Tarski algebra with running time for formulas of the form* (4) *polynomial in* $M(\kappa d)^{(O(n))^{4a-2}}$.

In the proof of Theorem 5, Theorems 3,4 are involved essentially. Observe that as in §3 one can draw the conclusion that the parameter a makes the most significant contribution to the complexity of the decision procedure.

As a corollary of Theorem 5 one can calculate the dimension of a semialgebraic set $S \subset \mathbf{R}^n$ consisting of the solutions of a system of the kind (3) within time polynomial in $M(\kappa d)^{(O(n))^{10}}$.

Note in conclusion that it would be possible to design a quantifier elimination procedure for Tarski algebra with the same time-bound as in Theorem 5, provided that one could solve within time e.g. $\mathcal{P}(M(\kappa d)^{n^2})$ at least one of two following computational problems. First: elimination of a single quantifier in a formula of Tarski algebra. Second: for a given semialgebraic set $S \subset \mathbf{R}^n$ to find its connected components S_i, i.e., to find quantifier-free formulas Ω_i of Tarski algebra such that S_i coincides with the set of points in $\mathbf{R}^n$ satisfying Ω_i.

REFERENCES

1. A. Aho, J. Hopcroft, and J. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, Reading, Mass., 1976.

2. L. Berman, *The complexity of logical theories*, Theoret. Comput. Sci. 11 (1980), 71–77.

3. A. L. Chistov and D. Yu. Grigor'ev, *Polynomial-time factoring of polynomials over a global field*, Preprint LOMI E-5-82, Leningrad, 1982.

4. ——, *Subexponential-time solving systems of algebraic equations.* I, II, Preprints LOMI E-9-83, E-10-83, Leningrad, 1983.

5. ——, *Complexity of quantifier elimination in the theory of algebraically closed fields*, Lecture Notes in Comput. Sci. **176** (1984), 17–31.

6. G. E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, Lecture Notes in Comput. Sci. **33** (1975), 134–183.

7. M. J. Fischer and M. O. Rabin, *Super-exponential complexity of Presburger arithmetic*, Complexity of Computations (Proc. SIAM-AMS Sympos., New York, 1973), SIAM-AMS Proc., Vol. 7, Amer. Math. Soc., Providence, R.I., 1974, pp. 27–41.

8. D. Yu. Grigor'ev and A. L. Chistov, *Fast decomposition of polynomials into irreducible ones and the solution of systems of algebraic equations*, Soviet Math. Dokl. **29** (1984), 380–383.

9. D. Yu. Grigor'ev, *Multiplicative complexity of a pair of bilinear forms and of the polynomial multiplication*, Lecture Notes in Comput. Sci. **64** (1978), 250–256.

10. ——, *Complexity of deciding the first-order theory of real closed fields*, Proc. All-Union Conf. Applied Logic, Novosibirsk, 1985, pp. 64–66. (Russian)

11. J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), 239–278.

12. E. Kaltofen, *A polynomial reduction from multivariate to bivariate integral polynomial factorization*, Proc. 14 ACM Sympos. Th. Comput. (May, 1982), pp. 261–266.

13. ——, *A polynomial-time reduction from bivariate to univariate integral polynomial factorization*, 23rd Annual Sympos. on Foundations of Comput. Sci. (Chicago, Ill., 1982), IEEE, 1982, pp. 57–64.

14. N. Karmarkar, *A new polynomial-time algorithm for linear programming*, Proc. 16 ACM Sympos. Th. Comput. (May, 1984), pp. 302–311.

15. L. G. Khachian, *A polynomial algorithm in linear programming*, Soviet Math. Dokl. **20** (1979), 191–194.

16. D. Knuth, *The art of computer programming*, vol. 2, Addison-Wesley, Reading, Mass., 1969.

17. D. Lazard, *Resolution des systemes d'équation algebriques*, Theoret. Comput. Sci. **15** (1981), 77–110.

18. A. K. Lenstra, H. W. Lenstra, and L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

19. J. Milnor, *On the Betti numbers of real varieties*, Proc. Amer. Math. Soc. **15** (1964), 275–280.

20. L. Monk, *An elementary-recursive decision procedure for* $\mathrm{Th}(R, +, \cdot)$, Ph.D. Thesis, Univ. of California, Berkeley, 1974.

21. A. Seidenberg, *A new decision method for elementary algebra*, Ann. of Math. **60** (1954), 365–374.

22. ——, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–314.

23. A. Tarski, *A decision method for elementary algebra and geometry*, Univ. of California Press, Berkeley, Calif., 1951.

24. N. N. Vorob'ev, Jr. and D. Yu. Grigor'ev, *Finding real solutions of systems of polynomial inequalities in subexponential time*, Soviet Math. Dokl. **32** (1985), 316–320.

25. B. L. van der Waerden, *Moderne Algebra*, B. I, II, Springer-Verlag, 1930, 1931.

26. H. Wüthrich, *Ein Entscheidungsverfahren für die Theorie der reell-abgeschlossenen Körper*, Lecture Notes in Comput. Sci. **43** (1976), 138–162.

27. O. Zariski and P. Samuel, *Commutative algebra*, vols. 1, 2, Van Nostrand, Princeton, N.J., 1958, 1960.

LENINGRAD BRANCH, STEKLOV MATHEMATICAL INSTITUTE, ACADEMY OF SCIENCES OF THE USSR, LENINGRAD 191011, USSR