

## THE COMPLEXITY OF THE DECISION PROBLEM FOR THE FIRST ORDER THEORY OF ALGEBRAICALLY CLOSED FIELDS

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

1987 Math. USSR Izv. 29 459

(<http://iopscience.iop.org/0025-5726/29/2/A10>)

View [the table of contents for this issue](#), or go to the [journal homepage](#) for more

Download details:

IP Address: 192.68.254.6

The article was downloaded on 19/04/2010 at 15:52

Please note that [terms and conditions apply](#).

**THE COMPLEXITY OF THE DECISION PROBLEM  
FOR THE FIRST ORDER THEORY  
OF ALGEBRAICALLY CLOSED FIELDS**

UDC 518.5

D. YU. GRIGOR'EV

**ABSTRACT.** An algorithm is described that constructs, from every formula of the first order theory of algebraically closed fields, an equivalent quantifier-free formula in time which is polynomial in  $\mathcal{L}^{n^{2a+1}}$ , where  $\mathcal{L}$  is the size of the formula,  $n$  is the number of variables, and  $a$  is the number of changes of quantifiers.

Bibliography: 15 titles.

**Introduction**

The decidability of the first order theory of algebraically closed fields was established by Tarski [1]. Tarski originally proposed a decision procedure based on the method of quantifier elimination for the theory of real closed fields, and then modified it for algebraically closed fields. The method of quantifier elimination [1] enables us to construct, for each formula of the form

$$\exists Z_{11} \dots \exists Z_{1s_1} ] \exists Z_{21} \dots \exists Z_{2s_2} \dots ] \exists Z_{a1} \dots \exists Z_{as_a} Q \quad (1)$$

in the first order theory of algebraically closed fields (where  $Q$  is a propositional formula with atomic subformulas of the form " $f_i = 0$ " and the polynomials  $f_i$  are in  $F[Z_1, \dots, Z_{s_0}, Z_{11}, \dots, Z_{as_a}]$ ) an equivalent quantifier-free formula. If (1) is a closed formula (that is  $s_0 = 0$ ), it is thereby possible to determine whether the formula is true on the basis of this method.

Tarski's method, as well as some similar ones based on elimination theory, have very large execution time. Later, in [4]–[7], methods of quantifier elimination were proposed with substantially better bounds on their execution times. Specifically, let  $N$  be the number of atomic subformulas of (1),  $n = s_0 + s_1 + \dots + s_a$  the number of variables in the formula, and let the degrees of the  $f_i$  be less than  $d$ . The time bound obtained in [4]–[7] is of order  $(Nd)^{n^{O(n)}}$ .

In the present article an algorithm is described (§§2 and 3) which for each formula of the form (1) constructs an equivalent quantifier-free formula, in time of order  $(Nd)^{O(n)^{2a+1}}$  (see Theorem 3). Thus the parameter which exerts the most essential influence on the estimate of complexity of quantifier elimination is the number  $a \leq n$  of alternations of quantifiers in (1). We remark that the exponential lower bound for the complexity of the decision problem for the first order theory of algebraically closed fields

1980 *Mathematics Subject Classification* (1985 Revision). Primary 68Q40; Secondary 03C10, 12L99.

[8] was established for a sequence of formulas in which the number of alternations of quantifiers has the same order of growth as the number of variables.

The algorithm described in §§2 and 3 uses the algorithms of subexponential complexity constructed in [9] and [10] for the decomposition of an algebraic variety into irreducible components (see §1), which rests in turn on a polynomial time algorithm for the factorization of multivariate polynomials into irreducible factors [9], [10].

We specify that in the present article we understand the execution time of an algorithm to be the number of steps in its execution by a RAM [2], [3]. The choice of a concrete model of computation is not very important, since the complexity bounds are given here only up to a polynomial, and all reasonable models of computation are equivalent up to a polynomial [2], [3].

There is no loss of generality in considering formulas (see (1)) in prenex normal form, since the size of the prenex normal form, and also the time necessary for the reduction to this form, are linearly bounded in terms of the size of the input formula.

**§1. Decomposition of a variety into irreducible components**

Let the ground field be  $F = H(T_1, \dots, T_l) [\eta]$ , where either  $H = \mathbf{Q}$  or  $H = \mathbf{F}_{q^\kappa}$ , with  $q = \text{char}(H)$ ; here the elements  $T_1, \dots, T_l$  are algebraically independent over  $H$ , the element  $\eta$  is separable and algebraic over  $H$ , and the element  $\eta$  is separable and algebraic over  $H(T_1, \dots, T_l)$ . We denote the minimal polynomial of  $\eta$  over  $H(T_1, \dots, T_l)$  by

$$\varphi = \sum_{0 \leq i < \deg_Z(\varphi)} (\varphi_i^{(1)} / \varphi^{(2)}) \in H(T_1, \dots, T_l)[Z];$$

its leading coefficient  $\text{lc}_Z(\varphi) = 1$ . Here  $\varphi_i^{(1)}, \varphi^{(2)} \in H[T_1, \dots, T_l]$  and the degree of  $\varphi^{(2)}$  is the least possible. Every polynomial  $f \in F[X_0, \dots, X_n]$  may be uniquely represented in the form

$$f = \sum_{0 \leq i < \deg_Z(\varphi; i_0, \dots, i_n)} (a_{i, i_0, \dots, i_n} / b) \eta^i X_0^{i_0} \dots X_n^{i_n},$$

where  $a_{i, i_0, \dots, i_n}, b \in H[T_1, \dots, T_l]$  and the degree of  $b$  is the least possible. We set

$$\deg_{T_1, \dots, T_l}(f) = \max_{i, i_0, \dots, i_n} \{ \deg_{T_1, \dots, T_l}(a_{i, i_0, \dots, i_n}), \deg_{T_1, \dots, T_l}(b) \}.$$

By the length of a notation  $l(h)$  in the case  $h \in \mathbf{Q}$  we mean its bit length, and in the case  $h \in \mathbf{F}_{q^\kappa}$ , the number  $\kappa \log_2 q$ . By the length of a notation  $l(f)$  for the coefficients of the polynomials  $f$  from the field  $H$ , we mean the maximum length of a notation for the coefficients in  $H$  of the polynomials  $a_{i, i_0, \dots, i_n}$  and  $b$  at monomials in the variables  $T_1, \dots, T_l$ . We define  $l(\varphi)$  similarly.

Below we will suppose in the formulation of Theorem 1 that as input the algorithm is given homogeneous polynomials  $f_0, \dots, f_k \in F[X_0, \dots, X_n]$  (we may suppose without loss of generality that  $f_0, \dots, f_k$  are linearly independent). Let

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

$l(\varphi) \leq M_1$ , and  $l(f_i) \leq M_2$  for all  $0 \leq i \leq k$ . Below, by the size  $\mathcal{L}(f_i)$  we will mean the quantity  $\binom{d+n}{n} d_1 d_2^l M_2$ , and similarly  $\mathcal{L}(\varphi) = d_1^{l+1} M_1$ ; that is, the size of a polynomial is defined as the size of its vector of coefficients.

We denote by  $\{f_0 = \dots = f_k = 0\} \subset \mathbf{P}^n(\bar{F})$  the variety of common roots of the polynomials  $f_0, \dots, f_k$ . The variety  $\{f_0 = \dots = f_k = 0\}$  may be decomposed into components as  $\bigcup_\alpha W_\alpha$ , where the components  $W_\alpha$  are defined and irreducible over the maximal purely inseparable extension  $F^{q^{-\infty}}$  of the field  $F$  [11]. The algorithm of Theorem 1 below finds all  $W_\alpha$  (in fact,  $W_\alpha$  is defined over some finite purely inseparable extension

of the field  $F$ , which the algorithm also finds). We will represent the components  $W_\alpha$  in two ways: by a generic point [11] or by giving some system of equations whose common roots constitute the given component; in the latter case we will say that the system of equations gives the component.

We will use the notation  $g_1 \leq g_2 \mathcal{P}(h_1, \dots, h_s)$  below, where  $g_1, g_2$ , and  $h_1, \dots, h_s$  are functions, to mean that  $g_1 \leq g_2 P(h_1, \dots, h_s)$  for a suitable polynomial  $P$ .

Let  $W$  be a projective subvariety of  $\mathbf{P}^n(\overline{F})$  of codimension  $m$ , defined and irreducible over some field  $F_1$  which is a finite extension of  $F$ , and let  $F_2$  be the maximal subfield of  $F_1$  which is a separable extension of  $F$ . Let  $t_1, \dots, t_{n-m}$  be algebraically independent over  $F$ . A generic point of variety  $W$  may be given by the following isomorphism of fields:

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

for some  $q^\nu$  and  $0 \leq j_0 \leq n$ , where  $\theta$  is an algebraic separable element over the field  $F_2(t_1, \dots, t_{n-m})$ , and  $\Phi(Z)$  is its minimal polynomial, with  $lc_Z(\Phi) = 1$ . The elements  $X_j/X_{j_0}$  are regarded as rational functions on the variety  $W$  here, where  $W$  is not contained in the hyperplane defined by the equation  $X_{j_0} = 0$ . Under the isomorphism (2) the element  $X_j/X_{j_0}$  is taken to the element  $t_i$ ,  $1 \leq i \leq n - m$ . Here and in the sequel we observe the convention that  $q^\nu \geq 1$  for  $q > 0$  and  $q^\nu = 1$  if  $q = 0$ . The algorithm presents a generic point of the variety  $W$  by giving the images of the rational functions  $(X_j/X_{j_0})^{q^\nu}$  in the field  $F_2(t_1, \dots, t_{n-m})[\theta]$  under the action of the isomorphism (2).

In the statement of the theorem below some component  $W_\alpha$  of the variety  $\{f_0 = \dots = f_k = 0\}$  is considered. We will use the following notation for a generic point of the component  $W_\alpha$  (cf. (2)) in the statement of the theorem:  $m = \text{codim } W_\alpha$ ,  $\theta_\alpha = \theta$ ,  $\Phi_\alpha = \Phi$ , and the remaining notation will be as in the isomorphism (2).

**THEOREM 1** [9], [10]. *An algorithm can be proposed which determines a generic point for each component  $W_\alpha$  and constructs a certain family of homogenous polynomials  $\Psi_1^{(\alpha)}, \dots, \Psi_p^{(\alpha)} \in F[X_0, \dots, X_n]$ , such that  $W_\alpha = \{\Psi_1^{(\alpha)} = \dots = \Psi_p^{(\alpha)} = 0\}$ . Further, the algorithm represents each polynomial  $\Psi_i^{(\alpha)}$  in the form  $\Psi_i^{(\alpha)} = \overline{\Psi_i^{(\alpha)}}(\overline{Z}_{i,0}, \dots, \overline{Z}_{i,n-m+2})$ , where the  $\overline{Z}_{i,\beta}$  are linear forms in  $X_0, \dots, X_n$  with coefficients from the field  $H$ . The following bounds hold for the elements constructed:*

$$\begin{aligned} q^\nu &\leq d^{2m}, & \deg_Z \Phi_\alpha &\leq \deg W_\alpha \leq d^m, & p &\leq m^2 d^{4m}, \\ \deg_{T_1, \dots, T_1, t_1, \dots, t_{n-m}}(\Phi_\alpha), \deg_{T_1, \dots, T_1, t_1, \dots, t_{n-m}}((X_j/X_{j_0})^{q^\nu}) &\leq d_2 \mathcal{P}(d^m, d_1), \\ l(\Phi_\alpha), l((X_j/X_{j_0})^{q^\nu}) &\leq (M_1 + M_2 + (n+l)d_2) \mathcal{P}(d^m, d_1), \\ \deg_{X_0, \dots, X_n}(\Psi_i^{(\alpha)}) &\leq d^{2m}, & \deg_{T_1, \dots, T_1}(\Psi_i^{(\alpha)}) &\leq d_2 \mathcal{P}(d^m, d_1), \\ l(\overline{\Psi_i^{(\alpha)}}) &\leq (M_1 + M_2 + (n+l)d_2) \mathcal{P}(d^m, d_1), & \mathcal{L}(\overline{Z}_{i,\beta}) &\leq \mathcal{P}(n, \log(dd_1 d_2)) \end{aligned}$$

for all  $1 \leq i \leq p$ ,  $0 \leq j \leq n$ , and  $0 \leq \beta \leq n - m + 2$ .

The total execution time of the algorithm for the construction of generic points and for producing systems of equations for all components  $W_\alpha$  is bounded above by a certain polynomial in  $M_1 M_2 (d^n d_1 d_2)^{n+l} (q+1)$ .

Below we will use the following remark due to A. L. Chistov, whose proof may be found in [10], Chapter II, §2.

REMARK. If a generic point is given for a certain component  $W_\alpha$  (with bounds on its parameters, as in Theorem 1), which is the closure  $W_\alpha = \overline{\pi'(V_1)}$  under projection  $\pi': \mathbf{P}^n \rightarrow \mathbf{P}^m$ , where  $\pi'(X_0 : \dots : X_n) = (X_0 : \dots : X_m)$ , of a suitable component  $V_1$  of the variety  $\{f_0 = \dots = f_k = 0\} \subset \mathbf{P}^n$ , then it is possible to construct a family of equations in the time specified in the theorem, with the same bounds on its parameters as for the family  $\{\Psi_s^{(\alpha)}\}$ , which gives  $W_\alpha$ .

We will now describe an important auxiliary construction from [12], which will be used below in §2. Let  $g_0, \dots, g_{k-1} \in F[X_0, \dots, X_n]$  be homogeneous polynomials of degrees  $\delta_0 \geq \dots \geq \delta_{k-1}$  respectively. We introduce new variables  $u_0, \dots, u_n$  which are algebraically independent over  $F(X_0, \dots, X_n)$ . We set

$$g_k = X_0 u_0 + \dots + X_n u_n \in F(u_0, \dots, u_n)[X_0, \dots, X_n]$$

and  $D = \sum_{0 \leq i \leq n} \delta_i - n$ ; here  $\delta_k = \dots = \delta_n = 1$  if  $k \leq n$ . We consider the linear mapping  $\mathfrak{A}: \mathcal{B}_0 \oplus \dots \oplus \mathcal{B}_k \rightarrow \mathcal{B}$  over  $F(u_0, \dots, u_n)$ , where the  $\mathcal{B}_i$  (respectively  $\mathcal{B}$ ) are the spaces of homogeneous polynomials in  $X_0, \dots, X_n$  of degree  $D - \delta_i$  (respectively  $D$ ) for  $0 \leq i \leq k$ , defined by

$$\mathfrak{A}(b_0, \dots, b_k) = \sum_{0 \leq i \leq k} b_i g_i.$$

Any element  $b = (b_0, \dots, b_k) \in \mathcal{B}_0 \oplus \dots \oplus \mathcal{B}_k$  can be expressed in the form

$$b = (b_{0,1}, \dots, b_{0,\rho_0}, b_{1,1}, \dots, b_{1,\rho_1}, \dots, b_{k,1}, \dots, b_{k,\rho_k})$$

where  $\rho_i = \binom{n+D-\delta_i}{n}$  and  $b_{i,1}, \dots, b_{i,\rho_i}$  are the coefficients of the polynomial  $b_i$ , under the condition that some indexing of the monomials of degree  $D - \delta_i$  is fixed. The elements of the space  $\mathcal{B}$  may be similarly represented. With respect to the chosen coordinates the mapping  $\mathfrak{A}$  has a matrix  $A$  of order

$$\binom{n+D}{n} \times \left( \sum_{0 \leq i \leq k} \rho_i \right).$$

The matrix  $A$  may be represented in the form  $A = (A', A'')$ , where  $A'$  (which we call the numerical portion of  $A$ ) contains  $\sum_{0 \leq i \leq k-1} \rho_i$  columns,  $A''$  (we call it the formal part of  $A$ ) contains  $\rho_k$  columns, and furthermore the elements of  $A'$  lie in  $F$ , while the elements of  $A''$  are linear forms over  $F$  in the variables  $u_0, \dots, u_n$  (cf. also [13]).

THEOREM 2 [12]. 1) The system  $g_0 = \dots = g_{k-1} = 0$  has a finite number of solutions in  $\mathbf{P}^n(\overline{F})$  if and only if the rank of  $A$  is  $\binom{n+D}{n}$  (we write  $r = \binom{n+D}{n}$ ).

2) All  $r \times r$  minors of  $A$  generate a principal ideal, whose generator  $R$  is their greatest common divisor.

3) The form  $R$ , homogeneous with respect to the variables  $u_0, \dots, u_n$ , factors as a product  $R = \prod_{1 \leq i \leq D_1} L_i$ , where  $L_i = \sum_{0 \leq j \leq n} \xi_j^{(i)} u_j$  is a linear form with coefficients from  $\overline{F}$ , and in addition  $(\xi_0^{(i)} : \dots : \xi_n^{(i)})$  is a root of the system and the number of occurrences of forms proportional to  $L$  in the product equals the multiplicity of corresponding root  $(\xi_0^{(i)} : \dots : \xi_n^{(i)})$  of the system ( $1 \leq i \leq D_1$ ). Furthermore,  $\deg R = D_1 = r - \text{rank}(A')$ .

For  $k = n$  the polynomial  $R$  is the  $u$ -resultant of the system  $g_0 = \dots = g_{n-1} = 0$ .

### §2. The construction of the projection of a variety

Let an initial formula

$$\exists X_1 \dots \exists X_s (\&_{1 \leq j \leq k-1} (f_j = 0) \& g \neq 0)$$

be given, where the parameters (the degrees and the lengths of the notation) of the polynomials  $f_i, g \in F[Z_1, \dots, Z_{n-s}, X_1, \dots, X_s]$  satisfy the same bounds as the parameters of the polynomials  $f_i$  in §1. The algorithm described in the present section constructs a quantifier-free formula equivalent to the initial one, of the form

$$\bigvee_{1 \leq i \leq N_1} \left( \&_{1 \leq j \leq k_i} (f_{ij}^{(1)} = 0) \& (g_i^{(1)} \neq 0) \right)$$

for suitable  $f_{ij}^{(1)}, g_i^{(1)} \in F[Z_1, \dots, Z_{n-s}]$ ; that is, the algorithm carries out the projection of the variety. We remark that formulas are equivalent if and only if they define the same constructible set in affine space  $\mathbf{A}^{n-s}(\bar{F})$ .

We introduce the homogeneous polynomials

$$\begin{aligned} \bar{f}_j(X_0, \dots, X_{s+1}) &= X_0^{\deg_{X_1, \dots, X_s}(f_j)} f_j(Z_1, \dots, Z_{n-s}, X_1/X_0, \dots, X_s/X_0), \\ \bar{g}(X_0, \dots, X_{s+1}) &= X_0^{\deg_{X_1, \dots, X_s}(g)} g(Z_1, \dots, Z_{n-s}, X_1/X_0, \dots, X_s/X_0), \\ \bar{f}_0 &= X_{s+1}\bar{g} - X_0^{1+\deg_{X_0, \dots, X_s}(\bar{g})}. \end{aligned}$$

We may suppose without loss of generality that  $\deg_{X_0, \dots, X_{s+1}}(\bar{f}_j) = d-1$  for  $0 \leq j \leq k-1$ , replacing the  $\bar{f}_j$  if necessary by the family of polynomials  $\{\bar{f}_j X_i^{d-1-\deg \bar{f}_j}\}_{0 \leq i \leq s+1}$ . The initial formula is equivalent to

$$\exists X_0 \exists X_1 \dots \exists X_s \exists X_{s+1} \left( \&_{0 \leq i \leq k-1} (\bar{f}_i = 0) \& (X_0 \neq 0) \right).$$

Then the projection  $\prod \subseteq \mathbf{A}^{n-s}(\bar{F})$ , which it is necessary to construct, consists of all those points  $(z_1, \dots, z_{n-s})$  for which the last formula is satisfied.

We introduce the variety

$$U = \{(z_1, \dots, z_{n-s}; (x_0 : \dots : x_{s+1})) \in (\mathbf{A}^{n-s} \times \mathbf{P}^{s+1})(\bar{F}) : \&_{0 \leq j \leq k-1} \bar{f}_j = 0\}$$

and the natural linear projection  $\pi: \mathbf{A}^{n-s} \times \mathbf{P}^{s+1} \rightarrow \mathbf{A}^{n-s}$ ; then the desired constructible set is  $\prod = \pi(U \cap \{X_0 \neq 0\})$ . Furthermore for each point  $z = (z_1, \dots, z_{n-s}) \in \mathbf{A}^{n-s}(\bar{F})$  we consider the variety (fiber)  $U_z = \pi^{-1}(z) \cap U \subseteq \{z\} \times \mathbf{P}^{s+1}(\bar{F}) \simeq \mathbf{P}^{s+1}(\bar{F})$ . The condition  $z \in \pi(U \cap \{X_0 \neq 0\})$  is equivalent to the existence for some  $m, 0 \leq m \leq s+1$ , in the fiber  $U_z$  of at least one component  $W$  of dimension  $s+1-m$  not lying at infinity; that is,  $W \not\subseteq \{X_0 = 0\}$ .

In the following discussion we will temporarily fix a point  $z \in \mathbf{A}^{n-s}$  and an index  $m$ .

We suppose below that the field  $H$ , if finite, contains enough elements, extending  $H$  if necessary. We set  $N' = ((k-1)(d-1)^{m+1} + 1)$ , and we suppose the nonzero elements  $\gamma_1, \dots, \gamma_{N'} \in H$  are distinct. Then clearly the family of  $N'$  vectors

$$\{v^{(i)} = (v_0^{(i)}, \dots, v_{k-1}^{(i)}) = (\gamma_i^0, \dots, \gamma_i^{k-1}) \in H^k\}_{1 \leq i \leq N'}$$

enjoys the property that any  $k$  of them are linearly independent (cf. Lemma 2.1 of [9]). We write

$$h_i = h_i(Z_1, \dots, Z_{n-s}) = \sum_{0 \leq j \leq k-1} v_j^{(i)} \bar{f}_j,$$

then  $h_i(z) \in \bar{F}[X_0, \dots, X_{s+1}]$ , and here the coordinates of the point  $z$  are substituted for the variables  $Z_1, \dots, Z_{n-s}$ .

We show by induction on  $0 \leq \beta \leq m$  (cf. [9], Chapter II, §3) that for suitable indices  $1 \leq i_1, \dots, i_\beta \leq N'$ , every component of codimension less than  $\beta$  of the variety  $\{h_{i_1}(z) = \dots = h_{i_\beta}(z) = 0\} \subset \mathbf{P}^{s+1}$  is simultaneously a component of the fiber  $U_z$ . We assume that the existence of indices  $i_1, \dots, i_\beta$  has already been shown, with  $\beta \leq m-1$ , and

we suppose that there is no index  $1 \leq i_{\beta+1} \leq N'$  with the desired property. If some component  $W_1$  of the variety  $\{h_{i_1}(z) = \dots = h_{i_\beta}(z) = 0\}$  is not a component of  $U_z$  (thus  $\text{codim } W_1 = \beta$ ), then there are no more than  $k - 1$  indices  $1 \leq i \leq N'$  for which the polynomial  $h_i(z)$  vanishes on the component  $W_1$ , in view of the property of the vectors  $v^{(1)}, \dots, v^{(N')}$ . By Bézout's inequality [14], there are at most  $(d - 1)^\beta$  components in the variety  $\{h_{i_1}(z) = \dots = h_{i_\beta}(z) = 0\}$ . Consequently there is an index  $1 \leq i_{\beta+1} \leq N'$  for which the polynomial  $h_{i_{\beta+1}}(z)$  is not identically zero on each component  $W_1$  of the variety  $\{H_{i_1}(z) = \dots = h_{i_\beta}(z) = 0\}$  which is not a component of the fiber  $U_z$ , which leads to a contradiction. Hence the existence of a suitable component  $W$  of the fiber  $U_z$  (see above) is equivalent to the existence of indices  $1 \leq i_1 < \dots < i_m \leq N'$  for which  $W$  is a component of the variety  $\{h_{i_1}(z) = \dots = h_{i_m}(z) = 0\}$  (not lying at infinity).

We will now construct a family  $\mathfrak{M} = \mathfrak{M}_{s,s-m,(d-1)^m}$  (see [9], Chapter II, §1) consisting of  $(s-m+1)$ -tuples of linear forms in the variables  $X_1, \dots, X_{s+1}$  with coefficients from  $H$ , enjoying the property that for every variety  $W_2 \subset \mathbf{P}^s(\overline{F})$  (here the coordinates in  $\mathbf{P}^s$  are  $(X_1 : \dots : X_{s+1})$ ) for which  $\dim W_2 \leq s-m$  and  $\deg W_2 \leq (d-1)^m$ , there is an  $(s-m+1)$ -tuple  $(Y_1, \dots, Y_{s-m+1}) \in \mathfrak{M}$  satisfying the condition  $W_2 \cap \{Y_1 = \dots = Y_{s-m+1} = 0\} = \emptyset$ . For the construction, as above, we consider a family of  $N'' = s(d-1)^m + 1$  vectors  $v^{(1)}, \dots, v^{(N'')} \in H^{s+1}$ , and  $s+1$  of which are linearly independent. For each  $1 \leq i \leq N''$  we define the linear form  $Y^{(i)} = \sum_{1 \leq j \leq s+1} v_j^{(i)} X_j$ , and we take for  $\mathfrak{M}$  the family of all possible  $(s-m+1)$ -tuples of the linear forms  $Y^{(1)}, \dots, Y^{(N'')}$ . The required property of the family  $\mathfrak{M}$  is verified similarly to the property of the polynomials  $h_1(z), \dots, h_{N'}(z')$  (see above).

We take as  $W_2$  the variety  $W \cap \{X_0 = 0\}$ . We extend the sequence of linear forms  $Y_0 = X_0, Y_1, \dots, Y_{s-m+1}$  to a basis  $Y_0, \dots, Y_{s+1}$  for the space of linear forms in  $X_0, \dots, X_{s+1}$  with coefficients in  $H$ . We make a change of variables under which  $\hat{h}_i(z) (Y_0, \dots, Y_{s+1}) = h_i(z)$ . As a result the assertion under consideration concerning the existence of  $W$  is equivalent to the existence for some  $0 \leq m \leq s+1$  of indices  $1 \leq i_1 < \dots < i_m \leq N'$  and linear forms  $(Y_1, \dots, Y_{s-m+1}) \in \mathfrak{M}$  for which the variety

$$\{\hat{h}_{i_1}(z)(Y_0, 0, \dots, 0, Y_{s-m+2}, \dots, Y_{s+1}) = \dots = \hat{h}_{i_m}(z)(Y_0, 0, \dots, 0, Y_{s-m+2}, \dots, Y_{s+1}) = 0\} \subset \mathbf{P}^m(\overline{F})$$

has as one of its components a point  $\hat{\Omega} = (\xi_0 : \xi_{s-m+2} : \dots : \xi_{s+1})$  such that

$$\Omega = (z, (\xi_0 : 0 : \dots : 0 : \xi_{s-m+2} : \dots : \xi_{s+1})) \in U_Z \cap \{Y_0 \neq 0\},$$

by the theorem on the dimension of an intersection [14] ( $\dim W$  is not fixed in the context of this equivalence).

We consider the system of equations

$$g_{i_j} = \hat{h}_{i_j}(z)(Y_0, 0, \dots, 0, Y_{s-m+2}, \dots, Y_{s+1}) - Y Y_{s-m+j+1}^{d-1} = 0, \quad 1 \leq j \leq m, \quad (3)$$

in the variables  $Y_0, Y_{s-m+2}, \dots, Y_{s+1}$  with coefficients from  $\overline{F}[Y] \subset K = \overline{F}(Y)$ , where  $Y$  is algebraically independent over  $F$ . From Lemma 2.1 of [10] it follows that system (3) has a (nonempty) finite set of roots in  $\mathbf{P}^m(\overline{K})$ . The minimal prime ideals

$$\mathfrak{p}_K \subset K^{q-\infty}[Y_0, Y_{s-m+2}, \dots, Y_{s+1}]/(g_{i_1}, \dots, g_{i_m})$$

correspond bijectively to classes  $V_{\mathfrak{p}_K} \subset \mathbf{P}^n(\overline{K})$  of roots of the system (3) which are conjugate over  $K^{q-\infty}$ . On the other hand, they correspond bijectively to those minimal prime ideals

$$\mathfrak{p}_F \subset \overline{F}[Y, Y_0, Y_{s-m+2}, \dots, Y_{s+1}]/(g_{i_1}, \dots, g_{i_m}),$$

which do not intersect the multiplicatively closed subset

$$\overline{F}[Y] \setminus (0) \subset \overline{F}[Y, Y_0, Y_{s-m+2}, \dots, Y_{s+1}] / (g_{i_1}, \dots, g_{i_m})$$

(see Lemma 2.2 of [10]).

We may also consider (3) as a system of equations in the variables  $Y, Y_0, Y_{s-m+2}, \dots, Y_{s+1}$  with coefficients from  $\overline{F}$ , which gives a variety  $U_z^{(F)} \subset \mathbf{A}^{m+2}(\overline{F})$ . The ideals  $\mathfrak{p}_F$  correspond bijectively to components  $V_{\mathfrak{p}_F}$  of the variety  $U_z^{(F)}$ , which do not lie in any finite union of hyperplanes of the form  $\{Y - \omega = 0\} \subset \mathbf{A}^{m+2}(\overline{F})$ , where  $\omega \in \overline{F}$ ; we remark that  $\dim V_{\mathfrak{p}_F} = 2$  (see Lemma 2.2 of [10]).

The algorithm constructs a matrix  $A$  with coefficients from the ring  $F[Y, Z_1, \dots, Z_{m-s}, U_0, U_{s-m+2}, \dots, U_{s+1}]$  corresponding to system (3), in which the polynomials  $\hat{h}_{i_j}(Z_1, \dots, Z_{m-s})$  are considered in place of the polynomials  $\hat{h}_{i_j}(z)$ , according to the construction sketched at the end of §1. The matrix  $A_z$  is obtained by substitution of the coordinates of the point  $z$  in the matrix  $A$ . Suppose the polynomial  $R_z \in \overline{F}[Y, U_0, U_{s-m+2}, \dots, U_{s+1}]$  corresponds to the matrix  $A_z$ , as in Theorem 2. We may assume without loss of generality that  $Y \nmid R_z$  (dividing  $R_z$  by the greatest possible power of the variable  $Y$ ).

We consider a representation

$$\bigcup_{\mathfrak{p}_F} V_{\mathfrak{p}_F} = \{\chi_0 = \dots = \chi_{k_1} = 0\},$$

where  $\chi_i \in \overline{F}[Y, Y_0, Y_{s-m+2}, \dots, Y_{s+1}]$ , with the polynomials  $\chi_i$  homogeneous in the variables  $Y_0, Y_{s-m+2}, \dots, Y_{s+1}$ . It is shown in Lemma 2.6 of [10] that for the system  $\chi_i(0, Y_0, Y_{s-m+2}, \dots, Y_{s+1}) = 0, 0 \leq i \leq k$ , taking Theorem 2 into account, we have  $R_z(0, U_0, U_{s-m+2}, \dots, U_{s+1}) = \prod_i L_i^{c_i}$ , and further the linear forms  $L_i = \sum_j \xi_j^{(i)} U_j$  correspond bijectively to points  $(\xi_0^{(i)} : \xi_{s-m+2}^{(i)} : \dots : \xi_{s+1}^{(i)}) \in W'_z \subset \mathbf{P}^m$ , where

$$\text{cone}(W'_z) = \left( \bigcup_{\mathfrak{p}_F} V_{\mathfrak{p}_F} \right) \cap \{Y = 0\}.$$

From Lemma 2.3 of [10] it follows that the point  $\tilde{\Omega} \in W'_z$ .

Thus in the notation introduced above we have established the following fact.

LEMMA 1. *The formula*

$$\exists X_1 \dots \exists X_s \left( \&_{1 \leq j \leq k-1} (f_j = 0) \& (g \neq 0) \right)$$

is valid at the point  $z \in \overline{F}^{n-s}$  if and only if for some  $0 \leq m \leq s+1$  there are indices  $1 \leq i_1 < \dots < i_m \leq N'$ , a sequence of linear forms  $(Y_1, \dots, Y_{s-m+1}) \in \mathfrak{M}$ , and a point  $\Omega \in U_z \cap \{X_0 \neq 0\}$ , where  $\Omega = (z, (\xi_0 : 0 : \dots : 0 : \xi_{s-m+2} : \dots : \xi_{s+1}))$  in coordinates  $z, (Y_0 : \dots : Y_{s+1})$ , such that the linear form  $(\xi_0 U_0 + \xi_{s-m+2} U_{s-m+2} + \dots + \xi_{s+1} U_{s+1})$  divides  $R_z(0, U_0, U_{s-m+2}, \dots, U_{s+1})$ , where the polynomials  $R_z$  corresponds to the system (3) according to Theorem 2 of §1.

Furthermore, we specify a variant we shall need of the Gaussian algorithm for reduction of matrices by means of elementary row transformations to generalized row echelon form. A variant of the Gauss algorithm for  $m_1 \times n_1$  matrices is defined as a sequence of pairs of indices  $(i_0, j_0), \dots, (i_\lambda, j_\lambda)$  with  $i_\mu \leq m_1, j_\mu \leq n_1$ . Here  $i_\alpha \neq i_\beta$  and  $j_\alpha \neq j_\beta$  if  $\alpha \neq \beta$ . For each initial  $m_1 \times n_1$  matrix  $A^{(0)}$  this sequence produces a chain of  $m_1 \times n_1$  matrices  $A^{(0)}, \dots, A^{(\lambda+1)}$ . We introduce the notation  $A^{(\alpha)} = (a_{ij}^{(\alpha)})$ , where the leading entry  $a_{i_\alpha, j_\alpha}^{(\alpha)} \neq 0$  and the  $i$ th row of the matrix  $A^{(\alpha+1)}$  is obtained from the  $i$ th row of

$A^{(\alpha)}$  by adding to it the  $i_\alpha$ th row of  $A^{(\alpha)}$  multiplied by  $a_{i,j_\alpha}^{(\alpha)}/a_{i_\alpha,j_\alpha}^{(\alpha)}$  for all  $i$  different from  $i_0, \dots, i_\alpha$ ; the rows with indices  $i_0, \dots, i_\alpha$  are not changed. The matrix  $A^{(\lambda+1)}$  has generalized row echelon form; in other words,  $a_{i,j}^{(\lambda+1)} = 0$  if either  $i$  is different from  $i_0, \dots, i_\lambda$ , or if  $i = i_\alpha, j = j_\beta$ , and  $\alpha > \beta$ ; at the same time  $a_{i_\alpha,j_\alpha}^{(\lambda+1)} = a_{i_\alpha,j_\alpha}^{(\alpha)} \neq 0$ .

We denote by  $\Delta_{i,j}^{(\alpha)}$  the determinant of the  $(\alpha + 1) \times (\alpha + 1)$  submatrix of  $A^{(0)}$  formed by the rows with indices  $i_0, \dots, i_{\alpha-1}, i$  and the columns with indices  $j_0, \dots, j_{\alpha-1}, j$  under the assumption that  $i$  is distinct from all  $i_0, \dots, i_{\alpha-1}$  and that  $j$  is distinct from all  $j_0, \dots, j_{\alpha-1}$ . Then under the preceding hypotheses  $a_{i,j}^{(\alpha)} = \Delta_{i,j}^{(\alpha)} / \Delta_{i_{\alpha-1},j_{\alpha-1}}^{(\alpha-1)}$  (see, for example, [15]).

We now return to the consideration of an arbitrary point  $z \in \mathbf{A}^{n-s}(\overline{F})$ . We temporarily fix  $0 \leq m \leq s + 1$ , indices  $1 \leq i_1 < \dots < i_m \leq N'$ , and a sequence of linear forms  $(Y_1, \dots, Y_{s-m+1}) \in \mathfrak{M}$  (see Lemma 1). We recall that  $r$  is the number of rows in the matrix  $A$  (cf. Theorem 2).

We will construct a certain sequence of variants of the Gauss algorithm  $\Gamma_1, \Gamma_2, \dots$  over the field  $F(Y, Z_1, \dots, Z_{n-s}, U_0, U_{s-m+2}, \dots, U_{s+1})$  and a sequence of polynomials  $P_1, P_2, \dots \in F[Y, Z_1, \dots, Z_{n-s}, U_0, U_{s-m+2}, \dots, U_{s+1}]$  so that application of the algorithm  $\Gamma_i$  to the matrix  $A_z$  is well defined (that is, pivots are nonzero) for all points  $z = (z_1, \dots, z_{n-s})$  (possibly empty) of the quasiprojective variety [14]  $\mathcal{W}_i \subset \mathbf{A}^{n-s}$  which is defined by the following conditions: the inequality

$$0 \neq P_i(Y, z_1, \dots, z_{n-s}, U_0, U_{s-m+2}, \dots, U_{s+1}) \in \overline{F}[Y, U_0, U_{s-m+2}, \dots, U_{s+1}]$$

holds, and also the equalities

$$0 = P_j(Y, z_1, \dots, z_{n-s}, U_0, U_{s-m+2}, \dots, U_{s+1})$$

for  $1 \leq j \leq i - 1$ . In addition, the variety

$$\{(z_1, \dots, z_{n-s}) : P_i(Y, z_1, \dots, z_{n-s}, U_0, U_{s-m+2}, \dots, U_{s+1}) = 0 \text{ for all } i\}$$

is empty, or in other words  $\bigcup_i \mathcal{W}_i = \mathbf{A}^{n-s}$ .

We apply the Gauss algorithms  $\Gamma_1, \Gamma_2, \dots$  to the matrix  $A$  below. We take as  $\Gamma_1$  any variant of the Gauss algorithm. Let the polynomial

$$P_1 = \prod_{0 \leq \alpha \leq \lambda_1} \Delta_{i_\alpha, j_\alpha}^{(\alpha)},$$

and see below for  $P_i$  (we use the notation introduced above for the Gauss algorithm under consideration at each given step). We suppose now that  $\Gamma_1, \dots, \Gamma_{i-1}$  and  $P_1, \dots, P_{i-1}$  have already been constructed. Then we take as  $\Gamma_i$  a variant of the Gauss algorithm in which for each  $0 \leq \alpha \leq \lambda_i$  the index of the pivotal column  $j_\alpha$  of the matrix  $A^{(\alpha)}$  is the least possible, and furthermore, such that  $j_\alpha > j_{\alpha-1}$  and the polynomials  $P_1, \dots, P_{i-1}$  and  $\prod_{0 \leq \beta \leq \alpha} \Delta_{i_\beta, j_\beta}^{(\beta)}$  are linearly independent over  $F$ . Finally, we set

$$P_i = \prod_{0 \leq \alpha \leq \lambda_i} \Delta_{i_\alpha, j_\alpha}^{(\alpha)}.$$

The process of constructing the Gauss algorithms  $\Gamma_1, \Gamma_2, \dots$  is terminated when no  $\Gamma_i$  can be constructed satisfying the conditions formulated above.

It is not hard to conclude on the basis of Theorem 2 that if  $\mathcal{W}_i \neq \emptyset$ , then for every  $z \in \mathcal{W}_i$  the polynomial  $R_z$  is obtained as the value at the point  $z$  of the polynomial  $\det \Lambda_i$  (up to a factor  $Y^\epsilon$  for suitable  $\epsilon$ ), where the  $r \times r$  submatrix  $\Lambda_i$  of the matrix  $A$  is formed from the columns with indices  $j_0, \dots, j_{r-1}$ , corresponding to the Gauss algorithm  $\Gamma_i$ .

Indeed, in the matrix  $(A^{(\alpha)})_z$  the elements  $a_{\beta j}^{(\alpha)} = 0$  for all  $\beta$  distinct from  $i_0, \dots, i_{\alpha-1}$ , and  $j < j_\alpha$ , in view of the choice of  $j_\alpha$ . Therefore if  $\alpha$  is such that the  $(i_{\alpha-1}, \dots, j_{\alpha-1})$  entry is found in the numerical portion  $A'$  of the matrix  $A$  (recall that  $A = (A', A'')$ ), and the  $(i_\alpha, j_\alpha)$  entry is found in the formal portion  $A''$ , then  $\text{rank}((A')_z) = \alpha$ , from which the required representation of the polynomial  $R_z$  follows. We remark that if  $\lambda_i < r - 1$  then  $\mathcal{W}_i = \emptyset$  (see (3) and Theorem 2).

We write

$$\det \Lambda_i = \sum_{\varepsilon} \Lambda_i^{(\varepsilon)} Y^\varepsilon,$$

where  $\Lambda_i^{(\varepsilon)}(Z_1, \dots, Z_{n-s}) \in F[Z_1, \dots, Z_{n-s}, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}]$ . We consider the quasiprojective varieties

$$\mathcal{W}_i^{(\varepsilon)} = \{(z_1, \dots, z_{n-s}) \in \mathcal{W}_i : \Lambda_i^{(j)}(z_1, \dots, z_{n-s}) = 0, \\ 0 \leq j \leq \varepsilon - 1; \Lambda_i^{(\varepsilon)}(z_1, \dots, z_{n-s}) \neq 0\}$$

for  $\varepsilon \geq 0$ . The variety  $\mathcal{W}_i^{(\varepsilon)}$  is quasiprojective, as the intersection of two quasiprojective varieties; namely, if

$$\Xi^{(j)} = \left\{ \& \mathcal{X}_{\beta} (G_{\beta}^{(j)} = 0) \& \bigvee_{\gamma} (C_{\gamma}^{(j)} \neq 0) \right\}$$

for  $j = 1, 2$ , then

$$\Xi^{(1)} \cap \Xi^{(2)} = \left\{ \& \mathcal{X}_{\beta, \delta} (G_{\beta}^{(1)} = G_{\delta}^{(2)} = 0) \& \bigvee_{\gamma, \kappa} (C_{\gamma}^{(1)} C_{\kappa}^{(2)} \neq 0) \right\}.$$

Furthermore  $\mathcal{W}_i^{(\varepsilon_1)} \cap \mathcal{W}_i^{(\varepsilon_2)} = \emptyset$  for  $\varepsilon_1 \neq \varepsilon_2$  and  $\bigcup_{\varepsilon} \mathcal{W}_i^{(\varepsilon)} = \mathcal{W}_i$ . We have

$$R_z(0, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}) = \Lambda_i^{(\varepsilon)}(z_1, \dots, z_{n-s})$$

for  $z \in \mathcal{W}_i^{(\varepsilon)}$ .

We further represent  $\Lambda_i^{(\varepsilon)}$  in the form

$$\Lambda_i^{(\varepsilon)} = \sum_{0 \leq j \leq D_2} e_i^{(\varepsilon, j)} \mathcal{U}_0^{D_2-j},$$

where  $e_i^{(\varepsilon, j)}(Z_1, \dots, Z_{n-s}) \in F[Z_1, \dots, Z_{n-s}, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}]$ . We introduce the quasiprojective varieties

$$\mathcal{W}_i^{(\varepsilon, j)} = \{(z_1, \dots, z_{n-s}) \in \mathcal{W}_i^{(\varepsilon)} : e_i^{(\varepsilon, \kappa)}(z_1, \dots, z_{n-s}) = 0 \text{ for } 0 \leq \kappa < j \\ \text{and } e_i^{(\varepsilon, j)}(z_1, \dots, z_{n-s}) \neq 0\};$$

then  $\mathcal{W}_i^{(\varepsilon, j_1)} \cap \mathcal{W}_i^{(\varepsilon, j_2)} = \emptyset$  for  $j_1 \neq j_2$ , and  $\bigcup_{0 \leq j \leq D_2} \mathcal{W}_i^{(\varepsilon, j)} = \mathcal{W}_i^{(\varepsilon)}$ . We remark that since

$$(\Lambda_i^{(\varepsilon)})_z = \Lambda_i^{(\varepsilon)}(z_1, \dots, z_{n-s}, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}) = \prod_{\beta} L_{\beta}^{c_{\beta}}$$

is a product of linear forms for  $z \in \mathcal{W}_i^{(\varepsilon)}$ , the relation

$$(e_i^{(\varepsilon, j)})_z = e_i^{(\varepsilon, j)}(z_1, \dots, z_{n-s}) | (\Lambda_i^{(\varepsilon)})_z$$

follows in the ring  $\overline{F}[\mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}]$  for all  $z \in \mathcal{W}_i^{(\varepsilon, j)}$ , since in this case  $(e_i^{(\varepsilon, j)})_z$  is equal to the product of the powers  $L_{\beta}^{c_{\beta}}$  of those linear forms  $L_{\beta}$  whose  $\mathcal{U}_0$ -coefficient is zero.

Our next goal is the computation of the quotient  $(\Lambda_i^{(\varepsilon)})_z / (e_i^{(\varepsilon,j)})_z$  for  $z \in \mathcal{W}_i^{(\varepsilon,j)}$ . We arrange all monomials in the variables  $u_{s-m+2}, \dots, u_{s+1}$  in lexicographic order on their multi-indices in the polynomials  $e_i^{(\varepsilon,j)} = \sum_I \mu_I u^I$ , where  $I = (I_{s-m+2}, \dots, I_{s+1})$  and  $u^I = u_{s-m+2}^{I_{s-m+2}} \cdots u_{s+1}^{I_{s+1}}$ . As usual the lexicographic order  $I < J$  means that for some  $1 \leq \kappa \leq m$  we have  $I_{s-m+2} = J_{s-m+2}, \dots, I_{s-m+\kappa} = J_{s-m+\kappa}$ , and  $I_{s-m+\kappa+1} < J_{s-m+\kappa+1}$ . Let  $I$  be a multi-index (to remain fixed in the considerations below) for which  $0 \neq \mu_I \in F[Z_1, \dots, Z_{n-s}]$ . We introduce the quasiprojective variety

$$\mathcal{W}_{i,I}^{(\varepsilon,j)} = \{(z_1, \dots, z_{n-s}) \in \mathcal{W}_i^{(\varepsilon,j)} : \mu_J(z_1, \dots, z_{n-s}) = 0 \text{ for all } J > I \text{ and } \mu_I(z_1, \dots, z_{n-s}) \neq 0\}.$$

Clearly  $\mathcal{W}_{i,J_1}^{(\varepsilon,j)} \cap \mathcal{W}_{i,J_2}^{(\varepsilon,j)} = \emptyset$  for  $J_1 \neq J_2$ , and  $\bigcup_J \mathcal{W}_{i,J}^{(\varepsilon,j)} = \mathcal{W}_i^{(\varepsilon,j)}$ . For all points  $(z_1, \dots, z_{n-s}) \in \mathcal{W}_{i,I}^{(\varepsilon,j)}$  the quotient  $(\Lambda_i^{(\varepsilon)})_z / (e_i^{(\varepsilon,j)})_z$  is obtained with the help of the division process described below, and the subsequent substitution of the coordinates  $z_1, \dots, z_{n-s}$  for the variables  $Z_1, \dots, Z_{n-s}$ .

Let

$$0 \neq \Psi \in F(Z_1, \dots, Z_{n-s})[u_{s-m+2}, \dots, u_{s+1}].$$

We introduce the notation  $\bar{\Psi} = \Psi(u_{s-m+2}^m, u_{s-m+3}^{m-1}, \dots, u_{s+1})$  and  $\partial(\Psi) = \text{deg}(\bar{\Psi})$ . We set

$$\tilde{e}_i^{(\varepsilon,j)} = e_i^{(\varepsilon,j)} - \sum_{J \neq I; \partial(u^J) \geq \partial(u^I)} \mu_J u^J.$$

Then  $\tilde{e}_i^{(\varepsilon,j)}_z = (e_i^{(\varepsilon,j)})_z$  for all points  $z \in \mathcal{W}_{i,I}^{(\varepsilon,j)}$ , bearing in mind that  $(e_{ii}^{(\varepsilon,j)})_z$  is the product of the linear forms whose highest monomials (in the sense of the lexicographic ordering) are  $(\mu_I)_z u^I$ , and consequently for every other nonzero monomial  $(\mu_J)_z u^J$  in the polynomial  $(e_i^{(\varepsilon,j)})_z$  we have  $\partial(u^J) < \partial(u^I)$ . We temporarily fix an index  $j < \kappa \leq D_2$ . The algorithm constructs a sequence of nonzero polynomials  $\Psi_0 = e_i^{(\varepsilon,\kappa)}, \Psi_1, \dots, \Psi_\rho \in F[Z_1, \dots, Z_{n-s}, u_{s-m+2}, \dots, u_{s+1}]$ . For every  $0 \leq \tau \leq \rho$  we may represent  $\Psi_\tau$  uniquely as  $\Psi_{\tau,1} + \Psi_{\tau,2} + \Psi_{\tau,3}$ , where the polynomials  $\bar{\Psi}_{\tau,1}$  and  $\bar{\Psi}_{\tau,2}$  are homogeneous with respect to the variables  $u_{s-m+2}, \dots, u_{s+1}$ , and further  $\partial(\Psi_{\tau,3}) < \partial(\Psi) = \partial(\Psi_{\tau,1}) = \partial(\Psi_{\tau,2})$ ; moreover, the quotient

$$\Psi_{\tau,1} / u^I \in F(Z_1, \dots, Z_{n-s}, u_{s-m+2}, \dots, u_{s+1});$$

finally, no nonzero monomial of the polynomial  $\Psi_{\tau,2}$  is divisible by  $u^I$ . We set

$$\Psi_{\tau+1} = \mu_I(\Psi_\tau - \Psi_{\tau,2}) - \Psi_{\tau,1} \tilde{e}_i^{(\varepsilon,j)} / u^I,$$

where  $\Psi_{\rho+1} = 0$ . Clearly  $\partial(\Psi_{\tau+1}) < \partial(\Psi_\tau)$ . We consider the polynomial

$$\Psi_{i,I}^{(\varepsilon,j,\kappa)} = \sum_{0 \leq \tau \leq \rho} \Psi_{\tau,1} \mu_I^{\rho-\tau} / u^I$$

and we write

$$\Psi_{i,I}^{(\varepsilon,j)} = \mu_I^{\rho+1} u_0^{D_2-j} + \sum_{j < \kappa \leq D_2} \Psi_{i,I}^{(\varepsilon,j,\kappa)} u_0^{D_2-j}.$$

For every  $z \in \mathcal{W}_{i,I}^{(\varepsilon,j)}$  it is easy to check by induction on  $\tau$  that  $(e_i^{(\varepsilon,j)})_z | (\Psi_\tau)_z$  in the ring  $\bar{F}[u_{s-m+2}, \dots, u_{s+1}]$  and  $(\Psi_{\tau,2})_z = 0$ , since  $(\mu_I^{\rho+1} e_i^{(\varepsilon,\kappa)})_z / (e_i^{(\varepsilon,j)})_z = (\Psi_{i,I}^{(\varepsilon,j,\kappa)})_z$ ; hence  $(\Lambda_i^{(\varepsilon)})_z / (e_i^{(\varepsilon,j)})_z = (\mu_I^{-\rho-1} \Psi_{i,I}^{(\varepsilon,j)})_z$  is equal to the product of the powers  $L_\beta^{c_\beta}$  of all the linear forms  $L_\beta$  whose  $u$ -coefficient is nonzero.

We also recall that  $\text{cone}(W'_2) = \bigcup_{p_f} V_{p_f} \cap \{Y = 0\}$ , and we write

$$W' = \bigcup_{z \in \mathcal{W}_{i,I}^{(\varepsilon,j)}} (\{z\} \times (W'_z \cap \{Y_0 \neq 0\}))$$

(we fix the indices  $i, \varepsilon, j$ , and  $I$  temporarily). We remark that

$$W' = \left\{ (z_1, \dots, z_{n-s}, (y_0 : y_{s-m+2} : \dots : y_{s+1})) \in \mathcal{W}_{i,I}^{(\varepsilon,j)} \right. \\ \left. \times \mathbf{A}^m(\overline{F}) \subset \mathcal{W}_{i,I}^{(\varepsilon,j)} \times \mathbf{P}^m(\overline{F}) : \right. \\ \left. 0 = \Psi_{i,I}^{(\varepsilon,j)} \left( - \sum_{s-m+2 \leq \alpha \leq s+1} y_\alpha u_\alpha, y_0 u_{s-m+2}, \dots, y_0 u_{s+1} \right)_z \right. \\ \left. \in \overline{F}[u_{s-m+2}, \dots, u_{s+1}] \right\}.$$

Writing out the polynomial

$$\Psi_{i,I}^{(\varepsilon,j)} \left( - \sum_{s-m+2 \leq \alpha \leq s+1} Y_\alpha u_\alpha, Y_0 u_{s-m+2}, \dots, Y_0 u_{s+1} \right) = \sum_J E_J u^J, \\ E_J \in F[Z_1, \dots, Z_{n-s}, Y_0, Y_{s-m+2}, \dots, Y_{s+1}],$$

we arrive at the equality

$$W' = \{ \&_J E_J = 0 \} \cap (\mathcal{W}_{i,I}^{(\varepsilon,j)} \times \mathbf{A}^m).$$

Thus the subset  $W'$  is closed in the quasiprojective variety  $\mathcal{W}_{i,I}^{(\varepsilon,j)} \times \mathbf{A}^m$ .

We introduce the natural linear projection  $\Pi_2: \mathbf{A}^{n-s} \times (\mathbf{P}^m \cap \{Y_0 \neq 0\}) \rightarrow \mathbf{A}^{n-s}$ , defined by

$$\pi_2(Z_1, \dots, Z_{n-s}, (Y_0 : Y_{s-m+2} : \dots : Y_{s+1})) = (Z_1, \dots, Z_{n-s}).$$

We consider the morphism  $\pi_1: W' \rightarrow \mathcal{W}_{i,I}^{(\varepsilon,j)}$  which is the restriction of  $\pi_2$  to  $W'$ . Our next goal is to prove that  $\pi_1$  is a finite morphism [14]. Clearly the preimage of any affine open subset  $\mathcal{V} \subseteq \mathcal{W}_{i,I}^{(\varepsilon,j)}$  under  $\pi_1$  is isomorphic with  $(\mathcal{V} \times \mathbf{A}^m) \cap W'$ , and consequently the preimage is an open subset of  $W'$  which is affine, since it is closed in  $\mathcal{V} \times \mathbf{A}^m$  [14]. We will now check that every coordinate function  $(Y_\alpha/Y_0)$  on the variety  $\pi_1^{-1}(\mathcal{V})$  satisfies an equation of integral dependence over the ring  $\overline{F}[\mathcal{V}]$ , where  $s-m+2 \leq \alpha \leq s+1$ . Let  $\Psi_{i,I}^{(\varepsilon,j)} = \Psi_{i,I}^{(\varepsilon,j)}(u_0, u_{s-m+2}, \dots, u_{s+1})$ . Then

$$\Psi_{i,I}^{(\varepsilon,j)}(Y_\alpha/Y_0, 0, \dots, 0, -1, 0, \dots, 0) = 0 \quad \text{on } \pi_1^{-1}(\mathcal{V}) \subset W',$$

where  $(-1)$  is substituted for the variable  $u_\alpha$ . As  $(\mu_I)_z \neq 0$  for  $z \in \mathcal{W}_{i,I}^{(\varepsilon,j)}$ , this gives an equation of integral dependence. Thus the morphism  $\pi_1$  is finite.

With the notation of Lemma 1 we conclude that the set  $\mathcal{V}_{i,I}^{(\varepsilon,j)}$  consisting of those  $z = (z_1, \dots, z_{n-s}) \in \mathcal{W}_{i,I}^{(\varepsilon,j)}$  for which there is a point  $\Omega = (z, (\xi_0 : 0 : \dots : 0 : \xi_{s-m+2} : \dots : \xi_{s+1})) \in U_z \cap \{X_0 \neq 0\}$ , is closed in  $\mathcal{W}_{i,I}^{(\varepsilon,j)}$ , since it coincides with the image under

the projection  $\pi_1$  of the closed subset  $\pi_1^{-1}(\mathcal{W}_{i,I}^{(\varepsilon,j)}) \cap \{\tilde{f}_0 = \dots = \tilde{f}_{k-1} = 0\}$  of the domain of  $\pi_1$  (i.e.  $W'$ ), where

$$\begin{aligned} \tilde{f}_\kappa(Z_1, \dots, Z_{n-s}, Y_0, Y_{s-m+2}, \dots, Y_{s+1}) \\ = \hat{f}_\kappa(Z_1, \dots, Z_{n-s}, Y_0, 0, \dots, 0, Y_{s-m+2}, \dots, Y_{s+1}) \end{aligned}$$

and

$$\hat{f}_\kappa(Z_1, \dots, Z_{n-s}, Y_0, Y_1, \dots, Y_{s+1}) = \bar{f}_\kappa(Z_1, \dots, Z_{n-s}, X_0, X_1, \dots, X_{s+1})$$

for  $0 \leq \kappa \leq k - 1$ , if one bears in mind that the image of a closed set under a finite morphism is again closed [14].

We describe an algorithm for the construction of  $\mathcal{V}_{i,I}^{(\varepsilon,j)}$ . Let the quasiprojective variety

$$\mathcal{W}_{i,I}^{(\varepsilon,j)} = \left\{ \&_{\beta} (G_{\beta} = 0) \& \bigvee_{\tau} (C_{\tau} \neq 0) \right\},$$

where the polynomials  $G_{\beta}, C_{\tau} \in F[Z_1, \dots, Z_{n-s}]$  were in fact constructed above. We introduce notation for the closure of the projection:

$$\begin{aligned} \overline{\pi_2 \left\{ \&_{\beta} (G_{\beta} = 0) \& \&_J (E_J = 0) \& \&_{0 \leq \kappa \leq k-1} (\tilde{f}_{\kappa} = 0) \right\}} \\ = \overline{\pi_2 \left( \overline{W'} \cap \left\{ \&_{0 \leq \kappa \leq k-1} \tilde{f}_{\kappa} = 0 \right\} \right)} = \mathfrak{W}_{i,I}^{(\varepsilon,j)} \subset \mathbf{A}^{n-s}. \end{aligned}$$

On the other hand,

$$\mathcal{V}_{i,I}^{(\varepsilon,j)} = \overline{\mathcal{V}_{i,I}^{(\varepsilon,j)}} \setminus \left\{ \&_{\tau} (C_{\tau} = 0) \right\} = \mathfrak{W}_{i,I}^{(\varepsilon,j)} \setminus \left\{ \&_{\tau} (C_{\tau} = 0) \right\}.$$

thus it remains only to construct the affine variety  $\mathcal{V}_{i,I}^{(\varepsilon,j)}$ .

Relying on Theorem 1, we find generic points of the components of the variety

$$\left\{ \&_{\beta} (G_{\beta} = 0) \& \&_J (E_J = 0) \& \&_{0 \leq \kappa \leq k-1} (\tilde{f}_{\kappa} = 0) \right\},$$

and it suffices for each such component  $\mathfrak{W}$  to find the closure of its projection  $\overline{\pi_2(\mathfrak{W})}$ . We now construct generic points for the irreducible varieties  $\overline{\pi_2(\mathfrak{W})}$ . For this we remark that the function field

$$\begin{aligned} F^{q^{-\infty}}(\overline{\pi_2(\mathfrak{W})}) &= F^{q^{-\infty}}(Z_1, \dots, Z_{n-s}) \subset F^{q^{-\infty}}(Z_1, \dots, Z_{n-s}, Y_1/Y_0, \dots, Y_{s+1}/Y_0) \\ &= F^{q^{-\infty}}(\mathfrak{W}). \end{aligned}$$

Therefore the generic point can be constructed, first finding a transcendence basis and then a primitive element. The determination of a transcendence basis, and also of a primitive element, is based on the procedure for the determination of a polynomial relation (when it exists) between elements

$$w_1, \dots, w_{\rho} \in F(t_1, \dots, t_{n-m_1})[\theta] \subset F^{q^{-\infty}}(\mathfrak{W})$$

( $m_1 = \text{codim } \mathfrak{W}$ ; cf. (2)) under the assumption that  $w_1, \dots, w_{\rho-1}$  are algebraically independent, which reduces in turn to the solution of a linear system for the coefficients of this relation (cf. §4 of [9]). Further, taking into account the remark after Theorem 1, the algorithm finds a representation

$$\overline{\pi_2(\mathfrak{W})} = \left\{ \&_{\sigma} (B_{\sigma} = 0) \right\},$$

where the polynomials  $B_{\sigma} \in F[Z_1, \dots, Z_{n-s}]$ .

To sum up the preceding exposition: we obtain an algorithm which represents the desired projection  $\prod = \pi(U \cap \{X_0 \neq 0\})$  (see Lemma 1 and the notation at the beginning of this section) in the form

$$\left\{ \bigvee_{0 \leq m \leq s+1} \bigvee_{1 \leq i_1 < \dots \leq i_m \leq N'} \bigvee_{(Y_1, \dots, Y_{s-m+1}) \in \mathfrak{M}^{i, \varepsilon, j, I} \mathfrak{W}, \tau} \bigvee_{\& \bigwedge_{1 \leq \sigma \leq N_1} (B_\sigma = 0) \& (C_\tau \neq 0)} \right\}.$$

We now estimate the size of this formula and the execution time of the algorithm. We recall that  $N' \leq d^{2n}$  and

$$\text{card}(\mathfrak{M}) = \binom{s(d-1)^m + 1}{s-m+1} \leq (s(d-1)^m + 2)^{s-m+1}.$$

In the construction of the variants  $\Gamma_1, \Gamma_2, \dots$  of the Gauss algorithm (see above) we may make the estimates

$$\begin{aligned} r &= \binom{md+m}{m} \leq (3d)^m, \\ \text{deg}_{Y, Z_1, \dots, Z_{n-s}, u_0, u_{s-m+2}, \dots, u_{s+1}}(P_i) &\leq dr^2 \leq (3d)^{2m+1}, \\ \text{deg}_{T_1, \dots, T_l}(P_i) &\leq d_2 \mathcal{P}(d^m, d_1) \end{aligned}$$

(see (3) and Theorem 2; cf. also [9], Chapter 2, §2).

Finally, the length of the notation for the coefficients is

$$l(P_i) \leq (M_1 + M_2 + (n+l) \log d_2) \mathcal{P}(d^m, d_1).$$

Hence, the number of quasiprojective varieties  $\mathcal{W}_i$  does not exceed

$$\binom{(3d)^{2m+1} + n - s + m - 2}{n - s + m + 2} \leq (3d)^{(2m+1)(n+2)},$$

since the  $P_i$  are linearly independent. Here each  $\mathcal{W}_i$  is represented by the algorithm in the form

$$\left\{ \& \bigwedge_{1 \leq \beta \leq N_2} (G_\beta^{(1)} = 0) \& \bigvee_{1 \leq \tau \leq N_3} (C_\tau^{(1)} \neq 0) \right\},$$

where the degrees satisfy

$$\begin{aligned} \text{deg}_{Z_1, \dots, Z_{n-s}}(G_\beta^{(1)}), \text{deg}_{Z_1, \dots, Z_{n-s}}(C_\tau^{(1)}) &\leq \text{deg}(P_i) \leq (3d)^{2m+1}, \\ \text{deg}_{T_1, \dots, T_l}(G_\beta^{(1)}), \text{deg}_{T_1, \dots, T_l}(C_\tau^{(1)}) &\leq d_2 \mathcal{P}(d^m, d_1), \end{aligned}$$

and the length of the notation for the coefficients

$$l(G_\beta^{(1)}), l(C_\tau^{(1)}) \leq (M_1 + M_2 + (n+l) \log d_2) \mathcal{P}(d^m, d_1).$$

Finally,  $N_2 \leq (3d)^{(2m+1)(n+m+5)}$  and  $N_3 \leq (3d)^{(2m+1)(m+2)}$ . At this stage time which is polynomial in  $M_1 + M_2$ ,  $d^{m(n+l)}$ , and  $(d_1 d_2)^l$  is sufficient for the algorithm.

Then the algorithm constructs quasiprojective varieties

$$\mathcal{W}_i^{(\varepsilon)} = \mathcal{W}_i \cap \left\{ \& \bigwedge_{1 \leq \beta \leq N_4} (G_\beta^{(2)} = 0) \& \bigvee_{1 \leq \tau \leq N_5} (C_\tau^{(2)} \neq 0) \right\}.$$

For all the parameters of the polynomials  $G_\beta^{(2)}$  and  $C_\tau^{(2)}$ , and also for  $N_4$  and  $N_5$ , there are bounds which are similar to the ones found above for  $G_\beta^{(1)}$ ,  $C_\tau^{(1)}$ ,  $N_2$ , and  $N_3$  respectively.

The same is true also for the parameters of the polynomials in the representations of the quasiprojective varieties

$$\mathcal{W}_i^{(\varepsilon,j)} = \mathcal{W}_i^{(\varepsilon)} \cap \left\{ \&_{1 \leq \beta \leq N_6} (G_\beta^{(3)} = 0) \& \bigvee_{1 \leq \tau \leq N_7} (C_\tau^{(3)} \neq 0) \right\},$$

and also for the quasiprojective varieties

$$\mathcal{W}_{i,I}^{(\varepsilon,j)} = \mathcal{W}_{i,I}^{(\varepsilon)} \cap \left\{ \&_{1 \leq \beta \leq N_8} (G_\beta^{(4)} = 0) \& \bigvee_{1 \leq \tau \leq N_9} (C_\tau^{(4)} \neq 0) \right\}.$$

We remark that  $\varepsilon, j \leq (3d)^{m+1}$ , and the number of multi-indices  $I$  is less than  $(3d)^{(m+1)^2}$ .

Further, the algorithm computes  $\Psi_{i,I}^{(\varepsilon,j,\kappa)}$  with the help of the process described above of division of a polynomial by a polynomial. For the parameters of the polynomial  $\Psi_{i,I}^{(\varepsilon,j,\kappa)}$ , and consequently for the polynomials  $E_J$  bounds hold, similar to those presented above for the polynomials  $G_\beta^{(1)}$  and  $C_\tau^{(1)}$ . The bound  $E_J$  on the execution time for the construction of  $\mathcal{W}_{i,I}^{(\varepsilon,j)}$ , as well as  $\Psi_{i,I}^{(\varepsilon,j,\kappa)}$  and is the same as above in the construction of  $\mathcal{W}_i$ . We mention only the bound

$$\deg_{Z_1, \dots, Z_{n-s}, u_{s-m+2}, \dots, u_{s+1}} (\Psi_{i,I}^{(\varepsilon,j,\kappa)}) \leq (3d)^{4m+1}.$$

Then the algorithm represents the quasiprojective variety

$$\mathcal{W}_{i,I}^{(\varepsilon,j)} = \left\{ \&_{\beta} (G_\beta = 0) \& \bigvee_{\tau} (C_\tau \neq 0) \right\}$$

according to the remark formulated above concerning the intersection of quasiprojective varieties. As a result we obtain similar bounds for the parameters of the polynomials  $G_\beta, C_\tau$ ; namely, we give here the bounds

$$\deg_{Z_1, \dots, Z_{n-s}} (G_\beta) \leq (3d)^{2m+1}, \quad \deg_{Z_1, \dots, Z_{n-s}} (C_\tau) \leq 4(3d)^{2m+1},$$

and also

$$\begin{aligned} \beta &\leq N_2 + N_4 + N_6 + N_8 \leq 4(3d)^{(2m+1)(n+m+5)}, \\ \tau &\leq N_3 N_5 N_7 N_9 \leq (3d)^{4(2m+1)(m+2)}. \end{aligned}$$

Further, the algorithm finds generic points of the components  $\mathfrak{W}$  (see above) of the variety

$$\left\{ \&_{\beta} (G_\beta = 0) \& \&_J (E_J = 0) \& \&_{0 \leq \kappa \leq k-1} (\tilde{f}_\kappa = 0) \right\},$$

and then the generic points and the defining systems of equations  $\&_{\sigma} (B_\sigma = 0)$  of the closures of the projections of these components. From Theorem 1 we derive the bounds

$$\deg_{Z_1, \dots, Z_{n-s}} (B_\sigma) < (3d)^{2(4m+1)(n+2)}$$

and

$$\deg_{T_1, \dots, T_l} (B_\sigma) \leq d_2 \mathcal{P}(d^{(m+1)n}, d_1)$$

while the length of the notation for the coefficients is

$$l(B_\sigma) \leq (M_1 + M_2 + (n+l)d_2) \mathcal{P}(d^{(m+1)n}, d_1);$$

finally,

$$\sigma \leq (n+2)^2 (3d)^{4(4m+1)(n+2)}.$$

We remark that the number of components  $\mathfrak{W}$  does not exceed  $(3d)^{(4m+1)(n+2)}$ .

The execution time for our algorithm for the construction of the polynomials  $B_\sigma$  is bounded above by a polynomial in  $M_1, M_2, d^{(m+1)n(n+l)}, (d_1 d_2)^{(n+l)}$ , and  $q$ .

We cast the result obtained in this section in the form of the following lemma.

LEMMA 2. An algorithm has been constructed, which finds the constructible set

$$\begin{aligned} \Pi &= \pi(U \cap \{X_0 \neq 0\}) \\ &= \left\{ (z_1, \dots, z_{n-s}) \in \mathbf{A}^{n-s}(\overline{F}) : \right. \\ &\quad \exists X_1 \cdots \exists X_s \left( \&_{1 \leq \kappa \leq k-1} (f_\kappa(z_1, \dots, z_{n-s}, X_1, \dots, X_s) = 0) \right. \\ &\quad \left. \left. \& g(z_1, \dots, z_{n-s}, X_1, \dots, X_s) \neq 0 \right) \right\}, \end{aligned}$$

that is, a projection, in the form

$$\left\{ \bigvee_\lambda \left( \&_{\sigma(B_\sigma^{(\lambda)})} = 0 \& C^{(\lambda)} \neq 0 \right) \right\}.$$

Here the following bounds are satisfied:

$$\begin{aligned} \deg_{Z_1, \dots, Z_{n-s}}(B_\sigma^{(\lambda)}) &\leq d^{4(4s+5)(n+2)}, \\ \deg_{T_1, \dots, T_1}(B_\sigma^{(\lambda)}) &\leq d_2 \mathcal{P}(d^{sn}, d_1), \quad l(B_\sigma^{(\lambda)}) \leq (M_1 + M_2 + (n+l)d_2) \mathcal{P}(d^{sn}, d_1), \\ \deg_{Z_1, \dots, Z_{n-s}}(C^{(\lambda)}) &\leq d^{4s+7}, \quad \deg_{T_1, \dots, T_1}(C^{(\lambda)}) \leq d_2 \mathcal{P}(d^2, d_1), \\ l(C^{(\lambda)}) &\leq (M_1 + M_2 + (n+l) \log d_2) \mathcal{P}(d^s, d_1). \end{aligned}$$

Furthermore,

$$\sigma \leq (n+2)^2 d^{8(4s+5)(n+2)}, \quad \lambda \leq d^{34(n+4)(s+1)}.$$

The execution time for the algorithm is bounded by some polynomial in  $M_1, M_2, d^{sn(n+l)}, (d_1 d_2)^{n+l}$ , and  $q$ .

We remark that the lemma gives in particular an upper bound for the degree of the projection of a constructible set, which is better than those known previously. Namely, let  $\pi_3(Z_1, \dots, Z_n) = (Z_1, \dots, Z_{n-s})$  and let  $\mathcal{E} \subseteq \mathbf{A}^n$  be a constructible set; then  $\deg(\pi_3(\mathcal{E})) \leq \mathcal{P}((\deg \mathcal{E})^{ns+1})$ .

### §3. Quantifier elimination in the first order theory of algebraically closed fields

Let a propositional formula  $Q$  with  $N$  atoms of the form  $f_i = 0$  be given, where the parameters of the polynomials  $f_i \in F[X_1, \dots, X_n]$  satisfy the same bounds as in §1; we denote by  $\mathcal{L}(Q)$  the size of the formula  $Q$ . First we describe an algorithm for the reduction of  $Q$  to disjunctive normal form.

Following [7], for  $g_1, \dots, g_\rho \in F[X_1, \dots, X_n]$  we call any nonempty quasiprojective variety of the form

$$\left\{ \&_{j_1 \in J_1} (g_{j_1} = 0) \& \&_{j_2 \in J_2} (g_{j_2} \neq 0) \right\},$$

with  $J_1 \cup J_2 = \{1, \dots, \rho\}$  and  $J_1 \cap J_2 = \emptyset$ , a  $(g_1, \dots, g_\rho)$ -cell. We set  $D_3 = \deg g_1 + \dots + \deg g_\rho$ . On the basis of Bézout's inequality it is shown in [7] that the number of all  $(g_1, \dots, g_\rho)$ -cells does not exceed  $(1 + D_3)^n$ . Now we describe an algorithm, partitioning the space  $\mathbf{A}^n(\overline{F})$  into  $(g_1, \dots, g_\rho)$ -cells, recursively in  $\rho$ . Let all  $(g_1, \dots, g_{\rho-1})$ -cells be constructed already ( $\rho \geq 1$ ). Each  $(g_1, \dots, g_\rho)$ -cell has the form either  $\mathcal{C} \cap \{g_\rho = 0\}$  or  $\mathcal{C} \cap \{g_\rho \neq 0\}$  for a certain  $(g_1, \dots, g_{\rho-1})$ -cell  $\mathcal{C}$ . Hence it suffices to distinguish all nonempty sets (using Theorem 1) among the quasiprojective varieties  $\mathcal{C} \cap \{g_\rho = 0\}$  and  $\mathcal{C} \cap \{g_\rho \neq 0\}$ .

Using the algorithm just described, we construct all  $(f_1, \dots, f_N)$ -cells. Again using Theorem 1 repeatedly, for each  $(f_1, \dots, f_N)$ -cell the algorithm checks by recursion on

the number of logical connectives in the formula  $Q$  whether this cell is contained in the constructive set  $\prod_Q = \{Q\} \subseteq \mathbf{A}^n$ , given by the formula  $Q$ . The algorithm thereby represents the set  $\prod_Q$  in the form of a union of suitable  $(f_1, \dots, f_N)$ -cells  $\mathfrak{C}^{(\lambda)}$ , which corresponds to the reduction of  $Q$  to disjunctive normal form

$$\bigvee_{\lambda} \left( \&_{\sigma \geq 1} (f_{\sigma}^{(\lambda)} = 0) \& (f_0^{(\lambda)} \neq 0) \right).$$

Here  $1 \leq \lambda \leq (1 + Nd)^n$ ,  $1 \leq \sigma \leq N$ , and each polynomial  $f_{\sigma}^{(\lambda)} = f_i$  for some  $i$ , while  $f_0^{(\lambda)} = \prod_{j \in J} f_j$  for a suitable subset  $J \subseteq \{1, \dots, N\}$ . The execution time of the proposed algorithm for reduction to disjunctive normal form is bounded according to Theorem 1 by a polynomial in  $\mathcal{L}(Q)$ ,  $N^n$ ,  $(d^n d_1 d_2)^{n+l}$ , and  $q$ .

Finally, we describe a quantifier elimination process in its application to formula (1), where the parameters of the polynomials  $f_i$  satisfy the same bounds as in §1. Applying the algorithm for reduction to disjunctive normal form presented earlier in this section and Lemma 2 of §2 alternately to formula (1), after carrying out  $\alpha$  stages we shall arrive at the equivalent formula

$$\exists Z_{1,1} \dots \exists Z_{1,s_1} ] \dots \exists Z_{a-\alpha,1} \dots \exists Z_{a-\alpha,s_{a-\alpha}} ] \left( \bigvee_{1 \leq i \leq N^{(\alpha)}} \left( \&_{1 \leq j \leq k^{(\alpha)}} (f_{i,j}^{(\alpha)} = 0) \& f_{i,0}^{(\alpha)} \neq 0 \right) \right).$$

We write

$$\begin{aligned} d^{(\alpha)} &= \max_{i,j} \deg_{Z_1, \dots, Z_{s_0}, Z_{1,1}, \dots, Z_{a-\alpha, s_{a-\alpha}}} (f_{ij}^{(\alpha)}), \\ d_2^{(\alpha)} &= \max_{i,j} \deg_{T_1, \dots, T_l} (f_{ij}^{(\alpha)}), \quad \mathcal{R}^{(\alpha)} = N^{(\alpha)} k^{(\alpha)} d^{(\alpha)}, \\ M_2^{(\alpha)} &= \max_{i,j} l(f_{ij}^{(\alpha)}), \quad \sigma = s_{a-\alpha+1}. \end{aligned}$$

Then in view of the bounds in Theorem 1 and in Lemma 2, the following inequalities hold:

$$\begin{aligned} d^{(\alpha)} &\leq (\mathfrak{R}^{(\alpha-1)})^{4(4\sigma+5)(n+2)}, \quad N^{(\alpha)} \leq (\mathfrak{R}^{(\alpha-1)})^{n+34(n+4)(\sigma+1)}, \\ k^{(\alpha)} &\leq (n+2)^2 (\mathfrak{R}^{(\alpha-1)})^{8(4\sigma+5)(n+2)}. \end{aligned}$$

Hence by induction we obtain

$$\mathfrak{R}^{(\alpha)} \leq (\mathfrak{R}^{(\alpha-1)})^{82(n+3)(\sigma+2)} \leq (Nd^n)^{\left(82(n+3) \sum_{a-\alpha+1 \leq j \leq a} (s_j+2)/\alpha\right)^\alpha}.$$

Furthermore,

$$\begin{aligned} d_2^{(\alpha)} &\leq d_2^{(\alpha-1)} \mathcal{P}(\mathfrak{R}^{(\alpha-1)}, d_1) \leq d_2 \mathcal{P}(\mathfrak{R}^{(\alpha)}, d_1^{(\alpha)}), \\ m_2^{(\alpha)} &\leq (M_1 + M_2 + ld_2^{(\alpha-1)}) \mathcal{P}(\mathfrak{R}^{(\alpha-1)}, d_1) \leq (M_1 + M_2 + ld_2) \mathcal{P}(\mathfrak{R}^{(\alpha)}, d_1^{(\alpha)}). \end{aligned}$$

The execution time for the algorithm described, after the completion of  $\alpha$  stages, may be bounded by a polynomial in

$$M_1, M_2, (Nd^N)^{\left(82(n+3)/\alpha\right)^\alpha \left(\sum_{a-\alpha+1 \leq j \leq a} (s_j+2)\right)^\alpha (n+1)}, (d_1^\alpha d_2)^{n+l}, \text{ and } q.$$

After completing  $\alpha$  stages of the algorithm the proof of our main result is completed.

**THEOREM 3.** *An algorithm has been constructed which finds for every formula of the form (1) an equivalent quantifier-free formula*

$$\bigvee_{1 \leq i \leq \mathcal{N}} \left( \&_{1 \leq j \leq \mathcal{K}} (g_{ij} = 0) \& g_{i0} \neq 0 \right), \quad \text{where } g_{ij} \in F[Z_1, \dots, Z_{s_0}];$$

here

$$\begin{aligned} \deg_{Z_1, \dots, Z_{s_0}}(g_{ij}) &\leq (Nd^n)^{(82(n+s)(n+2a)/a)^a} = D \leq (Nd)^{(9(n+3))^{2a+1}}, \\ \deg_{T_1, \dots, T_l}(g_{ij}) &\leq d_2 \mathcal{P}(D, d_1^a), \quad l(g_{ij}) \leq (M_1 + M_2 + ld_2) \mathcal{P}(D, d_1^a). \end{aligned}$$

Furthermore,  $\mathcal{N}, \mathcal{K} \leq D$ . Finally, the execution time for the algorithm is bounded by a polynomial in  $\mathcal{L}(Q)$ ,  $\mathcal{L}(\varphi)$ ,  $D^{n+l}$ ,  $(d_1^a d_2)^{n+l}$ , and  $q$ .

The author wishes to express his gratitude to A. L. Chistov for useful discussions.

Received 25/JULY/84

#### BIBLIOGRAPHY

1. Alfred Tarski, *A decision method for elementary algebra and geometry*, 2nd ed., Univ. of California Press, Berkeley, Calif., 1951.
2. Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman, *The design and analysis of computer algorithms*, Addison-Wesley, 1975.
3. A. O. Slisenko, *Complexity problems in computational theory*, Uspekhi Mat. Nauk **36** (1981), no. 6 (222), 21–103; English transl. in Russian Math. Surveys **36** (1981).
4. A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.
5. George E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, Automata Theory and Formal Languages (Second GI Conf., Kaiserslautern, 1975), Lecture Notes in Computer Sci., vol. 33, Springer-Verlag, 1975, pp. 134–183.
6. H. R. Wüthrich, *Ein Entscheidungsverfahren für die Theorie der reellabgeschlossenen Körper*, Komplexität von Entscheidungsproblemen—ein Seminar (1973/74), Lecture Notes in Computer Sci., vol. 43, Springer-Verlag, 1976, pp. 138–162.
7. Joos Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theoret. Computer Sci. **24** (1983), 239–277.
8. Michael J. Fischer and Michael O. Rabin, *Super-exponential complexity of Presburger arithmetic*, Complexity of Computation, SIAM-AMS Proc., vol. 7, Amer. Math. Soc., Providence, R.I., 1974, pp. 27–41.
9. D. Yu. Grigor'ev, *Factoring polynomials over a finite field and solution of systems of algebraic equations*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 20–79; English transl. in J. Soviet Math. **34** (1986), no. 4.
10. A. L. Chistov, *An algorithm of polynomial complexity for factoring polynomials, and determination of the components of a variety in a subexponential time*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 124–188; English transl. in J. Soviet Math. **34** (1986), no. 4.
11. Oscar Zariski and Pierre Samuel, *Commutative algebra*. Vols. I, II, Van Nostrand, Princeton, N.J., 1958, 1960.
12. Daniel Lazard, *Résolution des systèmes d'équations algébriques*, Theoret. Computer Sci. **15** (1981), 77–110.
13. D. Yu. Grigor'ev, *The relation between the rank and the multiplicative complexity of a bilinear form over a Noetherian commutative ring*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **86** (1979), 66–81; English transl. in J. Soviet Math. **17** (1981), no. 4.
14. I. R. Shafarevich, *Basic algebraic geometry*, "Nauka," Moscow, 1972; English transl., Springer-Verlag, 1974.
15. F. R. Gantmakher, *The theory of matrices*, 2nd ed., "Nauka," Moscow, 1966; English transl. of 1st ed., Vols. 1,2, Chelsea, New York, 1959.

Translated by G. L. CHERLIN