GBV-direkt-BESTELLUNG

Voelzmann-Scheiding, Anke
MPI fuer Mathematik -Bibliothek-
Vivatsgasse 7
DE-53111 Bonn

Kontaktperson

Kunden-/Zugangsnr: 3737153353

Lieferbibliothek:
Staats- und Universitätsbibliothek
Bremen
Bibliothekstraße
D-28359 Bremen

Tel. +49 (0421) 218-3622 (Fr. Fregin), Fax: -2040
E-Mail: femleihe@suub.uni-bremen.de

Liefererschein / delivery note
Lieferung einer Aufsatzkopie per / delivery of article by
Post / mail  E-Mail / ARIEL  Fax
Eildienst / express delivery
Fernleihe eines Buches - einer Mikroform / lending of book - microform
Wir berechnen für unsere Lieferung / price
Rechnung folgt - Bitte veranlassen Sie erst dann eine Zahlung, wenn die Rechnung bei Ihnen eingetroffen ist.
Bills are mailed every three months or according to arrangements.

Verfasser: Chistov
(Titel) Complexity of quantifier elimination in the theory of
(Aufsatz) algebraically clos
Seiten: 17-31

Band Heft  Jahrgang
1984-00-00

Titel (Monographie / Zeitschrift)
Mathematical foundations of computer science 1984 :
proceedings, 11th symposium,
Berlin [u.a.]
Springer

Lieferform: PDF
Lieferart: E-Mail alt. Post

Bemerkungen:
Wir weisen Sie als Empfänger darauf hin, dass Sie nach geltendem Urheberrecht die von uns übersandten Vervielfältigungsstücke ausschliesslich zum privaten oder sonstigen eigenen Gebrauch verwenden dürfen und weder entgeltlich noch unentgeltlich in Papierform oder als elektronische Kopie verbreiten dürfen. SuUB Bremen
Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

176

Mathematical Foundations of Computer Science 1984
Proceedings, 11th Symposium
Praha, Czechoslovakia
September 3–7, 1984

Edited by M. P. Chytil and V. Kouboek

Springer-Verlag
Berlin Heidelberg New York Tokyo 1984
COMPLEXITY OF QUANTIFIER ELIMINATION
IN THE THEORY OF ALGEBRAICALLY CLOSED FIELDS

A.I. Chistov, D.Yu. Grigorev
Leningrad Scientific Research Computer Centre
of the Academy of Sciences of the USSR,
Mendeleevskaya 1, Leningrad, 199164, USSR

Leningrad Department of V.A. Steklov Mathematical
Institute of the Academy of Sciences of the USSR,
Fontanka 27, Leningrad, 191011, USSR

Abstract

An algorithm is described producing for each formula of the
first order theory of algebraically closed fields an equivalent free
of quantifiers one. Denote by \( N \) a number of polynomials occurring
in the formula, by \( d \) an upper bound on the degrees of polynomials,
by \( n \) a number of variables, by \( a \) a number of quantifier alternations
(in the prefix form). Then the algorithm works within the poly-
nomial in the formula's size and in \( (Nd)^{(2a+4)} \) time. Up to now
a bound \( (Nd)^{O(n)} \) was known ([5], [7], [15]).

1. Fast algorithms for factoring multivariable
polynomials and for solving systems of al-
gebraic equations

Lately the considerable progress in the polynomial factoring
problem was achieved. Lenstra A.K., Lenstra H.W., Lovasz L. [12]
have designed an ingenious polynomial-time algorithm for factoring
one-variable polynomials over \( \mathbb{Q} \). Independently Kaltofen E. [8],
[9] has constructed a reduction of multivariable factoring over \( \mathbb{Q} \)
to onevariable factoring, running within the polynomial-time provi-
ded that the number of variables is fixed. The authors [1], [4],
have suggested a polynomial-time algorithm for factoring multi-
vARIABLE polynomials over \( \mathbb{Q} \) and over finite fields. Later another
polynomial-time algorithm for the case of finite fields was exhibited
in [13] spreading the method [12].

Also an essential progress has taken place in another important
problem of the commutative computational algebra, namely in the problem of solving systems of algebraic equations. Earlier a complexity bound of the order \( d^{kn} \) was known for it, e.g., from [5], [7], [15]. Lazard D. [11] has designed an algorithm for solving homogeneous systems of algebraic equations in the case when the variety of roots in the projective space of the system is null-dimensional, i.e., finite, working within the time \( d^{(kn)} \) if the coefficients of the input system are taken from a finite field (certainly, provided that we are supplied with a polynomial-time algorithm for polynomial factoring). The authors [2], [3], [4] involving the polynomial-time algorithm for polynomial factoring [1], [4] and the method from [11] have constructed an algorithm for solving an arbitrary system of algebraic equations, running within a polynomial in the size \( L_k \) of the input data (system) and in \( d^{kn} \) time. Moreover, the algorithm finds all the irreducible compounds \( W_d \subset \mathbb{P}^n(F) \) of the variety of roots of the homogeneous system within the polynomial time in \( d^{kn} \) and in \( L_k \), where \( C = \max \dim W_d \) (the general case is reducible here to homogeneous one). Finding \( W_d \) allows to answer the principal questions, e.g., emptiness, dimension of the variety of roots.

Now we turn ourselves to the exact formulations of the mentioned results. Let a ground field \( F = \mathbb{Q(T_1, \ldots, T_k)} \) where either \( H = \mathbb{Q} \) or \( H = \mathbb{F}_q[x] \), \( q = \text{char}(H) \), the elements \( T_1, \ldots, T_k \) be algebraically independent over \( H \); the element \( q \) is separable and algebraic over a field \( H(T_1, \ldots, T_k) \), denote by \( q^e = \sum_{a \leq j \leq \deg Z(q)} \frac{1}{j!} q^j \) its minimal polynomial over \( H(T_1, \ldots, T_k) \) with the leading coefficient \( \text{lc} Z(q) = 1 \), herewith \( q^e \in H(T_1, \ldots, T_k) \) and the degree \( \deg(q^e) \) is the least possible. Any polynomial \( f \in F[x_0, \ldots, x_n] \) can be uniquely represented in a form \( f = \sum (a_{i_1, i_2, \ldots, i_n} / b) x_0^{i_1} x_1^{i_2} \ldots x_n^{i_n} \) where \( a_{i_1, i_2, \ldots, i_n} \in \mathbb{Q(T_1, \ldots, T_k)} \). By a length of description \( \ell(h) \) in the case \( h \in \mathbb{Q} \) we mean its bitwise length, and in the case \( h \in \mathbb{F}_q \) we mean \( \log_q(q) \). By \( \ell(f) \) denote the maximum of the lengths of descriptions of the coefficients from \( H \) in the monomials in \( T_1, \ldots, T_k \); \( \ell(f) \leq M_2 \). As a size \( \ell(f) \) of the polynomial \( f \), we consider in the theorem I a value \( v_n \text{lc} h + \sum_{i=1}^{n} -M_2 \) and analogously \( \ell(q) = v_n \text{lc} q + M_2 \).
THEOREM I. ([1], [4]). One can factor the polynomial \( f \) over \( \mathbb{F} \) within the polynomial in \( L_n(f) \), \( L_n(q) \), \( q \) time.

Remark that it is possible within the same time to obtain also the absolute factorization of \( f \) i.e. the factors irreducible over the algebraic closure \( \overline{\mathbb{F}} \) of the field \( \mathbb{F} \) ([2], [4]).

Proceed to the problem of solving systems of algebraic equations.

Let an input system of algebraic equations \( f_0 = \ldots = f_K = 0 \) be given (we can assume w.l.o.g. that \( f_0, \ldots, f_K \) are linearly independent). As a matter of fact we suggest an algorithm which decomposes an arbitrary projective variety on the irreducible compounds, so one can suppose w.l.o.g. that \( f_0, \ldots, f_K \in F[\lambda_0, \ldots, \lambda_n] \) are homogeneous relatively to \( \lambda_0, \ldots, \lambda_n \) polynomials. Let \( d_{0i}, \ldots, d_{Ki}, (\forall) d_{0i} < d_{0i}, (\forall) 1 < d_{Ki} \) for all \( 0 \leq i \leq K \) and in the theorem 2 a size \( L_k^{(i)} = (d_{ni})^k d_{0i}^k \in M_n \), \( d_{0i} < d_{0i} \in M_n \).

Denote \( L = L_k^{(i)} + \ldots + L_k^{(i)} \).

The projective variety \( \{ f_0 = \ldots = f_K = 0 \} \subset P^n \overline{\mathbb{F}} \) of roots of the system \( f_0 = \ldots = f_K = 0 \) is decomposable on the compounds \( \{ f_0 = \ldots = f_K = 0 \} = \bigcup W_\alpha \), herewith each compound \( W_\alpha \) is defined and irreducible over the maximal purely inseparable extension \( \mathbb{F} \) of \( \mathbb{F} \). Moreover \( W_\alpha = \bigcup W_{\alpha,}\beta \) where the (absolutely irreducible) compounds \( W_{\alpha,}\beta \) are defined and irreducible over \( \overline{\mathbb{F}} \). Denote \( C = \dim_{\mathbb{F}} W_\alpha \). The algorithm designed in [2], [3], [4] finds all \( W_\alpha \) and thereupon \( W_{\alpha,}\beta \) (actually, \( W_\alpha \), \( W_{\alpha,}\beta \) are defined over some finite extensions of the field \( \mathbb{F} \) which are also constructed by the algorithm). We (and the algorithm) represent every compound \( W_\alpha \) or \( W_{\alpha,}\beta \) in two following manners: by its general point \([16]\) and on the other hand by a certain system of algebraic equations such that the compound under consideration coincides with a variety of the roots of this system, in the similar case we say that the system determines the variety.

For functions \( q_1, q_2, h_1, \ldots, h_2 \), a relation \( q_1, q_2, W_{h_1, \ldots, h_2} \) denotes further that \( q_1, q_2, W_{h_1, \ldots, h_2} \) for an appropriate polynomial \( P \).

Let \( W \subset P^n \overline{\mathbb{F}} \) be a closed projective variety, \( \text{codim}_{\mathbb{F}} (W) = m \), defined and irreducible over some field \( \mathbb{F} \) being a finite extension of \( F \), denote by \( F_\alpha \) the maximal subfield of \( \mathbb{F} \) which is a separable extension of \( F \). Let \( t_1, \ldots, t_{n-m} \) be algebraically independent over \( F \). A general point of the variety \( W \) can be given by the following fields isomorphism:

\[
F(t_1, \ldots, t_{n-m})[\Theta] \cong F_\alpha (X_{1}/X_{1}, \ldots, X_{n-m}/X_{1}, (X_{1}/X_{1})^{q_1}, \ldots, (X_{n}/X_{n})^{q_1}) < F_\alpha (W) \tag{1}
\]
for suitable $q^\gamma$ (here and further $\gamma > 0$ when $q > 0$ and we set $q^\gamma = 1$ when $\text{char}(\mathbb{F}) = 0$), index $0 < J_0 < n$ and an element $\theta$ is algebraic separable over a field $\mathbb{F}_2(t_1, \ldots, t_{n-m})$; denote by $\Phi(Z)$ its minimal polynomial such that $\mathcal{L}_Z(\Phi) = 1$. The elements $X_j/X_{J_0}$ are considered herein as the rational functions on the variety $\mathcal{W}$, where $\mathcal{W}$ is not situated in a hyperplane $\{X_{J_0} = 0\}$, under the isomorphism $t_i \to X_j/X_{J_0}$, $1 \leq i \leq n-m$. The algorithms further represent the isomorphism $\Phi$ by the images of rational functions $(X_j/X_{J_0})^{q^\gamma}$ in the field $\mathbb{F}_2(t_1, \ldots, t_{n-m})$.

Sometimes, when there is no misunderstanding, we identify a rational function with its image.

**Theorem 2.** ([2], [3], [4]). a) An algorithm is suggested which for every compound $W_\alpha$ produces its general point and constructs a certain family of homogeneous polynomials $Q_i^{(\alpha)}, \ldots, Q_N^{(\alpha)} \in \mathbb{F} [X_1, \ldots, X_n]$ such that a system $Q_i^{(\alpha)} = \ldots = Q_N^{(\alpha)} = 0$ determines the variety $W_\alpha$. Denote $m = \text{codim} W_\alpha$, $\theta = \theta(\alpha)$, $\Phi = \Phi(\alpha)$. Then $q^\gamma < d_{m-\gamma} \leq \text{deg}_Z(\Phi) < d_{m-\gamma}$, for all $i, j$ the degrees $\text{deg}_Z t_i t_j \ldots t_{n-m}(\Phi) \leq \text{deg}_Z(\Phi) + \text{deg}_Z t_i t_j \ldots t_{n-m}(X_j/X_{J_0})^{q^\gamma}$ (the latter two degrees are defined according to the isomorphism $\Phi$), analogously to how $\text{deg}_Z(\Phi)$ was defined above are less than $d_{m-\gamma} \mathcal{P}(d_{m-\gamma}, d_{\gamma})$, apart that $s_{\alpha}, l((X_j/X_{J_0})^{q^\gamma}) \leq (M_1 + M_2 + (n+1) \log d_{\gamma}) \mathcal{P}(d_{m}, d_{\gamma})$.

A number of equations $N \leq m^2 + \text{dim} k$, the degree $\text{deg}_Z t_i t_j \ldots t_{n-m}(\Phi) \leq d_{m-\gamma} \mathcal{P}(d_{m-\gamma}, d_{\gamma})$; besides that the algorithm represents each $\Phi^{(\alpha)}$ in a form $\Phi^{(\alpha)} = \Phi^{(\alpha)}(Z_{S_0}, \ldots, Z_{S_0, n-m+2})$ for suitable linear forms $Z_{S_0, \ldots, Z_{S_0, n-m+2}}$ in the variables $X_{S_0, \ldots, X_{n}}$ with the coefficients from $H$ and the polynomials $\Phi^{(\alpha)} \in \mathbb{F} [Z_{S_0}, \ldots, Z_{S_0, n-m+2}]$, thereto $l(\Phi^{(\alpha)}) < (M_1 + M_2 + (n+1) \log d_{\gamma}) \mathcal{P}(d_{m}, d_{\gamma})$, lastly the size $l(\Phi^{(\alpha)}) < \mathcal{P}(l, \log d_{m}, d_{\gamma})$ for all $S_0, \ldots, S_0, n-m+2$. The total running time of the algorithm can be bounded from above by $\mathcal{P}(M_1, M_2, d_{m}, d_{\gamma}, \log d_{m}, d_{\gamma})$.

Obviously, the latter value is less than $\mathcal{P}(l, \log d_{m} + \log d_{\gamma}, (n+1) \log d_{\gamma})$ if $n = d_{\gamma} = (n+1) \log d_{\gamma}$.

b) An algorithm is suggested which for every absolutely irreducible compound $W_{\alpha, \beta}$ finds the maximal separable subfield $\mathbb{F}_2 = \mathbb{F} [\xi_{\alpha, \beta}]$ of the minimal field of definition $\mathbb{F}_2$ (containing $\mathbb{F}_2$) of the variety $W_{\alpha, \beta}$. The algorithm produces a general point of $W_{\alpha, \beta}$ and some system of equations with the coefficients from the field $\mathbb{F}_2$ determining the variety $W_{\alpha, \beta}$. For the parameters of the general point and the system of equations hold the same bounds as in the item a) of the theorem. Denote by $\Phi^{(\alpha)} \in \mathbb{F} [Z]$ the minimal polynomial for $\xi_{\alpha, \beta}$ such that $\mathcal{L}_Z(\Phi^{(\alpha)}) = 1$, then $\text{deg}_Z(\Phi^{(\alpha)}) \leq \text{deg}_Z W_{\alpha, \beta}$ and the degrees $\text{deg}_Z t_i t_j \ldots t_{n-1}(\Phi^{(\alpha)}) \leq d_{\gamma} \mathcal{P}(d_{m}, d_{\gamma})$, lastly $l(\Phi^{(\alpha)}) < (M_1 + M_2 + (n+1) \log d_{\gamma}) \mathcal{P}(d_{m}, d_{\gamma})$. The time bound is the same as in the item a).
REMARK. If we are supplied with a general point (with the same bounds on its parameters as in the theorem 2) of a closed irreducible variety \( V_4 = \pi (W_4) \) where \( \pi (X_0 : \ldots : X_n) = (X_0 : \ldots : X_m) \) is a linear projection \( \pi : \mathbb{P}^n \rightarrow \mathbb{P}^m \) and \( W_4 \) is some compound of the variety \( \{ t_i = \ldots = t_k = 0 \} \subset \mathbb{P}^n (F) \), then we can produce a system of equations determining \( V_4 \) with the same bounds on the parameters as for the family \( U_4 (i) \) in the theorem 2 within the same time bound.

In conclusion of the section 1. The authors make a conjecture that one can find the compounds within time \( P(d_1, c+\ell+1) \) where \( d_1 = \max \min \{ \dim W_4 + 1, \text{codim} W_4 \} \).

2. Projecting a constructive set

Let an input formula \( \exists X_1 \ldots \exists X_5 (\wedge_{i<\j \leq k} (t_i = 0) \& (t_j \neq 0)) \) be given, herein the parameters of the polynomials \( t_i, t_j \in \mathbb{F} [Z_{i1}, \ldots, Z_{i-k}, X_{11}, \ldots, X_{51}] \) satisfy the same bounds as for \( t_i \) in the section 1. The goal in the present section is to produce an equivalent quantifier-free formula \( V_{i<\j \leq k} (\wedge_{i<\j \leq k} (t_i = 0) \& (t_j \neq 0)) \) where \( t_i, t_j \in \mathbb{F} [Z_{i1}, \ldots, Z_{i-k}, X_{11}, \ldots, X_{51}] \).

The input formula is equivalent to \( \exists X_0 \exists X_1 \ldots \exists X_5 (\pi (X_0) \neq 0) \) wherein \( X_0, X_1, \ldots, X_5 \) are new variables and \( t_i = \pi (X_0: \ldots : X_5) \) \( (t_j = 0, t_i = 0, \ldots, t_i = 0) \). The desired projection, i.e., the constructive set consisting of all the points \( (z_1, \ldots, z_{k-5}) \in \mathbb{A}^{k-5} (\mathbb{F}) \) satisfying the latter formula, we denote by \( \Pi \). One can assume further w.l.o.g. that \( \deg X_0 : \ldots : X_5 = d+1 \), \( 0 \leq j \leq k \), replacing \( t_i \) by the family of polynomials \( \{ t_j : X_0: \ldots : X_5 = d+1 \} \) \( (t_j = 0) \) and a natural linear projection \( \pi : \mathbb{A}^{k-5} x \mathbb{A}^{5+1} \rightarrow \mathbb{A}^{k-5} \), then the desired \( \Pi = \pi (U \cup \{ X_0 = 0 \}) \) for each point \( z = (z_1, \ldots, z_{k-5}) \in \mathbb{A}^{k-5} (\mathbb{F}) \) consider the variety (the layer) \( U_z = \pi^{-1} (z) \cap \mathbb{A}^{k-5} \mathbb{P}^{5+1} \). The condition \( z \in \Pi \) is true iff for an appropriate \( 0 \leq m \leq 5+1 \) the layer \( U_z \) has at least one compound \( W \) with the dimension \( 5+1-m \) such that \( \mathbb{W} \subset \{ X_0 = 0 \} \).

Fix a point \( z \) in the following speculations for some time. It is not difficult (see e.g. [2]) to indicate a family of \( N^1 = \mathbb{K}^{5+1} \) vectors \( u_0, \ldots, u_K \) \( \in \mathbb{H}^{5+1} \) any \( K+1 \) from which are linearly independent (we suppose here and below that \( \mathbb{H} \) contains sufficiently many element, extending it if necessary). Denote \( k_i = \sum_{0 \leq \j < K} u_{\j}^i \) \( \mathbb{I} \), herewith \( u_i^1 = (u_0^i, \ldots, u_K^i) \). The relevant compound \( W \) of \( U_z \) exists iff there are such indices \( 0 \leq \i_1 < \ldots < \i_m \leq N \).
that \( W \) is a compound of the variety \( \{ h_i(z) = \ldots = h_i(z) = 0 \} \subset \mathbb{P}^{d+1} \), wherein the coordinates of the point \( z \) are substituted instead of \( Z_1, \ldots, Z_{n-4} \), i.e., \( h_i(\mathcal{Z}) \in \mathbb{F}[X_0, \ldots, X_{d+1}] \) (cf. §4a [2]).

One can construct (see §2 [2]) a family \( \mathcal{M} = \mathcal{M}_{s, s-m, d} \) consisting of \((s-m+1)\)-tuples of linear forms in \( \lambda_1, \ldots, \lambda_{s+1} \), with the coefficients from \( \mathcal{H} \) such that for every variety \( W \subset \mathbb{P}^s \) satisfying the inequalities \( \dim W \leq s-m, \deg W \leq d \), there is \((s-m+1)\)-tuple \((\lambda_1, \ldots, \lambda_{s-m+1}) \in \mathcal{M} \) for which \( W \cap \{ \lambda_1 = \ldots = \lambda_{s-m+1} = 0 \} = \emptyset \). Therefore, for any \((s-m+1)\)-tuple \((\lambda_1, \ldots, \lambda_{s-m+1}) \in \mathcal{M} \), we can take a variety \( W \cap \{ \lambda_1 = 0 \} \) as \( W_1 \). Supplement linear forms \( \lambda_1 = \lambda_2, \ldots, \lambda_{s-m+1} \) up to a basis \( \lambda_0, \ldots, \lambda_{s+1} \) with the coefficients from \( \mathcal{H} \) of the space of linear forms in \( \lambda_0, \ldots, \lambda_{s+1} \) (in arbitrary manner). Replacing variables denote \( h_i(z, \lambda_0, \ldots, \lambda_{s+1}) = h_i(z) \) and \( \tilde{h}_i(z) = \tilde{h}_i(z, \lambda_0, \ldots, \lambda_{s+1}) = h_i(z, \lambda_0, \lambda_1, \ldots, \lambda_{s+1}) = \tilde{h}_i(z, \lambda_0, \lambda_1, \ldots, \lambda_{s+1}) \). Thus, the condition under consideration is equivalent to that there are indices \( 1 \leq i_1 < \ldots < i_m \leq s+1 \) and linear forms \( \lambda_{i_1}, \ldots, \lambda_{i_m} \) for which the variety \( \{ \tilde{h}_i(z) = \tilde{h}_i(z) = 0 \} \subset \mathbb{P}^m \) as one of its compounds has a certain point \( \Omega = (\xi_0, \xi_1, \ldots, \xi_{s-m+1}) \) such that the point \( \Omega = (\xi_0 : 0 : \ldots : 0 : \xi_{s-m+1} : \ldots : \xi_{s+1}) \in \mathbb{U}_0 \cap \{ \lambda_0 \neq 0 \} \)

(in force of the theorem about the dimension of intersection [14].).

Introduce a system of homogeneous algebraic equations

\begin{equation}
\tilde{h}_i(z) - \lambda_j Y_{s-m+j+1} = 0; \quad 1 \leq j \leq m
\end{equation}

in the variables \( \lambda_0, \lambda_1, \ldots, \lambda_{s+1} \) with the coefficients from \( \mathbb{F}[\lambda] \) where \( \lambda \) is algebraically independent over \( \mathbb{F} \). One can prove (see also lemma 11 § 5 [3]) that the set of roots in \( \mathbb{P}^m(\mathbb{K}) \) of the system (2) is finite. The variety of roots is decomposable on the irreducible and defined over \( \mathbb{K} \) multidimensional compounds \( V_{P_k} \) corresponding to the minimal prime ideals \( \mathfrak{p}_k \subset \mathbb{K}[\lambda_0, \lambda_1, \ldots, \lambda_{s+1}] \),\( \{ h_i(z) - \lambda Y_{s-m+j+1} \} \in \mathbb{K} \).

The system (2) can be considered apart that as the system in the variables \( \lambda, \lambda_0, \lambda_1, \ldots, \lambda_{s+1} \) with the coefficients from \( \mathbb{F} \) which determines a variety \( \tilde{U}_{m+1}^{p_{\mathbb{F}}} \subset \mathbb{A}^{m+1}(\mathbb{F}) \). It is not difficult to show (cf. lemma 12 § 5 [3]) that there is a bijective correspondence between the points \( V_{P_k} \) and on the other side such compounds \( V_{P_{\mathbb{F}}} \) of the variety \( \tilde{U}_{m+1}^{p_{\mathbb{F}}} \) that \( V_{P_{\mathbb{F}}} \) is not isomorph in any union of finite number of hyperplanes of the kind \( \{ -c_1 = 0 \} \subset \mathbb{A}^{m+1} \) for \( c_1 \in \mathbb{F} \), notice that \( \dim V_{p_{\mathbb{F}}} = \lambda \).

Now we exhibit an important auxiliary device from [11] (see also §3 [2]). Let \( g_0, \ldots, g_{K-1} \in \mathbb{F}[\lambda_0, \lambda_1, \ldots, \lambda_{s+1}] \) be homogeneous polynomials of degrees \( \delta_{0,2}, \ldots, \delta_{K-1} \) respectively. Introduce new variables
\[ U_{n}, \ldots, U_{n} \text{ algebraically independent over } F(\lambda_{0}, \ldots, \lambda_{n}) \]. Set
\[ q_{k} = \lambda_{0} U_{0} + \cdots + \lambda_{k} U_{n} \in \mathbb{F}(U_{0}, \ldots, U_{n}) \] and
\[ D = \sum_{\alpha \leq k} \delta_{\alpha} - \nu, \]
herein \( \delta_{\alpha} = 1 \) if \( k \leq j \leq \kappa \). Consider linear over \( \mathbb{F}(U_{0}, \ldots, U_{n}) \) mapping \( \mathcal{O} : B_{0} \oplus \cdots \oplus B_{k} \rightarrow B \) where \( B_{0} \) (correspondingly \( B_{k} \)) is the space of homogeneous polynomials in \( \lambda_{0}, \ldots, \lambda_{n} \) over the field \( \mathbb{F}(U_{0}, \ldots, U_{n}) \) of degree \( D - \delta_{\alpha} \) (correspondingly \( D \)) for \( 0 \leq \alpha \leq k \), namely \( \mathcal{O}(b_{0}, \ldots, b_{k}) = \sum_{\alpha \leq k} \delta_{\alpha} \mathcal{O}_{\alpha} \).

Any element \( b = (b_{0}, \ldots, b_{k}) \in B_{0} \oplus \cdots \oplus B_{k} \) can be written in the form
\[ b = (b_{0}, \ldots, b_{0} \cdot \delta_{0}, b_{1}, \ldots, b_{1} \cdot \delta_{1}, \ldots, b_{k+1}, \ldots, b_{k} \cdot \delta_{k}) \]
where \( b_{i} = (\sum_{\alpha \leq k} \delta_{\alpha} b_{i}^{\alpha} \delta_{\alpha}) \) and \( b_{i} \cdot \delta_{i} \) are the coefficients of the polynomial \( b_{i} \) provided that a certain numeration of all the monomials of the degree \( D - \delta_{i} \) is fixed. Analogously one can write the elements of the space \( B \). In the chosen system of coordinates the mapping \( \mathcal{O} \) has a matrix \( \mathbf{A} \) of the size \( (\kappa+D) \times (\sum_{\alpha \leq k} \delta_{\alpha}) \). One can represent \( \mathbf{A} = (\mathbf{A}', \mathbf{A}^\prime) \) where \( \mathbf{A}' \) (call it the number part of \( \mathbf{A} \)) contains \( \sum_{\alpha \leq k} \delta_{\alpha} \) columns and \( \mathbf{A}^\prime \) (call it the formal part) contains \( \kappa \) columns, besides that the entries of \( \mathbf{A}' \) belong to \( \mathbb{F} \), the entries of \( \mathbf{A}^\prime \) are linear forms over \( \mathbb{F} \) in variables \( U_{0}, \ldots, U_{n} \) (cf. [6]).

There is proved in [10] that the system \( q_{0} = \cdots = q_{k-1} = 0 \) has no roots in \( \mathbb{P}^{n}(\mathbb{F}) \) iff the ideal \( (q_{0}, \ldots, q_{k-1}) \subset (\lambda_{0}, \ldots, \lambda_{n})^{D} \). Besides that, the following proposition is ascertained in [11].

1. The system \( q_{0} = \cdots = q_{k-1} = 0 \) has a finite number of roots in \( \mathbb{P}^{n}(\mathbb{F}) \) iff the rank \( \gamma = (\kappa+D) = \gamma' \);
2. All \( n \times n \) minors of \( \mathbf{A} \) generate a principal ideal whose generator \( \mathbf{R} = \mathbb{F}[U_{0}, \ldots, U_{n}] \) is their g.c.d.;
3. The homogeneous form \( \mathbf{R} = \prod_{i \in D_{1}} L_{i} \) where \( L_{i} = \sum_{\alpha \leq k} \xi_{i}^{(\alpha)} U_{i} \) is a linear form over \( \mathbb{F} \), moreover \( (\xi_{0}^{(i)}, \ldots, \xi_{n}^{(i)}) \) is a root of the system and the number of occurring of the forms proportional to \( L_{i} \) for each \( i \in D_{1} \) equals to the multiplicity of the corresponding root. Apart that \( \dim \mathbf{R} = D_{1} = \gamma - \gamma' \).

The algorithm designs the matrix \( \mathbf{A} \) with the entries from the ring \( \mathbb{F}[Y, Z_{1}, \ldots, Z_{n-5}, U_{0}, U_{n-5-m+1}, \ldots, U_{n-5+1}] \) corresponding to the modified system (2) in which \( Z_{1}, \ldots, Z_{n-5} \) are considered as variables (instead of \( Z_{1}, \ldots, Z_{n-5} \)) according to the only exhibited device.

Denote by \( \mathbf{A}_{\mathbf{X}} \) the matrix obtained from \( \mathbf{A} \) by means of substituting the coordinates of the point \( \mathbf{X} \) instead of \( Z_{1}, \ldots, Z_{n-5} \). Let the polynomial \( \mathbf{R}_{X} \subset \mathbb{F}[Y, U_{0}, U_{n-5-m+1}, \ldots, U_{n-5+1}] \) correspond to the matrix \( \mathbf{A}_{\mathbf{X}} \) as in the proposition. One can suppose w.l.o.g. that \( X \neq R_{X} \) (dividing \( R_{X} \) on the greatest possible power of the variable \( Y \)).
Regard a certain representation of the union $\bigcup_{\mathbb{F}_p} V_{\mathbb{F}_p} = \{S_0, \ldots, S_{k-1}\}$ for suitable polynomials $S_i \in \mathbb{F}[Y_1, Y_2, Y_5, m+2, \ldots, Y_{5+k}]$ homogeneous relatively to $Y_0, Y_5, m+2, \ldots, Y_{5+k}$. Considering a system $S_i(0, Y_0, Y_5, m+2, \ldots, Y_{5+k}) = 0$, $0 \leq k < 1$ and basing on the proposition (see also lemma 16 § 3 [3]), one proves that $R_k(\alpha_{\mathbb{F}_p}, \beta_{\mathbb{F}_p}, m+2, \ldots, m+5) = \prod L_i^{k_i}$ and moreover the linear forms $L_i = \sum_{j} \xi_{i}^{(j)} U_j$ correspond bijectively to the points $(\xi_i^{(j)}, \xi_i^{(j)}, \xi_i^{(j)}, \xi_i^{(j)}, \xi_i^{(j)}) \in W'_2 \subset \mathbb{P}^m$ where the cone $\text{cone}(W'_2) = (\bigcup_{\mathbb{F}_p} V_{\mathbb{F}_p}) \cap \{ Y = 0 \}$. Thereupon it is not difficult to check that $\alpha_{\mathbb{F}_p} \in W'_2$ (cf. lemma 13 § 5 [3]). Summarizing and utilizing the notations introduced above, we have ascertained the following.

**Lemma 1.** The formula $\exists X_0 \exists Y \exists \phi (E_{1, k < 1} (\phi = 0) \& (\phi \neq 0))$ is valid in a point $\mathbb{F}_p$ iff for appropriate $0 \leq m \leq s+1$ there exist such indices $i_1 < \cdots < i_m < N'$, a set of linear forms $(Y_1, \ldots, Y_{5+m}) \in \mathcal{M}$ and a point $\Omega = (z_0, \ldots, z_{5+m}, \ldots, z_{5+s}) \in \mathbb{U}_x \cap \{ X_0 \neq 0 \}$ (in the coordinates $Y_0, Y_1, \ldots, Y_{5+k}$) that the linear form $(\xi_0, u_0 + \xi_0, u_0 + \xi_0, u_0 + \xi_0, u_0 + \xi_0, u_0 + \xi_0) \in \mathbb{R}_{x} (0, u_0, u_0, u_0, u_0, u_0)$. Now make more precise the definition of a version of Gaussian algorithm (v.g.a.) for reducing the matrices to the generalized trapezium form (cf. [7]) v.g.a. is determined by a succession of pairs of indices $(i_0, j_0), (i_1, j_1), \ldots, (i_s, j_s)$. Here with $i_0 \neq j_0$ and $i_s \neq j_s$ for $s > 0$. For any initial matrix $A^{(a)}$, v.g.a. yields the chain of matrices $A^{(0)}, A^{(a+0)}, \ldots, A^{(n)}$. Introduce a notation $A^{(a+0)} = (a_i^{(a)})$. Apart that $a_i^{(a+0)} = 0$, $a_i^{(a+0)} = a_i^{(a)} + a_i^{(a)}\lambda d_i^{(a)}$, for all $i$ distinguished from $i_0, \ldots, i_s$, lastly $a_i^{(a+1)} = \lambda a_i^{(a+0)}$ where $0 \leq s < a$ in the generalized trapezium form, namely, $A^{(a+0)} = 0$ when either $i$ differs from $i_0, \ldots, i_s$ or $i = j, j = j_0$ and $a_i > a$, besides that $a_i^{(a+1)} = a_i^{(a+0)}$. Denote by $A_i^{(a)}$ the determinant of $(a+1)_{i,j}^{(a+1)}$ matrix formed by the rows with the indices $i_0, \ldots, i_s$ and the columns with the indices $j_0, \ldots, j_s$, provided that $i \neq i_0, \ldots, i \neq i_s$ and $j \neq j_0, \ldots, j \neq j_s$. Then $a_i^{(a+1)} = \lambda a_i^{(a)} / a_i^{(a+0)}$ (see e.g. lemma 7 [7]).

Now we turn ourselves to considering an arbitrary point $x \in A_{\mathbb{F}_p}$. Fix for some time $0 \leq m \leq s+1$ and a set of linear forms $(Y_1, \ldots, Y_{5+m}) \in \mathcal{M}$ (see lemma 1). By $a_i$ denote the number of rows of the matrix $A$. Produce a certain succession of v.g.a.s $\Gamma_0, \Gamma_1, \ldots$ over a field $F(Y_1, \ldots, Y_{5+m}, u_0, u_0, u_0, \cdots, u_0)$ and a succession of polynomials $p_0, p_1, \ldots \in F[Y_1, \ldots, Y_{5+m}, u_0, u_0, u_0, \cdots, u_0]$ thereto v.g.a. $\Gamma_i$ can be applied
correctly to the matrix $A_z$ for all points $z=(z_1, \ldots, z_{n-5})$ of (possibly empty) quasiprojective variety $[14]$ \( W_i \subseteq A^{n-5} \), which is defined by the following conditions: inequality $0 \notin P_i(Y, z_1, \ldots, \bar{z}_{n-5}, u_0, u_{n-5}, \ldots, u_{n+4}) \in \mathbb{F}$ \([Y, u_0, u_{n-5}, \ldots, u_{n+4}] \) and equalities $0 = P_i(Y, z_1, \ldots, \bar{z}_{n-5}, u_0, u_{n-5}, \ldots, u_{n+4})$ for $1 \leq i \leq 7$ are fulfilled. Apart from the variety $[\{z_1, \ldots, z_{n-5}\}; P_i(Y, z_1, \ldots, \bar{z}_{n-5}, u_0, u_{n-5}, \ldots, u_{n+4}) = 0$ for all $i \}$, henceforth $U_i W_i = A^{n-5}$. Exposed below construction is close to the proof of the lemma $9$ $[7]$.

Later on we apply the v.g.a.s. $\Gamma^i, \Gamma^ii, \ldots$ to the initial matrix $A$. As $\Gamma^i$ one can take an arbitrary v.g.a. Set a polynomial $P_i = \prod_{0 \leq i \leq \beta} \Delta_i$ (for v.g.a. regarded at the current step the same notations as above are utilized). Assume that $\Gamma^i, \ldots, \Gamma^ii; P_i, \ldots, P_i$ are already produced. Then as $\Gamma^i+1$ we take v.g.a. in which for every $0 \leq i \leq \beta i+1$, the column index $j_{\beta i+1}$ of the pivot in the matrix $A_i$ is the least possible, moreover $j_{\beta i+1} > j_{\beta i-1}$ and the polynomials $P_i, \ldots, P_i, \prod_{0 \leq i \leq \beta} \Delta_i$ are linearly independent over $\mathbb{F}$. Finally, put $P_i = \prod_{0 \leq i \leq \beta} \Delta_i$ (for v.g.a. $\Gamma^i, \ldots, \Gamma^ii$ when it is impossible to produce $\Gamma^i+1$ satisfying formulated above requirements (if $P_i+1$ then $W_i = \emptyset$).

One can ascertain that if $W_i \neq \emptyset$ then for each $z \in W_i$ the polynomial $R_z$ (see proposition) is obtained as the value in the point $z$ of the polynomial $\det \Delta_i$ (up to a factor $V^E$ for a suitable $E_i$), where $V \chi$ submatrix $\Delta_i$ of the matrix $A$ is generated by the columns with the indices $j_0, \ldots, j_{n-1}$ corresponding to v.g.a. $\Gamma^i$. This follows from the fact that in the matrix $A_i$ an entry $a_{i, j}$ is $0$ when $\beta \neq j_1, \ldots, j_{n-1}$ and $j \neq j_{\beta i}$. In force of the choice of $j_{\beta i}$. Therefore, if for an appropriate $\beta$ a cell $(j_{\beta i}, j_{\beta i})$ belongs to the number part $A'$ of $A$, and a cell $(i_1, j_{i_1})$ belongs to the formal part $A''$ of $A$ then $\gamma((A')_E) = \delta$ that implies the mentioned representation of $R_z$.

Write $\det \Delta_i = \sum \delta \Delta_i^{(E)} V^E$, herewith $\Delta_i^{(E)}(z_1, \ldots, z_{n-5}) \in \mathbb{F}[z_1, \ldots, z_{n-5}]$. Introduce varieties $W_i^{(E)} = \{(z_1, \ldots, z_{n-5}) \in W_i : \Delta_i^{(E)}(z_1, \ldots, z_{n-5}) = 0\}$ for $E \geq 0$. The variety $W_i^{(E)}$ is quasiprojective as the intersection of two quasiprojective varieties, namely, if $\Sigma_i^{(E)} = \{G^{(E)} = 0\} \cap \mathbb{V}_i^{(E)}$ then $\Sigma_i^{(E)} = \{G^{(E)} = 0\}$ and $\mathbb{V}_i^{(E)}$. Moreover $W_i^{(E)} \cap \mathbb{V}_i^{(E)} = \emptyset$ for $E_1 \neq E_2$ and $U_j W_i^{(E_j)} = W_i$.

Thereupon represent $\Delta_i^{(E)} = \sum_{0 \leq i \leq j} \epsilon_i(E) U_i^{(E)}$ where $\epsilon_i^{(E)}(z_1, \ldots, z_{n-5}) \in \mathbb{F}[z_1, \ldots, z_{n-5}, u_{n-5}, \ldots, u_{n+4}]$. Consider quasiprojec-
tive varieties $W_{t_{2}}^{(g_{2})} = \{(z_{1},\ldots,z_{n_2}) \in W_{t_{2}}^{(g_{2})} : c_{t_{2}}^{(x_{2})}(z_{1},\ldots,z_{n_2}) = 0, 0 \leq x < j_{2} \}$, $e_{t_{2}}^{(x_{2})}(z_{1},\ldots,z_{n_2}) \neq 0 \}$, then $W_{t_{2}}^{(g_{2})} \cap W_{t_{1}}^{(g_{1})} = \emptyset$ when $j_{1} \neq j_{2}$ and $U_{t_{0}} \in \text{De}_{t_{0}} W_{t_{1}}^{(g_{1})}$.

Observe that the proposition and the ascertained earlier entail that $(\Delta_{t_{1}}^{(g_{1})})_{x} = \Delta_{t_{2}}^{(g_{2})}(z_{1},\ldots,z_{n_{2}},U_{t_{0}},U_{t_{0}}^{n_{1}+2},\ldots,U_{t_{0}}^{n_{1}+l})$ is a product of linear forms for $x \in W_{t_{1}}^{(g_{1})}$. This implies that for $x \in W_{t_{1}}^{(g_{1})}$, the polynomial $(c_{t_{1}}^{(x_{1})})_{x}$ equals to the product of powers of linear forms $L_{t_{1}}^{(x_{1})}$ of all linear forms $L_{t_{1}}^{(x_{1})}$ in which the coefficient at $U_{t_{0}}$ vanishes.

Henceforth $(c_{t_{1}}^{(x_{1})})_{x}$ in the ring $K[Z_{t_{0}},U_{t_{0}}^{n_{1}+2},\ldots,U_{t_{0}}^{n_{1}+l}]$.

Our nearest purpose is to calculate the quotient $(\Delta_{t_{1}}^{(g_{1})})_{x}/(c_{t_{1}}^{(x_{1})})_{x}$ for $x \in W_{t_{1}}^{(g_{1})}$. If $I = (t_{0},m_{1}+1,\ldots,t_{0}+l)$ is a multiindex then denote $U_{t_{0}}^{I_{1}} = U_{t_{0}}^{I_{1}+m_{1}+1},\ldots,U_{t_{0}}^{I_{1}+l}$ apart that by $I < J$ denote the lexicographical order on multiindices. Write $c_{t_{1}}^{(x_{1})} = \sum_{I} u_{I}^{I}$ and let $0 \neq u_{I}^{I} \in F[Z_{t_{0}},\ldots,Z_{t_{0}-s}]$ for certain $I$ (fixed in further speculations).

Introduce a quasiprojective variety $W_{t_{1}}^{(g_{1})} = \{(z_{1},\ldots,z_{n_{2}}) \in W_{t_{1}}^{(g_{1})}: y_{t_{0}}^{(x_{1},\ldots,z_{n_{2}})} = 0 \}$. Evidently $W_{t_{1}}^{(g_{1})} \cap W_{t_{1}}^{(g_{1})} = \emptyset$ if $I < J$. and $U_{t_{0}},W_{t_{1}}^{(g_{1})} = W_{t_{1}}^{(g_{1})}$. For any point $(z_{1},\ldots,z_{n_{2}}) \in W_{t_{1}}^{(g_{1})}$ the quotient $(\Delta_{t_{1}}^{(g_{1})})_{x}/(c_{t_{1}}^{(x_{1})})_{x}$ can be obtained by means of the described below process of dividing polynomial on polynomial and after that substituting the coordinates $z_{1},\ldots,z_{n_{2}}$ instead of variables $Z_{t_{0}},\ldots,Z_{t_{0}-s}$.

Let $0 \neq a \in F[Z_{t_{0}},\ldots,Z_{t_{0}-s}][U_{t_{0}}^{m_{1}+1},\ldots,U_{t_{0}}^{n_{1}+l}]$. Denote by $\Delta_{t_{1}}^{(g_{1})}(a)_{x}$ the monomial of $\Psi$ in variables $W_{t_{0}}^{m_{1}+1},\ldots,U_{t_{0}}^{n_{1}+l}$ for which $a_{x}$ occurs only the monomials less than $a_{x}$. set $\Psi = \Psi(W_{t_{0}}^{m_{1}+1},U_{t_{0}}^{n_{1}+2},\ldots,U_{t_{0}}^{n_{1}+l})$ and $\Psi(a_{x}) = \deg(a_{x})$. Delete from $c_{t_{1}}^{(x_{1})}$ all the monomials $u_{I}^{I}$ (except $u_{I}^{I}$) with $\Psi(a_{x}) > \Psi(u_{I}^{I})$ and denote obtained polynomial by $c_{t_{1}}^{(x_{1})}_{a_{x}}$. Then $(c_{t_{1}}^{(x_{1})})_{a_{x}}(c_{t_{1}}^{(x_{1})})_{a_{x}} = \prod_{I}^{l} y_{t_{0}}^{I}$ where $(c_{t_{1}}^{(x_{1})})_{a_{x}}$ is the product of linear forms. For any index $j < x \leq \delta_{t_{1}}$, the algorithm designs a succession of non-zero monomials $\Psi_{y} = e_{t_{1}}^{(x_{1})}(y_{1},\ldots,y_{p})$ and $\Psi_{y} = \Psi_{y}(y_{1},\ldots,y_{p})$. Represent uniquely $\Psi = \Psi_{y}^{(0)},\Psi_{y}^{(1)},\Psi_{y}^{(2)}$, where $\Psi_{y}^{(0)}$ are homogeneous, $\Psi_{y}^{(0)}(y_{1},\ldots,y_{p}) = \Psi_{y}^{(0)}(y_{1},\ldots,y_{p})$ and $\Psi_{y}^{(0)}(y_{1},\ldots,y_{p}) = \Psi_{y}^{(0)}(y_{1},\ldots,y_{p})$ [for $0 \leq y_{j} < \delta_{t_{1}}$], lastly each monomial from $\Psi_{y}^{(0)}$ is not divided by $\Psi_{y}^{(0)}$. Then $\Psi_{y}^{(0)} = \Psi_{y}^{(0)} - \Psi_{y}^{(0)}(y_{1},\ldots,y_{p}) / \Psi_{y}^{(0)}$ for every $0 \leq y_{j} < \delta_{t_{1}}$ (obviously, $\Psi_{y}^{(0)} < \Psi_{y}^{(0)}$). Regard a polynomial $\Psi_{y}^{(0)} = \sum_{y_{j} < \delta_{t_{1}}} y_{j}^{(y_{j})} / \Psi_{y}^{(0)} \in F[Z_{t_{0}},\ldots,Z_{t_{0}-s},U_{t_{0}}^{m_{1}+2},\ldots,U_{t_{0}}^{n_{1}+l}]$ and set $\Psi_{y}^{(0)} = \Psi_{y}^{(0)} / \Psi_{y}^{(0)} + \sum_{y_{j} < \delta_{t_{1}}} y_{j}^{(y_{j})} / \Psi_{y}^{(0)} \in F[Z_{t_{0}},\ldots,Z_{t_{0}-s},U_{t_{0}}^{m_{1}+2},\ldots,U_{t_{0}}^{n_{1}+l}]$.

One can check that $(c_{t_{1}}^{(x_{1})})_{a_{x}}(c_{t_{1}}^{(x_{1})})_{a_{x}}(c_{t_{1}}^{(x_{1})})_{a_{x}} = \Psi_{y}^{(0)}(y_{1},\ldots,y_{p})$ for $x \in W_{t_{1}}^{(g_{1})}$ and therefore $(\Delta_{t_{1}}^{(g_{1})})_{x}/(c_{t_{1}}^{(x_{1})})_{x} = \Psi_{y}^{(0)}(y_{1},\ldots,y_{p})$ for all linear forms $L_{t_{1}}^{(x_{1})}$ in which the coefficient for all linear forms $L_{t_{1}}^{(x_{1})}$
at the variable \( U_\sigma \) does not vanish.

Thereupon remind that \( \text{Con} W_\xi = U_\sigma V_\gamma \bigcap \{ Y = 0 \} \) and introduce \( W'_i = \bigcup_{\xi \in W_i} (\{ z \times (W' \cap \{ Y_\sigma \neq 0 \}) \} \) (as above we fix \( i, \xi \)).

Observe that \( W'_i = \{ (z_1, \ldots, z_{K-5}, (y_\sigma, y_\sigma + m + 2, \ldots, y_{N+i}) \in W_i \} \times \bigcap_{\xi \in W_i} (z_1, \ldots, z_{K-5}, (y_\sigma, y_\sigma + m + 2, \ldots, y_{N+i}) \in W_i \} \times A^m(F) \). Representing the polynomial \( \psi^{(C)}_i (\sum_{-m+2}^{4} z_{8+i}, y_\sigma, y_\sigma + m + 2, \ldots, y_{N+i}, y_{8+i}) \in \text{Con} W_i \) leads to an equality \( W'_i = \{ \} \bigcap (W_i \bigcap A^m) \). Because of that the subset \( W'_i \) is closed in the quasi-projective variety \( W_i \bigcap A^m \).

Consider the natural linear projection \( \pi_i : \mathbb{P}^m(\mathbb{F}^m \bigcap \{ Y_\sigma = 0 \}) \to \mathbb{P}^{m-5} \) defined by the formula \( \pi_i (Z_1, \ldots, Z_{K-5}, (y_\sigma, y_\sigma + m + 2, \ldots, y_{N+i}) = (Z_1, \ldots, Z_{K-5}) \).

Let a morphism \( \pi_i : W_i \to W'_i \) be the restriction of \( \pi_i \) on \( W_i \).

Our nearest goal is to show that \( \pi_i \) is finite (\cite{14}). Obviously, the inverse image \( W'_i \) is isomorphic to \( W_i \bigcap A^m \bigcap \{ Y_\sigma = 0 \} \), henceforth \( \pi_i^{-1}(W'_i) \) is open in \( W'_i \) and besides that \( \pi_i^{-1}(W'_i) \) is affine since \( \pi_i^{-1}(W'_i) \) is closed in the open affine set \( \pi_i(W_i) \bigcap A^m \) (\cite{14}). Now we check that every coordinate function \( Y_\sigma \bigcap A^m \) on the variety \( \pi_i^{-1}(W'_i) \) satisfies a suitable relation of integral dependence over the ring \( \mathbb{F}[V] \) where \( \sigma - m + 2 \leq \sigma \leq \sigma + 1 \). Let \( \psi^{(C)}_i (Y_\sigma, y_\sigma, y_\sigma + m + 2, \ldots, y_{N+i}) = 0 \) on \( W_i \), herein \(-1\) is substituted instead of the variable \( U_{\sigma \sigma} \). Taking into account that \( \{ Y_\sigma \} \neq 0 \) when \( z \in W_i \) this yields an equation of integral dependence.

So, we infer that the morphism \( \pi_i \) is finite.

Utilizing the notations from the lemma 1 one concludes that a set \( \{ \pi_i^{-1}(W'_i) \} \) consisting of all such points \( z = (z_1, \ldots, z_{K-5}) \) in \( W_i \) that there exists a point \( \Omega_i (z_1, \ldots, z_{K-5}) \in U_\xi \) in \( W_i \) as \( \pi_i^{-1}(W'_i) \) coincides with the image under projection \( \pi_i \) of the closed domain of definition of \( \pi_i \) (i.e. in \( W_i \) set \( \pi_i^{-1}(W'_i) \) \bigcap \{ \sum_{-m+2}^{4} z_{8+i} = 0 \} \) where \( \sum_{-m+2}^{4} z_{8+i} = \sum_{-m+2}^{4} y_\sigma + m + 2, \ldots, y_{N+i} \) and \( \pi_i^{-1}(W'_i) \) for \( \xi = \xi \leq \kappa \) and since the image of the closed set under a finite morphism is again closed (\cite{14}).

Now we describe a procedure for constructing the required \( V^{(i)}_i \).

Let the quasi-projective variety \( W_i \) be \{ \pi_i (G_\sigma \neq 0) \} \times \{ Y_\sigma \neq 0 \} \), herewith the polynomials \( G_\sigma, C_\sigma \in F[Z_{-m+2}, \ldots, Z_{K-5}] \) were actually produced earlier. Denote the closure of the projection \( \pi_i (G_\sigma \neq 0) \) by \( \pi_i^{-1}(W'_i) \) \bigcap \{ Y_\sigma \bigcap A^m \} \) \bigcap \{ \pi_i (G_\sigma \neq 0) \} \bigcap \{ Y_\sigma \neq 0 \} \). On the other hand in force of the aforesaid the equalities hold \( \pi_i^{-1}(W'_i) \), \( V^{(i)}_i \), \( \pi_i^{-1}(W'_i) \bigcap \{ \pi_i (C_\sigma = 0) \} \).
Involving the theorem 2 (see section 1) the algorithm finds the general points of the compounds \( \mathcal{P} \) of the variety \( \{ B_0 = 0 \} \) and \( \{ E_0 = 0 \} \). It is sufficient for each \( \mathcal{P} \) to construct the closure of its projection \( \mathcal{S}_d(\mathcal{P}) \). Notice that there is an imbedding of the fields of functions \( F^d(\mathcal{S}_d(\mathcal{P})) = F^d(\mathcal{Z}_{\mathcal{P}}) \subseteq F^d(\mathcal{Z}_{\mathcal{P}}) \). Therefore, the algorithm can produce the general point of \( \mathcal{S}_d(\mathcal{P}) \) yielding firstly a transcendental basis and after that a primitive element (cf. (1), section 1). Searching a transcendental basis and also a primitive element is based on the procedure for calculating a polynomial relation over \( F^d(\mathcal{P}) \) (if it exists) between the elements \( a_1, \ldots, a_{d+1} \in F[t_1, \ldots, t_{d-1}, t_d] \) if \( 0 \in F^d(\mathcal{P}) \), provided that \( a_1, \ldots, a_{d+1} \) are algebraically independent over \( F \), the procedure in its turn is reducible to solving a linear system whose indeterminates are the coefficients of the relation (cf. § 1 [2], § § 4, 6 [3]). Thereupon with the help of the remark just after the theorem 2 the algorithm computes a representation \( \mathcal{S}_d(\mathcal{P}) = \{ b_0 = 0 \} \) where the polynomials \( b_0 = 0 \) where the polynomials \( b_0 \in F[z_{d+1}, \ldots, z_{d+s}] \).

We summarize the results of the present section in the following lemma, in which bounds are obtained making use of the theorem 2.

LEMMA 2. An algorithm is suggested which outputs the constructive set \( \mathcal{P}(U \cup \{ X_0 \neq 0 \}) \cup \{ (z_1, \ldots, z_{d+s}) \in N^{d+s} : (F) \} = \{ (z_1, \ldots, z_{d+s}) : (F) \} \). Then, the projection \( V_{d+s} \) from \( \mathcal{S}_d(\mathcal{P}) \) to \( \mathcal{S}_d(\mathcal{P}) \), i.e. the projection in the form \( \{ (z_1, \ldots, z_{d+s}) \} \in \mathcal{S}_d(\mathcal{P}) \). Thereby \( \deg_{z_{d+1}, \ldots, z_{d+s}}(B_0(\mathcal{P})) \leq d^4 + O(d^4) \). And \( \deg_{z_{d+1}, \ldots, z_{d+s}}(B_0(\mathcal{P})) \leq d_2 \cdot \mathcal{P}(d_3 + \mathcal{P}(d_4)) \). Apart that \( \deg_{z_{d+1}, \ldots, z_{d+s}}(C(\mathcal{P})) \leq d_2 \cdot \mathcal{P}(d_3 + \mathcal{P}(d_4)) \). Besides that, \( \mathcal{P}(d_3 + \mathcal{P}(d_4)) \) is the running time of the algorithm can be estimated by \( \mathcal{P}(d_3 + \mathcal{P}(d_4)) \).

3. Subexponential-time deciding the first order theory of algebraically closed fields

Let a Boolean formula \( Q \) with \( N \) atoms of the kind \( \mathcal{L}_a = 0 \) where \( \mathcal{L}_a \in F[x_1, \ldots, x_N] \) satisfies the same bounds as in the section 1, be given, \( \mathcal{L}_a(Q) \) denotes the size of \( Q \). Firstly we exhibit a procedure reducing \( Q \) to a disjunctive normal form.
Following [7] name \((q_1, \ldots, q_p)\)-cell for \(q_i \in F[X_1, \ldots, X_n]\) any nonempty quasiprojective variety of the kind \(\{j \in \mathbb{N} \mid q_j = 0\} \cup \{j \in \mathbb{N} \mid q_j \neq 0\}\) is a \(\mathbb{A}^n_k\) cell, herewith \(\gamma_1 \cup \gamma_2 = \{1, \ldots, p\}\), \(\gamma_1 \cap \gamma_2 = \emptyset\).

By means of the Besout inequality [14] it is ascertained in [7] that a number of all \((q_1, \ldots, q_p)\)-cells is less or equal to \((1 + \deg q_1 + \ldots + \deg q_p)^k\). We shall describe the method for decomposing the space \(\mathbb{A}^n_k\) on \((q_1, \ldots, q_p)\) -cells by recursion on \(p\). Assume that we are supplied with all \((q_1, \ldots, q_{p-1})\)-cells \((\rho = i)\). Every \((q_1, \ldots, q_p)\)-cell is of the form either \(K \cap \{q_p = 0\}\) or \(K \cap \{q_p \neq 0\}\) for a pertinent \((q_1, \ldots, q_{p-1})\)-cell \(K\). Henceforth it is sufficient to pick out (involving the theorem 2 from the section 1) all nonempty sets among quasiprojective varieties of the forms \(K \cap \{q_p = 0\}\) and \(K \cap \{q_p \neq 0\}\).

Applying the just described method the algorithm yields all \(\{i_1, \ldots, i_N\}\)-cells. Again repeatedly making use of the theorem 2 by induction on the number of logical signs in \(Q\) the algorithm for each \(\{i_1, \ldots, i_N\}\)-cell checks, whether this cell is contained in the constructive set \(\Pi_{Q = \{Q\}} \subseteq \mathbb{A}^n_k\) determined by the formula \(Q\), and thereby represents \(\Pi_Q\) as a union of \(\{i_1, \ldots, i_N\}\)-cells \(K^{(\mu)}\) that means reducing \(Q\) to a disjunctive normal form \(\bigvee_{\mu} (\bigwedge_{\delta \neq 4} (\{f_{i_1}^{(\mu)}\} = \{j\}^0))\). Moreover \(i \leq \mu \leq (\{N + 1\})^k\), \(1 \leq \delta \leq N\), any polynomial \(f_{i_1}^{(\mu)}\) for a relevant \(i\) and \(f_{j}^{(\mu)} = \bigwedge_{i \leq \delta} f_{i}^{(\mu)}\) for an appropriate \(j \in \{1, \ldots, N\}\). The working time of the exhibited procedure can be estimated according to the theorem 2 by \(\mathcal{O}(L_2(Q), N^k, (d_1^\mu d_2^\mu)^N, \varphi)\).

Finally we pass to the general case. Let an input formula of the first order theory

\[
\exists Z_{i_1} \ldots \exists Z_{i_N} \forall Z_{k_1} \ldots \forall Z_{k_m} \exists Z_{a_1} \exists Z_{a_2} \quad Q
\]

be given where the formula \(Q\) is of the kind as at the beginning of the section, \(i_1 < \cdots F[Z_1, \ldots, Z_{a+1}, \ldots, Z_{a+b}]\), herein \(Z_1, \ldots, Z_{a+b}\) occur free, \(a = s_0 + s_1 + \cdots + s_b\), by \(L_2\) denote the size of \((3). Applying to (3) alternatively the just exhibited procedure for reducing to a disjunctive normal form and the lemma 2 (section 2) the algorithm arrives after performing \(\infty\) steps at an equivalent to (3) formula

\[
\exists Z_{i_1} \cdots \exists Z_{i_N} \exists Z_{a_1} \exists Z_{a_2} \ldots \exists Z_{a_2} \exists Z_{a_2} (V_{i_1, i_2, i_3} (\alpha) \land i_1 \in \mathbb{A}^n_k (\alpha, (i_1^{(0)} = 0) \land (i_1^{(\infty)} = 0))).
\]

Denote \(d_{i_1}^{(\infty)} = \max i_1 \deg Z_{i_1, \ldots, i_1} Z_{j_1, \ldots, j_1} Z_{a_1, \ldots, a_1} (V_{i_1, i_2, i_3} (\alpha); d_{i_1}^{(2)} = \max i_1 \deg Z_{i_1, \ldots, i_1} (V_{i_1, i_2, i_3} (\alpha); Q(\alpha) = N(\alpha) K(\alpha) d_{i_1}^{(\infty)}; M_{i_1}^{(\infty)} = \max i_1 (V_{i_1, i_2, i_3} (\alpha); \sigma = s_0 \cdot a_{a+1}. Then in force of the theorem 2 and the inequalities hold: \(d^{(\infty)} \leq \)}
THEOREM 3. An algorithm is proposed which for a formula (3) outputs an equivalent to it a quantifier-free one \( \forall x \exists y \exists z \exists w \ldots \exists \eta \phi(x,y,z,w,\ldots,\eta) \) where \( x = \{x_1, \ldots, x_n\} \) and the running time of the algorithm (after \( \ell \) steps) is less than \( O\left(\frac{M}{\log M} + \frac{\log d_4}{\ell}\right)^{n+\ell} \), \( d_4 = p, d_5, d_6 \).

Performing \( \ell \) steps completes the proof of the following

REFERENCES


