Complexity of quantifier elimination in the theory of algebraically closed fields

Alexander Chistov, Dima Grigoriev

COMPLEXITY OF QUANTIFIER ELIMINATION IN THE THEORY OF ALGEBRAICALLY CLOSED FIELDS

A.L.Chistov, D.Yu.Grigor'ev
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 occuring 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 polynomial in the formula's size and in $(Nd)^{n^{(2a+2)}}$ time. Up to now a bound $(Nd)^{n^{O(n)}}$ was known ([5] , [7] , [15]).

1. Fast algorithms for factoring multivariable polynomials and for solving systems of algebraic 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 onevariable 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 provided that the number of variables is fixed. The authors [1] , [4] , have suggested a polynomial-time algorithm for factoring multivariable 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 computer algebra, namely in the problem of solving systems of algebraic equations. Earlier a complexity bound of the order d^{2^n} 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 $d^{O(n)}$ 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_2 of the input data (system) and in d^{n^2} time. Moreover, the algorithm finds all the irreducible compounds $W_\alpha \subset \mathbb{P}^n(\bar{F})$ of the variety of roots of the homogeneous system within the polynomial time in d^{nC} and in L_2 where $C = 1 + \max_\alpha \dim W_\alpha$ (the general case is reducible here to homogeneous one). Finding W_α allows to answer the principle 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 $F = H(T_1, \ldots, T_\ell)[\eta]$ where either $H = \mathbb{Q}$ or $H = \mathbb{F}_{q^\varkappa}$, $q = \mathrm{char}(H)$, the elements $T_1, \ldots, T_\ell$ be algebraically independent over H; the element η is separable and algebraic over a field $H(T_1, \ldots, T_\ell)$, denote by $\varphi = \sum_{0 \leq i < \deg_Z(\varphi)} (\varphi_i^{(1)}/\varphi^{(2)}) \cdot Z^i \in H(T_1, \ldots, T_\ell)[Z]$ its minimal polynomial over $H(T_1, \ldots, T_\ell)$ with the leading coefficient $lc_Z(\varphi) = 1$, herewith $\varphi_i^{(1)}, \varphi^{(2)} \in H[T_1, \ldots, T_\ell]$ and the degree $\deg(\varphi^{(2)})$ is the least possible. Any polynomial $f \in F[X_0, \ldots, X_n]$ can be uniquely represented in a form $f = \sum_{0 \leq i < \deg_Z \varphi;\, i_0, \ldots, i_n} (a_{i, i_0, \ldots, i_n}/b) \eta^i X_0^{i_0} \ldots X_n^{i_n}$ where $a_{i, i_0, \ldots, i_n}, b \in H[T_1, \ldots, T_\ell]$, the degree $\deg(b)$ is the least possible; the polynomials $a_{i, i_0, \ldots, i_n}, b$ are determined uniquely up to a factor from H^*. Set $\deg_{T_j} f = \max_{i, i_0, \ldots, i_n} \{\deg_{T_j}(a_{i, i_0, \ldots, i_n}), \deg_{T_j}(b)\}$. By a length of description $l(h)$ in the case $h \in \mathbb{Q}$ we mean its bitwise length, and in the case $h \in \mathbb{F}_{q^\varkappa}$ we mean $\varkappa \log_2(q)$. By $l(f)$ denote the maximum of the lengths of descriptions of the coefficients from H in the monomials in $T_1, \ldots, T_\ell$ of the polynomials $a_{i, i_0, \ldots, i_n}, b$.

Let $\deg_{X_j}(f) < r$, $\deg_{T_j}(f) < r_2$, $\deg_{T_j}(\varphi) < r_1$, $\deg_Z(\varphi) < r_1$, $l(f) \leq M_2$, $l(\varphi) \leq M_1$. As a size $L_1(f)$ of the polynomial f we consider in the theorem I a value $r^{n+\ell} r_2^{\ell} r_1 M_2$ and analogously $l(\varphi) = r_1^{\ell+1} M_1$.

THEOREM I. ([1] , [4]). One can factor the polynomial f over F within the polynomial in $L_1(f)$, $L_1(\varphi)$, 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 $\bar{F}$ of the field 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 $f_0, \ldots, f_K \in F[X_0, \ldots, X_n]$ are homogeneous relatively to $X_0, \ldots, X_n$ polynomials. Let $deg_{T_1,\ldots,T_\ell,Z}(\varphi) < d_1$, $\ell(f_i) \leqslant M_2$, $deg_{X_0,\ldots,X_n}(f_i) < d$, $deg_{T_1,\ldots,T_\ell}(f_i) < d_2$ for all $0 \leqslant i \leqslant K$ and in the theorem 2 a size $L_2(f_i) = \binom{d+n}{n} d_1 d_2^\ell M_2$ and $L_2(\varphi) = d_1^{\ell+1} M_1$. Denote $L = L_2(f_0) + \ldots + L_2(f_K)$.

The projective variety $\{f_0 = \ldots = f_K = 0\} \subset \mathbb{P}^n(\bar{F})$ of roots of the system $f_0 = \ldots = f_K = 0$ is decomposable on the compounds $\{f_0 = \ldots = f_K = 0\} = \bigcup_\alpha W_\alpha$, herewith each compound W_α is defined and irreducible over the maximal purely inseparable extension $F^{q^{-\infty}}$ of F. Moreover $W_\alpha = \bigcup_\beta W_{\alpha\beta}$ where the (absolutely irreducible) compounds $W_{\alpha\beta}$ are defined and irreducible over $\bar{F}$. Denote $c = 1 + \max_\alpha \dim W_\alpha$. The algorithm designed in [2], [3], [4] finds all W_α and thereupon $W_{\alpha\beta}$ (actually, W_α, $W_{\alpha\beta}$ are defined over some finite extensions of the field F which are also constructed by the algorithm). We (and the algorithm) represent every compound W_α 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 $g_1, g_2, h_1, \ldots, h_s$ a relation $g_1 \leqslant g_2 \mathcal{P}(h_1, \ldots, h_s)$ denotes further that $g_1 \leqslant g_2 P(h_1, \ldots, h_s)$ for an appropriate polynomial P.

Let $W \subset \mathbb{P}^n(\bar{F})$ be a closed projective variety, $\mathrm{codim}_{\mathbb{P}^n}(W) = m$, defined and irreducible over some field F_1 being a finite extension of F, denote by F_2 the maximal subfield of F_1 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

$$F(t_1,\ldots,t_{n-m})[\theta] \simeq F_2(X_{j_1}/X_{j_0},\ldots,X_{j_{n-m}}/X_{j_0},(X_0/X_{j_0})^{q^\nu},\ldots,(X_n/X_{j_0})^{q^\nu}) \subset F_1(W) \quad (1)$$

for suitable q^{ν} (here and further $\nu \geqslant 0$ when $q > 0$ and we set $q^{\nu} = 1$ when $char(F) = 0$), index $0 \leqslant j_0 \leqslant n$ and an element θ is algebraic separable over a field $F_2(t_1, \ldots, t_{n-m})$; denote by $\Phi(Z)$ its minimal polynomial such that $lc_Z(\Phi) = 1$. The elements X_j / X_{j_0} are considered herein as the rational functions on the variety W , herewith W is not situated in a hyperplane $\{X_{j_0} = 0\}$, under the isomorphism (1) $t_i \to X_{j_i}/X_{j_0}$, $1 \leqslant i \leqslant n-m$. The algorithms further represent the isomorphism (1) by the images of rational functions $(X_j / X_{j_0})^{q^{\nu}}$ in the field $F_2(t_1, \ldots, t_{n-m})[\theta]$. 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_α produces its general point and constructs a certain family of homogeneous polynomials $\psi_1^{(\alpha)}, \ldots, \psi_N^{(\alpha)} \in F[X_0, \ldots, X_n]$ such that a system $\psi_1^{(\alpha)} = \ldots = \psi_N^{(\alpha)} = 0$ determines the variety W_α . Denote $m = codim\, W_\alpha$, $\theta_\alpha = \theta$, $\Phi_\alpha = \Phi$. Then $q^{\nu} \leqslant d^{2m}$, $deg_Z(\Phi_\alpha) \leqslant deg\, W_\alpha \leqslant d^m$, for all i, j the degrees $deg_{T_1, \ldots, T_\ell, t_1, \ldots, t_{n-m}}(\Phi_\alpha)$, $deg_{T_1, \ldots, T_\ell, t_1, \ldots, t_{n-m}}(X_j/X_{j_0})^{q^{\nu}}$ (the latter two degrees are defined according to the isomorphism (1) analogously to how $deg_{T_i}(f)$ was defined above) are less than $d_2 \mathcal{P}(d^m, d_1)$, apart that $l(\Phi_\alpha), l((X_j/X_{j_0})^{q^{\nu}}) \leqslant (M_1 + M_2 + (n+\ell)\log d_2)\mathcal{P}(d^m, d_1)$. A number of equations $N \leqslant m^2 d^{4m}$, the degrees $deg_{X_0, \ldots, X_n}(\psi_s^{(\alpha)}) \leqslant d^{2m}$ and the degrees $deg_{T_1, \ldots, T_\ell}(\psi_s^{(\alpha)}) \leqslant d_2 \mathcal{P}(d^m, d_1)$; besides that the algorithm represents each $\psi_s^{(\alpha)}$ in a form $\psi_s^{(\alpha)} = \bar{\psi}_s^{(\alpha)}(Z_{s,0}, \ldots, Z_{s,n-m+2})$ for suitable linear forms $Z_{s,j}$ in the variables $X_0, \ldots, X_n$ with the coefficients from H and the polynomials $\bar{\psi}_s^{(\alpha)} \in F[Z_{s,0}, \ldots, Z_{s,n-m+2}]$, thereto $l(\bar{\psi}_s^{(\alpha)}) \leqslant (M_1 + M_2 + (n+\ell)\log d_2)\mathcal{P}(d^m, d_1)$, lastly the size $L_2(Z_{s,j}) \leqslant \mathcal{P}(n, \log d d_1 d_2)$ for all s, j . The total running time of the algorithm can be bounded from above by $\mathcal{P}(M_1, M_2, (d^n d_1 d_2)^{c+\ell})$ Obviously, the latter value is less than $\mathcal{P}(L^{c+\ell}(q+1)) \leqslant \mathcal{P}(L^{\log L}(q+1))$ if $n = O(d)$.

b) An algorithm is suggested which for every absolutely irreducible compound $W_{\alpha\beta}$ finds the maximal separable subfield $F_2 = F[\xi_{\alpha\beta}]$ of the minimal field of definition F_1 (containing F) 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 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 $\varphi_{\alpha\beta} \in F[Z]$ the minimal polynomial for $\xi_{\alpha\beta}$ such that $lc_Z(\varphi_{\alpha\beta}) = 1$, then $deg_Z(\varphi_{\alpha\beta}) \leqslant deg\, W_{\alpha\beta}$ and the degrees $deg_{T_1, \ldots, T_\ell}(\varphi_{\alpha\beta}) \leqslant d_2 \mathcal{P}(d^m, d_1)$, lastly $l(\varphi_{\alpha\beta}) \leqslant (M_1 + M_2 + (n+\ell)\log d_2)\mathcal{P}(d^m, d_1)$. 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 $V_1 = \pi(W_\alpha)$ where $\pi(X_0:\ldots:X_n) = (X_0:\ldots:X_m)$ is a lenear projection $\pi: \mathbb{P}^n \to \mathbb{P}^m$ and W_α is some compound of the variety $\{f_0 = \ldots = f_K = 0\} \subset \mathbb{P}^n(F)$, then we can produce a system of equations determining V_1 with the same bounds on the parameters as for the family $\psi_s^{(\alpha)}$ 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 $\mathcal{P}(d^{(c'+\ell+1)n}, (d_1 d_2)^{n+\ell}, L)$ where $c' = \max_{\alpha} \min\{\dim W_\alpha + 1, \operatorname{codim} W_\alpha\}$.

2. Projecting a constructive set

Let an input formula $\exists X_1 \ldots \exists X_s (\&_{1 \le j \le K} (f_j = 0) \& (g \ne 0))$ be given, herein the parameters of the polynomials $f_j, g \in F[Z_1, \ldots, Z_{n-s}, X_1, \ldots, X_s]$ satisfy the same bounds as of f_j in the section 1. The goal in the present section is to produce an equivalent quantifier-free formula $\vee_{1 \le i \le N} (\&_{1 \le j \le \varkappa_i} (f_{ij}^{(1)} = 0) \& (g_i^{(1)} \ne 0))$ where $f_{ij}^{(1)}, g_i^{(1)} \in F[Z_1, \ldots, Z_{n-s}]$.

The input formula is equivalent to $\exists X_0 \exists X_1 \ldots \exists X_s \exists X_{s+1} ((X_0 \ne 0) \& \&_{1 \le j \le K} (\bar{f}_j = 0) \& (\bar{f}_0 = X_{s+1} \bar{g} - X_0^{1+\deg \bar{g}} = 0))$, therein X_0, X_{s+1} are new variables and $\bar{f}_j = X_0^{\deg_{X_1 \ldots X_s}(f_j)} f_j(Z_1, \ldots, Z_{n-s}, X_1/X_0, \ldots, X_s/X_0)$, $\bar{g} = X_0^{\deg_{X_1 \ldots X_s}(g)} g(Z_1, \ldots, Z_{n-s}, X_1/X_0, \ldots, X_s/X_0)$ (cf. [7]). The desired projection, i.e. the constructive set consisting of all the points $(z_1, \ldots, z_{n-s}) \in \mathbb{A}^{n-s}(\bar{F})$ satisfying the latter formula, we denote by Π. One can assume further w.l.o.g. that $\deg_{X_0, \ldots, X_{s+1}} \bar{f}_j = d-1$, $0 \le j \le K$, replacing $\bar{f}_j$ by the family of polynomials $\{\bar{f}_j X_i^{d-1-\deg \bar{f}_j}\}_{0 \le i \le s+1}$.

Introduce a variety $U = \{(z_1, \ldots, z_{n-s}; (x_0 : \ldots : x_{s+1})) \in (\mathbb{A}^{n-s} \times \mathbb{P}^{s+1})(\bar{F}) : \&_{0 \le j \le K} (\bar{f}_j = 0)\}$ and a natural linear projection $\pi: \mathbb{A}^{n-s} \times \mathbb{P}^{s+1} \to \mathbb{A}^{n-s}$, then the desired $\Pi = \pi(U \cap \{X_0 \ne 0\})$. For each point $z = (z_1, \ldots, z_{n-s}) \in \mathbb{A}^{n-s}(\bar{F})$ consider the variety (the layer) $U_z = \pi^{-1}(z) \cap U \subset \{z\} \times \mathbb{P}^{s+1} \simeq \mathbb{P}^{s+1}$. The condition $z \in \Pi$ is true iff for an appropriate $0 \le m \le s+1$ the layer U_z has at least one compound W with the dimension $s+1-m$ such that $W \not\subset \{X_0 = 0\}$.

Fix a point z in the following speculations for some time. It is not difficult (see e.g. § 2 [2]) to indicate a family of $N' = Kd^m + 1$ vectors $u^{(1)}, \ldots, u^{(N')} \in H^{K+1}$ any $K+1$ from which are linearly independent (we suppose here and below that H contains sufficiently many element, extending it if necessary). Denote $h_i = \sum_{0 \le j \le K} u_j^{(i)} \bar{f}_j$, herewith $u^{(i)} = (u_0^{(i)}, \ldots, u_K^{(i)})$. The relevant compound W of U_z exists iff there are such indices $1 \le i_1 \le \ldots < i_m \le N'$

that W is a compound of the variety $\{h_{i_1}(z)=\ldots=h_{i_m}(z)=0\}\subset \mathbb{P}^{s+1}$, herein the coordinates of the point z are substituted instead of $Z_1,\ldots,Z_{n-s}$, i.e. $h_{i_j}(z)\in \bar{F}[X_0,\ldots,X_{s+1}]$ (cf. §4a [2]).

One can construct (see § 2 [2]) a family $\mathfrak{M}=\mathfrak{M}_{s,s-m,d^m}$ consisting of $(s-m+1)$-tuples of linear forms in variables $X_1,\ldots,X_{s+1}$ with the coefficients from H such that for every variety $W_1\subset \mathbb{P}^s$ satisfying the inequalities $\dim W_1\leqslant s-m$, $\deg W_1\leqslant d^m$ there is $(s-m+1)$-tuple $(Y_1,\ldots,Y_{s-m+1})\in\mathfrak{M}$ for which $W_1\cap\{Y_1=\ldots=Y_{s-m+1}=0\}=\emptyset$. Thereto $\mathrm{card}(\mathfrak{M})\leqslant\binom{(s+1)d^m+1}{s-m}$. Let us take a variety $W\cap\{X_0=0\}$ as W_1. Supplement linear forms $Y_0=X_0, Y_1,\ldots,Y_{s-m+1}$ up to a basis $Y_0,\ldots,Y_{s+1}$ with the coefficients from H of the space of linear forms in $X_0,\ldots,X_{s+1}$ (in arbitrary manner). Replacing variables denote $\hat{h}_i(z,Y_0,\ldots,Y_{s+1})=h_i(z)$ and $\tilde{h}_i(z)=\hat{h}_i(z,Y_0,0,\ldots,0,Y_{s-m+2},\ldots,Y_{s+1})$. Thus, the condition under consideration about the existence of W is equivalent to that there are indices $1\leqslant i_1<\ldots<i_m\leqslant N'$ and linear forms $Y_1,\ldots,Y_{s-m+1}$ for which the variety $\{\tilde{h}_{i_1}(z)=\ldots=\tilde{h}_{i_m}(z)=0\}\subset\mathbb{P}^m$ as one of its compounds has a certain point $\tilde{\Omega}=(\xi_0:\xi_{s-m+2}:\ldots:\xi_{s+1})$ such that the point $\Omega=(z,(\xi_0:0:\ldots:0:\xi_{s-m+2}:\ldots:\xi_{s+1}))\in U_z\cap\{Y_0\neq 0\}$ (in force of the theorem about the dimension of intersection [14]).

Introduce a system of homogeneous algebraic equations

$$\tilde{h}_{i_j}(z)-YY^{d-1}_{s-m+j+1}=0;\qquad 1\leqslant j\leqslant m \tag{2}$$

in the variables $Y_0,Y_{s-m+2},\ldots,Y_{s+1}$ with the coefficients from $\bar{F}[Y]\subset\bar{F}(Y)=K$ where Y is algebraically independent over F. One can prove (see also lemma 11 §5 [3]) that the set of roots in $\mathbb{P}^m(\bar{K})$ of the system(2) is finite. The variety of roots is decomposable on the irreducible and defined over K nulldimensional compounds $V_{\mathfrak{p}_K}$ corresponding to the minimal prime ideals $\mathfrak{p}_K\subset K[Y_0,Y_{s-m+2},\ldots,Y_{s+1}]/(\{\tilde{h}_{i_j}(z)-YY_{s-m+j+1}\}_{1\leqslant j\leqslant m})$. The system (2) can be considered apart that as the system in the variables $Y,Y_0,Y_{s-m+2},\ldots,Y_{s+1}$ with the coefficients from F which determines a variety $\tilde{U}_z^{(F)}\subset\mathbb{A}^{m+2}(\bar{F})$. It is not difficult to show (cf.lemma 12 §5 [3]) that there is a bijective correspondence between the points $V_{\mathfrak{p}_K}$ and on the other side such compounds $V_{\mathfrak{p}_F}$ of the variety $\tilde{U}_z^{(F)}$ that $V_{\mathfrak{p}_F}$ is not contained in any union of finite number of hyperplanes of the kind $\{Y-c_1=0\}\subset\mathbb{A}^{m+2}$ for $c_1\in\bar{F}$, notice that $\dim V_{\mathfrak{p}_F}=2$.

Now we exhibit an important auxiliary device from [11] (see also §3 [2]). Let $g_0,\ldots,g_{k-1}\in F[X_0,\ldots,X_n]$ be homogeneous polynomials of degrees $\delta_0\geqslant\ldots\geqslant\delta_{k-1}$ respectively. Introduce new variables

$U_0,\dots,U_n$ algebraically independent over $F(X_0,\dots,X_n)$. Set $g_K=X_0U_0+\dots+X_nU_n\in F(U_0,\dots,U_n)[X_0,\dots,X_n]$ and $D=\sum_{0\leq i\leq n}\delta_i-n$, herein $\delta_j=1$ if $K\leq j\leq n$. Consider linear over $F(U_0,\dots,U_n)$ mapping $\mathfrak{A}:\mathfrak{B}_0\oplus\dots\oplus\mathfrak{B}_K\to\mathfrak{B}$ where $\mathfrak{B}_i$ (correspondingly $\mathfrak{B}$) is the space of homogeneous polynomials in $X_0,\dots,X_n$ over the field $F(U_0,\dots,U_n)$ of degree $D-\delta_i$ (correspondingly D) for $0\leq i\leq K$, namely $\mathfrak{A}(b_0,\dots,b_K)=\sum_{0\leq i\leq K}b_ig_i$. Any element $b=(b_0,\dots,b_K)\in\mathfrak{B}_0\oplus\dots\oplus\mathfrak{B}_K$ can be written in the form $b=(b_{0,1},\dots,b_{0,s_0},b_{1,1},\dots,b_{1,s_1},\dots,b_{K,1},\dots,b_{K,s_K})$ where $s_i=\binom{n+D-\delta_i}{n}$ and $b_{i,1},\dots,b_{i,s_i}$ 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 $\mathfrak{B}$. In the chosen system of coordinates the mapping $\mathfrak{A}$ has a matrice A of the size $\binom{n+D}{n}\times\left(\sum_{0\leq i\leq K}s_i\right)$. One can represent $A=(A',A'')$ where A' (call it the number part of A) contains $\sum_{0\leq i\leq K-1}s_i$ columns and A'' (call it the formal part) contains s_K columns, besides that the entries of A' belong to F, the entries of A'' are linear forms over F in variables $U_0,\dots,U_n$ (cf. [6]). There is proved in [10] that the system $g_0=\dots=g_{K-1}=0$ has no roots in $\mathbb{P}^n(\bar F)$ iff the ideal $(g_0,\dots,g_{K-1})\supset(X_0,\dots,X_n)^D$. Besides that, the following proposition is ascertained in [11].

PROPOSITION. ([11]). 1) The system $g_0=\dots=g_{K-1}=0$ has a finite number of roots in $\mathbb{P}^n(\bar F)$ iff the rank $rg\,A=\binom{n+D}{n}=r$;

2) all $r\times r$ minors of A generate a principal ideal whose generator $R\in F[U_0,\dots,U_n]$ is their g.c.d.;

3) the homogeneous form $R=\prod_{1\leq i\leq D_1}L_i$ where $L_i=\sum_{0\leq j\leq n}\xi_j^{(i)}U_j$ is a linear form over $\bar F$, moreover $(\xi_0^{(i)}:\dots:\xi_n^{(i)})$ is a root of the system and the number of occuring of the forms proportional to L_i for each i in the product equals to the multiplicity of the corresponding root. *Apart that* $\deg R=D_1=r-rg(A')$.

The algorithm designes the matrix A with the entries from the ring $F[Y,Z_1,\dots,Z_{n-s},U_0,U_{s-m+2},\dots,U_{s+1}]$ corresponding to the modified system (2) in which $Z_1,\dots,Z_{n-s}$ are considered as variables (instead of $z_1,\dots,z_{n-s}$) according to the just exhibited device. Denote by A_z the matrix obtained from A by means of substituting the coordinates of the point z instead of $Z_1,\dots,Z_{n-s}$. Let the polynomial $R_z\in F[Y,U_0,U_{s-m+2},\dots,U_{s+1}]$ correspond to the matrix A_z as in the proposition. One can suppose w.l.o.g. that $Y\nmid R_z$ (dividing R_z on the greatest possible power of the variable Y).

Regard a certain representation of the union $\bigcup_{\gamma_F} V_{\gamma_F} = \{S_0 = \ldots = S_{K'-1} = 0\}$ for suitable polynomials $S_i \in \bar{\bar{F}}[Y, Y_0, Y_{s-m+2}, \ldots, Y_{s+1}]$ homogeneous relatively to $Y_0, Y_{s-m+2}, \ldots, Y_{s+1}$. Considering a system $S_i(0, Y_0, Y_{s-m+2}, \ldots, Y_{s+1}) = 0;\ 0 \leq i \leq K'-1$ and basing on the proposition (see also lemma 16 §5 [3]), one proves that $R_z(0, U_0, U_{s-m+2}, \ldots, U_{s+1}) = \prod_i L_i^{c_i}$ and moreover the linear forms $L_i = \sum_j \xi_j^{(i)} U_j$ correspond bijectively to the points $(\xi_0^{(i)} : \xi_{s-m+2}^{(i)} : \ldots : \xi_{s+1}^{(i)}) \in W_z' \subset P^m$ where the cone $con(W_z') = (\bigcup_{\gamma_F} V_{\gamma_F}) \cap \{Y = 0\}$. Thereupon it is not difficult to check that $\tilde{\Omega} \in W_z'$ (cf. lemma 13 §5 [3]). Summarizing and utilizing the notations introduced above, we have ascertained the following.

LEMMA 1. The formula $\exists X_1 \ldots \exists X_s (\&_{1 \leq j \leq K} (f_j = 0) \& (g \neq 0))$ is valid in a point $z \in \bar{\bar{F}}^{n-s}$ iff for appropriate $0 \leq m \leq s+1$ there exist such indices $1 \leq i_1 < \ldots < i_m \leq N'$, a set of linear forms $(Y_1, \ldots, Y_{s-m+1}) \in \mathcal{M}$ and a point $\Omega = (z, (\xi_0 : 0 : \ldots : 0 : \xi_{s-m+2} : \ldots : \xi_{s+1})) \in U_z \cap \{X_0 \neq 0\}$ (in the coordinates $Y_0, Y_1, \ldots, Y_{s+1}$) that the linear form $(\xi_0 U_0 + \xi_{s-m+2} U_{s-m+2} + \ldots + \xi_{s+1} U_{s+1}) \mid R_z(0, U_0, U_{s-m+2}, \ldots, U_{s+1})$.

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 (pivots) $(i_0, j_0), (i_1, j_1), \ldots, (i_p, j_p)$. Herewith $i_\alpha \neq i_\beta$ and $j_\alpha \neq j_\beta$ if $\alpha \neq \beta$. For any initial matrix $A^{(0)}$ v.G.a. yields the chain of matrices $A^{(0)}, A^{(1)}, \ldots, A^{(p+1)}$. Introduce a notation $A^{(\alpha)} = (a_{ij}^{(\alpha)})$. Apart that $a_{i_\alpha j_\alpha}^{(\alpha)} \neq 0$ and $a_{ij}^{(\alpha+1)} = a_{ij}^{(\alpha)} + a_{ij_\alpha}^{(\alpha)} a_{i_\alpha j}^{(\alpha)} / a_{i_\alpha j_\alpha}^{(\alpha)}$ for all i distinguished from $i_0, \ldots, i_\alpha$, lastly $a_{i_\beta j}^{(\alpha+1)} = a_{i_\beta j}^{(\alpha)}$ where $0 \leq \beta \leq \alpha$. The matrix $A^{(p+1)}$ is in the generalized trapezium form, namely, $a_{ij}^{(p+1)} = 0$ when either i differs from $i_0, \ldots, i_p$ or $i = i_\alpha, j = j_\beta$ and $\alpha > \beta$, besides that $a_{i_\alpha j_\alpha}^{(p+1)} = a_{i_\alpha j_\alpha}^{(\alpha)} \neq 0$.

Denote by $\Delta_{ij}^{(\alpha)}$ the determinant of $(\alpha+1) \times (\alpha+1)$ matrix formed by the rows with the indices $i_0, \ldots, i_{\alpha-1}, i$ and the columns with the indices $j_0, \ldots, j_{\alpha-1}, j$ provided that $i \neq i_0, \ldots, i \neq i_{\alpha-1}$ and $j \neq j_0, \ldots, j \neq j_{\alpha-1}$. Then $a_{ij}^{(\alpha)} = \Delta_{ij}^{(\alpha)} / \Delta_{i_{\alpha-1} j_{\alpha-1}}^{(\alpha-1)}$ (see e.g. lemma 7 [7]).

Now we turn ourselves to considering an arbitrary point $z \in A^{n-s}$. Fix for some time $0 \leq m \leq s+1$ indices $1 \leq i_1 < \ldots < i_m \leq N'$ and a set of linear forms $(Y_1, \ldots, Y_{s-m+1}) \in \mathcal{M}$ (see lemma 1). By r denote the number of rows of the matrix A. Produce a certain succession of v.G.a.s $\Gamma_1, \Gamma_2, \ldots$ over a field $F(Y, Z_1, \ldots, Z_{n-s}, U_0, U_{s-m+2}, \ldots, U_{s+1})$ and a succession of polynomials $P_1, P_2, \ldots \in F[Y, Z_1, \ldots, Z_{n-s}, U_0, U_{s-m+2}, \ldots, U_{s+1}]$ thereto v.G.a. Γ_i can be applied correctly to the matrix A_z for all points $z=(z_1,\dots,z_{n-s})$ of (possibly empty) quasiprojective variety ([14]) $W_i \subset \mathbb{A}^{n-s}$ which is defined by the following conditions: inequality $0 \neq P_i(Y, z_1, \dots, z_{n-s}, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}) \in \bar{F}[Y, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}]$ and equalities $0 = P_j(Y, z_1, \dots, z_{n-s}, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1})$ for $1 \leq j \leq i-1$ are fulfilled. Apart that the variety $\{(z_1,\dots,z_{n-s}) : P_i(Y, z_1, \dots, z_{n-s}, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}) = 0$ for all $i\} = \emptyset$, henceforth $\bigcup_i W_i = \mathbb{A}^{n-s}$. Exposed below construction is close to the proof of the lemma 9 [7].

Later on we apply the v.G.a.s $\Gamma_1, \Gamma_2, \dots$ to the initial matrix A. As Γ_1 one can take an arbitrary v.G.a. Set a polynomial $P_1 = \prod_{0 \leq \alpha \leq \rho_1} \Delta^{(\alpha)}_{i_\alpha j_\alpha}$ (for v.G.a. regarded at the current step the same notations as above are utilized). Assume that $\Gamma_1, \dots, \Gamma_i$; $P_1, \dots, P_i$ are already produced. Then as Γ_{i+1} we take v.G.a. in which for every $0 \leq \alpha \leq \rho_{i+1}$ the column index j_α of the pivot in the matrix $A^{(\alpha)}$ is the least possible, moreover $j_\alpha > j_{\alpha-1}$ and the polynomials $P_1, \dots, P_i$, $\prod_{0 \leq \beta \leq \alpha} \Delta^{(\beta)}_{i_\beta j_\beta}$ are linearly independent over F. Finally, put $P_{i+1} = \prod_{0 \leq \alpha \leq \rho_{i+1}} \Delta^{(\alpha)}_{i_\alpha j_\alpha}$. The algorithm stops producing v.G.a.s $\Gamma_1, \Gamma_2, \dots$ when it is impossible to produce Γ_{i+1} satisfying formulated above requirements (if $\rho_{i+1} < r-1$ then $W_{i+1} = \emptyset$).

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 Y^ε for a suitable ε), where $r \times r$ submatrix Δ_i of the matrix A is generated by the columns with the indices $j_0, \dots, j_{r-1}$ corresponding to v.G.a. Γ_i. This follows from the fact that in the matrix $(A^{(\alpha)})_z$ an entry $a^{(\alpha)}_{\beta j} = 0$ when $\beta \neq i_0, \dots, i_{\alpha-1}$ and $j < j_\alpha$ in force of the choice of j_α. Therefore, if for an appropriate α a cell $(i_{\alpha-1}, j_{\alpha-1})$ belongs to the number part A' of A and a cell (i_α, j_α) belongs to the formal part A'' of A then $rg((A')_z) = \alpha$ that implies the mentioned representation of R_z.

Write $\det \Delta_i = \sum_\varepsilon \Delta^{(\varepsilon)}_i Y^\varepsilon$, herewith $\Delta^{(\varepsilon)}_i(Z_1,\dots,Z_{n-s}) \in F[Z_1,\dots,Z_{n-s}, \mathcal{U}_0, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}]$. Introduce varieties $W^{(\varepsilon)}_i = \{(z_1,\dots,z_{n-s}) \in W_i : \Delta^{(0)}_i(z_1, \dots, z_{n-s}) = \dots = \Delta^{(\varepsilon-1)}_i(z_1,\dots,z_{n-s}) = 0; \Delta^{(\varepsilon)}_i(z_1,\dots,z_{n-s}) \neq 0\}$ for $\varepsilon \geq 0$. The variety $W^{(\varepsilon)}_i$ is quasiprojective as the intersection of two quasiprojective varieties, namely, if $\Xi^{(j)} = \{\&_\beta (G^{(j)}_\beta = 0) \& \vee_\gamma (C^{(j)}_\gamma \neq 0)\}$; $j = 1, 2$ then $\Xi_1 \cap \Xi_2 = \{\&_{\beta^{(1)}, \beta^{(2)}} (G^{(1)}_{\beta^{(1)}} = 0) \& G^{(2)}_{\beta^{(2)}} = 0) \& \vee_{\gamma^{(1)}, \gamma^{(2)}} (C^{(1)}_{\gamma^{(1)}} C^{(2)}_{\gamma^{(2)}} \neq 0)\}$. Moreover $W^{(\varepsilon_1)}_i \cap W^{(\varepsilon_2)}_i = \emptyset$ for $\varepsilon_1 \neq \varepsilon_2$ and $\bigcup_\varepsilon W^{(\varepsilon)}_i = W_i$.

Thereupon represent $\Delta^{(\varepsilon)}_i = \sum_{0 \leq j \leq D_2} e^{(\varepsilon, j)}_i \mathcal{U}_0^{D_2 - j}$ where $e^{(\varepsilon,j)}_i(Z_1,\dots,Z_{n-s}) \in F[Z_1,\dots,Z_{n-s}, \mathcal{U}_{s-m+2}, \dots, \mathcal{U}_{s+1}]$. Consider quasiprojective varieties $W_i^{(\varepsilon,j)}=\{(z_1,\dots,z_{n-s})\in W_i^{(\varepsilon)}: e_i^{(\varepsilon,\varkappa)}(z_1,\dots,z_{n-s})=0,\ 0\leq\varkappa<j;\ e_i^{(\varepsilon,j)}(z_1,\dots,z_{n-s})\neq 0\}$, then $W_i^{(\varepsilon,j_1)}\cap W_i^{(\varepsilon,j_2)}=\emptyset$ when $j_1\neq j_2$ and $\bigcup_{0\leq j\leq D_2}W_i^{(\varepsilon,j)}=W_i^{(\varepsilon)}$. Observe that the proposition and the ascertained earlier entail that $(\Delta_i^{(\varepsilon)})_z=\Delta_i^{(\varepsilon)}(z_1,\dots,z_{n-s},U_0,U_{s-m+2},\dots,U_{s+1})=\prod_\varkappa L_\varkappa^{c_\varkappa}$ is a product of linear forms for $z\in W_i^{(\varepsilon)}$. This implies that for $z\in W_i^{(\varepsilon,j)}$ the polynomial $(e_i^{(\varepsilon,j)})_z$ equals to the product of powers $L_\varkappa^{c_\varkappa}$ of all linear forms $L_\varkappa$ in which the coefficient at U_0 vanishes. Henceforth $(e_i^{(\varepsilon,j)})_z\mid(\Delta_i^{(\varepsilon)})_z$ in the ring $\bar F[U_0,U_{s-m+2},\dots,U_{s+1}]$.

Our nearest purpose is to calculate the quotient $(\Delta_i^{(\varepsilon)})_z/(e_i^{(\varepsilon,j)})_z$ for $z\in W_i^{(\varepsilon,j)}$. If $I=(I_{s-m+2},\dots,I_{s+1})$ is a multiindex then denote $U^I=U_{s-m+2}^{I_{s-m+2}}\dots U_{s+1}^{I_{s+1}}$, apart that by $I<J$ denote the lexicographical order on multiindices. Write $e_i^{(\varepsilon,j)}=\sum_I\gamma_I U^I$ and let $0\neq\gamma_I\in F[Z_1,\dots,Z_{n-s}]$ for a certain I (fixed in further speculations). Introduce a quasiprojective variety $W_{i,I}^{(\varepsilon,j)}=\{(z_1,\dots,z_{n-s})\in W_i^{(\varepsilon,j)}:$ $\gamma_J(z_1,\dots,z_{n-s})=0$ when $J>I$ and $\gamma_I(z_1,\dots,z_{n-s})\neq 0\}$. Evidently $W_{i,I_1}^{(\varepsilon,j)}\cap W_{i,J_1}^{(\varepsilon,j)}=\emptyset$ if $I_1\neq J_1$ and $\bigcup_{I_1}W_{i,I_1}^{(\varepsilon,j)}=W_i^{(\varepsilon,j)}$. For any point $(z_1,\dots,z_{n-s})\in W_{i,I}^{(\varepsilon,j)}$ the quotient $(\Delta_i^{(\varepsilon)})_z/(e_i^{(\varepsilon,j)})_z$ can be obtained by means of the described below process of dividing polynomial on polynomial and after that substituting the coordinates $z_1,\dots,z_{n-s}$ instead of variables $Z_1,\dots,Z_{n-s}$.

Let $0\neq\Psi\in F(Z_1,\dots,Z_{n-s})[U_{s-m+2},\dots,U_{s+1}]$. Denote by $lex(\Psi)\neq 0$ the monomial of Ψ in variables $U_{s-m+2},\dots,U_{s+1}$ for which in $\Psi-lex(\Psi)$ occur only the monomials less than $lex(\Psi)$, set $\bar{\bar\Psi}=\Psi(U_{s-m+2}^{m},U_{s-m+3}^{m-1},\dots,U_{s+1})$ and $\sigma(\Psi)=deg(\bar{\bar\Psi})$. Delete from $e_i^{(\varepsilon,j)}$ all the monomials $\gamma_J U^J$ (except $\gamma_I U^I$) with $\sigma(U^J)\geq\sigma(U^I)$ and denote obtained polynomial by $\tilde{\tilde e}_i^{(\varepsilon,j)}$. Then $(e_i^{(\varepsilon,j)})_z=(\tilde{\tilde e}_i^{(\varepsilon,j)})_z$, when $z\in W_{i,I}^{(\varepsilon,j)}$ since $(e_i^{(\varepsilon,j)})_z$ is the product of linear forms. For any index $j<\varkappa\leq D_2$ the algorithm designs a succession of nonzero polynomials $\Psi_0=e_i^{(\varepsilon,\varkappa)},\Psi_1,\dots,\Psi_\rho$. Represent uniquely $\Psi_t=\Psi_t^{(1)}+\Psi_t^{(2)}+\Psi_t^{(3)}$, herewith $\bar{\bar\Psi}_t^{(1)},\bar{\bar\Psi}_t^{(2)}$ are homogeneous, $\sigma(\Psi_t^{(3)})<\sigma(\Psi_t)=\sigma(\Psi_t^{(1)})=\sigma(\Psi_t^{(2)})$ and $\Psi_t^{(1)}/U^I\in F(Z_1,\dots,Z_{n-s})[U_{s-m+2},\dots,U_{s+1}]$, lastly each monomial from $\Psi_t^{(2)}$ is not divided by U^I. Then $\Psi_{t+1}=\gamma_I(\Psi_t-\Psi_t^{(2)})-\Psi_t^{(1)}\tilde{\tilde e}_i^{(\varepsilon,j)}/U^I$ for every $0\leq t\leq\rho-1$ (obviously, $\sigma(\Psi_{t+1})<\sigma(\Psi_t)$). Regard a polynomial $\Psi_{i,I}^{(\varepsilon,j,\varkappa)}=\sum_{0\leq t\leq\rho-1}\Psi_t^{(1)}\gamma_I^{\rho-t-1}/U^I\in F[Z_1,\dots,Z_{n-s},U_{s-m+2},\dots,U_{s+1}]$ and set $\Psi_{i,I}^{(\varepsilon,j)}=\gamma_I^{\rho}U_0^{D_2-j}+\sum_{j<\varkappa\leq D_2}\Psi_{i,I}^{(\varepsilon,j,\varkappa)}U_0^{D_2-\varkappa}$. One can check that $(e_i^{(\varepsilon,\varkappa)})_z/(\gamma_I^{-\rho}e_i^{(\varepsilon,j)})_z=(\Psi_{i,I}^{(\varepsilon,j,\varkappa)})_z$ for $z\in W_{i,I}^{(\varepsilon,j)}$ and therefore $(\Delta_i^{(\varepsilon)})_z/(e_i^{(\varepsilon,j)})_z=(\gamma_I^{-\rho}\Psi_{i,I}^{(\varepsilon,j)})_z$ equals to the product of $L_\mu^{c_\mu}$ for all linear forms L_μ in which the coefficient at the variable U_0 does not vanish.

Thereupon remind that $\mathrm{con}\, W'_z = \cup_{\wp_F} V_{\wp_F} \cap \{Y = 0\}$ and introduce $W' = \cup_{z\in W^{(\varepsilon,j)}_{i,I}} (\{z\}\times(W'_z \cap \{Y_0 \neq 0\}))$ (as above we fix i, ε, j, I). Observe that $W' = \{(z_1,\dots,z_{n-s},(y_0:y_{s-m+2}:\dots:y_{s+1}))\in W^{(\varepsilon,j)}_{i,I}\times \mathbb{A}^m(\bar F)\subset W^{(\varepsilon,j)}_{i,I}\times \mathbb{P}^m(\bar F) : 0 = (\varphi^{(\varepsilon,j)}_{i,I}(-\sum_{s-m+2\le\alpha\le s+1} U_\alpha y_\alpha, y_0 U_{s-m+2},\dots,y_0 U_{s+1}))_z \in \bar F[U_{s-m+2},\dots,U_{s+1}]\}$. Representing the polynomial $\psi^{(\varepsilon,j)}_{i,I}(-\sum_{s-m+2\le\alpha\le s+1} U_\alpha Y_\alpha, Y_0 U_{s-m+2},\dots,Y_0 U_{s+1}) = \sum_J E_J U^J$ leads to an equality $W' = \{\&_J(E_J = 0)\}\cap(W^{(\varepsilon,j)}_{i,I}\times\mathbb{A}^m)$. Because of that the subset W' is closed in the quasiprojective variety $W^{(\varepsilon,j)}_{i,I}\times\mathbb{A}^m$.

Consider the natural linear projection $\pi_2 : \mathbb{A}^{n-s}\times(\mathbb{P}^m\cap\{Y_0\neq 0\})\to\mathbb{A}^{n-s}$ defined by the formula $\pi_2(Z_1,\dots,Z_{n-s},(Y_0:Y_{s-m+2}:\dots:Y_{s+1})) = (Z_1,\dots,Z_{n-s})$. Let a morphism $\pi_1 : W'\to W^{(\varepsilon,j)}_{i,I}$ be the restriction of π_2 on W'. Our nearest goal is to show that π_1 is finite ([14]). Obviously, the inverse image $\pi_1^{-1}(V)\subset W'$ of any open affine subset $V\subset W^{(\varepsilon,j)}_{i,I}$ is isomorphic to $(V\times\mathbb{A}^m)\cap W'$, henceforth $\pi_1^{-1}(V)$ is open in W' and besides that $\pi_1^{-1}(V)$ is affine since $\pi_1^{-1}(V)$ is closed in the open affine set $V\times\mathbb{A}^m$ ([14]). Now we check that every coordinate function $Y_\varkappa/Y_0$ on the variety $\pi_1^{-1}(V)$ satisfies a suitable relation of integral dependence over the ring $\bar F[V]$ where $s-m+2\le\varkappa\le s+1$. Let $\psi^{(\varepsilon,j)}_{i,I} = \psi^{(\varepsilon,j)}_{i,I}(U_0,U_{s-m+2},\dots,U_{s+1})$. Then $\psi^{(\varepsilon,j)}_{i,I}(Y_\varkappa/Y_0,0,\dots,0,-1,0,\dots,0) = 0$ on W', herein -1 is substituted instead of the variable $U_\varkappa$. Taking into account that $(\gamma_I)_z\neq 0$ when $z\in W^{(\varepsilon,j)}_{i,I}$ this yields an equation of integral dependence. So, we infer that the morphism π_1 is finite.

Utilizing the notations from the lemma 1 one concludes that a set $V^{(\varepsilon,j)}_{i,I}$ consisting of all such points $z = (z_1,\dots,z_{n-s})\in W^{(\varepsilon,j)}_{i,I}$ that there exists 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 $W^{(\varepsilon,j)}_{i,I}$ as $V^{(\varepsilon,j)}_{i,I}$ coincides with the image under projection π_1 of the closed in the domain of definition of π_1 (i.e. in W') set $\pi_1^{-1}(W^{(\varepsilon,j)}_{i,I})\cap\{\hat f_0 = \dots = \hat f_K = 0\}$ where $\hat f_\varkappa(Y_0,Y_{s-m+2},\dots,Y_{s+1}) = \tilde f_\varkappa(Y_0,0,\dots,0,Y_{s-m+2},\dots,Y_{s+1})$ and $\tilde f_\varkappa(Y_0,Y_1,\dots,Y_{s+1}) = \bar f(Z_1,\dots,Z_{n-s},X_0,\dots,X_{s+1})$ for $0\le\varkappa\le K$ and since the image of the closed set under a finite morphism is again closed ([14]).

Now we describe a procedure for constructing the required $V^{(\varepsilon,j)}_{i,I}$. Let the quasiprojective variety $W^{(\varepsilon,j)}_{i,I} = \{\&_\beta(G_\beta = 0)\&(\vee_\gamma(C_\gamma\neq 0))\}$, herewith the polynomials $G_\beta, C_\gamma\in F[Z_1,\dots,Z_{n-s}]$ <u>were actually produced earlier. Denote the closure</u> of the projection $\pi_2\{\&_\beta(G_\beta = 0)\&\&_J(E_J = 0)\&\&_{0\le\varkappa\le K}(\hat f_\varkappa = 0)\} = \tilde V^{(\varepsilon,j)}_{i,I}$. On the other hand in force of the aforesaid the equalities hold $V^{(\varepsilon,j)}_{i,I} = \tilde V^{(\varepsilon,j)}_{i,I}\setminus\{\&_\gamma(C_\gamma = 0)\}$

$=\mathcal{V}_{i,I}^{(\varepsilon,j)} \setminus \{\&_\gamma (C_\gamma = 0)\}$. Thus, it remains only to design the affine variety $\mathcal{V}_{i,I}^{(\varepsilon,j)}$.

Involving the theorem 2 (see section 1) the algorithm finds the general points of the compounds $\mathcal{Y}$ of the variety $\{\&_\beta(G_\beta=0)\&\&_J(E_J=0)\&\&_{0\leq\varkappa\leq K}(\tilde{f}_\varkappa=0)\}$. It is sufficient for each $\mathcal{Y}$ to construct the closure of its projection $\overline{\pi_2(\mathcal{Y})}$. Notice that there is an imbedding of the fields of functions $F^{q^{-\infty}}(\overline{\pi_2(\mathcal{Y})})=F^{q^{-\infty}}(Z_1,\dots,Z_{n-s})\in F^{q^{-\infty}}(Z_1,\dots,Z_{n-s},Y_1/Y_0,\dots,Y_{s+1}/Y_0)=F^{q^{-\infty}}(\mathcal{Y})$. Therefore, the algorithm can produce the general point of $\overline{\pi_2(\mathcal{Y})}$ yielding firstly a trascendental 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 (if it exists) between the elements $a_1,\dots,a_{p+1}\in F(t_1,\dots,t_{n-m_1})[\theta]\subset F^{q^{-\infty}}(\mathcal{Y})$ provided that $a_1,\dots,a_p$ 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] , §§ 4b, 6 [3]). Thereupon with the help of the remark just after the theorem 2 the algorithm computes a representation $\overline{\pi_2(\mathcal{Y})}=\{\&_\delta(B_\delta=0)\}$ where the polynomials $B_\delta\in F[Z_1,\dots,Z_{n-s}]$.

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 $\Pi=\pi(U\cap\{X_0\neq 0\})=\{(z_1,\dots,z_{n-s})\in\mathbb{A}^{n-s}(\bar{F}):\exists X_1\dots\exists X_s(\&_{1\leq\varkappa\leq K}(f_\varkappa(z_1,\dots,z_{n-s},X_1,\dots,X_s)=0)\&\, g(z_1,\dots,z_{n-s},X_1,\dots,X_s)\neq 0)\}$, i.e. the projection in the form $\{\bigvee_{0\leq m\leq s+1}\bigvee_{1\leq i_1<\dots<i_m\leq N'}\bigvee_{(Y_1,\dots,Y_{s-m+1})\in\mathfrak{M}}\bigvee_{i,\varepsilon,j,I}\bigvee_{\mathcal{Y},\gamma}(\&_{1\leq\delta\leq N_1}(B_\delta=0)\&(C_\gamma\neq 0))\}=\{\bigvee_\mu(\&_\delta(B_\delta^{(\mu)}=0)\&(C^{(\mu)}\neq 0))\}$. Thereat $\deg_{Z_1,\dots,Z_{n-s}}(B_\delta^{(\mu)})\leq d^{4(n+2)(2s+3)}$, $\deg_{T_1,\dots,T_\ell}(B_\delta^{(\mu)})\leq d_2\mathcal{P}(d^{(s+1)n},d_1)$, lengths of descriptions $\ell(B_\delta^{(\mu)})\leq(M_1+M_2+(n+\ell)\log d_2)\times\mathcal{P}(d^{(s+1)n},d_1)$. Apart that $\deg_{Z_1,\dots,Z_{n-s}}(C^{(\mu)})\leq(3d)^{(2s+3)}$, $\deg_{T_1,\dots,T_\ell}(C^{(\mu)})\leq d_2\mathcal{P}(d^{(s+1)},d_1)$ and $\ell(C^{(\mu)})\leq(M_1+M_2+(n+\ell)\log d_2)\mathcal{P}(d^{(s+1)},d_1)$. Besides that, $\delta\leq(s+1)^2(3d)^{4(2s+3)(n+2)}$, $\mu\leq d^{12(s+2)(n+s+3)}$. The running time of the algorithm can be estimated by $\mathcal{P}(M_1+M_2,d^{sn(n+\ell)},(d_1+d_2)^{n+\ell},q)$.

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

Let a Boolean formula Q with N atoms of the kind $f_i=0$ where $f_i\in F[X_1,\dots,X_n]$ satisfies the same bounds as in the section 1, be given, $L_2(Q)$ denotes the size of Q . Firstly we exhibit a procedure reducing Q to a disjunctive normal form.

Following [7] name $(g_1,\dots,g_p)$-cell for $g_1,\dots,g_p\in F[X_1,\dots,X_n]$ any nonempty quasiprojective variety of the kind $\{\&_{j\in\mathcal{J}_1}(g_j=0)\,\&\,\&_{j\in\mathcal{J}_2}(g_j\neq 0)\}\subset\mathbb{A}^n(\bar{F})$, herewith $\mathcal{J}_1\cup\mathcal{J}_2=\{1,\dots,p\}$, $\mathcal{J}_1\cap\mathcal{J}_2=\emptyset$. By means of the Bezout inequality [14] it is ascertained in [7] that a number of all $(g_1,\dots,g_p)$-cells is less or equal to $(1+\deg g_1+\dots+\deg g_p)^n$. We shall describe the method for decomposing the space $\mathbb{A}^n$ on $(g_1,\dots,g_p)$-cells by recursion on p. Assume that we are supplied with all $(g_1,\dots,g_{p-1})$-cells $(p\geq 1)$. Every $(g_1,\dots,g_p)$-cell is of the form either $K\cap\{g_p=0\}$ or $K\cap\{g_p\neq 0\}$ for a pertinent $(g_1,\dots,g_{p-1})$-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 $K\cap\{g_p=0\}$ and $K\cap\{g_p\neq 0\}$.

Applying the just described method the algorithm yields all $(\{f_i\}_{1\leq i\leq N})$-cells. Again repeatedly making use of the theorem 2 by induction on the number of logical signs in Q the algorithm for each $(\{f_i\}_{1\leq i\leq N})$-cell checks, whether this call is contained in the constructive set $\Pi_Q=\{Q\}\subset\mathbb{A}^n$ determined by the formula Q, and thereby represents Π_Q as a union of $(\{f_i\}_{1\leq i\leq N})$-cells $K^{(\mu)}$ that means reducing Q to a disjunctive normal form $\bigvee_\mu(\&_{\delta\geq 1}(f_\delta^{(\mu)}=0)\&(f_0^{(\mu)}\neq 0)))$. Moreover $1\leq\mu\leq(1+Nd)^n$, $1\leq\delta\leq N$, any polynomial $f_\delta^{(\mu)}=f_i$ for a relevant i and $f_0^{(\mu)}=\prod_{j\in\mathcal{J}}f_j$ for an appropriate $\mathcal{J}\subset\{1,\dots,N\}$. The working time of the exhibited procedure can be estimated according to the theorem 2 by $\mathcal{P}(L_2(Q),N^n,(d^n d_1 d_2)^{n+\ell},q)$.

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

$$\exists Z_{1,1}\dots\exists Z_{1,s_1}\forall Z_{2,1}\dots\forall Z_{2,s_2}\dots\exists Z_{a,1}\dots\exists Z_{a,s_a}Q \tag{3}$$

be given where the formula Q is of the kind as at the beginning of the section, $f_i\in F[Z_1,\dots,Z_{s_0},Z_{1,1},\dots,Z_{a,s_a}]$, herein $Z_1,\dots,Z_{s_0}$ occur free, $n=s_0+s_1+\dots+s_a$, 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 $\varkappa$ steps at an equivalent to (3) formula

$$\exists Z_{1,1}\dots\exists Z_{1,s_1}\neg\dots\exists Z_{a-\varkappa,1}\dots\exists Z_{a-\varkappa,s_{a-\varkappa}}\neg(\bigvee_{1\leq i\leq N^{(\varkappa)}}(\&_{1\leq j\leq K^{(\varkappa)}-1}(f_{ij}^{(\varkappa)}=0)\&(f_{i0}^{(\varkappa)}\neq 0))).$$

Denote $d^{(\varkappa)}=\max_{ij}\deg_{Z_1,\dots,Z_{s_0},Z_{1,1},\dots,Z_{a-\varkappa,s_{a-\varkappa}}}(f_{ij}^{(\varkappa)})$; $d_2^{(\varkappa)}=\max_{ij}\deg_{T_1,\dots,T_\ell}(f_{ij}^{(\varkappa)})$; $q^{(\varkappa)}=N^{(\varkappa)}K^{(\varkappa)}d^{(\varkappa)}$; $M_2^{(\varkappa)}=\max_{ij}l(f_{ij}^{(\varkappa)})$; $\sigma=s_{a-\varkappa+1}$. Then in force of the theorem 2 and the lemma 2 the inequalities hold: $d^{(\varkappa)}\leq$

$(q^{(\varkappa-1)})^{8(\sigma+2)(n+2)}$, $N^{(\varkappa)} \le (q^{(\varkappa-1)})^{n+12(\sigma+2)(n+\sigma+3)}$, $K^{(\varkappa)} \le (\sigma+1)^2 (3q^{(\varkappa-1)})^{8(\sigma+2)(n+2)}$. Therefore $q^{(\varkappa)} \le (q^{(\varkappa-1)})^{48n(\sigma+8)} \le (Nd)^{(48n\sum_{a-\varkappa+1\le j\le a}(s_j+8)/\varkappa)^{\varkappa}}$. Apart that $d_2^{(\varkappa)} \le d_2^{(\varkappa-1)} \times \mathcal{P}(q^{(\varkappa-1)}, d_1) \le d_2 \mathcal{P}(q^{(\varkappa)}, d_1^{(\varkappa)})$, $M_2^{(\varkappa)} \le (M_1+M_2+\ell \log d_2)\mathcal{P}(q^{(\varkappa)}, d_1^{\varkappa})$. Lastly the running time of the algorithm (after $\varkappa$ steps) is less than $\mathcal{P}(M_1+M_2, (Nd^n)^{(48n/\varkappa)^{\varkappa}(\sum_{a-\varkappa+1\le j\le a}(s_j+8))^{\varkappa}(n+\ell)}, (d_1^{\varkappa} d_2)^{n+\ell}, q)$.

Performing a steps completes the proof of the following

THEOREM 3. An algorithm is proposed which for a formula (3) outputs an equivalent to it a quantifier-free one $\vee_{1\le i\le \mathcal{N}}(\&_{1\le j\le \mathcal{K}} (g_{ij}=0) \& (g_{i0}\ne 0))$ where $g_{ij} \in F[Z_1,\dots,Z_{s_0}]$, herewith $\deg_{Z_1,\dots,Z_{s_0}}(g_{ij}) \le (Nd^n)^{(48n(n+8a)/a)^a} = \mathcal{D}$, $\deg_{T_1,\dots,T_\ell}(g_{ij}) \le d_2 \mathcal{P}(\mathcal{D}, d_1^a)$; besides that $\ell(g_{ij}) \le (M_1+M_2+\ell \log d_2)\mathcal{P}(\mathcal{D}, d_1^a)$. The integers $\mathcal{N}, \mathcal{K} \le \mathcal{D}$. Finally, the algorithm works within the time $\mathcal{P}(L_2, L_2(\varphi), (Nd^n)^{(48n(n+8a)/a)^a(n+\ell)}, (d_1^a d_2)^{n+\ell}, q)$.

REFERENCES

1. Chistov A.L., Grigor'ev D.Yu. Polynomial-time factoring of the multivariable polynomials over a global field. - LOMI preprint E-5-82, Leningrad, 1982.
2. Chistov A.L., Grigor'ev D.Yu. Subexponential-time solving systems of algebraic equations. I. - LOMI preprint E-9-83, Leningrad, 1983.
3. Chistov A.L., Grigor'ev D.Yu. Subexponential-time solving systems of algebraic equations. II. - LOMI preprint E-10-83, Leningrad, 1983.
4. Chistov A.L., Grigor'ev D.Yu. Polynomial-time factoring of polynomials and subexponential-time solving systems and quantifier elimination. - Notes of Scientific seminars of LOMI, Leningrad, 1984, vol.137.
5. Collins G.E. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. - Lect.Notes Comput.Sci., 1975, vol.33, p.134-183.
6. Grigor'ev D.Yu. Multiplicative complexity of a bilinear form over a commutative ring. - Lect.Notes Comp.Sci., 1981, vol.118, p.281-286.
7. Heintz J. Definability and fast quantifier elimination in algebraically closed fields. - Prepr.Univ.Frankfurt, West Germany, December, 1981.

8. Kaltofen E. A polynomial reduction from multivariate to bivariate integral polynomial factorization. - Proc.14-th ACM Symp.Th. Comput., May, N.Y., 1982, p.261-266.
9. Kaltofen E. A polynomial-time reduction from bivariate to univariate integral polynomial factorization. - Proc.23-rd IEEE Symp.Found Comp.Sci., October, N.Y., 1982, p.57-64.
10. Lazard D. Algébre linéaire sur $k[X_1,\dots,X_n]$ et élimination. - Bull.Soc.Math.France, 1977, vol.105, p.165-190.
11. Lazard D. Résolutions des systèmes d'équations algébriques. - Theor Comput.Sci., 1981, vol.15, p.77-110.
12. Lenstra A.K., Lenstra H.W., Lovasz L. Factoring polynomials with rational coefficients. - Math.Ann., 1982, vol.261, p.515-534.
13. Lenstra A.K. Factoring multivariate polynomials over finite fields. - Preprint Math.Centrum Amsterdam, IW 221/83, Februari, 1983.
14. Shafarevich I.R. Basic algebraic geometry. - Springer-Verlag, 1974.
15. Wüthrich H.R. Ein Entscheidungsverfahren für die Theorie der reellabgeschlossenen Körper. - Lect.Notes Comput.Sci., 1976, vol.43, p.138-162.
16. Zariski O., Samuel P. Commutative algebra, vol.1, 2. - van Nostrand, 1960.