

FINDING REAL SOLUTIONS OF SYSTEMS OF ALGEBRAIC INEQUALITIES IN SUBEXPONENTIAL TIME

UDC 519.5+512.46

N. N. VOROB'EV, JR., AND D. YU. GRIGOR'EV

1. Suppose polynomials $f_1, \dots, f_k \in \mathbf{Z}[X_1, \dots, X_n]$ are given. In this note we describe an algorithm that determines whether the system of inequalities

$$(1) \quad f_1 \geq 0, \dots, f_i \geq 0, \quad f_{i+1} > 0, \dots, f_k > 0$$

has a solution in \mathbf{R}^n , and if so, then indicates some of them. Let the degrees $\deg f_i$ be bounded by d , and suppose that the coefficients of the polynomials f_i are bounded by 2^M . Then the size of the system (1) can be bounded (cf. [5] and [6]) by the quantity $L = kMd^n$.

THEOREM. *It is possible to construct an algorithm that determines whether the system (1) has a solution in \mathbf{R}^n , and if so, indicates at least one point on each connected component of the semialgebraic set in \mathbf{R}^n defined by this system. The execution time for this algorithm can be bounded by a polynomial in $M(kd)^{n^2} \leq L^{\log^2 L}$ (i.e. it is subexponential as a function of input size).*

Concerning the representation of points, see the lemma below.

Previously a bound of order $(Mkd)^{2^n}$ was known for this problem (see, for example, [1] and [2]). We mention further that in the case $\deg f_i = 1$ for $1 \leq i \leq k$ (the problem of linear programming), an algorithm of polynomial complexity was obtained in [3].

Below an algorithm of subexponential complexity for the solution of systems of algebraic equations over an algebraically closed field (see [5] and [6]) will be used essentially.

2. First an important special case will be considered: the system of equations $f_1 = \dots = f_k = 0$, where $f_1, \dots, f_k \in \mathbf{Z}[X_1, \dots, X_{n-1}]$. In (4) it was established that every connected component of the variety $\{f_1 = \dots = f_k = 0\} \subset \mathbf{R}^{n-1}$ consisting of points satisfying the system $f_1 = \dots = f_k = 0$ has nonempty intersection with a closed ball $D_r \subset \mathbf{R}^{n-1}$ of radius $r \leq \exp(p(L))$ for a suitable polynomial p . Therefore we may restrict ourselves to the intersection $\{f_1 = \dots = f_k = 0\} \cap D_r$, and locate points on the components of this compact set. Namely, we adjoin an additional equation to the system under consideration, containing a new variable X_n , and we obtain a new system $f_1 = \dots = f_k = X_1^2 + \dots + X_n^2 - r^2 = 0$. Since the set of real roots of the last system coincides with the manifold $V_0 = \{f = 0\}$ of real roots of the polynomial $f = f_1^2 + \dots + f_k^2 + (X_1^2 + \dots + X_n^2 - r^2)^2$, we also consider the manifold V_0 .

Let ε be transcendental over \mathbf{R} . Then we may consider the field $\mathbf{R}(\varepsilon)$ as a formally real field (see [7], Chapter XI), taking ε to be infinitesimal, i.e. $0 < \varepsilon < a$ for every $0 < a \in \mathbf{R}$. Then the field $F = \mathbf{R}((\varepsilon^{1/\infty})) \supset \mathbf{R}(\varepsilon)$ of Puiseux series, i.e. power series with rational exponents having bounded denominators, is real closed, and the field $\bar{F} = F[\sqrt{-1}] = \mathbf{C}((\varepsilon^{1/\infty}))$ is algebraically closed (see [7], Chapter XI).

Then ε cannot be a critical value [9] of the polynomial f as a function $F^n \rightarrow F$; in other words, the system $f - \varepsilon = \partial f / \partial X_1 = \dots = \partial f / \partial X_n = 0$ has no root in F^n , since

1980 *Mathematics Subject Classification* (1985 Revision). Primary 65H10; Secondary 14G30, 14J25.

all critical values of
Consequently the
implicit function t
 $V'_\varepsilon \subset V_\varepsilon \subset F^n$ the
(2)

Observe that if
 $(x_1, \dots, x_n) \in V'_\varepsilon$,
zeros in F^n of the
We denote by I
[10] vanishes. In
 $x \notin V'_\varepsilon \cap K$ holds
We introduce t
 $M(X_1, \dots, X_n)$

$$= \prod_{3 \leq j \leq n}$$

with entries in \mathbf{Z}
 $M(x)x \in F^n$ is a

(3) $f(M^{-1}$
in the variables
then $M(x)K$ co
in F^n of the po
function $g_1(X)$
where $X = (X$
 $x \in K$ is satisf
 $(g_1(x))(\partial f(M^{-1}$
Now suppose g_1
prime; we write

The set K c
of a compact a
 $\dim(V_\varepsilon \cap \{g = 0\})$

We note tha
a family Γ of $(i$
runs independe
the polynomial

$$(4) \quad f - \varepsilon =$$

Indeed, we con
 $\partial f / \partial X_n$). The

or equal to $\deg(\{f - \varepsilon = g = 0\}) \cdot (2d)^n < N$ [11]. Therefore for some $\gamma \in \Gamma$ the point $(1, \gamma) \in \mathbb{F}^n$ does not lie on the cone of the variety $\overline{\varphi(\{f - \varepsilon = g = 0\})}$; this is the desired γ .

Thus, there is a vector $\gamma \in \Gamma$ such that in every connected component of the variety $V_\varepsilon \subset \mathbb{F}^n$ there are at least two points which are solutions of (4), and (4) has no solution in K .

The algorithm runs over the elements $\gamma \in \Gamma$; we fix one such γ . We construct the nonsingular $n \times n$ matrix

$$B = \prod_{2 \leq j \leq n} \left(\begin{array}{ccc} \overbrace{1 \quad \dots \quad \gamma_j}^j & & \\ -\gamma_j & \mathbf{0} & \\ & \mathbf{0} & 1 \end{array} \right) \Bigg\}^j.$$

We set $f^{(1)} = f(B^{-1}X) \in \mathbb{Z}[X_1, \dots, X_n]$, and we consider the system (see (2))

$$(5) \quad f^{(1)} - \varepsilon = \partial f^{(1)} / \partial X_2 = \dots = \partial f^{(1)} / \partial X_n = 0.$$

We denote its root variety by $V^{(1)} \subset \mathbb{F}^n$.

Applying the algorithms of [5] and [6] to the system (5), we decompose the variety $V^{(1)} = \bigcup_q V_q^{(1)}$ into irreducible components over $\mathbb{Q}(\varepsilon)$. Then, applying the method of [6], Chapter II, §1, to each component $V_q^{(1)}$ for which $\dim V_q^{(1)} = 0$, the algorithm finds zero-dimensional varieties $V^{(2)} \subset \mathbb{C}^n$, irreducible over \mathbb{Q} , that are contained in the variety of zeros of the system $f^{(1)} = \partial f^{(1)} / \partial X_2 = \dots = \partial f^{(1)} / \partial X_n = 0$.

Here the zero-dimensional varieties $V_m^{(2)}$ are presented in the following form. For each variety $V_m^{(2)}$ the algorithm constructs an irreducible (over \mathbb{Q}) polynomial $\Phi \in \mathbb{Q}[2]$, such that for every point $(\xi_1, \dots, \xi_n) \in V_m^{(2)}$ the field $\mathbb{Q}(\xi_1, \dots, \xi_n)$ is isomorphic to $\mathbb{Q}[2]/(\Phi) \simeq \mathbb{Q}[\theta]$, where $\Phi(\theta) = 0$ and the primitive element $\theta = \sum_1^n \lambda_i \xi_i$ for suitable natural numbers $1 \leq \lambda_i \leq \deg \Phi \leq (2d)^n$. Furthermore, the algorithm finds explicitly

$$\xi_i = \sum_{0 \leq j < \deg \Phi} \beta_i^{(j)} \theta^j,$$

with $\beta_i^{(j)} \in \mathbb{Q}$, for $1 \leq i \leq n$, $0 \leq j < \deg \Phi$.

For each component $V_m^{(2)}$ the algorithm checks whether or not it contains at least one of the real points $(\xi_1, \dots, \xi_n) \in V_m^{(2)} \cap \mathbb{R}^n$. This is equivalent to $\theta = \sum_1^n \lambda_i \xi_i \in \mathbb{R}$. Thus, it is sufficient for the algorithm to check whether the polynomial Φ has at least one real zero, which may be accomplished using the Sturm sequence [7]. If $\Phi(\theta) = 0$ and $\theta \in \mathbb{R}$, then the vector $B^{-1}(\xi_1, \dots, \xi_n) \in \mathbb{R}^n$ is a real zero of the polynomial f .

On the basis, e.g., of [12] the algorithm can find a rational approximation $\theta^{(s)} \in \mathbb{Q}$ such that $|\theta - \theta^{(s)}| < 2^{-s}$ for any fixed natural number s , in a time that is polynomial in s and the size of the polynomial Φ . This completes the description of the algorithm for finding zeros of f .

We make a few remarks concerning the justification of our algorithm. We recall that there is a $\gamma \in \Gamma$ such that in each connected component of the variety V_ε there is a zero $x = (x_1, \dots, x_n) \in \mathbb{F}^n \setminus K$ of the system (4), and here the gradient $(\text{grad } f)(x)$ is proportional to the vector $(1, \gamma)$. Then $(\text{grad } f^{(1)})(Bx)$ is proportional to $(1, 0, \dots, 0)$, and consequently the vector $(\chi_1, \dots, \chi_n) = Bx \in \mathbb{F}^n \setminus K_1$ satisfies (5), where $K_1 = BK$ is the set of points of zero curvature of the variety $\{f^{(1)} - \varepsilon = 0\}$. The vector $(\chi_1, \dots, \chi_n) \in V_q^{(1)}$ for an appropriate zero-dimensional component $V_q^{(1)} \subset \mathbb{F}^n$ (see (2) and the remark thereafter). Since every element $0 \neq \chi \in F$ is uniquely representable in the form $\chi = \varepsilon^\alpha (\chi^{(0)} + \omega)$, where $\alpha \in \mathbb{Q}$, $0 \neq \chi^{(0)} \in \mathbb{R}$ and the element ω is infinitesimal, on taking into account the fact that $\|(\chi_1, \dots, \chi_n)\| \leq (Nn)^n \|x\| \leq (Nn)^n (r + \varepsilon)$, we

find the representation $0, \dots, \alpha_n \geq 0$. Then

lies on an appropriate component of the variety V_0 in mind that each point of the corresponding (the bound)

LEMMA. a) It solutions (ξ_1, \dots, ξ_n) of the variety $V_0 =$ each point $(\xi_1, \dots,$

which give a field isomorphic to $\mathbb{Q}[\theta]$ for θ a polynomial for θ coefficients $1 \leq \lambda_i$ a polynomial in k b) Furthermore, to find a rational which is polynomi

REMARK. The polynomials f_1 (see (1)) played by an elem

3. We now turn to the system (1), equalities, we may

and we apply the

As a result the set $\{g = 0\} \subset \mathbb{F}^n$, Then for each point $f_i(\xi_1, \dots, \xi_n) =$ lemma (cf. [5] and inequality $|\theta - \theta_1|$ algorithm finds a using e.g. [12] (cf. $h_i(\theta^{(s)}) \in \mathbb{Q}$. If for all $1 \leq i$ $(\xi_1, \dots, \xi_n) \in V$. set of all points (

Bearing in mind the Euclidean topology equalities $g \geq 0$

find the representation $(\chi_1, \dots, \chi_n) = (\varepsilon^{\alpha_1}(\chi_1^{(0)} + \omega_1), \dots, \varepsilon^{\alpha_n}(\chi_n^{(0)} + \omega_n))$, with $\alpha_1 \geq 0, \dots, \alpha_n \geq 0$. Then the vector

$$(\chi_1^{(1)}, \dots, \chi_n^{(1)}) = \lim_{\delta \rightarrow 0} (\delta^{\alpha_1} \chi_1^{(0)}, \dots, \delta^{\alpha_n} \chi_n^{(0)}) \in \mathbf{R}^n$$

lies on an appropriate 0-dimensional component $V_m^{(2)} \subset \mathbf{C}^n$. We call the number $\chi_j^{(1)} \in \mathbf{R}$ the real part of the element $\chi_j \in F$. Hence, the vector $(\xi_1, \dots, \xi_n) = \beta^{-1}(\chi_1^{(1)}, \dots, \chi_n^{(1)}) \in V_0$, and in view of the properties of $\gamma \in \Gamma$, in each connected component of the variety V_0 the algorithm finds at least one point of this type, bearing in mind that each connected component of V_0 coincides with the set of real parts of all points of the corresponding connected component of V_ε . Thus the following lemma is proved (the bounds here use [5] and [6]):

LEMMA. a) It is possible to construct an algorithm that produces a finite set of real solutions $(\xi_1, \dots, \xi_n) \in \mathbf{R}^n$ for the equation $f = 0$, so that in each connected component of the variety $V_0 = \{f = 0\} \subset \mathbf{R}^n$ there is at least one point of this set. Moreover, for each point (ξ_1, \dots, ξ_n) the algorithm constructs expressions

$$\xi_i = \sum_{0 \leq j < \deg \Phi} \beta_i^{(j)} \theta^j \in \mathbf{Q}[\theta]$$

which give a field isomorphism $\mathbf{Q}(\xi_1, \dots, \xi_n) = \mathbf{Q}[\theta] \simeq \mathbf{Q}[Z]/(\Phi)$, where Φ is the minimal polynomial for θ over the field \mathbf{Q} , and further $\theta = \sum_{1 \leq i \leq n} \lambda_i \xi_i$ with natural number coefficients $1 \leq \lambda_i \leq \deg \Phi \leq (2d)^n$. The execution time for the algorithm is bounded by a polynomial in $kMd^{n^2} \leq L^n \leq L^{\log L}$.

b) Furthermore, for every zero (ξ_1, \dots, ξ_n) and for each natural number s , it is possible to find a rational approximation $(\xi_1^{(s)}, \dots, \xi_n^{(s)}) \in \mathbf{Q}^n$ so that $|\xi_i - \xi_i^{(s)}| < 2^{-s}$, in time which is polynomial in $Md^{n^2}s$.

REMARK. The proof of the lemma in fact also goes through when the initial polynomials f_1 (see (1)) have coefficients in the ring $\mathbf{Z}[\varepsilon]$, where the role of ε in the proof is played by an element $\varepsilon_1 > 0$ which is infinitesimal with respect to ε .

3. We now turn to the consideration of the case of weak inequalities $f_1 \geq 0, \dots, f_k \geq 0$ in the system (1), which determine a semialgebraic set $V \subset \mathbf{R}^n$. Just as in the case of equalities, we may assume that $V \subset D_r$. We consider the polynomial

$$g = (f_1 + \varepsilon)(f_2 + \varepsilon) \cdots (f_k + \varepsilon) - \varepsilon^k \in \mathbf{Z}[\varepsilon][X_1, \dots, X_n],$$

and we apply the lemma to it, bearing in mind the last remark.

As a result the algorithm finds points in each connected component of the variety $\{g = 0\} \subset F^n$, and then, as above, the real parts $(\xi_1, \dots, \xi_n) \in \mathbf{R}^n$ of these points. Then for each point (ξ_1, \dots, ξ_n) the algorithm checks for which $i, 1 \leq i \leq k$, the equality $f_i(\xi_1, \dots, \xi_n) = h_i(\theta) = 0$ holds, where $h_i \in \mathbf{Q}[Z]$, on the basis of assertion a) of the lemma (cf. [5] and [6]). If $h_1(\theta) \neq 0$, then for any zero $\theta_1 \in \mathbf{C}$ of the polynomial h_1 , the inequality $|\theta - \theta_1| > \exp(-p_1(L))$ holds for a suitable polynomial p_1 (cf. [12]). Further, the algorithm finds a rational approximation $\theta^{(s)} \in \mathbf{Q}$ such that $|\theta - \theta^{(s)}| < \exp(-p_1(L))/2$, using e.g. [12] (cf. assertion b) of the lemma). Then $h_i(\theta) \in \mathbf{R}$ has the same sign as $h_i(\theta^{(s)}) \in \mathbf{Q}$. The algorithm computes $h_i(\theta^{(s)})$ for all $1 \leq i \leq k$ for which $h_i(\theta) \neq 0$. If for all $1 \leq i \leq k$ either $f_i(\xi_1, \dots, \xi_n) = 0$ or $h_i(\theta^{(s)}) > 0$ holds, then the point $(\xi_1, \dots, \xi_n) \in V$. The set of solutions of (1) required in the theorem coincides with the set of all points (ξ_1, \dots, ξ_n) which satisfy these conditions.

Bearing in mind that V coincides with the set of real parts of the closed (in the Euclidean topology) semialgebraic set $V^{(\varepsilon)} \subset F^n$ of all solutions of the system of inequalities $g \geq 0, f_1 + \varepsilon > 0, \dots, f_k + \varepsilon > 0$, and in addition that the boundary of

each connected component of the set $V^{(\epsilon)}$ lies in the variety $\{g = 0\} \subset F^n$ (cf. [8]), we find that there is at least one point (ξ_1, \dots, ξ_n) constructed by the algorithm on each connected component of the set V .

We turn finally to the consideration of the system (1). We introduce a new variable Z and we consider the system $f_1 \geq 0, \dots, f_l \geq 0, f_{l+1} \geq 0, \dots, f_k \geq 0, Z \cdot f_{l+1} \cdots f_k = 1$. Applying the algorithm described in the case of weak inequalities to this system, we complete the proof of the theorem.

4. We will call nonempty semialgebraic point set in \mathbf{R}^n an (f_1, \dots, f_k) -cell if it consists of points satisfying the conditions

$$\{f_{i_1} = 0\}_{i_1 \in I_1}, \quad \{f_{i_2} > 0\}_{i_2 \in I_2}, \quad \{f_{i_3} < 0\}_{i_3 \in I_3},$$

for some partition $I_1 \cup I_2 \cup I_3 = \{1, \dots, k\}$. Then \mathbf{R}^n is decomposed into (f_1, \dots, f_k) -cells.

REMARK. It is possible to construct an algorithm which enumerates all the (f_1, \dots, f_k) -cells and indicates at least one point on every connected component of each cell. The execution time of this algorithm is polynomial in $M(kd)^{n^2}$.

Leningrad State University
Leningrad Branch
Steklov Institute of Mathematics
Academy of Sciences of the USSR

Received 11/JULY/84

BIBLIOGRAPHY

1. George E. Collins, Automata Theory and Formal Languages (Second GI Conf., Kaiserslautern, 1975), Lecture Notes in Computer Sci., vol. 33, Springer-Verlag, 1975, pp. 134-183.
2. H. R. Wüthrich, Komplexität von Entscheidungsproblemen—ein Seminar (1973/74), Lecture Notes in Computer Sci., vol. 43, Springer-Verlag, 1976, pp. 138-162.
3. L. G. Khachiyan, Dokl. Akad. Nauk SSSR **244** (1979), 1093-1096; English transl. in Soviet Math. Dokl. **20** (1979).
4. N. N. Vorob'ev, Jr., Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 7-19; English transl., to appear in J. Soviet Math.
5. D. Yu. Grigor'ev, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 20-79; English transl., to appear in J. Soviet Math.
6. A. L. Chistov, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 124-188; English transl., to appear in J. Soviet Math.
7. Serge Lang, *Algebra*, Addison-Wesley, 1965.
8. J. Milnor, Proc. Amer. Math. Soc. **15** (1964), 275-280.
9. a) John W. Milnor, *Topology from the differentiable viewpoint*, Univ. Press of Virginia, Charlottesville, Va., 1965.
b) Andrew H. Wallace, *Differential topology. Initial steps*, Benjamin, 1968.
10. John A. Thorpe, *Elementary topics in differential geometry*, Springer-Verlag, 1979.
11. David Mumford, *Algebraic geometry*, Vol. I, Springer-Verlag, 1976.
12. A. G. Akritas, Computing **24** (1980), 299-313.

Translated by G. L. CHERLIN

Докл. Акад. Наук СССР
Том 283 (1985), № 6

ON CA

UDC 517.98

1. The problem of de
the problem of approxi
emerges as a criterion fo
the possible accuracy of

2. Suppose that a fe
[0, 1] is given on a real l
1) $\|Q_t\| \leq 1$ for all t
2) $Q_s Q_t = Q_t Q_s = C$

By analogy with a
Banach space with decc
For the special choic

the space $C = C(0, 1)$ i
canonical decompositio

Let (X, Q_t) and $(Y,$
with domain $\mathcal{D}(A) \subset X$
 $Q_t x_1 = Q_t x_2$ for som
 $S_t A(x_2)$ for the same

The set of all bou
 $\mathcal{L}_c(X, Y)$; this is a sul

3. We consider th
 X , and let $A \in \mathcal{L}(X_n$
restriction $B|_{X_n}$ to X

THEOREM 1. For

$$(1) \quad \|A -$$

Here (and below)

The estimate (1) i
decomposition:

THEOREM 2. Fo

$$(2) \quad \inf_B$$

1980 Mathematics
Secondary 94A12.