

## Feasibility Testing for Systems of Real Quadratic Equations\*

Alexander I. Barvinok

Department of Mathematics, Royal Institute of Technology,  
S-100 44 Stockholm, Sweden  
barvinok@math.kth.se

**Abstract.** We consider the problem of deciding whether a given system of quadratic homogeneous equations over the reals has nontrivial solution. We design an algorithm which, for a fixed number of equations, uses a number of arithmetic operations bounded by a polynomial in the number of variables only.

### 1. Introduction

Let  $G_i = \langle x, \Psi_i x \rangle$ ,  $i = 1, \dots, m$ , be a family of quadratic forms on  $\mathbb{R}^n$ , so  $\Psi_i$ ,  $i = 1, \dots, m$ , are  $n \times n$  real square symmetric matrices and  $\langle \cdot, \cdot \rangle$  is the standard scalar product in  $\mathbb{R}^n$ . Let  $S^{n-1} = \{x \in \mathbb{R}^n, \|x\| = 1\}$  be the unit sphere. We denote by  $\|\Psi\|$  the usual norm of  $\Psi$ :  $\|\Psi\| = \max\{\|\Psi(x)\|, x \in S^{n-1}\}$ . We consider the following problem:

**(1.1) Problem.** Find whether there exists an  $x \in S^{n-1}$  such that

$$G_1(x) = \dots = G_m(x) = 0.$$

Without loss of generality we assume that  $\|\Psi_i\| \leq \frac{1}{2}$  for  $i = 1, \dots, m$ .

In other words we are interested in whether a given family of projective quadrics has nonempty intersection. We study the computational complexity of this problem. If  $m = 1$ , then Problem (1.1) has no solution if and only if the form  $G_1$

---

\* A preliminary version of this paper with a weaker result appeared in the *Proceedings of STOC'92*. This research was supported by the Mittag-Leffler Institute and KTH, Stockholm.

is definite. In this case the Sylvester criterion provides a polynomial algorithm. If  $m = 2$ , then the Toeplitz–Hausdorff theorem (see, for example, [11]) can be used to design a polynomial-time algorithm for the “generic” forms  $G_i$ . No such results seem to be known for  $m = 3$ . In this paper we prove the following main result.

**(1.2) Theorem.** *Assume that  $m$  is fixed. Then, for any  $n \in \mathbb{N}$  and any quadratic forms  $G_1, \dots, G_m: \mathbb{R}^n \rightarrow \mathbb{R}$ , Problem (1.1) can be solved using a number of arithmetic operations which is polynomial in  $n$ .*

Problem (1.1) is universal in a class of semialgebraic problems since an arbitrary system of polynomial equations and inequalities over the field  $\mathbb{R}$  can be reduced to Problem (1.1). Of course, the number  $m$  of quadratic forms will be large in general. Usually, algorithms in real algebraic geometry have a complexity which is exponential in the number of variables (for an exposition of algorithmic problems in real algebraic geometry and the history of the subject see, for example, [14]–[16]). Theorem (1.2) allows the distinction of “simple” systems of polynomial equations and inequalities, namely, those which can be reduced to a few quadratic equations. It also inspires a hope that other algorithmic problems of algebraic geometry involving intersections of a small number of quadrics can be solved polynomially.

As the main tool to solve (1.1) we study the following optimization problem.

**(1.3) Optimization Problem.** Let  $F_i = \langle x, \Phi_i x \rangle$ ,  $i = 1, \dots, k$ , be positive definite quadratic forms on  $\mathbb{R}^n$ . Find

$$l = \max \left\{ \prod_{i=1}^k F_i(x) : x \in S^{n-1} \right\}.$$

Without loss of generality we assume that  $F_i(x) \geq \frac{1}{2}\|x\|^2$  for  $i = 1, \dots, k$ .

Putting  $k = 2m$ ,  $F_{2i-1}(x) = \|x\|^2 - G_i(x)$ ,  $F_{2i}(x) = \|x\|^2 + G_i(x)$  for  $i = 1, \dots, m$  for Problem (1.1) we conclude that

$$\max \left\{ \prod_{i=1}^k F_i(x) : x \in S^{n-1} \right\} = \begin{cases} 1 & \text{if the forms } G_1, \dots, G_m \text{ have a} \\ & \text{common nontrivial zero,} \\ l < 1 & \text{if the forms } G_1, \dots, G_m \text{ do not} \\ & \text{have a common nontrivial zero.} \end{cases}$$

The main part of this paper deals with Problem (1.3) and only in Section 4 do we consider the source problem (1.1) which initiates and justifies the study of (1.3). In Section 2 we characterize the optimal value  $l$  of (1.3) by constructing a univariate polynomial  $P$  of degree  $O(n^k)$  such that  $P(l) = 0$ . In Section 3 we design a polynomial algorithm for (1.3) when  $k$  is fixed and the forms  $F_1, \dots, F_k$  are in a

general position. We also construct a polynomial algorithm for pushing forms into general position.

By arithmetic operations we mean addition, subtraction, multiplication, division, and comparison of real numbers.

## 2. A Polynomial Equation for the Maximal Value

Here we prove the following main result.

**(2.1) Theorem.** *Assume that  $k$  is fixed. Then, for any given  $n \in \mathbb{N}$  and any given quadratic forms  $F_1, \dots, F_k: \mathbb{R}^n \rightarrow \mathbb{R}$ , a univariate nonzero polynomial  $P(z)$  of degree not more than  $(k+1) \cdot n^k$  such that  $P(l) = 0$ , where  $l$  is the solution of (1.3), can be computed. To do that a number of arithmetic operations which is polynomial in  $n$  (the degree of this polynomial is linear in  $k^2$ ) can be used.*

Let  $I$  denote the identity  $n \times n$  matrix. Consider an expansion

$$(2.2) \quad \det^{-1/2} \left( I - \sum_{i=1}^k t_i \Phi_i \right) = 1 + \sum_{0 \leq m_1, \dots, m_k} q(m_1, \dots, m_k) \cdot t_1^{m_1} \cdots t_k^{m_k}$$

in a small neighborhood of the point  $t_1 = \dots = t_k = 0$ . Our first lemma deals with the geometric meaning of the coefficients  $q(m_1, \dots, m_k)$ .

Let  $\Gamma(z) = \int_0^{+\infty} x^{z-1} \exp\{-x\} dx$  be the usual Gamma function and let  $ds$  be the measure on the sphere  $S^{n-1}$ .

**(2.3) Lemma.** *The following identity for the coefficients of (2.2) holds:*

$$q(m_1, \dots, m_k) = \pi^{-n/2} \cdot \frac{\Gamma(m_1 + \dots + m_k + n/2)}{2 \cdot m_1! \cdots m_k!} \int_{S^{n-1}} F_1^{m_1}(s) \cdots F_k^{m_k}(s) ds.$$

*Proof.* Put  $G(x) = F_1^{m_1}(x) \cdots F_k^{m_k}(x)$ . For  $r > 0$  set  $S(r) = \{x: \|x\| = r\}$  and  $\psi(r) = \int_{S(r)} G(s) ds$ , where  $ds$  is the measure on the sphere  $S(r)$  induced from  $\mathbb{R}^n$ . Since  $G(x)$  is homogeneous of degree  $2m = 2(m_1 + \dots + m_k)$  we have

$$\psi(r) = \psi(1) \cdot r^{n+2m-1}.$$

Therefore we have

$$\begin{aligned} \int_{\mathbb{R}^n} G(x) \cdot \exp\{-\|x\|^2\} dx &= \psi(1) \cdot \int_0^{+\infty} r^{n+2m-1} \exp\{-r^2\} dr \\ &= \frac{1}{2} \cdot \psi(1) \cdot \Gamma\left(m + \frac{n}{2}\right). \end{aligned}$$

The left-hand side integral is equal to

$$\frac{\partial^m}{\partial t_1^{m_1} \cdots \partial t_k^{m_k}} \int_{\mathbb{R}^n} \exp\{-\|x\|^2 + t_1 F_1(x) + \cdots + t_k F_k(x)\} dx \Big|_{t_1 = \cdots = t_k = 0}.$$

To compute the last integral the well-known formula for the integral over  $\mathbb{R}^n$  of the exponential function of a quadratic form can be used (see, for example, [10]). So we have

$$\int_{\mathbb{R}^n} \exp\{-\|x\|^2 + t_1 F_1(x) + \cdots + t_k F_k(x)\} dx = \pi^{n/2} \cdot \det^{-1/2} \left( I - \sum_{i=1}^k t_i \Phi_i \right).$$

Finally we obtain

$$q(m_1, \dots, m_k) = \pi^{-n/2} \cdot \frac{\Gamma(m_1 + \cdots + m_k + n/2)}{2 \cdot m_1! \cdots m_k!} \psi(1),$$

and the proof follows.  $\square$

We also need the following result which is known in many different forms.

**(2.4) Lemma.** *Let  $H: \mathbb{R}^n \rightarrow \mathbb{R}$  be a continuous function which is positive on  $S^{n-1}$ . Assume that  $\rho: S^{n-1} \rightarrow \mathbb{R}$  is a continuous density such that  $\rho(s) > 0$  for all  $s \in S^{n-1}$ . Then*

$$\lim_{m \rightarrow +\infty} \left( \frac{\int_{S^{n-1}} H^{m+1}(s) \rho(s) ds}{\int_{S^{n-1}} H^m(s) \rho(s) ds} \right) = \max\{H(x): x \in S^{n-1}\}.$$

*Proof.* For the one-dimensional interval this result is proved, for example, in Section 2, Chapter 5, §1, Ex. 199 of [13]. We omit the proof for  $S^{n-1}$  since it is completely analogous.  $\square$

**(2.5) Corollary.** *Let us fix  $a_1, \dots, a_k \in \mathbb{N}$  and denote  $Q_i = q(a_1 + i, \dots, a_k + i)$ . Then, for any  $j \in \mathbb{N}$ ,*

$$\lim_{i \rightarrow +\infty} \frac{Q_{j+i}}{Q_i} = k^{kj} \cdot l^j,$$

where  $l$  is the maximal value in (1.3).

*Proof.* Put  $\rho(s) = F_1^{a_1}(s) \cdots F_k^{a_k}(s)$  and  $H(s) = F_1(s) \cdots F_k(s)$  in Lemma (2.4). Then using Lemma (2.3) we deduce that  $\lim_{i \rightarrow +\infty} Q_{i+1}/Q_i = k^k \cdot l$ . Since  $Q_{j+i}/Q_i = \prod_{r=1}^j (Q_{i+r}/Q_{i+r-1})$  the proof follows.  $\square$

In the previous version of this paper [2] an analogous relation was used to design an approximate algorithm for solving (1.1).

To prove Theorem (1.2) we need a computational version of one result of Gessel (see Theorem 2 of [5]) on rational power series in few variables.

Let  $Z(t_1, \dots, t_k)$  be a polynomial in complex variables  $t_1, \dots, t_k$  with constant term 1 and let  $\alpha$  be a complex number. Let us consider the expansion

$$Z^{-\alpha}(t_1, \dots, t_k) = 1 + \sum_{0 \leq m_1, \dots, m_k} \zeta(m_1, \dots, m_k) \cdot t_1^{m_1} \cdots t_k^{m_k}$$

in a small neighborhood of the point  $t_1 = \dots = t_k = 0$ . Then Theorem 2 from [5] asserts that there exist polynomials  $r_0(m_1, \dots, m_k), \dots, r_d(m_1, \dots, m_k)$ , not all equal to zero, such that

$$(2.6) \quad \sum_{j=0}^d r_j(m_1, \dots, m_k) \cdot \zeta(m_1 + j, \dots, m_k + j) = 0$$

for all  $m_1, \dots, m_k$ .

In fact, in [5] a more general result is proved not only for polynomials but also for rational functions. We need explicit estimates of  $d$  and of the computational complexity of these polynomials  $r_j$ . The desired estimates can be easily extracted from the proof in [5], but since [5] does not deal with computational complexity questions we briefly describe its method. We assume that the polynomial  $Z$  is given by its coefficients. To compute a polynomial means to compute its decomposition into a sum of monomials.

**(2.7) Lemma.** *Let us fix  $k$ . For any given  $\alpha$  and any given polynomial  $Z$  such that  $\deg Z \leq v$ , polynomials  $r_j(m_1, \dots, m_k)$ ,  $j = 0, \dots, d$ , can be computed such that (2.6) holds,  $d \leq (k+1) \cdot v^k$ , and  $\deg r_j \leq k \cdot (k+1) \cdot v^k$  for all  $j$ . To compute these polynomials  $r_j$  it is necessary to perform  $v^{O(k^2)}$  arithmetic operations.*

*Proof.* We follow Theorem 2 of [5] converting the proof into an algorithm and adding explicit estimates.

Let us choose  $D \in \mathbb{N}$ . For  $\beta = (\beta_1, \dots, \beta_k) \in \mathbb{N}_0^k$ ,  $j \in \mathbb{N}_0$ :  $\beta_1 + \dots + \beta_k + k \cdot j \leq D$ , let us consider the following family of functions:

$$\left( \frac{t^k}{\partial t_1 \cdots \partial t_k} \right)^j \prod_{i=1}^k \left( t_i \cdot \frac{\partial}{\partial t_i} \right)^{\beta_i} Z^{-\alpha}(t_1, \dots, t_k) = U_{j,\beta}(t_1, \dots, t_k) \cdot Z^{-\alpha-D}(t_1, \dots, t_k).$$

Here  $U_{j,\beta}$  are polynomials of degree at most  $D \cdot v$ . These polynomials  $U_{j,\beta}$  can be computed in a straightforward way using  $(D \cdot v)^{O(k)}$  arithmetic operations. It turns out by counting arguments that if  $D$  is chosen so that

$$\binom{k + D \cdot v}{k} < \frac{1}{k} \binom{k + D}{k + 1},$$

then the polynomials  $U_{j,\beta}$  are linearly dependent. If  $\{c_{j,\beta}\}$  are the coefficients of this dependence, then we put

$$r_j(m_1, \dots, m_k) = \prod_{i=1}^k \frac{(m_i + j)!}{m_i!} \sum_{\beta} c_{j,\beta} (m_1 + j)^{\beta_1} \cdots (m_k + j)^{\beta_k}.$$

Thus we have  $\deg r_j \leq D$  for all  $j$ . We can rewrite  $r_j$  as a sum of monomials in  $m_1, \dots, m_k$  using  $D^{O(k)}$  arithmetic operations.

Hence the problem is reduced to finding a linear dependence between certain polynomials  $U_{j,\beta}$  in  $k$  variables of degree less than  $D \cdot v$ . We can choose  $D = k \cdot (k + 1) \cdot v^k$ , so  $d \leq (k + 1) \cdot v^k$ . Now we obtain the desired estimates.  $\square$

We need the following purely technical result on the expansion of the determinant of a matrix of polynomials.

**(2.8) Proposition.** *Let us fix  $k \in \mathbb{N}$ . Then, for any given  $n \times n$  square matrices  $A_0, \dots, A_k$ , the expansion of*

$$Z(t_1, \dots, t_k) = \det \left( A_0 + \sum_{i=1}^k t_i \cdot A_i \right)$$

*into a sum of monomials in  $t_1, \dots, t_k$  can be computed using  $n^{O(k)}$  arithmetic operations.*

*Proof.* First we note that the degree of  $Z$  does not exceed  $n$ . Note that the determinant of an  $n \times n$  square matrix can be computed using  $O(n^3)$  arithmetic operations. Therefore computing the values of  $Z(t_1, \dots, t_k)$  in points

$$(t_1, \dots, t_k) \in [0:n]^k$$

from the resulting system of linear equations using  $n^{O(k)}$  arithmetic operations we obtain an explicit decomposition of  $Z(t_1, \dots, t_k)$  into a sum of monomials.  $\square$

Now we can prove the main result of this section.

*Proof of Theorem (2.1).* Let us denote

$$Z(t_1, \dots, t_k) = \det \left( I - \sum_{i=1}^k t_i \Phi_i \right).$$

So  $Z(t_1, \dots, t_k)$  is a polynomial in  $t_1, \dots, t_k$  of degree not more than  $n$ . The right-hand side of (2.2) is the expansion of  $Z^{-1/2}(t_1, \dots, t_k)$  into a power series in  $t_1, \dots, t_k$ . By Proposition (2.8) we obtain an explicit decomposition of  $Z(t_1, \dots, t_k)$

into a sum of monomials in  $t_1, \dots, t_k$ . Then by Lemma (2.7) using  $n^{O(k^2)}$  arithmetic operations we compute polynomials  $r_0(m_1, \dots, m_k), \dots, r_d(m_1, \dots, m_k)$ , not all equal to zero, such that

$$\sum_{j=0}^d r_j(m_1, \dots, m_k) \cdot q(m_1 + j, \dots, m_k + j) = 0$$

for all  $m_1, \dots, m_k$ . Here  $d \leq (k+1) \cdot n^k$ .

Let us choose  $a_1, \dots, a_k$  such that  $r_u(a_1, \dots, a_k) \neq 0$  for some  $u$ . Let us put

$$Q_i = q(a_1 + i, \dots, a_k + i), \quad R_j(i) = r_j(a_1 + i, \dots, a_k + i), \quad j = 0, \dots, d, \quad i \in \mathbb{N}.$$

So we have got a polynomial recursion

$$\sum_{j=0}^d R_j(i) \cdot Q_{i+j} = 0 \quad (*)$$

for all  $i \in \mathbb{N}$ , where  $R_j$  are polynomials not all of which are identically zero. Let  $g = \max\{\deg R_j, j = 0, \dots, d\}$ , so  $R_j(i) = \alpha_j \cdot i^g + \text{lower-order terms}$ . Divide each summand of  $(*)$  by  $Q_i \cdot i^g$  as  $i \rightarrow +\infty$ . Since by Corollary (2.5)

$$\lim_{i \rightarrow +\infty} Q_{i+j}/Q_i = k^{kj} \cdot l^j,$$

we obtain finally the desired polynomial equation:

$$\sum_{j=0}^d \alpha_j \cdot k^{kj} \cdot l^j = 0.$$

So we put  $P(z) = \sum_{j=0}^d \alpha_j \cdot k^{kj} \cdot z^j$ . Since by Lemma (2.7) we have that

$$\deg r_j \leq k \cdot (k+1) \cdot n^k$$

for all  $j$ , we get the desired estimate of the complexity of the algorithm. □

**Remark.** In the proof above we show that for a certain choice of  $a_1, \dots, a_k$  the sequence  $q(a_1 + i, \dots, a_k + i)$  is polynomially recursive. In fact, this sequence is polynomially recursive for any  $a_1, \dots, a_k$  (see [12]). However, known bounds on the degree of the resulting polynomial equation are much worse than for a sequence with a “generic” starting point.

**Example.** If  $k = 1$ , then  $l$  is the maximal eigenvalue of the matrix  $\Phi_1$ . Then we have  $\chi(l) = 0$ , where  $\chi$  is the characteristic polynomial of degree not more than  $n$ .

### 3. Maximum in a General Position

Here we consider the case of “general position” in (1.3). We begin with the following standard result.

**(3.1) Lemma.** *Let  $x \in S^{n-1}$  be a point where the maximum  $l$  in (1.3) is attained. Then for some positive  $t_1, \dots, t_k$  the following equation holds:*

$$\left( I - \sum_{i=1}^k t_i \Phi_i \right) x = 0.$$

*Proof.* Note that the maximum of  $H = \sum_{i=1}^k \ln F_i$  on  $S^{n-1}$  is also attained in  $x$ . Thus for the differential  $dH$  we get

$$\sum_{i=1}^k \frac{1}{F_i(x)} \Phi_i(x) = \lambda \cdot x$$

for some  $\lambda \in \mathbb{R}$ . Applying  $\langle \cdot, x \rangle$  to both sides of the relation we deduce that  $\lambda = k$ .  $\square$

It is known that in the space of real symmetric  $n \times n$  matrices the set of matrices of corank  $r$  is a real analytic submanifold of codimension  $r(r+1)/2$  (see, for example, the corollary on p. 994 of the English translation of [1]). From this it can be derived that, for  $k$  symmetric  $n \times n$  matrices  $\Phi_1, \dots, \Phi_k$  in general position, the following condition holds:

$$\text{rank} \left( I - \sum_{i=1}^k t_i \cdot \Phi_i \right) \geq n - \frac{\sqrt{1+8k}-1}{2}$$

for all  $t_1, \dots, t_k \in \mathbb{R}$ .

The words “in general position” mean that the last inequality holds for all matrices from an open dense set in the vector space of all  $k$ -tuples  $(\Phi_1, \dots, \Phi_k)$  of symmetric  $n \times n$  matrices. In fact, for us it is essential that the corank of a linear combination cannot be greater than a certain function in  $k$  alone. We say that  $\Phi_1, \dots, \Phi_k$  are in general position if

$$(3.2) \quad \text{rank} \left( I - \sum_{i=1}^k t_i \cdot \Phi_i \right) \geq n - f(k)$$

for all  $t_1, \dots, t_k \in \mathbb{R}$ , where  $f(k)$  is a certain function such that

$$f(k) \geq \frac{\sqrt{1+8k}-1}{2}.$$

For example,  $f(k) = k$  can be chosen.



Instead of Problem (1.3) we now consider the following “yes-or-no” problem.

**(3.3) Problem.** For given  $a, \varepsilon \in \mathbb{R}$ , decide whether  $|l - a| < \varepsilon$ , where  $l$  is the maximal value in (1.3).

The idea of the following result was suggested by A. Megretsky.

**(3.4) Theorem.** Assume that  $k$  is fixed. Then, for given quadratic forms  $F_1, \dots, F_k: \mathbb{R}^n \rightarrow \mathbb{R}$  such that (3.2) holds and any given  $a, \varepsilon \in \mathbb{R}$ , Problem (3.3) can be solved using a number of arithmetic operations which is polynomial in  $n$ .

*Proof.* Let us denote  $H(x) = \prod_{i=1}^k F_i(x)$ . Put

$$\mathcal{A} = \left\{ x \in S^{n-1} : \left( I - \sum_{i=1}^k t_i \cdot \Phi_i \right) x = 0 \text{ for some } t_1, \dots, t_k \right\}.$$

By Lemma (3.1) it follows that  $l = \max\{H(x) : x \in \mathcal{A}\}$ , whereas by (3.2) we deduce that  $\mathcal{A}$  is a semialgebraic set of dimension not more than  $k + f(k)$ . Here it is essential that  $\dim \mathcal{A}$  is bounded by a function in  $k$  alone. We construct a decomposition of the set  $\mathcal{A}$  into a union of (possibly intersecting) semialgebraic sets  $\{\mathcal{B}_m : m \in M\}$  called *pieces* such that, for each piece  $\mathcal{B}_m$ , the problem

**(3.4.1)** given  $b \in \mathbb{R}$ , decide whether  $H(x) > b$  for some  $x \in \mathcal{B}_m$

reduces to solving a system of algebraic equations and inequalities in at most  $k + f(k)$  variables. The number card  $M$  of such pieces is bounded by a polynomial in  $n$ . The answer to Problem (3.3) is “yes” if for some  $m \in M$  and  $b = a - \varepsilon$  the answer to Problem (3.4.1) is “yes” and for all  $m \in M$  and  $b = a + \varepsilon$  the answer to Problem (3.4.1) is “no.”

An index  $m \in M$  consists of a number  $r \in \mathbb{N}$  such that  $n - f(k) \leq r < n$  and of a pair  $(I, J)$ , where  $I, J \subset \{1, \dots, n\} : \text{card } I = \text{card } J = r$ . For  $t = (t_1, \dots, t_k)$  let us denote the matrix  $I - \sum_{i=1}^k t_i \cdot \Phi_i$  by  $\Phi(t)$  and its  $r \times r$  submatrix with row indices in  $I$  and column indices in  $J$  by  $\Phi(t; I, J)$ . Put

$$T_m = \{t = (t_1, \dots, t_k) \text{ such that all } (r+1) \times (r+1) \text{ minors of } \Phi(t) \text{ are equal to 0 and } \det \Phi(t; I, J) \neq 0\}.$$

Then define

$$\mathcal{B}_m = \{x \in S^{n-1} : \Phi(t)x = 0 \text{ for some } t \in T_m\}.$$

Now we can design the desired system of polynomial equations and inequalities for solving (3.4.1). To simplify notation we assume that the nonsingular submatrix  $\Phi(t; I, J)$  occupies the upper left-hand side corner of the matrix  $\Phi(t)$ . Let us denote

by  $u_j(t), j = r + 1, \dots, n$ , the vector consisting of the first  $r$  entries of the  $j$ th column of  $\Phi(t)$ . Finally put

$$x_j(t) = \begin{cases} -\Phi(t; I, J)^{-1} u_j(t) & \text{for the first } r \text{ coordinates,} \\ 1 & \text{for the } j\text{th coordinate,} \\ 0 & \text{elsewhere.} \end{cases}$$

Then

$$\mathcal{B}_m = \left\{ \sum_{j=r+1}^n \lambda_j x_j(t), \lambda_j \in \mathbb{R}, t \in T_m, \left\| \sum_{j=r+1}^n \lambda_j x_j(t) \right\|^2 = 1 \right\}.$$

Using Proposition (2.8) we obtain an explicit representation of the entries of  $\Phi(t; I, J)^{-1}$  as rational functions in  $t_1, \dots, t_k$ . Now it is clear that (3.4.1) is written as a system of polynomial equations and inequalities in at most  $k + f(k)$  variables  $t_1, \dots, t_k, \lambda_{r+1}, \dots, \lambda_n$ . Since the degree of these equations and inequalities is  $O(n)$  and their number is polynomial in  $n$  when  $k$  is fixed then (see, for example, [14] and [15]) it follows that Problem (3.4.1) can be solved using a number of arithmetic operations which is polynomial in  $n$  (the degree of this polynomial is linear in the number of variables, i.e., in  $k + f(k)$ ). Since  $\text{card } M \leq n \cdot n^{2 \cdot f(k)}$  we have reduced the initial problem (3.3) to a set of problems of type (3.4.1) whose cardinality is bounded by a certain polynomial in  $n$ .  $\square$

Now we describe a way to disturb effectively given matrices  $\Phi_i \mapsto \hat{\Phi}_i$  to ensure (3.2) with  $f(k) = k$ . Here we basically follow [7] although we present a weaker construction (in [7] a sharp bound for  $f(k)$  is achieved).

**(3.5) Theorem.** *Assume that  $k$  is fixed. Then, for any given symmetric  $n \times n$  matrices  $\Phi_1, \dots, \Phi_k$  and any given  $\varepsilon > 0$ ,  $n \times n$  matrices  $\hat{\Phi}_1, \dots, \hat{\Phi}_k$  such that condition (3.2) holds with  $f(k) = k$  and  $\|\Phi_i - \hat{\Phi}_i\| < \varepsilon$  can be constructed using a number of arithmetic operations which is polynomial in  $n$ . (The degree of this polynomial is linear in  $k$ .)*

First we reduce the problem to the following one, written in symmetric form.

**(3.5.1) Problem.** Given real symmetric matrices  $A_0, \dots, A_k$  and  $\varepsilon > 0$  find symmetric matrices  $\hat{A}_i, i = 0, \dots, k$ , such that  $\|A_i - \hat{A}_i\| < \varepsilon$  for all  $i$  and

$$\text{rank} \left( \sum_{i=0}^k t_i \cdot \hat{A}_i \right) \geq n - k$$

for all complex  $t_0, \dots, t_k$ , not all of which are equal to 0.

If (3.5.1) can be solved in polynomial time, then Theorem (3.5) is proved. One has to choose  $A_0 = I$ ,  $A_i = \Phi_i$ ,  $i = 1, \dots, k$ , and then put  $\hat{\Phi}_i = G' \hat{A}_i G$ , where  $G$  is a nondegenerate matrix such that  $G' \hat{A}_0 G = I$  and  $\hat{A}_i$  are computed with regard to  $\varepsilon/2$  (we assume that  $\varepsilon < \frac{1}{2}$ ).

Let  $B_i$ ,  $i = 0, \dots, k$ , be the following diagonal matrices:

$$B_i(j, j) = j^i.$$

Then for the family  $B_i$ ,  $i = 0, \dots, k$ , condition (3.2) obviously holds with  $f(k) = k$ . We construct the desired deformation of  $A_i$  using  $B_i$ .

**(3.6) Lemma.** *There exist not more than  $N = n^{O(k)}$  different numbers  $z \in \mathbb{C}$  such that*

$$\text{rank} \left( \sum_{i=0}^k t_i \cdot (A_i + z \cdot B_i) \right) < n - k$$

for some  $t_0, \dots, t_k$ , not all of which are equal to 0.

*Proof.* Let us consider two complex projective spaces  $\mathbf{P}^k = \{t = (t_0 : t_1 : \dots : t_k)\}$ ,  $\mathbf{P}^1 = \{z = (z_0 : z_1)\}$  and the algebraic variety

$$V = \left\{ (t, z) \in \mathbf{P}^k \times \mathbf{P}^1 : \text{rank} \left( \sum_{i=0}^k t_i \cdot z_1 \cdot A_i + t_i \cdot z_0 \cdot B_i \right) < n - k \right\}$$

together with the projection  $pr: V \rightarrow \mathbf{P}^1$ ,  $(t, z) \mapsto z$ . The image  $pr(V)$  is a certain subvariety in  $\mathbf{P}^1$  such that the point  $(1:0)$  does not belong to the image. Therefore  $pr(V)$  is a finite set in  $\mathbf{P}^1$  and the number of points in  $pr(V)$  does not exceed the number of irreducible components of  $V$ . Note that  $V$  can be defined by  $O(n^{2k})$  polynomial equations of degree not more than  $n$  in  $2k + 2$  variables  $w_{ij} = t_i \cdot z_j$  of  $\mathbf{P}^{2k+1}$ . To estimate the number of irreducible components of  $V$  the results of [6] and [3] (see also [8]) can be used.  $\square$

*Proof of Theorem (3.5).* We design an algorithm for Problem (3.5.1). For a given  $\varepsilon$  choose sufficiently small  $\delta > 0$  such that  $\|\delta \cdot B_i\| < \varepsilon$  for  $i = 0, \dots, k$ . Then let us put consecutively  $z = 0, \delta/N, 2 \cdot \delta/N, \dots, \delta$ ,  $\hat{A}_i = A_i + z \cdot B_i$ , where  $N$  is an upper bound from Lemma (3.6). Note that, for any given  $z$ , condition (3.2) can be tested using a number of arithmetic operations which is polynomial in  $n$ , since it reduces to solving systems of polynomial equations in a fixed number of variables. By Lemma (3.6) it follows that for at least one  $z$  from these  $N$  the matrices  $\hat{A}_i$  are desired. Another way to get such a  $z$  is to use a quantifier elimination method (see [15] and [16]) which has polynomial complexity since the number of variables is fixed.  $\square$

#### 4. Feasibility Testing

Now we turn to Problem (1.1) and prove the main result of this paper.

*Proof of Theorem (1.2).* Our algorithm is the following. First we construct the forms  $F_1, \dots, F_k$  as in Section 1. Then we have to check whether  $l = 1$  where  $l$  is the solution of (1.3). Let us construct the polynomial  $P$  as in Theorem (2.1). If  $P$  does not vanish on 1, then  $G_1, \dots, G_m$  have no common nontrivial root and we are done; thus we may assume that  $P(1) = 0$ . Then we find a number  $\delta > 0$  such that  $|\alpha_i - \alpha_j| > \delta$  for any two different real roots of the polynomial  $P$ . To do this we divide  $P$  by g.c.d.  $(P(z), dP/dz)$ , reducing to the case of polynomial without multiple roots, and then estimate  $\delta$  using the usual discriminant argument (see, for example, [4]). To compute such a  $\delta$  it is necessary to perform a number of arithmetic operations which are polynomial in  $\deg P$ , and therefore are polynomial in  $n$ . Then using Theorem (3.5) we construct a perturbation  $F_i \mapsto \hat{F}_i$ ,  $i = 1, \dots, k$ , such that  $|l - \hat{l}| < \delta/2$ , where

$$\hat{l} = \max\{\hat{F}_1(x) \cdots \hat{F}_k(x) : x \in S^{n-1}\}.$$

Finally, using Theorem (3.4) we check whether  $|\hat{l} - 1| < \delta/2$ . If the inequality holds, then there exists a common nontrivial root of  $G_1, \dots, G_m$ . Otherwise these forms have no common nontrivial root.  $\square$

We conclude the paper with two remarks.

Our algorithm is designed for arbitrary real data. If the forms  $G_1, \dots, G_m$  are given by their *rational* coefficients, then it can be checked that the size of all numbers involved in the algorithm is bounded by a polynomial in the input size and thus our algorithm is strongly polynomial in the number of variables.

Theorem (1.2) gives us  $n^{O(m^2)}$  as an upper bound for the complexity of an algorithm. Grigor'ev told the author that using ideas from [9] an estimate  $n^{O(m)}$  can be achieved. He also noted that an estimate  $O(\log^m n)$  for the parallel complexity can be achieved.

#### Acknowledgments

I am grateful to A. M. Vershik who has introduced me to real algebraic geometry and to N. Mnëv, A. Megretsky, and D. Grigor'ev for many stimulating discussions and valuable suggestions. I am indebted to M.-F. Coste-Roy for her remarks and interest and to anonymous referees for their recommendations.

#### References

1. A. A. Agrachev, Topology of quadratic maps and Hessians of smooth maps, *Itogi Nauki i Tekhniki, Seriya Algebra, Topologiya, Geometriya*, **26** (1988), 85–124 (translated in *Journal of Soviet Mathematics*, **49**(3) (1990), 990–1013).

2. A. I. Barvinok, Feasibility testing for systems of real quadratic equations, in: *Proceedings of the 24th Symposium on the Theory of Computing*, ACM Press, New York, 1992, pp. 126–132.
3. A. L. Chistov, Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time, *Zapiski Nauchnykh Seminarov LOMI*, **137** (1984), 124–188 (translated in *Journal of Soviet Mathematics*, **34**(4) (1986), 1838–1882).
4. G. E. Collins and R. Loos, Real zeros of polynomials, in: *Computer Algebra. Symbolic and Algebraic Computation* (B. Buchberger, G. E. Collins, and R. Loos, eds.), Springer-Verlag, New York, 1982, pp. 83–94.
5. I. M. Gessel, Two theorems on rational power series, *Utilitas Mathematica*, **19** (1981), 247–254.
6. D. Yu. Grigor'ev, Factorization of polynomials over a finite field and the solution of systems of algebraic equations, *Zapiski Nauchnykh Seminarov LOMI*, **137** (1984), 20–79 (translated in *Journal of Soviet Mathematics*, **34**(4) (1986), 1762–1803).
7. D. Yu. Grigor'ev, Private communication, 1992.
8. D. Yu. Grigor'ev and A. L. Chistov, Fast decomposition of polynomials into irreducible ones and the solution of systems of algebraic equations, *Doklady Akademii Nauk SSSR*, **275**(6) (1984), 1302–1306 (translated in *Soviet Mathematics. Doklady*, **29**(2) (1984), 380–383).
9. D. Yu. Grigor'ev and N. N. Vorobjov, Solving systems of polynomial inequalities in subexponential time, *Journal of Symbolic Computation*, **5**(1–2) (1988), 37–64.
10. J. Hadamard, *Cours D'Analyse*, vol. 1, Hermann, Paris, 1927.
11. P. R. Halmos, *A Hilbert Space Problem Book*, Van Nostrand, London, 1967.
12. L. Lipshitz, The diagonal of a  $D$ -finite series is  $D$ -finite, *Journal of Algebra*, **113** (1988), 373–378.
13. G. Pólya and G. Szegő, *Aufgaben und Lehrsätze aus der Analysis*, Vol. 1, Dover, New York, 1945.
14. J. Renegar, On the computational complexity and geometry of the first order theory of the reals. Part 1. Introduction. Preliminaries. The geometry of semi-algebraic sets. The decision problem for the existential theory of the reals, *Journal of Symbolic Computation*, **13**(3) (1992), 255–299.
15. J. Renegar, On the computational complexity and geometry of the first order theory of the reals. Part 2. The general decision problem. Preliminaries for quantifier elimination, *Journal of Symbolic Computation*, **13**(3) (1992), 301–327.
16. J. Renegar, On the computational complexity and geometry of the first order theory of the reals. Part 3. Quantifier elimination, *Journal of Symbolic Computation*, **13**(3) (1992), 329–352.

*Received November 9, 1991, and in revised form September 14, 1992.*

