Mathematical Notes, vol. 74, no. 4, 2003, pp. 483–490.
Translated from Matematicheskie Zametki, vol. 74, no. 4, 2003, pp. 508–516.

A Generalization of the Hilbert Basis Theorem

K. Yu. Gorbunov

Received November 8, 2001; in final form, February 10, 2003

Abstract—A generalization of the Hilbert basis theorem in the geometric setting is proposed. It asserts that, for any well-describable (in a certain sense) family of polynomials, there exists a number C such that if P is an everywhere dense (in a certain sense) subfamily of this family, a is an arbitrary point, and the first C polynomials in any sequence from P vanish at the point a, then all polynomials from P vanish at a.

Key words: *the Hilbert basis theorem, quasipolynomial, numbers servicing sequences of quasipolynomials, interpolation with multiple nodes, pseudoremainder.*

The Hilbert basis theorem in the geometric setting asserts that a sequence of embedded algebraic varieties[1] stabilizes. In other words, for any sequence S of polynomials in variables $x_1, \dots, x_k$, there exists a number C such that if $a = \langle x_1^*, \dots, x_k^* \rangle$ is an arbitrary point and the first C polynomials in the sequence S vanish at a, then all polynomials from S vanish at this point (in this case, we say that the number C *services* the sequence S). This statement is a corollary of the usual Hilbert basis theorem, and for the radical ideals (i.e., for the ideals closed with respect to root extraction), it is equivalent to this theorem. We shall generalize it by proving the existence of a C servicing a whole family of sequences of polynomials. Certainly, for the generalization to be nontrivial, the family must contain polynomials of arbitrarily high degree, and it must not be a family of polynomials in finitely many expressions. Taking this into account, we give the following definition.

Definition. A *quasipolynomial* in variables $x_1, x_2, \dots, x_k$ is a syntactic expression which is a polynomial in $x_1, x_2, \dots, x_k$, in the expressions $F(x_1), F(x_2), \dots, F(x_k)$ and in their derivatives $F'(x_1), \dots, F'(x_k), \dots, F^{(i)}(x_1), \dots, F^{(i)}(x_k), \dots$;[2] for example, $x_2F(x_1)F'''(x_1) + x_3F''(x_2)F''(x_2)$ is a quasipolynomial.

Suppose that $S = q_1, q_2, \dots$ is a given sequence of quasipolynomials. Let

$$p = p_n x^n + p_{n-1}x^{n-1} + \dots + p_1 x + p_0$$

be a polynomial. Substituting the polynomials $p(x_i)$ for $F(x_i)$ ($i = 1, \dots, k$) and the corresponding polynomials for the derivatives of $F(x_i)$ everywhere in S, we obtain a sequence of polynomials $S(p) = q_1(p), q_2(p), \dots$. Certainly, we cannot guarantee the existence of one number c servicing the sequences $S(p)$ for all polynomials p. Indeed, if $S = F(x), F'(x), F''(x), \dots$ and $p = x^n$, then the first n terms of $S(p)$ do vanish at the point $x = 0$, while the $(n+1)$th does not. However, the theorem stated below asserts that there exists a number c which services $S(p)$ for

[1] Here and in what follows, by an *algebraic manifold* we understand the union of the zero sets of a finite system of polynomials in an affine space over the field of real or complex numbers.

[2] The term *quasipolynomial* is conventionally used for a polynomial in variables and their exponentials. We naturally generalize this notion.

polynomials p from an everywhere dense (in a certain sense) set. To be more precise, we say that a condition P holds *for almost all polynomials* if, for any sufficiently large n, any $p_0, \dots, p_n$, and any ε, there exist an ε_1 and $\overline{p}_0, \dots, \overline{p}_n$ such that $|\overline{p}_i - p_i| < \varepsilon$ and, for arbitrary $\overline{p}_0^*, \dots, \overline{p}_n^*$ with $|\overline{p}_i^* - \overline{p}_i| < \varepsilon_1$, the polynomial $\overline{p}_n^* x^n + \dots + \overline{p}_0^*$ satisfies the condition P.

Theorem. *For any infinite sequence S of quasipolynomials in $x_1, x_2, \dots, x_k$, there exists a number c such that, for almost all polynomials p and any point $a = \langle x_1^*, \dots, x_k^* \rangle$, either all polynomials in the sequence $S(p)$ vanish at a or some polynomial with number not exceeding c in $S(p)$ does not vanish at the point a.*

Proof. First, we prove an auxiliary lemma, which gives a necessary and sufficient condition for a quasipolynomial q to have the following property: if p is a polynomial and $q(p)$ vanishes at a point a, then an arbitrarily small change of the coefficients of lower terms in the polynomial p (their number does not depend on the degree of p) yields a polynomial $\overline{p}$ such that the polynomial $q(\overline{p})$ does not vanish at the point a.

Lemma 1. *Let q be a quasipolynomial in $x_1, \dots, x_k$. Then there exists a number m such that, for any polynomial $p = p_n x^n + \dots + p_0$ of degree $n > m$ and any point $a = \langle x_1^*, \dots, x_k^* \rangle$, the following two conditions are equivalent:*

(1) *if the polynomial $q(p)$ vanishes at the point a, then, for any $\varepsilon > 0$, there exist numbers $\overline{p}_0, \dots, \overline{p}_m$ such that $|\overline{p}_i - p_i| < \varepsilon$ for $i = 0, \dots, m$ and the polynomial $q(\overline{p})$, where $\overline{p} = p_n x^n + \dots + p_{m+1} x^{m+1} + \overline{p}_m x^m + \dots + \overline{p}_0$, does not vanish at the point a;*

(2) *the substitution of $x_1^*, \dots, x_k^*$ into q yields a nonzero polynomial in*

$$F(x_i^*), F'(x_i^*), F''(x_i^*), \dots .$$

Proof. The implication (1)$\Rightarrow$(2) is obvious. Let us prove the implication (2)$\Rightarrow$(1). By the *type of a point a* we mean the data sppecifying which of its coordinates x_i^* are pairwise equal. Obviously, it is sufficient to prove the lemma for points of one arbitrary type. Identifying the expressions $F(x_i)$ and $F(x_j)$ in q for $x_i^* = x_j^*$, we can assume that all the x_i^* are different. Take an $m \ge \sum_{i=1}^k (\alpha_i + 1)$, where α_i is the maximal order of the derivatives of $F(x_i)$ in q. Choose values $F^{(j)}(x_i^*) = \beta_{ij}$ for $j = 0, \dots, \alpha_i$ so that q with these $F^{(j)}(x_i^*)$ does not vanish at a (this is possible by condition (2)). According to the theory of interpolation with multiple nodes (see, e.g., [1, Chap. 3, Sec. 6]), there exists a polynomial g of degree not exceeding m such that $g^{(j)}(x_i^*) = \beta_{ij}$ for all i and j. Therefore, substituting an mth-degree polynomial with indeterminate coefficients for F in q, we obtain a nonzero (at the point a) polynomial q_m in these coefficients. On the other hand, substituting a polynomial of arbitrary degree $n > m$ with indeterminate coefficients for F, we obtain a polynomial q_n of the form $q_m + \overline{q}$, and each term of $\overline{q}$ contains at least one indeterminate coefficient p_i with $i > m$. Thus, the polynomial q_n is nonzero in this case too. Now, the assertion of the lemma follows from the geometrically obvious fact that a nonzero polynomial on a space determines an algebraic variety of dimension smaller than that of the space, and we can always leave the variety by moving an arbitrarily small distance from a root of this polynomial (a rigorous argument can be readily carried out by induction on the number of variables). This completes the proof of Lemma 1. □

Let us demonstrate the main idea of the proof of the theorem on an example.

Example. Suppose that a sequence S begins with $yx^2, x^3 + z, \dots$ and we want to simplify its second term, knowing that the first term vanishes. It is natural to consider the following two cases:

(1) $y = 0$; in this case, we cannot simplify the second term, but the first term can be replaced by y;

(2) $y \ne 0$; in this case, the second term can be replaced by z.

Thus, one sequence gives rise to the two sequences

$$y = 0,\ \ x^3 + z = 0,\ \ \dots \qquad \text{and} \qquad (yx^2 = 0 \,\&\, y \neq 0),\ \ z = 0,\ \ \dots .$$

It is natural to represent these two sequences in the form of a tree with supplementary (empty) root and two branches. Then the consideration of possible cases (as above) corresponds to splitting one vertex into several.

We proceed to the formal proof of the theorem.

Recall that the *type* of a point is the data specifying which of its coordinates are pairwise equal. Let $t_1, \dots, t_d$ be all possible types. We process the sequence S for each type t separately as follows. Let us identify equal variables and the corresponding expressions $F(x_i), F'(x_i), \dots$ by replacing all variables from the class of equal variables by the variable with minimal index from this class. We obtain a sequence S_t.

We shall construct an infinite (but with vertices of finite degrees) tree T (we imagine it growing upward). Each of its vertices will be marked by finitely many equalities of the form $q = 0$ and inequalities of the form $q \neq 0$, where q is a nonzero quasipolynomial (a vertex may have an empty mark). First, for T we take the tree T_t in which every vertex has precisely one "son" and, for every i, the ith vertex from the bottom is marked by the ith term of the sequence S_t equated to zero. A path (finite or infinite) beginning at the root and going upward all the time is said to be a *root path*. The marking *components* are the variables $x_1, \dots, x_k$ and the expressions

$$F(x_1), \dots, F(x_k), \qquad F'(x_1), \dots, F'(x_k), \dots .$$

After the tree T is constructed, it will have the following four *fundamental properties*.

1. If γ_1 is a finite root path in T_t and a is a point at which all the equalities marking the vertices on the path γ_1 hold, then there exists a root path γ_2 of the same length in T such that all the relations (both equalities and inequalities) marking the vertices on this path hold at the point a.
2. If γ is a finite root path in T and a is a point at which all the relations marking the vertices on the path γ hold, then, at the point a, all the equalities marking the vertices on a root path of the same length in T_t hold.
3. The marking of an arbitrary vertex in T either is empty or contains at least one equality.
4. An infinite root path in T can contain only finitely many vertices whose markings have a given component.

We order the marking components as follows:

$$x_1, \dots, x_k, \quad F(x_1), \dots, F(x_k), \quad F'(x_1), \dots, F'(x_k), \quad \dots .$$

Each component is processed as described below. We assume that, during the processing, the following "intermediate" condition holds in addition to the first three fundamental properties.

4^*. An infinite root path in the tree can contain only finitely many vertices whose markings have components or inequalities already processed.

We say that a vertex is *active* if its current marking has no already processed components but does have the component being processed. Let us describe the processing. Suppose that the component to be processed is, say, $F(x_1)$. We treat the left-hand sides of all the equalities as polynomials in one variable (the component $F(x_1)$) whose coefficients are polynomials in the other components (by the *degree* of such a polynomial we mean the maximal power of $F(x_1)$ in this polynomial). We process only the active vertices of the tree and start with the bottom ones; thus, before processing the current vertex v, all active vertices below it are already processed, and all coefficients of the powers of $F(x_1)$ in the equalities marking these vertices are the left-hand sides of some inequalities in the markings.

We process v as follows. If the degrees of all polynomials on the left-hand sides of the equalities marking v are less than the degrees of all polynomials in the markings of the active vertices on the path from v to the root, then we split the vertex v into finitely many vertices with the same parent. Each of them corresponds to a distribution of zeros among the coefficients in the polynomials on the left-hand sides of the equalities marking v (all possible cases are considered). When a coefficient is equal to zero, we add this equality to the marking of the corresponding new vertex and remove the term with this coefficient from the polynomial, and when it is not equal to zero, we add this inequality to the marking. For example, if v has marking

$$F(x_2)F^2(x_1) + F(x_3)F(x_1) + 1 = 0,$$

then it splits into eight vertices with markings

(1) $F(x_2) \neq 0,\ F(x_3) \neq 0,\ 1 \neq 0,\ F(x_2)F^2(x_1) + F(x_3)F(x_1) + 1 = 0;$
(2) $F(x_2) = 0,\ F(x_3) \neq 0,\ 1 \neq 0,\ F(x_3)F(x_1) + 1 = 0;$
(3) $F(x_2) \neq 0,\ F(x_3) = 0,\ 1 \neq 0,\ F(x_2)F^2(x_1) + 1 = 0;$
(4) $F(x_2) \neq 0,\ F(x_3) \neq 0,\ 1 = 0,\ F(x_2)F^2(x_1) + F(x_3)F(x_1) = 0;$
(5) $F(x_2) \neq 0,\ F(x_3) = 0,\ 1 = 0,\ F(x_2)F^2(x_1) = 0;$
(6) $F(x_2) = 0,\ F(x_3) \neq 0,\ 1 = 0,\ F(x_3)F(x_1) = 0;$
(7) $F(x_2) = 0,\ F(x_3) = 0,\ 1 \neq 0,\ 1 = 0;$
(8) $F(x_2) = 0,\ F(x_3) = 0,\ 1 = 0.$

Above each of these vertices, we place a copy of the set of vertices above v. The vertex splitting operation described above preserves the fundamental property 1 (because we consider all the cases), the fundamental property 2 (because the relations marking the new vertex imply the relations marking the old one), and the fundamental property 3 (because if some coefficient in a polynomial is nonzero, then the polynomial is nonzero as well).

Now, consider the case in which the marking of a vertex u below v includes the equality to zero of a polynomial p_u of nonzero degree m and the marking of the vertex v includes the equality to zero of a polynomial p_v, and the vertex v has degree $n \geq m$ (we assume that the vertex u is chosen in such a way that m is minimal). For every such p_v, we perform the following procedure. We multiply p_v by the $(n-m+1)$th power of the leading coefficient of p_u, so that the division of the obtained polynomial by p_u does not give fractions. Having performed this division, we obtain the equality $p_m^{n-m+1}p_v = qp_u + r$, where p_m is the leading coefficient of p_u and the polynomial r is the so-called *pseudoremainder* (or the modified remainder); the degree of r is strictly less than the degree of p_u (the notion of pseudoremainder was used by Chinese mathematician Wu Wen-tsun to algorithmically prove theorems of Euclidean geometry (see, e.g., [2, Chap. 6, Sec. 5]) and by Muchnik in a new simpler proof of the Tarski theorem on the elimination of quantifiers (see [3, Chap. 3, Sec. 8])). For example, if

$$p_v = F^2(x_3)F^3(x_1) - F(x_1), \qquad p_u = F^3(x_3)F(x_1) - 2,$$

then

$$(F^3(x_3))^3 p_v = (F^8(x_3)F^2(x_1) + 2F^5(x_3)F(x_1) + 4F^2(x_3) - F^6(x_3))p_u + (8F^2(x_3) - 2F^6(x_3)).$$

Since the marking of the vertex u includes the inequality $p_m \neq 0$, we have $p_v = 0$ if and only if $r = 0$. If r is a nonzero polynomial, we replace p_v by r in the marking of v, and if it is zero, we remove the equality $p_v = 0$ from this marking. Obviously, this operation preserves the fundamental properties 1 and 2, and it preserves the fundamental property 3, because the vertex v is active and, hence, its marking contains no inequalities. Performing all possible divisions and replacements of the dividends by the remainders, we reduce the situation to the case already considered; after that, we split the vertex v as described above.

It is easy to see that such a processing of a component (i.e., the described processing of a countable set of vertices) preserves the fundamental properties 1, 2, and 3. The intermediate condition 4^* also holds, because the degrees of polynomials in the equalities marking the vertices on a root path strictly decrease, and each inequality is included in the marking of a vertex together with an equality containing the same component.

In the processing of a countable set of components, the vertices of given height can be active only finitely many times. Therefore, we can consider the limit tree T, which obviously has the four fundamental properties. Property 4 implies the following lemma. We call the minimal order of the derivatives in the marking of a vertex v the *rank* of this vertex and denote it by $\operatorname{rank}(v)$; if the marking contains at least one variable x_i which is not an argument of F or if the marking is empty, we set the rank to be -1. The rank of a set M of vertices is defined as $\operatorname{rank}(M) = \min_{v\in M} \operatorname{rang}(v)$ (we assume that $\operatorname{rank}(\varnothing) = \infty$). A vertex from which an infinite upward path on vertices with empty markings goes is said to be *extreme* (this vertex itself may have a nonempty marking).

Lemma 2. *For any numbers r and h, the limit tree T contains a finite subset M of vertices with the following properties*:

(1) $\operatorname{rank}(M) > r$ *and the heights of all vertices from M are larger than h*;

(2) *there exists a number h_1 such that any infinite root path in T either intersects M in precisely one vertex or passes through an extreme vertex of height no larger than h_1.*

Proof. Note that there exists a height $h_1 > h$ such that any infinite root path in the interval between the heights h and h_1 passes through either an extreme vertex or a vertex of rank larger than r. Indeed, otherwise, by the compactness property (the König lemma), there exists an infinite root path passing through an infinite number of vertices of bounded rank with nonempty markings, which contradicts the fundamental property 4. Thus, the set M is formed as follows: for each root path, we include its first vertex having rank larger than r and height between h and h_1 (if the path contains such vertices) in M. This completes the proof of Lemma 2. □

Thus, for each point type, we have constructed a processed tree. Let us arbitrarily order these trees: $T_1, T_2, \dots, T_d$. In each T_i, we construct $k+1$ finite sets $M_i^1, M_i^2, \dots, M_i^{k+1}$ of vertices (we call these sets *levels*). They are linearly ordered (we say that M_i^j is *below* M_s^l if either $i < s$ or $i = s$ and $j < l$) and have the following properties.

1. For any level M, $\operatorname{rank}(M) > 0$ and, if there are nonempty levels below M, then $\operatorname{rank}(M) > \operatorname{rank}(\overline{M}) + m$, where $\overline{M}$ is the nonempty level nearest to M from below and m is the maximal number among those corresponding (by Lemma 1) to the polynomials from the equalities marking the vertices from $\overline{M}$ (the existence of such equalities is ensured by the fundamental property 4).
2. The heights of all vertices on each level are larger than all heights of the vertices on the preceding levels.
3. There exists a number h such that, in every T_i, any infinite root path either intersects each of the levels $M_i^1, \dots, M_i^{k+1}$ in precisely one vertex or passes through an extreme vertex of height not exceeding h.

Obviously, using Lemma 2, we can construct the required M_i^j successively, starting with the lowest one. The property 1 of levels expresses the main idea of the further argument; namely, we shall shift the coefficients $p_0, p_1, \dots, p_m$ in F so as to change the function on the left-hand side of an equality marking a vertex on some level but leave all functions from the markings of vertices on higher levels intact.

Choose a degree n larger than the ranks of all levels. Take any polynomial p of degree n. In the markings of level vertices, we replace F by the polynomial p (and the derivatives of F by the corresponding expressions). Let us fix one equality in the marking of each level vertex v. This equality determines an algebraic variety (we denote it by $R(v)$) in the space of variables $x_1, \dots, x_{k(i)}$ ($k(i) \le k$, because we have identified equal variables; here $v \in T_i$). If $u \in M_i^j$,

$v \in M_i^l$, $j < l$, and v is a descendant of the vertex $u \neq v$ in the tree T_i, then we say that the variety $R(v)$ is a *descendant* of the variety $R(u)$.

We search levels starting with the highest ones; for each vertex v, we shift the coefficients in the (current) polynomial p so that the manifold $R(v)$ occupies the most general position with respect to the set of its descendants. To be more precise, for each path going from v upward, we consider the algebraic variety R equal to the intersection of all descendants of the manifold $R(v)$ on this path. As is known from algebraic geometry (see, e.g., [4, Chap. 1, Sec. 3, Theorem 1; 2, Chap. 4, Sec. 6, Theorem 2]), any variety is a finite union of irreducible (i.e., not representable as a union of two nonempty varieties) varieties, which are called its irreducible components. We shall consider components of R which are irreducible over the field of complex numbers and contain points with pairwise different coordinates (recall that we are interested only in points all of whose coordinates x_i are pairwise different; for the other points, different trees are "responsible"). We wish to move the coefficients of p in a small neighborhood in such a way that R remains fixed and each of its irreducible components R^* of the form specified above intersects the variety $R(v)$ in a variety of dimension smaller than that of R. It is clear from geometric considerations that it suffices to shift $R(v)$ away from an arbitrary point of the component R^*; the shift must be so small that the dimensions of the intersections of the other (finitely many) varieties would remain smaller than the dimensions of the varieties themselves.

By Lemma 1, if n is sufficiently large, we can perform such a shift from any point with pairwise different coordinates. Indeed, since the coordinates are different and the rank of the vertex v is positive, assertion (2) from Lemma 1 holds. By property 1 of levels, the variety R and all varieties on higher levels are invariant. This implies that each shift can be made so small that all "general positions" of varieties achieved previously are retained. As is known from algebraic geometry (see, e.g., [4, Chap. 1, Sec. 6, Theorem 1; 2, Chap. 9, Sec. 4, Proposition 10]), if a variety X is a proper subset of an irreducible variety Y, then the dimension of X is strictly smaller that the dimension of Y. Therefore, every time we cut the (shifted) current manifold by the intersection of its descendants on the path, the dimension of the section decreases. Having shifted the coefficients as described above, we obtain a polynomial $\overline{p}$ from p.

For the number c mentioned in the statement of the theorem we take any number larger than the number h from the property 3 of levels. We claim that this c services $S(\overline{p})$. Indeed, suppose that the first c equalities in the sequence S hold at a point a of type t. Then the first c equalities in the sequence S_t hold at the point a_t obtained from a by identifying equal coordinates. Let T_i be the tree corresponding to the type t. By the fundamental property 1, T_i has a root path γ of length c such that all the relations marking its vertices hold at the point a_t. There are two possibilities.

Case 1. Suppose that γ intersects each of the levels $M_i^1, \dots, M_i^{k+1}$ in one vertex. Let us denote these vertices by $v_1, \dots, v_{k+1}$, respectively. By construction, the dimensions of the irreducible components of the manifolds

$$R(v_{k+1}), \quad R(v_{k+1)} \cap R(v_k), \quad \dots, \quad R(v_{k+1}) \cap R(v_k) \cap \dots \cap R(v_1)$$

that contain the point a_t (with pairwise different coordinates) strictly decrease. Since the dimension of the space does not exceed k, this case is impossible.

Case 2. Suppose that γ passes through an extreme vertex v. Consider an infinite root path $\overline{\gamma}$ which coincides with γ up to v and then passes through vertices with empty markings. Applying the fundamental property 2 to an arbitrary beginning vertex of the path $\overline{\gamma}$, we conclude that all the equalities from the sequence S_t hold at the point a_t and, hence, all the equalities from the sequence S hold at the point a.

To complete the proof of the theorem, it remains to make the number c service not only $\overline{p}$ itself, but also one of its neighborhoods. Let us show how this can be achieved by arbitrarily small shifts of any coefficients in the polynomial p. For the degree n chosen above, we replace F in the markings of all trees T_i by a polynomial of degree n with indeterminate coefficients. For every tree and every root path which intersects the levels of this tree in the vertices $v_1, \dots, v_k$, we write a formula Φ_i^γ expressing the emptiness of the intersection of the varieties $R(v_i)$. The indeterminate coefficients in the polynomial p are the free variables of this formula. By the Tarski theorem on the elimination of quantifiers (which is valid both over the field of real numbers and over the field of complex numbers; see, e.g., [3, Chap. 3, Sec. 8]), there exists an equivalent quantifier-free formula. We shift the coefficients of p in such a way that all the polynomials in coefficients in all the quantifier-free formulas obtained have nonzero values. Let us show that this makes all the formulas Φ_i^γ true. Indeed, if some formula were false, we could make it true by applying the arbitrarily small shifts of coefficients used above to move the corresponding varieties into general position. This is a contradiction, because small shifts do not change the signs of the polynomials of equivalent quantifier-free formulas. For the same reason, all the formulas Φ_i^γ are true not only for the polynomial $\overline{p}$ itself, but also for all polynomials in its small coefficient neighborhood, as required. This concludes the proof of the theorem. □

Remark 1. It is easy to see that the sequence S in the statement of the theorem can be replaced by an arbitrary tree S (marked by equalities). Then the assertion of the theorem is that there exists a c such that, for almost all p and an arbitrary point, either there exists an infinite root path such that all the equalities marking its vertices hold at this point or any infinite root path has a vertex of height not exceeding c such that some equality from its marking does not hold. To prove this assertion, we must reformulate the fundamental property 2 as follows: If γ is a finite root path in T and a is a point at which all the relations marking the vertices on the path γ hold, then there exists a root path of the same length in T_t such that all the equalities marking its vertices hold at the point a (this path is the preimage of γ under splitting the vertices). The remaining part of the proof does not change.

Remark 2. It is easy to generalize the theorem proved above to the case in which the function F has several arguments and the quasipolynomials may include partial derivatives (for instance, $\partial^4 F/(\partial x_1 \partial x_2 \partial x_2 \partial x_3)$; instead of F, polynomials in the corresponding number of variables are now substituted). For convenience, we can assume that the derivatives with respect to the variables are always taken in the order of increasing numbers of these variables. The only essential complication of the proof is that, in the proof of Lemma 1, the following proposition should be used instead of the above-mentioned result from the theory of multiple interpolation.

Proposition. *Any finite set of conditions, that is, of values of a function and its partial derivatives at given points, is satisfied by a polynomial whose degree depends only on the number of variables, the number of points, and the maximal order of the derivatives involved in the conditions.*

This proposition can be proved, for example, as follows.

We refer to the condition that a partial derivative of order i (of order i with respect to a variable x) takes a given value as a *condition of order* i (respectively, a *condition of order* i *with respect to the variable* x). (The value of the polynomial itself corresponds to $i = 0$.) We linearly order the points in an arbitrary way and the partial derivatives in such a way that their orders do not decrease. Using these orderings, we linearly order all the conditions by the points; if the points coincide, we order them by the partial derivatives. We shall consider the conditions in this order and construct the required polynomial step by step. At the ith step, to the polynomial q_i already constructed, we add a polynomial p_i such that the values of its all derivatives involved in the conditions considered earlier vanish and the value of the derivative involved in the ith condition is such that this condition holds for $q_i + p_i$.

Suppose that the ith condition corresponds to a point $a = \langle a_1, \dots, a_k \rangle$ and the conditions already considered correspond to points $b_1, \dots, b_m$ and, possibly, to a. The polynomial p_i is a number c multiplied by the product of powers of binomials having the form $x - t$, where x ranges over all the variables and, for each variable x_j, t ranges over the different values of the coordinate x_j encountered among the coordinates of the points $b_1, \dots, b_m$, a. For the jth coordinate of a point b_n (if it is not equal to a_j), we take the corresponding factor raised to a power larger than the orders of all conditions; then all the derivatives of p_i in the conditions corresponding to this points vanish. For the point a, we take the factor $x_j - a_j$ to the order of the ith condition with respect to the variable x_j. First, this ensures that the arbitrary derivative d of p_i involved in the already considered conditions corresponding to the point a vanishes at a. Indeed, since the order of d does not exceed the order of the ith condition, there exists a variable x_j whose order in d is strictly less than in the ith condition. Therefore, in any product of binomials naturally included in $d(p_i)$ as a term, the power of the binomial $x_j - a_j$ is nonzero.

Second, the partial derivative of p_i in the ith condition is nonzero. Indeed, an arbitrary term where differentiation with respect to x_j is applied at least once, but not applied to the corresponding factor $x_j - a_j$, contains this factor to a nonzero power and is killed by it. The unique term where differentiation is always applied to "proper" factors contains only factors of the form $x_j - t$, where $t \neq a_j$. Therefore, the partial derivative under consideration does not vanish at the point a, and it can be assigned any required value by choosing the number c. This completes the proof of the proposition.

ACKNOWLEDGMENTS

The author wishes to express his thanks to An. A. Muchnik for discussions which helped to substantially improve the exposition and to N. K. Vereshchagin for valuable comments.

This research was supported in part by the Russian Foundation for Basic Research under grant no. 01-01-01028.

REFERENCES

1. N. S. Bakhvalov, N. P. Zhidkov, and G. M. Kobel′kov, *Numerical Methods* [in Russian], Laboratoriya Bazovykh Znanii, Moscow, 2001.
2. D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer-Verlag, New York, 1997.
3. N. K. Vereshchagin and A. Kh. Shen′, *Languages and Calculi* [in Russian], Mosk. Tsentr Nepreryvnogo Matematicheskogo Obrazovaniya, Moscow, 2000.
4. I. R. Shafarevich, *Foundations of Algebraic Geometry* [in Russian], vol. 1, Nauka, Moscow, 1998.

Institute for Information Transmission Problems,
Russian Academy of Sciences
E-mail: gorbunov@iitp.ru