Math. Ann. 207, 87–97 (1974)

A Nullstellensatz and a Positivstellensatz in Semialgebraic Geometry

Gilbert Stengle

1. Introduction

Let k be an ordered field, K a real closed field containing k. Our purpose is to study finite systems of polynomial inequalities $P_i \geqq 0$, $P_i \in k[x_1 \ldots x_n]$, $i = 1, \ldots, m$, and the associated $(k - K)$ semialgebraic sets, that is, the set of points in K^n satisfying the given inequalities. Our main result, Theorem 1, is a semialgebraic nullstellensatz which characterizes the ideal of polynomials vanishing on a semialgebraic set. In the special case that the set is algebraic we obtain Theorem 2, a new and superior real counterpart of the Hilbert nullstellensatz of a kind which appears in the investigations of Dubois [1]. As a direct consequence of Theorem 1 we obtain Theorem 3, a positivstellensatz which gives a purely algebraic characterization of the semiring of polynomials nonnegative on a semialgebraic set. This semiring is, in our opinion, the most natural and important algebraic object associated with a semialgebraic set. As a special case we obtain Theorem 4, a new characterization of definite polynomial functions which gives a subtle addendum to Artin's solution of Hilbert's 17th problem. We then derive a series of easy consequences which bear upon the study of systems of polynomial inequalities and polynomial programming. Here our positivstellensatz takes on the color of a nonlinear Fourier-Kuhn Theorem (see [2]) which describes the complete set of inequalities deducible from a given set.

2. Basic Definitions

Let k be an ordered field, K a real closed field containing k as an ordered subfield. Let $x = (x_1, \ldots, x_n)$ denote n indeterminates. We establish the following correspondences between subsets of K^n and subsets of $k[x] = k[x_1, \ldots, x_n]$.

Definition 1. Given a subset X of K^n, let $\mathscr{I}(X)$ be the ideal of polynomials in $k[x]$ which vanish on X, let $\mathscr{A}(X)$ be the semiring of polynomials in $k[x]$ which are nonnegative on X. Given a subset B of $k[x]$, let $\mathscr{V}(B)$ be the set of common zeros in K^n of polynomials in B, let

$\mathscr{W}(B)$ be the set of common points of nonnegativity in K^n of polynomials in B.

Definition 2. A subset W of K^n is semialgebraic if $W = \mathscr{W}(B)$ for some finite set $B \in k[x]$.

The purpose of the next definition is to assign to $\mathscr{W}(B)$ a simple, constructively defined semiring of polynomials $S[B]$ nonnegative on $\mathscr{W}(B)$. It should be appreciated that this semiring is only a subsemiring of the generally much larger (and as yet undetermined) semiring $\mathscr{A}(\mathscr{W}(B))$ of all polynomials nonnegative on $\mathscr{W}(B)$.

Definition 3. For any subset C of a ring containing k, let $S(C)$ be the semiring generated by k^+, the positive elements of k, and the squares of elements in C. Given another subset B, let $S(C)[B]$ be the semiring generated by $S(C)$ and B. In the case that the containing ring and C are both $k[x]$, abbreviate $S(k[x])$ to S, $S(k(x))[B]$ to $S[B]$.

We shall be using semirings of the form $S[P_1, \ldots, P_m]$ associated with the semialgebraic set $\mathscr{W}(P_1, \ldots, P_m) = \mathscr{W}(S[P_1, \ldots, P_m])$. We observe that $S[P_1, \ldots, P_m]$ is a finitely generated semimodule over S having as a set of generators the set of all 2^m products of the P_i's without repeated subscripts (including 1 as the empty product). Since the set of inequalities $P_i \geqq 0$ is equivalent to the set using these generators we frequently assume without loss of generality that a system of inequalities has this special form. To refer conveniently to systems of this form we make the following definition.

Definition 4. We say that a set of polynomials $\{P_1, \ldots, P_m\}$ is *standard* if $\{P_1, \ldots, P_m\}$ is a semimodule basis for $S[P_1, \ldots, P_m]$ over S. A system of inequalities $\{P_i \geqq 0\}$ is standard if the set $\{P_1, \ldots, P_m\}$ is standard.

Our most important definition is the following which defines a kind of generalized radical of an ideal relative to a semiring. This definition makes sense in a general commutative ring although we only use it here in $k[x]$.

Definition 5. Let C be a commutative ring, I an ideal in C, and A a subsemiring of C containing all squares in C. Then the *A-radical* of I is the subset of C

$$\varrho_A(I) = \{c \mid c^{2m} + a \in I \text{ for some } m > 0 \text{ and some } a \in A\}.$$

An ideal is an *A-radical ideal* if it is its own A-radical.

The following argument shows that $\varrho_A(I)$ is actually an ideal.

Lemma 1. *$\varrho_A(I)$ is an A-radical ideal.*

Proof. If $c^{2m} + a \in I$, then for any $c' \in C$ we have $(cc')^{2m} + (c')^{2m} a \in I$ or $(cc')^{2m} + a' \in I$, $a' \in A$. Hence $\varrho_A(I)$ is closed under multiplication by elements of C. Less obvious is that $\varrho_A(I)$ is closed under subtraction.

To show this suppose $c_1^{2m}+a_1\in I$, $c_2^{2n}+a_2\in I$, $n\geqq m$. Then

$$\{(c_1-c_2)^2+(c_1+c_2)^2\}^{2n+1}=\{2c_1^2+2c_2^2\}^{2n+1}=c_1^{2m}a_3+c_2^{2n}a_4\,.$$

This relation has the form

$$(c_1-c_2)^{4n+2}+a_5=c_1^{2m}a_3+c_2^{2n}a_4\,,\qquad a_i\in A\,.$$

Hence $(c_1-c_2)^{4n+2}+a_5+a_1a_3+a_2a_4=(c_1^{2m}+a_1)\,a_3+(c_2^{2n}+a_2)\,a_4\in I$. Since this has the form $(c_1-c_2)^{2N}+a\in I$ we conclude that $\varrho_A(I)$ is an ideal. To show that $\varrho_A(I)$ is its own A-radical suppose $c^{2m}+a\in\varrho_A(I)$. Then $(c^{2m}+a)^{2n}+a'\in I$. This has the form

$$c^{4mn}+a''\in I\,,\qquad a''\in A\,,\qquad \text{hence}\qquad c\in\varrho_A(I)\,.$$

3. The Semialgebraic Nullstellensatz

Our semialgebraic nullstellensatz gives the geometric meaning of $\varrho_A(I)$ in $k[x]$ in the case that $A=S[P_1,\ldots,P_m]$.

Theorem 1 (semialgebraic nullstellensatz). *Let $A=S[P_1,\ldots,P_m]$. Then for any ideal I in $k[x]$*

$$\varrho_A(I)=\mathscr{I}\{\mathscr{V}(I)\cap\mathscr{W}(A)\}\,.$$

Our proof combines a standard proof of the Hilbert Nullstellensatz (e.g. Jacobsen [3]) with the most basic arguments of Artin-Schreier theory. We incorporate the main steps of the proof into two separate propositions. The first proposition establishes the theorem in the special case that I is prime and A-radical.

Proposition 1. *Let J be a prime A-radical ideal in $k[x]$ where $A=S[P_1,\ldots,P_m]$. Let g be a polynomial not in J. Then there is a zero of J contained in $\mathscr{W}(A)$ at which g does not vanish.*

Proof. Let $(\bar{\ })$ denote the quotient mapping from $k[x]$ to $k[x]/J=\Gamma$. Let G be the quotient field of Γ. Then G is formally real over k in the sense that if $\Sigma r_ig_i^2=0$, $r_i\in k^+$, $g_i\in G$, then $g_i=0$. Indeed we even have that $\Sigma\alpha_ig_i^2=0$, $\alpha_i\in\bar{A}-\{0\}$, implies $g_i=0$. To show this let $g_i=\gamma_0^{-1}\gamma_i$, $\gamma_i\in\Gamma$, $\gamma_0\neq 0$ and suppose that $\gamma_i=\bar{f}_i,\alpha_i=\bar{a}_i$, f_i, $a_i\in k[x]$. Then $\sum_1^N a_if_i^2\in J$ which implies that $a_i^2f_i^4+a_i'\in J$ where $a_i'\in A$. Since J is A-radical this implies that $a_if_i^2\in J$. But $\bar{a}_i=\alpha_i\neq 0$ implies $a_i\notin J$. Since J is prime, $f_i\in J$. Hence $\gamma_i=\bar{f}_i=0$ and $g_i=0$.

Now suppose that G can be given an ordering extending that of k in which $\bar{P}_1,\ldots,\bar{P}_m$ are all nonnegative. Then by Lang's Theorem (Lang [4]) there is a homomorphism φ extending the imbedding of k

into K to a homomorphism from $k[\bar{x}_1, \ldots, \bar{x}_n, \bar{g}, \bar{P}_1, \ldots, \bar{P}_m]$ into K such that $\varphi(\bar{g}) \neq 0$, and $\varphi(\bar{P}_i) \geqq 0$. Let $\xi = (\bar{X}_1, \ldots, \bar{X}_n) \in K^n$. Then $f \in J$ implies $f(\xi) = \varphi(\bar{f}) = 0$. Moreover $g(\xi) = \varphi(\bar{g}) \neq 0$. Finally $P_i(\xi) = \varphi(\bar{P}_i) \geqq 0$ so that $\xi \in \mathscr{W}(A)$. Thus ξ is the required zero of J.

It remains to show that G has at least one ordering in which the $\bar{P}_i$'s are nonnegative. We know that there are no nontrivial relations of the form

$$\Sigma \alpha_i g_i^2 = 0, \quad \alpha_i \in \bar{A} - \{0\}, \quad g_i \in G.$$

Let G' be a maximal algebraic extension of G with this property. We show that each element of $\bar{A} - \{0\}$ is a square in G'. For if $\alpha \in \bar{A} - \{0\}$ is not a square then in the proper algebraic extension $G'(\sqrt{\alpha})$ we must have some nontrivial relation

$$\Sigma \alpha_i \{g_i + \sqrt{\alpha} h_i\}^2 = 0, \quad \alpha_i \in \bar{A} - \{0\}.$$

Taking traces we find the relation in G'

$$\Sigma \alpha_i g_i^2 + \Sigma \alpha \alpha_i h_i^2 = 0.$$

But this implies $g_i = h_i = 0$ contradicting the nontriviality of the relation in $G'(\sqrt{\alpha})$. Hence each element of $\bar{A}$ is a square in G'. Obviously G' is formally real over k. But any such field has at least one ordering extending the ordering of k. In this ordering the elements of $\bar{A}$ must be nonnegative since they are squares. To complete the proof order G as a subfield of G'.

In the light of the conclusion of this proposition we can describe prime A-radical ideals as the ideals of irreducible real varieties V which have the special property that $V \cap \mathscr{W}(A)$ is Zariski dense in V.

Proposition 2. *$\varrho_A(I)$ is the intersection of all prime A-radical ideals containing I.*

Proof. Suppose J is an A-radical prime ideal containing I and suppose $f \in \varrho_A(I)$. Then $f^{2m} + a \in I \subset J$. Since J is A-radical, $f \in J$. This shows that $\varrho_A(I) \subset \cap J$.

To show the reverse inclusion suppose $f \notin \varrho_A(I)$. Then it suffices to show that there is a prime A-radical ideal not containing f. By hypothesis there is at least one A-radical ideal containing no power of f, namely $\varrho_A(I)$. Let J be an ideal maximal with respect to both of these properties. We complete the proof by showing that J is prime. Suppose $f_1, f_2 \notin J$. Then $\varrho_A\{(J, f_1)\}$ and $\varrho_A\{(J, f_2)\}$ are A-radical ideals strictly containing J. Hence each contains some power of f, that is, $f^{2m_i} + a_i = b_i f + j_i$, $i = 1, 2$, where $a_i \in A$, $b_i \in k[x]$, $j_i \in J$. These equations imply $f^{2(m_1+m_2)} + a = b f_1 f_2 + j$, $a \in A$, $j \in J$. If $f_1 f_2$ belonged to J we could conclude that $f^{2m} + a \in J$, which, since J is A-radical, would imply that $f^{2(m_1+m_2)} \in J$, a contradiction. Thus $f_1, f_2 \notin J$ implies $f_1 f_2 \notin J$, that is, J is prime.

Proof of Theorem 1. It is obvious that $\varrho_A(I) \subset \mathscr{I}\{\mathscr{V}(I) \cap \mathscr{W}(A)\}$. To show the reverse inclusion suppose that f vanishes on $\mathscr{V}(I) \cap \mathscr{W}(A)$. Then if J is any prime A-radical ideal containing I, f vanishes on the subset $\mathscr{V}(J) \cap \mathscr{W}(A)$ which implies, using Proposition 1, that $f \in J$. Thus $f \in \cap J$ which, by Proposition 2, is $\varrho_A(I)$.

If we specialize Theorem 1 to the case in which $A = S$ [that is, $\mathscr{W}(A) = K^n$] we obtain a new and superior version of a real nullstellensatz discovered by Dubois [1].

Theorem 2 (real nullstellensatz),

$$\varrho_S(I) = \mathscr{I}\{\mathscr{V}(I)\} = \{f \mid f^{2m} + \Sigma r_i f_i^2 \in I, r_i \in k^+, f_i \in k[x]\}.$$

It is interesting to elucidate the relationship between this result and Dubois' theorem which asserts that $\mathscr{I}(\mathscr{V}(I))$ is

$$\sqrt[R]{I} = \{f \mid f^m(1 + \Sigma r_i \phi_i^2) \in I, r_i \in k^+, \phi_i \in k(x)\}.$$

The main difference is that the latter involves rational functions. Let $\mathscr{S}$ be the complete semiring of nonnegative polynomial functions. We can suppose without loss of generality that m is even in Dubois' condition. Since any element of $\varrho_S(I)$ satisfies a relation $f^{2m} + \Sigma r_i f_i^2 \in I$ which can be written $f^{2m}(1 + \Sigma r_i [f_i f^{-m}]^2) \in I$, we have $\varrho_S(I) \subset \sqrt[R]{I}$. Likewise, since $f^{2m}(1 + \Sigma r_i \phi_i^2) \in I$ has the form $f^{2m} + \phi \in I$ where $\phi \in \mathscr{S}$, we have $\sqrt[R]{I} \subset \varrho_{\mathscr{S}}(I)$. Thus directly from the definitions $\varrho_S(I) \subset \sqrt[R]{I} \subset \varrho_{\mathscr{S}}(I)$. But since $\mathscr{W}(S) = \mathscr{W}(\mathscr{S}) = K^n$, an immediate consequence of Theorem 1 is $\varrho_S(I) = \varrho_{\mathscr{S}}(I)$.

4. The Positivstellensatz

The semiring $A = S[P_1, \ldots, P_m]$ is in general a proper subset of $\mathscr{A} = \mathscr{A}(\mathscr{W}(P_1, \ldots, P_m))$ and might be described as the largest subsemiring of $\mathscr{A}$ that can be identified with no more than a moment's thought. The following theorem will explain our success in using A without going over, as in Hilbert's 17th problem, to objects defined in terms of rational functions. This theorem asserts that $\mathscr{A}$ is a kind of restricted integral closure of A in $k[x]$.

Theorem 3 (positivstellensatz). *Let* $A = S[P_1, \ldots, P_m]$. *Then*

$$\mathscr{A}\{\mathscr{W}(P_1, \ldots, P_m)\} = \{f \mid f^{2\mu+1} + a_1 f = a_2, a_1, a_2 \in A\}.$$

Proof. Let $\mathscr{A}$ denote $\mathscr{A}\{\mathscr{W}(P_1, \ldots, P_m)\}$, let $\mathscr{A}'$ denote $\{f \mid f^{2\mu+1} + a_1 f = a_2, a_1, a_2 \in A\}$. Clearly $\mathscr{A}' \subset \mathscr{A}$ so we need only show that

$\mathscr{A} \subset \mathscr{A}'$. Suppose $f \in \mathscr{A}$. Then $P_1 \geqq 0, \ldots, P_m \geqq 0$ implies $1 + t^2 f \neq 0$, $t \in K$. Let $S^* = S(k[x, t])$ and let $A^* = S^*[P_1, \ldots, P_m]$. Then by Theorem 1 $\varrho_{A^*}\{(1 + t^2 f)\} = \mathscr{I}\{\mathscr{V}((1 + t^2 f)) \cap \mathscr{W}(P_1, \ldots, P_m)\}$ where, of course, $\mathscr{V}$, $\mathscr{W}$ indicate sets in K^{n+1} and $\mathscr{I}$ and ϱ_{A^*} indicate ideals in $k[x, t]$. But $\mathscr{V}((1 + t^2 f)) \cap \mathscr{W}(P_1, \ldots, P_m) = \emptyset$. Hence $\varrho_{A^*}\{(1 + t^2 f)\} = \mathscr{I}(\emptyset) = k[x, t]$. In particular $1 \in \varrho_{A^*}\{(1 + t^2 f)\}$, that is

$$1 + a^*(x, t) = p(x, t)\{1 + t^2 f(x)\}$$

where $a^* \in A^*$, $p(x, t) \in k[x, t]$. More explicitly this relation can be written

$$1 + \sum_i \sum_j r_{ij} a_{ij}^2(x, t) P_i = p(x, t)\{1 + t^2 f(x)\}, \qquad r_{ij} > 0$$

(here for convenience we suppose that $\{P_i\}$ is a standard set). With the purpose of extracting the even part in t we can write this even more explicitly as

$$1 + \Sigma\Sigma r_{ij}(b_{ij}(x, t^2) + t c_{ij}(x, t^2))^2 P_i = (b(x, t^2) + t c(x, t^2))\{1 + t^2 f\}.$$

Extracting the even part in t and replacing t^2 by t we find

$$1 + a_1^*(x, t) + t a_2^*(x, t) = b(x, t)\{1 + tf\} \quad \text{where} \quad a_1^*, a_2^* \in A^*.$$

Now relacing t by $1/t$ and clearing all denominators with an odd power of t we obtain a relation of the form

$$t^{2\mu+1} + t a_3^*(x, t) + a_4^*(x, t) = d(x, t)\{f + t\}.$$

Letting $t = -f$ we finally obtain

$$f^{2\mu+1} + a_3^*(x, f) f = a_4^*(x, f).$$

Since $a_k^*(x, f) \in A$ we conclude that $f \in \mathscr{A}'$.

In the special case $A = S$ the semiring $\mathscr{A}(\mathscr{W}(S))$ is simply the semiring of all *positive semidefinite* polynomials. Thus we have obtained a characterization of these polynomials more refined then that given by Artin's solution of Hilbert's 17th problem. The latter characterizes nonnegative polynomials as those which have a rational representation $\Sigma r_i \phi_i^2$, $r_i \in k^+$, $\phi_i \in k(x)$. Instead we have the following result.

Theorem 4 (integral characterization of nonnegative polynomials). *A polynomial $f \in k[x]$ is nonnegative as a function from K^n to K if and only if f satisfies an equation*

$$f^{2m+1} + (\Sigma r_i g_i^2) f = \Sigma s_i h_i^2, \qquad r_i, s_i \in k^+, \qquad g_i, h_i \in k[x].$$

We remark that it is of no consequence that the representation involving squares of rational functions follows from this theorem since the same resources of Artin-Schreier theory are used to prove both. However more subtle information about relationships involving rational functions flows from the integrality of Theorem 4 as we will show in Section 5 (see, for example, the Corollary to Theorem 9).

5. Systems of Polynomial Inequalities. Polynomial Programming

"Programming" is a name used to describe the constructive or computational study of systems of inequalities. While our methods and results are very far from being constructive (typically involving, for example, a sum of squares with no estimate on the number of summands) such questions have been instrumental in our thinking. We give some consequences of our theorems which bring some notions of programming securely within the scope of algebraic methods. We also favor the fresh and concrete language of programming.

A vital distinction in programming must be made between *singular* inequalities $f \geqq 0$ which are in fact satisfied only with equality, $f = 0$, and *slack* inequalities which are somewhere satisfied with inequality, $f > 0$. A simple restatement of Theorem 1 with $I = \{0\}$ yields an algebraic description of the singular inequalities which are consequences of a given system.

Theorem 5 (characterization of singular inequalities).

$$\mathscr{I}(\mathscr{W}(P_1, \ldots, P_m)) = \{f \mid f^{2m} \in -S[P_1, \ldots, P_m]\}$$

If the system of inequalities $\{P_i \geqq 0,\ i = 1, \ldots, m\}$ *is standard then* $P_j \geqq 0$ *is singular if and only if for some* $m > 0$

$$P_j^{2m} = -\sum_1^m \sigma_i P_i, \qquad \sigma_i \in S.$$

The first conclusion of the following theorem looks like a result that one could get for continuous or differentiable functions on R^n by reasonably constructive methods using partitions of unity. Moreover these methods are not farfetched here since in many real fields (unlike the complex case) one can construct reasonable rational approximations to partitions of unity. However we have only succeeded in establishing these results using the wildly nonconstructive resources of field theory.

Theorem 6 (synthesis of globally definite functions from locally definite data). *Let* $\{P_i,\ i = 1, \ldots, m\}$ *be a standard set of polynomials. Then at each point of* K^n *at least one* P_i *is negative (nonpositive) if and only if there are nonnegative polynomials* Q_i *not all zero such that* $\Sigma P_i Q_i = -1$ $(\Sigma P_i Q_i = 0)$.

Proof. The hypothesis first implies $\mathscr{W}(P_1, \ldots, P_m) = \emptyset$. Hence $-1 \in \mathscr{A}(\mathscr{W}(P_1, \ldots, P_m))$. Theorem 3 then implies

$$(-1)^{2m+1} + (-1)\, a_1 = a_2, \quad a_i \in S[P_1, \ldots, P_m]$$

or $a_1 + a_2 = -1$. Since $\{P_i\}$ is standard this relation has the form $\Sigma\, \sigma_i P_i = -1$.

The weaker hypothesis only implies $\mathscr{W}\{-1 + t^2 P_i\} = \emptyset$ in K^{n+1}. Hence $\Sigma\, \sigma_i(x,t)(-1 + t^2 P_i) = -1$. Extracting the coefficients of the highest power of t appearing in this relation we obtain the desired conclusion. The sufficiency of the polynomial equalities is obvious.

We now consider relationships involving rational functions. We shall view Theorem 3, our positivstellensatz, as a characterization of all the polynomial inequalities which are consequences of a given set. An immediate consequence of this Theorem is the following variant of a result of A. Robinson [5].

Theorem 7 (rational representation of consequence relations on a real variety). *Let V be a real variety and let $I = \mathscr{I}(V)$. If $P \geqq 0$ on V is a consequence of the standard system $\{P_i \geqq 0$ on V, $i = 1, \ldots, m\}$ then $a^2 P = \Sigma\, s_i P_i \,(\mathrm{mod}\, I)$ where $a \notin I$ and $s_i \in S$.*

Proof. Let $Q_1 \ldots Q_p$ be a basis for I. Then $\{P_i \geqq 0, Q_i \geqq 0, -Q_i \geqq 0\} \Rightarrow P \geqq 0$. Hence $P(P^{2m} + s_1') = s_2'$ where $s_i' \in S[P_1, \ldots, P_m, Q_1, \ldots, Q_p, -Q_1, \ldots, -Q_p]$. This implies $(P^{2m} + s_1)^2 P = s_2 \,(\mathrm{mod}\, I)$ where $s_i \in S \cdot [P_1, \ldots, P_m]$. If $P \in I$ the conclusion is trivial, so assume $P \notin I$. Then also $P^{2m} + s_1 \notin I$. For $I = \varrho_{S[P_1, \ldots, P_m]}(0)$ is an $S[P_1, \ldots, P_m]$-radical ideal for which $P^{2m} + s_1 \in I$ would imply $P \in I$. In this case we have a relation of the required form with $a = P^{2m} + s_1$.

Motzkin [6] has suggested that the representation of consequence inequalities given by this theorem in the case $V = K^n$ can be regarded as the counterpart for inequalities of the Hilbert Nullstellensatz. Certainly this relation is strikingly simple: in each consequence $P \geqq 0$ of $\{P_i \geqq 0\}$, P must have the simple form $\Sigma\, \emptyset_i P_i$ where the $\emptyset_i$'s are non-negative rational functions. Nonetheless a comparison with the Hilbert Theorem is inappropriate because this rational representation is merely necessary and is not sufficient. In fact there is a deplorable tendency for *all* polynomials to be so representable. For example consider the system $\{x_1 \geqq 0, -x_1 \geqq 0\}$. In this case any $f \in k[x]$ can be represented

$$f = \left\{\frac{x_1 + f}{2x_1}\right\}^2 (x_1) + \left\{\frac{x_1 - f}{2x_1}\right\}^2 (-x_1).$$

Of course the trouble here is caused by singular inequalities. The domain $\mathscr{W}(P_1, \ldots, P_m)$ on which we are attempting to study function values sits in a lower dimensional real variety to which many rational functions will not specialize. A natural way to attack these difficulties is to divide out the ideal $\mathscr{I}\{\mathscr{W}(P_1, \ldots, P_m)\} = I$ or equivalently (by Theorem 2, the real nullstellensatz) to cut down polynomial functions to their restrictions to the real variety V of zeros of this ideal. We thus arrive at the necessity of studying systems of inequalities on real algebraic varieties as in Theorem 7. However, even if we reduce to the appropriate variety or even restrict ourselves to the case $V = K^n$, there are further difficulties as the following example shows.

$W = \mathscr{W}\{(1 - x^2 - y^2)([x-2]^2 + y^2)\}$ is the union of the closed unit disc $\{x^2 + y^2 \leqq 1\}$ and the point $(2, 0)$. Even though in this case $V = K^2$, the pathology illustrated above occurs at the isolated point $(2, 0)$. For example $g = (x-2)^2(\frac{3}{2} - x)$ is nonnegative on W, but $\frac{1}{(x-2)^2} g = \frac{3}{2} - x$ is not. It thus seems doubtful whether Theorem 7, even in its full form, can by itself be a significant tool for studying polynomial inequalities. One view of the difficulty is that a natural passage to a collection of geometrically significant quotients seems more complicated for semi-rings than for rings. However in the following definitions we isolate a very special situation in which representations in terms of quotients are both necessary and sufficient. Much more should be done here. For example these definitions should be made on a real algebraic variety. However to do this properly we need resources of real algebraic geometry which seem disproportionate here. We therefore give only the simplest case, obtaining a result (Theorem 8) for which we claim only suggestiveness and illustrative value.

Definition 7. The system $\{P_i \geqq 0, i = 1, \ldots, m\}$ is *slack* if the ideal $\mathscr{I}\{\mathscr{W}(P_1, \ldots, P_m\}$ given by Theorem 5 is $\{0\}$. If the system is not slack then it is *singular*.

Of course the geometric idea is (say if $k = K = R$) that a slack system defines a semialgebraic set with nonempty interior.

Definition 8. The system $\{P_i \geqq 0, i = 1, \ldots, m\}$ is *locally slack* if for each $f \in k[x]$ the $n+1$ dimensional system $\{P_i \geqq 0, i = 1, \ldots, m, t^2 f - 1 \geqq 0\}$ is slack.

The geometric idea here is obscured by a technical device and appears more clearly in the following description in terms of sets in K^n.

Lemma. *$\{P_i \geqq 0, i = 1, \ldots, m\}$ is locally slack if and only if for each f the ideal $\mathscr{I}\{\mathscr{W}(P_1, \ldots, P_m) \cap \{f > 0\}\}$ is improper.*

Proof. Let $W = \mathscr{W}(P_1, \ldots, P_m)$. If $\{P_i \geqq 0, t^2 f - 1 \geqq 0\}$ is not slack then for some $g(x, t) \neq 0$ $W \times K \cap \mathscr{W}(t^2 f - 1) \subset \mathscr{V}(h(x, t))$. If $x \in W \cap \{f > 0\}$, then for all $t > \frac{1}{\sqrt{f(x)}}$, $(x, t) \in W \times K \cap \mathscr{W}(t^2 f - 1)$

and hence $h(x,t)$ vanishes. Let $g(x)$ be the leading coefficient of $h(x,t)$. Then $x \in W \cap \{f>0\}$ implies $g(x)=0$. Hence $\mathscr{I}(W \cap \{f>0\})$ is a proper ideal. Conversely if this ideal is not proper then $x \in W \cap \{f>0\}$ implies $g(x)=0$ for some nontrivial $g \in k[x]$. Then if $(x,t) \in W \times K \cap \mathscr{W}\{t^2 f - 1\}$ we have $x \in W$ and $f>0$, hence $g(x)=0$. This means $W \times K \cap \mathscr{W}\{t^2 f - 1\} \subset \mathscr{V}(g(x))$ so that $P_i \geqq 0, t^2 f - 1 \geqq 0)$ is not slack.

The geometric meaning of local slackness (again suppose $k=K=R$) is that the intersection of W with an open set is either empty or contains an open set. However a direct definition in terms of the sets $\{P_i \geqq 0\} \cap \{f>0\}$ is inappropriate here since we have not given an algebraic description of the ideal of polynomials vanishing on such a set.

For locally slack systems we immediately have the following satisfactory rational representation of consequence inequalities. Here we understand $\phi \geqq 0$, $\phi \in k(x)$ to mean: ϕ is nonnegative on its domain of definition.

Theorem 8 (rational representation of consequence relations). *Let $\{P_i \geqq 0, i=1,\dots,m\}$ be a standard locally slack system. Then the rational inequality $\emptyset \geqq 0$ is a consequence of $\{P_i \geqq 0\}$ if and only if $\phi = \Sigma \phi_i P_i$ where the $\emptyset_i$'s are nonnegative rational functions.*

Proof. Let $\phi = P/Q$. Let $W = \mathscr{W}(P_1,\dots,P_m)$. Then on $W \cap \{Q \neq 0\}$, $PQ = Q^2 \phi$ is nonnegative. Hence $PQ \geqq 0$ on W which implies $PQ = \Sigma\, \psi_i P_i$ or $\phi = \Sigma \frac{\psi_i}{Q^2} P_i$. Conversely suppose $\phi = \Sigma\, \phi_i P_i$. Let $\phi_i = Q_i/D$. Then $PD^2 Q = \Sigma\, Q_i Q^2 P_i$. Since $\Sigma\, Q_i Q^2 P_i$ is nonnegative on W we must have $W \cap \{PQ<0\} \subset \mathscr{V}(D^2)$. By local slackness we conclude that $W \cap \{PQ<0\} = \emptyset$, that is, $PQ \geqq 0$ on W. Thus for $Q \neq 0$ we have $\{P_i \geqq 0\} \Rightarrow \phi = \frac{1}{Q^2} PQ \geqq 0$.

This result invites a geometric interpretation. The set of nonnegative rational functions on a semialgebraic set defined by a locally slack system is a finite dimensional semivector space (or convex polyhedral cone) over the semifield of definite rational functions. This polyhedron seems to be a natural kind of dual body to the semialgebraic set. It is an infinite dimensional object (over k) but with some finite dimensional attributes.

We next obtain finer consequences of Theorem 3 simply by noting that in representations in terms of rational functions we have some information about the denominators. We say that an element of $k(x)$ is *regular on a set X in K^n* if it can be represented in the form P/Q where Q does not vanish on X. If $X=K^n$ we say the element is *regular*.

Theorem 9 (rational representation of positive consequence relations). *If $P>0$ is a consequence of the standard system $\{P_i \geqq 0, i=1,\dots,m\}$*

then $P = \Sigma \phi_i P_i$ *where the* ϕ_i *are elements of* $S(k(x))[P_1, \ldots, P_m]$ *regular on* $\mathscr{W}(P_1, \ldots, P_m)$.

Proof. The denominators in the ϕ_i's can all be taken to be $(P^{2m} + s)^2$, $s \in S[P_1, \ldots, P_m]$, which by hypothesis does not vanish on $\mathscr{W}(P_1, \ldots, P_m)$.

Corollary. *Let* $P(x)$ *be a real polynomial which assumes only positive values. Then* $P = \Sigma \phi_i^2$ *where the* ϕ_i*'s are regular rational functions.*

In conclusion we note a problem suggested by Theorem 4 (which we state for simplicity in the case $k = K = R$). Is some high odd power of every nonnegative real polynomial a sum of squares of polynomials?

References

1. Dubois, D. W.: A nullstellensatz for ordered fields. Ark. Mat. **8**, 111—114 (1969)
2. Stoer, J., Witzgall, C.: Convexity and optimization in finite dimensions. Chap. 1. Berlin-Heidelberg-New York: Springer 1970
3. Jacobsen, N.: Lectures in abstract algebra, III. pp. 251—254, 269—294. Princeton-London-Toronto: Van Nostrand Co. 1964
4. Lang, S.: Algebra, p. 278. Reading: Addison-Wesley, Publ. Co. Inc. 1965
5. Robinson, A.: Introduction to model theory and to the metamathematics of algebra. pp. 214—224. Amsterdam: North Holland Publ. Comp. 1963
6. Motzkin, T. S.: Algebraic inequalities. In "Inequalities", (O. Shisha ed.), Vol. 1, pp. 199—203. New York: Academic Press 1967

Gilbert Stengle
Department of Mathematics
Lehigh University
Bethlehem, Pennsylvania 18015
USA

(Received February 9, 1972)