PACIFIC JOURNAL OF MATHEMATICS
Vol. 136, No. 1, 1989

HOMOGENEOUS STELLENSÄTZE IN SEMIALGEBRAIC GEOMETRY

ZENG GUANGXIN

In this paper, we introduce homogeneous (U, W)-radical ideals of a commutative graded ring A with 1, where both U and W are two multiplicative subsemigroups of homogeneous elements in A such that $U \subseteq W$, and apply these results to prove the homogeneous semialgebraic Stellensätze. Finally, we investigate some quantitative aspects related to these Stellensätze, and Problem 2 posed by G. Stengle is answered affirmatively as a special example.

0. Introduction. In the study of real algebraic geometry, the Nullstellensatz, Positivstellensatz and Nichtnegativstellensatz are important results. These Stellensätze characterize polynomial functions which are zero, positive or nonnegative on certain kinds of semialgebraic sets. Various versions of these Stellensätze can be found in Bochnak, Coste, and Roy [**1**], Colliot-Thelene [**2**], Delzell [**3**], Dubois [**4**], Lam [**5**], and Stengle [**9**, **10**]. In this paper, we give several more general results, i.e., the so-called Homogeneous Stellensätze in semialgebraic geometry, so that all results in the above-mentioned papers will be obtained as direct consequences in some special cases.

First, in §1, we introduce the homogeneous (U, W)-radical of a homogeneous ideal and homogeneous (U, W)-radical ideals in a graded commutative ring A with 1, for two multiplicative subsemigroups U, W of A, which are similar to the usual real radical of an ideal and real radical ideals in a commutative ring. We obtain some basic results.

Next, in §§2, 3 and 4, by the basic results in §1 we prove the homogeneous semialgebraic Nullstellensatz, Positivstellensatz and Nichtnegativstellensatz, respectively. Here, our proofs are different from Stengle's method [**10**] of homogenizing his Positivstellensatz.

Now let R be a real closed field, let K be an ordered subfield (with the inherited ordering), and write $K^+ = \{a \in K | a \geq 0\}$. Let I be an X-homogeneous ideal of $K[X, Y]$, where $X := (X_0, X_1, \dots, X_n)$, $Y := (Y_1, \dots, Y_m)$ are indeterminates, let $f, u_1, \dots, u_s, w_1, \dots, w_t$ be X-homogeneous forms in $K[X, Y]$, let U be the multiplicative subsemigroup of $K[X, Y]$ generated by the u_i, and let W be the multiplicative subsemigroup of $K[X, Y]$ generated by the u_i, and the w_j.

Our Stellensätze here is:

THEOREM 2.3 (*Homogeneous Semialgebraic Nullstellensatz*). *The following are equivalent*:

(1) f *is vanishing in* R *with respect to* $\{U > 0; W \geq 0; I = 0\}$.

(2) *There is an* X*-homogeneous inclusion*

$$uf^{2e} + \sum_v a_v w_v g_v^2 \in I,$$

where $e \in \mathbf{N}$, $a_v \in K^+$, $g_v \in K[X, Y]$, u *is a product of the* u_i, *and the* w_v *are (not necessarily distinct) products of the* u_i *and* w_j.

THEOREM 3.3. (*Homogeneous Semialgebraic Positivstellensatz*). *The following are equivalent*:

(1) f *is positive in* R *with respect to* $\{U > 0; W \geq 0; I = 0\}$.

(2) *There is an* X*-homogeneous inclusion*

$$\left(\sum_v a_v w_v g_v^2\right) f \equiv u + \sum_z a'_z w'_z g'^2_z \qquad (\operatorname{mod} I)$$

where a_v, $a'_z \in K^+$, g_v, $g'_z \in K[X, Y]$, u *is a product of the* u_i, *and the* w_v, w'_z *are (not necessarily distinct) products of the* u_i *and* w_j.

THEOREM 4.3.(*Homogeneous Semialgebraic Nichtnegativstellensatz*). *The following are equivalent*:

(1) f *is nonnegative in* R *with respect to* $\{U > 0; W \geq 0; I = 0\}$.

(2) *There is an* X*-homogeneous inclusion*

$$\left(uf^{2e} + \sum_v a_v w_v g_v^2\right) f \equiv \sum_z a'_z w'_z g'^2_z \qquad (\operatorname{mod} I)$$

where $e \in \mathbf{N}$, a_v, $a'_z \in K^+$, g_v, $g'_z \in K[X, Y]$, u *is a product of the* u_i, *and the* w_v, w'_z *are (not necessarily distinct) products of the* u_i *and* w_j.

In Theorem 2.3, if the number of the indeterminates X is zero, then every element in $K[Y]$ is an X-homogeneous form of X-degree 0. So the inhomogeneous semialgebraic Nullstellensatz (see **[5]** or **[9]**) is a direct consequence of Theorem 2.3. When $U = \{1\}$, as a direct consequence, we may obtain Theorem 4.2 in Delzell **[3]**.

Provided that the number of the indeterminates X is zero in Theorem 3.3, we may establish the inhomogeneous semialgebraic Positivstellensatz, see (1) of Theorem 8.6 in **[5]**, by Theorem 3.3 and the remark in §3.

If we specialize Theorem 4.3 to the case in which $s = t = 1$, $u_1 = w_1 = 1$, and $m = 0$, then we obtain the main result in **[10]**. When the number of the indeterminates X is zero, we may obtain the inhomogeneous semialgebraic Nichtnegativstellensatz, see Theorem 3 in **[9]** or (2) of Theorem 8.6 in **[5]**.

Finally, in §5, we investigate quantitative aspects related to these Stellensätze. Problem 2 in Stengle **[10]** is such a special example. We show the existence of upper bounds related to the Stellensätze, by the following result:

THEOREM 5. *Given n, m, s, t and $d \in \mathbf{N}$ there exist α, $\beta \in \mathbf{N}$ depending only on (n, m, s, t, d) such that, in the X-homogeneous inclusions of Theorem* 2.3(2), *Theorem* 3.3(2) *and Theorem* 4.3(2), *the number of summands and the* (*total*) *degrees of all appearing forms may be taken to be bounded by α and β, respectively, whenever all of the* (*total*) *degrees of the u_i, w_j, f and $I \leq d$.*

Hereinabove, by the degree of an ideal I of $K[X, Y]$ we mean the smallest nonnegative integer d such that I can be written in the form $I = (h_1, \dots, h_r)$, where the degree of $h_k \leq d$, $k = 1, \dots, r$.

Throughout this paper, the following symbols are kept:

$\mathbf{N} := \{0, 1, 2, \dots\}$; $\mathbf{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$;

$\mathbf{Q} :=$ the field of rational numbers; and

$\mathbf{R} :=$ the field of real numbers.

1. Basic results. In this section, for the preliminaries, we give some notions and prove some lemmas.

Let A be a graded ring, i.e., A is a commutative ring with 1 equipped with a direct decomposition of the underlying additive group, $A = \bigoplus_{n=0}^{\infty} A_n$, such that $A_n \cdot A_m \subseteq A_{n+m}$. Thus $a = \sum_{n=0} a_n$ for $a \in A$, where $a_n \in A_n$ is the homogeneous component of degree n of a, and almost all of the components are zero. For $0 \neq a \in A$, we can write $a = a_0 + a_1 + \cdots + a_d$ with $a_d \neq 0$. Then we say that the degree of a is d. It will be convenient also to say that the degree of 0 is the symbol $-\infty$ and to adopt the conventions that $-\infty < n$ for every $n \in \mathbf{N}$. From now on, we use the special symbol $(a)_n$ to denote the homogeneous component of degree n of a, where $n \in \mathbf{N}$. Therefore $a = \sum_{n=0}^{\infty} (a)_n$ for every $a \in A$. For technical reasons, it is convenient to define $(a)_q = 0$ for every $a \in A$ and every negative integer q. An ideal I of A is said to be a homogeneous ideal if $I = \bigoplus_{n=0}^{\infty} (I \cap A_n)$, i.e., all homogeneous components of every element in I are also in I. We shall call a relation of the form $f+g+\cdots \in I$, in which all summands are homogeneous of the same degree, a homogeneous inclusion.

Now let U, W be two multiplicative subsemigroups of homogeneous elements in A such that $U \subseteq W$. Then, for a homogeneous ideal I of A, we define the set

$H_{(U,W)}(I) = \{f \in A | f$ is homogeneous and for some $e \in \mathbf{N}$, $u \in U$, $w_1, \ldots, w_n \in W$, $a_1, \ldots, a_n \in A$, $uf^{2e} + \sum_{i=1}^{n} w_i a_i^2 \in I$ is a homogeneous inclusion$\}$.

By a proof similar to that of Delzell in [3], we can prove that the set $H_{(U,W)}(I)$ has the following properties:

(1) If $f \in H_{(U,W)}(I)$, and $g \in A$ is homogeneous, then $gf \in H_{(U,W)}(I)$.

(2) If $f, g \in H_{(U,W)}(I)$ have the same degree, then $f+g \in H_{(U,W)}(I)$.

(3) If $u_1 g^{2e} + u_2 f + \sum_i w_i a_i^2 \in I$ is a homogeneous inclusion, and if $f \in H_{(U,W)}(I)$, then $g \in H_{(U,W)}(I)$.

In general, $H_{(U,W)}(I)$ is not closed under addition. However, we denote the additive semigroup generated by $H_{(U,W)}(I)$ by $\sqrt[(U,W)]{I}$, and we can obtain the following

LEMMA 1. *With A, I, U and W as above, we have:*

(1) *$\sqrt[(U,W)]{I}$ is a homogeneous ideal of A and $I \subseteq \sqrt[(U,W)]{I}$.*

(2) *If f is homogeneous, then $f \in H_{(U,W)}(I)$ if and only if $f \in \sqrt[(U,W)]{I}$.*

Proof. (1) If $f \in \sqrt[(U,W)]{I}$ and $h \in A$, then, by the definition of $\sqrt[(U,W)]{I}$, $f = \sum_i f_i$, where $f_i \in H_{(U,W)}(I)$. So

$$hf = \left(\sum_{j=0}^{\infty}(h)_j\right)\left(\sum_i f_i\right) = \sum_{j=0}^{\infty}\sum_i (h)_j f_i.$$

By Property (1) of $H_{(U,W)}(I)$, $(h)_j f_i \in H_{(U,W)}(I)$, and $hf \in \sqrt[(U,W)]{I}$. Hence $\sqrt[(U,W)]{I}$ is an ideal of A. Further, extracting the terms f_i of degree d, $(f)_d$ is the sum of all summands f_i of degree d, and $(f)_d \in \sqrt[(U,W)]{I}$. Thus $\sqrt[(U,W)]{I}$ is homogeneous. Moreover, if $g \in I$, then $(g)_i \in I$ for every $i \in \mathbf{N}$, since I is homogeneous. Therefore, for one $u \in U$, $u(g)_i^2 \in I$ is a homogeneous inclusion, and $(g)_i \in H_{(U,W)}(I)$. Therefore $g = \sum_{i=0}^{\infty}(g)_i \in \sqrt[(U,W)]{I}$ by the definition of $\sqrt[(U,W)]{I}$. Thus we complete the proof of (1).

(2) It is obvious that $f \in H_{(U,W)}(I) \Rightarrow f \in \sqrt[(U,W)]{I}$. Conversely, if $f \in \sqrt[(U,W)]{I}$ is homogeneous of degree d, then, by the definition of

${}^{(U,W)}\!\sqrt{I}$, $f \in \sum f_i$, where $f_i \in H_{(U,W)}(I)$. Extracting the terms f_i of degree d, f is the sum of all summands of degree d. By Property (2) of $H_{(U,W)}(I)$, $f \in H_{(U,W)}(I)$. □

The ideal ${}^{(U,W)}\!\sqrt{I}$ will be said to be the (U, W)-radical of I. A homogeneous ideal I of A will be said to be a (homogeneous) (U, W)-radical if $I = {}^{(U,W)}\!\sqrt{I}$.

When $0 \in U$, obviously $1 \in H_{(U,W)}(I)$, and $1 \in {}^{(U,W)}\!\sqrt{I}$. By Lemma 1(1), ${}^{(U,W)}\!\sqrt{I} = A$.

LEMMA 2. *With A, I, U and W as in Lemma 1, we have:*

(1) *${}^{(U,W)}\!\sqrt{I}$ is a homogeneous (U, W)-radical.*

(2) *I is a homogeneous (U, W)-radical if and only if the (possibly inhomogeneous) inclusion $uf^2 + \sum_i w_i a_i^2 \in I$, where $u \in U$, $w_i \in W$, and f, $a_i \in A$, implies that $f \in I$ and $w_i a_i \in I$.*

Proof. (1) If $f \in {}^{(U,W)}\!\sqrt{{}^{(U,W)}\!\sqrt{I}}$, then $f = \sum f_i$ where $f_i \in H_{(U,W)}({}^{(U,W)}\!\sqrt{I})$. Fix i. Then we have homogeneous inclusions $uf_i^{2e} + \sum_k w_k a_k^2 \in {}^{(U,W)}\!\sqrt{I}$, where $u \in U$, $w_k \in W$, $a_k \in A$. By Lemma 1(2), $uf_i^{2e} + \sum_k w_k a_k^2 \in H_{(U,W)}(I)$, and there exist homogeneous inclusions

$$\left(uf_i^{2e} + \sum_k w_k q_k^2\right)^{2s} + \sum_j w'_j a'^2_j \in I,$$

where $w'_j \in W$, $a'_j \in A$. Expanding out the binomial on the left, we have homogeneous inclusions

$$u^{2s} f_i^{4es} + \sum_{m=1}^{2s} \binom{2s}{m} u^{2s-m} f_i^{2e(2s-m)} \left(\sum_k w_k a_k^2\right)^m + \sum_j w'_j a'^2_j \in I.$$

Upon expanding $(\sum_k w_k a_k^2)^m$, we see $f_i \in H_{(U,W)}(I)$, and $f = \sum f_i \in {}^{(U,W)}\!\sqrt{I}$. Therefore ${}^{(U,W)}\!\sqrt{I}$ is a homogeneous (U, W)-radical.

(2) First we prove the "if" part. Let $f \in H_{(U,W)}(I)$. Then we have a homogeneous inclusion $uf^{2e} + \sum_i w_i a_i^2 \in I$. By the hypothesis, $f^e \in I$, and for some $s \in \mathbf{N}$ such that $2^s \geq e$, $uf^{2^s} \in I$. Again using the hypothesis, $f^{2^{s-1}} \in I$. So, reusing the hypothesis $s - 1$ times, we have $f \in I$, and $H_{(U,W)}(I) \subseteq I$. By the definition of ${}^{(U,W)}\!\sqrt{I}$, we have ${}^{(U,W)}\!\sqrt{I} \subseteq I$, and ${}^{(U,W)}\!\sqrt{I} = I$. Therefore I is an (U, W)-radical.

Next we prove the "only if" part. Suppose that I is a homogeneous (U, W)-radical and that despite the inclusion $uf^2 + \sum_i w_i a_i^2 \in I$, where $u \in U$, $w_i \in W$, f, $a_i \in A$, either $f \notin I$ or $w_i a_i \notin I$. By the preceding inclusion, we have

$$\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}u(f)_m(f)_n+\sum_{j=0}^{\infty}\sum_{k=0}^{\infty}\sum_{i}w_i(a_i)_j(a_i)_k\in I.$$

Now we may assert that at least one among the $u(f)_m^2$ and the $w_i(a_i)_j^2$, where $m, j \in \mathbf{N}$, is not in I. Indeed, if $u(f)_m^2 \in I$ for every $m \in \mathbf{N}$, and $w_i(a_i)_j^2 \in I$ for every i and every $j \in \mathbf{N}$, then, since $u(w_i(a_i)_j)^2 \in I$ and I is an (U, W)-radical, we have $(f)_m \in I$, and $w_i(a_i)_j \in I$. Thus $f = \sum_{m=0}^{\infty}(f)_m \in I$, and $w_ia_i = \sum_{j=0}^{\infty} w_i(a_i)_j \in I$ for every i. This contradicts our supposition.

Let d be the smallest integer such that at least one component of degree d is not in I among the $u(f)_m(f)_n$ and $w_i(a_i)_j(a_i)_k$, where m, n, j, $k \in \mathbf{N}$. Then we may assert that every component of degree d, which is not in I, is just of the form $u(f)_m^2$ or $w_i(a_i)_j^2$. Indeed, if a component $u(f)_m(f)_n$ of degree d is not in I, and $m \neq n$, say $m > n$, then $u(f)_n^2 \in I$, for the degree of $u(f)_n^2 < d$. Since I is an (U, W)-radical, $(f)_n \in I$. Thus $u(f)_m(f)_n \in I$, a contradiction. Moreover, if a component $w_i(a_i)_j(a_i)_k$ of degree d is not in I, and $j \neq k$, say $j > k$, then we have $w_i(a_i)_k^2 \in I$, and $u(w_i(a_i)_k)^2 \in I$. Thus $w_i(a_i)_k \in I$, and $w_i(a_i)_j(a_i)_k \in I$, a contradiction.

Assume that some component of degree d, which is not in I, is of the form $u(f)_{n_0}^2$. By the homogeneity of I, extracting all the components outside I of degree d from the left of the preceding inclusion, we have the homogeneous inclusion $u(f)_{n_0}^2 + \sum_v w_v(a_v)_{k_v}^2 \in I$, where v ranges over some subset of the set of index i. Since I is an (U, W)-radical, we have $(f)_{n_0} \in I$. Thus $u(f)_{n_0}^2 \in I$, a contradiction. Now assume that every component outside I of degree d is not of the form $u(f)_n^2$. Then, by extraction, we have $\sum_v w_v(a_v)_{k_v}^2 \in I$, where v ranges over some subset of the set of index i. Hence we have $u(w_v(a_v)_{k_v})^2 + \sum_{z\neq v}(uw_vw_z)(a_z)_{k_z}^2 \in I$. Therefore $w_v(a_v)_{k_v} \in I$ for every v. This is a contradiction. □

By the lemma above, it is easy to see that a (homogeneous) (U, W)-radical is also a radical in the usual sense. In fact, if $f^e \in I$ $(a(U, W)$-radical), then, for an arbitrary $u \in U$ and some $s \in \mathbf{N}$ such that $2^s \geq e$, $uf^{2^s} \in I$, By Lemma 2(2), $f^{2^{s-1}} \in I$. Repeating the procedure, we have $f \in I$.

LEMMA 3. *Let A, U, W and I be as above, and let M be another multiplicative subsemigroup of homogeneous elements in A. Let Ω be* *the set of all homogeneous (U, W)-radical J of A such that $I \subseteq J$, and $J \cap M = \varnothing$. If we suppose further that I is a proper (U, W)-radical ideal of A such that $I \cap M = \varnothing$, then Ω is inductive under set inclusion, and every maximal member in Ω is a prime ideal of A. In particular, Ω contains at least one prime ideal.*

Proof. Let $\{J_\lambda\}_{\lambda \in \Lambda}$ be a chain in Ω. Putting $J = \bigcup_{\lambda \in \Lambda} J_\lambda$, it is easy to prove that J is a homogeneous ideal of A such that $J \cap M = \varnothing$ and $I \subseteq J$. Moreover, if $uf^{2e} + \sum_i w_i a_i^2 \in J$, then for some $\lambda_0 \in \Lambda$, $uf^{2e} + \sum w_i a_i^2 \in J_{\lambda_0}$. Since J_{λ_0} is an (U, W)-radical, $f \in J_{\lambda_0} \subseteq J$, that is, J is also an (U, W)-radical. Thus $J \in \Omega$, and Ω is inductive.

Let Q be a maximal member in Ω. If Q is not prime, then there exist $a, b \in A$ such that $ab \in Q$, $a \notin Q$ and $b \notin Q$. Since $a \notin Q$, not all of the homogeneous components of a are in Q. Let i_0 be the smallest integer such that $(a)_{i_0} \notin Q$. Likewise, j_0 is the smallest integer such that $(b)_{j_0} \notin Q$. Since $ab \in Q$ and Q is homogeneous, $(ab)_{i_0+j_0} \in Q$, i.e.,

$$(a)_{i_0}(b)_{j_0} + \sum_{i<i_0}(a)_i(b)_{i_0+j_0-i} + \sum_{j<j_0}(a)_{i_0+j_0-j}(b)_j \in Q.$$

By the choice of the i_0 and j_0,

$$\sum_{i<i_0}(a)_i(b)_{i_0+j_0-i} + \sum_{j<j_0}(a)_{i_0+j_0-j}(b)_j \in Q;$$

thus $(a)_{i_0}(b)_{j_0} \in Q$.

It is easy to prove that $Q + A(a)_{i_0}$ is a homogeneous ideal. Indeed, if $f \in Q + A(a)_{i_0}$, i.e., $f = q + c(a)_{i_0}$, where $q \in Q$, and $c \in A$, then $(f)_n = (q)_n + (c(a)_{i_0})_n = (q)_n + (c)_{n-i_0}(a)_{i_0}$. By the homogeneity of Q, $(q)_n \in Q$, and $(f)_n \in Q + A(a)_{i_0}$. Similarly, $Q + A(b)_{j_0}$ is homogeneous. So both $\sqrt[(U,W)]{Q + A(a)_{i_0}}$ and $\sqrt[(U,W)]{Q + A(b)_{j_0}}$ are homogeneous (U, W)-radicals properly containing Q. By the maximality of Q in Ω, we have $M \cap \sqrt[(U,W)]{Q + A(a)_{i_0}} \neq \varnothing$ and $M \cap \sqrt[(U,W)]{Q + A(b)_{j_0}} \neq \varnothing$. By Lemma 1(2),

$$M \cap H_{(U,W)}(Q + A(a)_{i_0}) \neq \varnothing \quad \text{and} \quad M \cap H_{(U,W)}(Q + A(b)_{j_0}) \neq \varnothing.$$

So we have two homogeneous inclusions,

$$um^{2e} + \sum_i w_i a_i^2 \in Q + A(a)_{i_0}$$

and

$$u'm'^{2s} + \sum_j w'_j a'^2_j \in Q + A(b)_{j_0},$$

where $u, u' \in U$, $w_i, w'_j \in W$, $m, m' \in M$, and $a_i, a'_j \in A$.

Furthermore, we may assume $e = s$. Indeed, if $e \neq s$, say $e > s$, then we may multiply the left of the latter inclusions by $m'^{2(e-s)}$.

Since $(a)_{i_0}(b)_{j_0} \in Q$, the product of the preceding expressions gives:

$$(uu')(mm')^{2e} + \sum_i (u'w_i)(m'^e a_i)^2 + \sum_j (uw'_j)(m^e a'_j)^2 + \sum_i \sum_j (w_i w'_j)(a_i a'_j)^2 \in Q,$$

where $uu' \in U$, and $u'w_i$, uw'_j and $w_i w'_j \in W$. Since Q is an (U, W)-radical, $mm' \in Q$. Hence $Q \cap M \neq \emptyset$, a contradiction. Therefore Q is prime.

The last conclusion follows from Zorn's lemma. □

2. The homogeneous semialgebraic Nullstellensatz. Let F be a formally real field, and let $X := (X_0, X_1, \dots, X_n)$ and $Y := (Y_1, \dots, Y_m)$ be indeterminates. Then $F[X, Y] = \bigoplus_{k=0}^{\infty} A_k$, where A_k is the additive group of all X-homogeneous forms of X-degree k. Under this convention, $F[X, Y]$ can be regarded as a graded ring, in which the so-called homogeneity is only related to the indeterminates X. Therefore, we prefer to use the precise word "X-homogeneity" instead of the word "homogeneity".

Now, let I be an X-homogeneous ideal of $F[X, Y]$, $U \subseteq W$ be two multiplicative subsemigroups of $F[X, Y]$, which consist of X-homogeneous forms, and $f \in F[X, Y]$ be an X-homogeneous form. Let (F^*, P^*) be an ordered extension of F, that is, F^* is an extension of F with an ordering P^*. Then, we shall say f is vanishing in (F^*, P^*) with respect to $\{U > 0; W \geq 0; I = 0\}$, if $f(x, y) = 0$ for every $(x, y) \in F^{*n+1} \times F^{*m}$ such that $u(x, y) >_{P^*} 0$, $\forall u \in U$; $w(x, y) \geq_{P^*} 0$, $\forall w \in W$; and $h(x, y) = 0$, $\forall h \in I$.

THEOREM 2.1. *With $F[X, Y]$, I, U, W and f as above, the following are equivalent:*

(1) *f is vanishing in every ordered extension of F with respect to $\{U > 0; W \geq 0; I = 0\}$.*

(2) $f \in H_{(U,W)}(I)$.

Proof. (2) $\Rightarrow$ (1): Obvious.

(1) $\Rightarrow$ (2): Suppose that $f \notin H_{(U,W)}(I)$. Then, by Lemma 1(2), $f \notin \sqrt[(U,W)]{I}$. Putting $M = \{f^s | s \in N\}$, then $M \cap \sqrt[(U,W)]{I} = \emptyset$, for $\sqrt[(U,W)]{I}$ is a radical in the usual sense. By Lemma 3, the set $\Omega := \{J | J \supseteq \sqrt[(U,W)]{I}$ is an X-homogeneous (U, W)-radical ideal of $F[X, Y]$ and $M \cap J = \emptyset\}$ contains a prime ideal Q of $F[X, Y]$.

In the integral domain $A^* := F[X, Y]/Q$, each element is of the form $\overline{a} = a + Q$, where $a \in F[X, Y]$. Since $F \cap Q = \{0\}$, we can consider, by abuse of notation, that $F \subseteq A^*$. Let F^* be the field of fractions of A^*. Then F^* is an extension of F. We denote the set $\{\sum_i \overline{w}_i \overline{a}_i^2 | w_i \in W \cup \{1\}, \overline{a}_i \in F^*\}$ by T. Then, obviously, $T + T \subseteq T$, $T \cdot T \subseteq T$, and $F^{*2} \subseteq T$. Furthermore, if $-1 \in T$, then $-1 = \sum_i \overline{w}_i (\overline{b}_i \overline{c}_i^{-1})^2$, where $w_i \in W \cup \{1\}$, $\overline{b}_i$, $0 \neq \overline{c}_i \in A^*$. Thus, $d^2 + \sum_i w_i (b_i d_i)^2 \in Q$, where $d = \prod_k c_k$, and $d_i = \prod_{k \neq i} c_k$. Upon multiplying this inclusion by any element $u \in U$ at all, we see, by Lemma 2(2), that $d \in Q$, i.e., $\prod_k \overline{c}_k = 0$, a contradiction. Therefore T is a preordering of F^*. By Corollary 3.7 in [5], T is contained in an ordering P^* of F^*. So, for every $w \in W$, $\overline{w} \geq_{P^*} 0$.

Notice that $U \cap Q = \emptyset$; otherwise $u \in U \cap Q \Rightarrow u1^2 \in Q \Rightarrow$ (since Q is an X-homogeneous (U, W)-radical) $1 \in Q$. Hence $\overline{u} >_{P^*} 0$, $\forall u \in U$. Therefore, for $(\overline{X}, \overline{Y}) \in F^{*n+1} \times F^{*m}$, where $\overline{X} = (\overline{X}_0, \overline{X}_1, \dots, \overline{X}_n)$ and $\overline{Y} = (\overline{Y}_1, \dots, \overline{Y}_m)$, we have the following relations $(*)$:

$$
\begin{aligned}
u(\overline{X}, \overline{Y}) &= \overline{u(X, Y)} >_{P^*} 0, \quad \forall u(X, Y) \in U;\\
w(\overline{X}, \overline{Y}) &= \overline{w(X, Y)} \geq_{P^*} 0, \quad \forall w(X, Y) \in W;\\
h(\overline{X}, \overline{Y}) &= \overline{h(X, Y)} = 0, \quad \forall h(X, Y) \in I, \quad \text{and}\\
f(\overline{X}, \overline{Y}) &= \overline{f(X, Y)} \neq 0.
\end{aligned}
$$

This contradicts (1). □

In order to establish the homogeneous Nullstellensatz on a semialgebraic set, we must give the following further notion.

Let V be a multiplicative subsemigroup of X-homogeneous forms in $F[X, Y]$. We shall say that V is finitely expressed, if there exist finitely many X-homogeneous forms $g_1(X, Y), \dots, g_s(X, Y)$ such that every $v(X, Y) \in V$ can be expressed in the form $v(X, Y) = a g_1^{k_1} \cdots g_s^{k_s}$, where $a \in F$, and $k_i \in \mathbf{N}$ for $i = 1, \dots, s$. In this case, we say also that V is expressed by $g_1, \dots, g_s$ for the sake of precision. Notice that we do not say that a and the g_i, $i = 1, \dots, s$, must belong to V.

Let $U \subseteq W$ be two multiplicative subsemigroups of $F[X,Y]$, and let W be finitely expressed. It is easy to see that U is also finitely expressed.

By the above notion, we can obtain the following

THEOREM 2.2. *Let $F[X,Y]$, I, U, W and f be as above, and let W be finitely expressed. Then the following are equivalent*:

(1) *f is vanishing in every real closure of F with respect to* $\{U > 0; W \geq 0; I = 0\}$.

(2) $f \in H_{(U,W)}(I)$.

Proof. (2) $\Rightarrow$ (1): Obvious.

(1) $\Rightarrow$ (2): If (2) is false, then, by the proof of Theorem 2.1, for some ordered extension $(F(\overline{X},\overline{Y}), P^*)$ of F we have the relations $(*)$ in the proof of Theorem 2.1.

Let R be the real closure of F with respect to its ordering $P^* \cap F$, and let W be expressed by $g_1, \dots, g_s$. Then, by Lang's Homomorphism Theorem (see **[6]** or [7]), there is an F-algebra homomorphism τ from $F[\overline{X},\overline{Y}]$ to R satisfying the following conditions:

(i) $g_i(a^*, b^*)$ and $g_i(\overline{X},\overline{Y})$ have the same sign, $i = 1, \dots, s$; that is, $g_i(a^*, b^*) = 0$ if $g_i(\overline{X},\overline{Y}) = 0$, or $g_i(a^*, b^*) >_{R^+} 0$ if $g_i(\overline{X},\overline{Y}) >_{P^*} 0$, or $g_i(a^*, b^*) <_{R^+} 0$ if $g_i(\overline{X},\overline{Y}) <_{P^*} 0$; and

(ii) $f(a^*, b^*) \neq 0$, where

$$a^* = (\tau(\overline{X}_0), \tau(\overline{X}_1), \dots, \tau(\overline{X}_n)), \quad b^* = (\tau(\overline{Y}_1), \dots, \tau(\overline{Y}_m)).$$

Observe that for every $w \in W$ the sign of $w(a^*, b^*)$ (resp. $w(\overline{X},\overline{Y})$) depends only on the signs of the $g_i(a^*, b^*)$ (resp. the $g_i(\overline{X},\overline{Y})$). So, for every $u \in U$ ($\subseteq W$) and every $w \in W$, $u(a^*, b^*)$ and $u(\overline{X},\overline{Y})$ have the same sign, and $w(a^*, b^*)$ and $w(\overline{X},\overline{Y})$ have the same sign. Therefore we have:

$$u(a^*, b^*) >_{R^+} 0, \quad \forall u \in U;$$
$$w(a^*, b^*) \geq_{R^+} 0, \quad \forall w \in W.$$

Moreover, it is evident that $h(a^*, b^*) = 0$, $\forall h \in I$. Thus f is not vanishing in the real closure R of F with respect to $\{U > 0; W \geq 0; I = 0\}$, refuting (1). $\square$

By the theorem above, we can prove Theorem 2.3 in the introduction without difficulty as follows.

Proof of Theorem 2.3. (2) $\Rightarrow$ (1) is clear. It only remains to prove (1) $\Rightarrow$ (2). Now let $W^* = \{aw | a \in K^+, \text{ and } w \in W\}$. Then $W \subseteq W^*$, and W^* is obviously a multiplicative semigroup expressed by $u_1, \ldots, u_s, w_1, \ldots, w_t$.

Suppose that (2) is false. Then $f \notin H_{(U,W^*)}(I)$. By Theorem 2.2, f is not vanishing in some real closure $\overline{K}$ of K with respect to $\{U > 0; W^* \geq 0; I = 0\}$. Thus, for some $(a^*, b^*) \in \overline{K}^{n+1} \times \overline{K}^m$, we have:

$$u(a^*, b^*) >_{\overline{K}^+} 0, \quad \forall u \in U;$$
$$aw(a^*, b^*) \geq_{\overline{K}^+} 0, \quad \forall a \in K^+, \quad \forall w \in W;$$
$$h(a^*, b^*) = 0, \quad \forall h \in I, \quad \text{but} \quad f(a^*, b^*) \neq 0.$$

Pick one $u \in U$. Then, for every $a \in K^+$, $au \in W^*$, and $au(a^*, b^*) \geq_{\overline{K}^+} 0$. Since $u(a^*, b^*) >_{\overline{K}^+} 0$, $a \geq_{\overline{K}^+} 0$. Thus $K^+ \subseteq \overline{K}^+$. Therefore $\overline{K}$ is a real closure of the ordered field (K, K^+).

Let $\tilde{K}$ be the algebraic closure of K in R. Then, by Lemma 3.13 in **[8]**, $\tilde{K}$ is real closed, and is a real closure of K. By the uniqueness of real closures of an ordered field (see Theorem 3.10 in **[8]**), we may agree that $\overline{K} = \tilde{K} \subseteq R$. Therefore, f is not vanishing in R with respect to $\{U > 0; W^* \geq 0; I = 0\}$, of course, with respect to $\{U > 0; W \geq 0; I = 0\}$. This refutes (1). $\square$

3. The homogeneous semialgebraic Positivstellensatz. In this section, the notation F, $F[X, Y]$, I, U, W and f is the same as in §2. Let (F^*, P^*) be an ordered extension of F. Then we shall say that f is positive (nonnegative) in (F^*, P^*) with respect to $\{U > 0; W \geq 0; I = 0\}$, if $f(x, y) >_{P^*} 0$ ($f(x, y) \geq_{P^*} 0$) for every $(x, y) \in F^{*n+1} \times F^{*m}$ such that $u(x, y) >_{P^*} 0$, $\forall u \in U$; $w(x, y) \geq_{P^*} 0$, $\forall w \in W$; and $h(x, y) = 0$, $\forall h \in I$.

THEOREM 3.1. *With $F[X, Y]$, I, U, W and f as above, the following are equivalent*:

(1) *f is positive in every ordered extension of F with respect to* $\{U > 0; W \geq 0; I = 0\}$.

(2) *There is an X-homogeneous inclusion*

$$\left(\sum_i w_i g_i^2\right) f \equiv u + \sum_j w'_j g'^2_j \qquad (\operatorname{mod} I)$$

where $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X, Y]$.

Proof. (2) $\Rightarrow$ (1): Obvious.

(1) $\Rightarrow$ (2): Let W^* be the multiplicative semigroup generated by W and $-f$. Then we can assert that $1 \in {}^{(U,W^*)}\sqrt{I}$. Indeed, if $1 \notin {}^{(U,W^*)}\sqrt{I}$, then, by Lemma 3, the set $\Omega := \{J | J \supseteq {}^{(U,W^*)}\sqrt{I}$ is an X-homogeneous (U, W^*)-radical in $F[X, Y]$, and $J \cap \{1\} = \varnothing\}$ contains a prime ideal Q.

As in the proof of Theorem 2.1, the field F^* of fractions of the integral domain $A^* = F[X, Y]/Q$ possesses an ordering P^* such that $u(\overline{X}, \overline{Y}) >_{P^*} 0, \forall u \in U$; $w^*(\overline{X}, \overline{Y}) \geq_{P^*} 0, \forall w^* \in W^*$; and $h(\overline{X}, \overline{Y}) = 0$, $\forall h \in I$. Since $W \subseteq W^*$ and $-f \in W^*$, $w(\overline{X}, \overline{Y}) \geq_{P^*} 0$, $\forall w \in W$; and $-f(\overline{X}, \overline{Y}) \geq_{P^*} 0$, i.e., $f(\overline{X}, \overline{Y}) \leq_{P^*} 0$. This contradicts (1).

Thus $1 \in {}^{(U,W^*)}\sqrt{I}$, hence $1 \in H_{(U,W^*)}(I)$ by Lemma 1(2). So we have an X-homogeneous inclusion $u + \sum_k w_k^* h_k^2 \equiv 0 \pmod{I}$, where $u \in U$, $w_k^* \in W^*$, $h_k \in F[X, Y]$. Now the w_k^* can be written in the form $w_k(-f)^{s_k}$, where $w_k \in W$, and $s_k \in \mathbf{N}$; the even powers of $-f$ may be included in h_k^2. Thus, we obtain the following X-homogeneous inclusion:

$$u + \sum_i w_i(-f)g_i^2 + \sum_j w'_j g_j'^2 \equiv 0 \pmod{I}$$

where $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X, Y]$. Therefore we have

$$\left(\sum_i w_i g_i^2\right) f \equiv u + \sum_j w'_j g_j'^2 \pmod{I}. \qquad \square$$

When W is finitely expressed, we have

THEOREM 3.2. *Let $F[X, Y]$, I, U, W and f be as above, and let W be finitely expressed. Then the following are equivalent:*

(1) *f is positive in every real closure of F with respect to $\{U > 0; W \geq 0; I = 0\}$.*

(2) *There is an X-homogeneous inclusion*

$$\left(\sum_i w_i g_i^2\right) f \equiv u + \sum_j w'_j g_j'^2 \pmod{I}$$

where $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X, Y]$.

Proof. (2) $\Rightarrow$ (1): Obvious.

(1) $\Rightarrow$ (2): If (2) is false, then, by the proof of Theorem 3.1, f is not positive in some ordered extension $(F(\overline{X}, \overline{Y}), P^*)$ of F with

respect to $\{U > 0; W \geq 0; I = 0\}$, that is, $u(\overline{X}, \overline{Y}) >_{P^*} 0$, $\forall u \in U$; $w(\overline{X}, \overline{Y}) \geq_{P^*} 0$, $\forall w \in W$; $h(\overline{X}, \overline{Y}) = 0$, $\forall h \in I$; but $f(\overline{X}, \overline{Y}) \leq_{P^*} 0$.

Let R be the real closure of F with respect to its ordering $P^* \cap F$, and let W be expressed by $g_1, \ldots, g_s$. By Lang's Homomorphism Theorem, there is an F-algebra homomorphism τ from $F[\overline{X}, \overline{Y}]$ to R satisfying

(i) $g_i(a^*, b^*)$ and $g_i(\overline{X}, \overline{Y})$ have the same sign, $i = 1, \ldots, s$ and

(ii) $f(a^*, b^*) \leq_{R^+} 0$, where $a^* = (\tau(X_0), \tau(X_1), \ldots, \tau(X_n))$, $b^* = (\tau(Y_1), \ldots, \tau(Y_m))$. From this, we have: $u(a^*, b^*) >_{R^+} 0$, $\forall u \in U$; $w(a^*, b^*) \geq_{R^+} 0$, $\forall w \in W$; and it is evident that $h(a^*, b^*) = 0$, $\forall h \in I$. Thus f is not positive in the real closure R of F with respect to $\{U > 0; W \geq 0; I = 0\}$. This refutes (1). □

By Theorem 3.2, Theorem 3.3 in the introduction can be easily established. The proof of Theorem 3.3 is similar to that of Theorem 2.3, and we leave it to the reader as an exercise.

REMARK. In the inhomogeneous semialgebraic Poisitivstellensatz, the required congruence is written in the form

$$\left(u + \sum_i w_i g_i^2\right) f \equiv u + \sum_j w'_j g_j'^2 \qquad (\operatorname{mod} I)$$

where u, w_i and w'_j have the character similar to that in Theorem 3.1(2) (cf. Theorem 8.6(1) in [5]).

Here, we point out that for homogeneous forms such a homogeneous inclusion cannot in general be obtained. For example, in the polynomial ring $F[X_0]$, let U be the multiplicative semigroup generated by X_0^2, and W the one generated by X_0, and let $I = 0$. Then, evidently, the homogeneous form X_0 is positive in every ordered extension of F with respect to $\{U > 0; W \geq 0; I = 0\}$. But the following homogeneous inclusion is impossible:

$$\left(u + \sum_i w_i g_i^2\right) X_0 = u + \sum_j w'_j g_j'^2$$

where $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X_0]$. Indeed, the homogeneous forms on the left hand side must be of odd degree, and the one on the right hand side must be of even degree.

However, provided that there exist some u_1, $u_2 \in U$ such that $u_1 f$ and u_2 have the same X-degree, then the expression in Theorem 3.1(2) may be improved as follows:

$$\left(uu_1 + \sum_i w_i g_i^2\right) f \equiv uu_2 + \sum_j w'_j g'^2_j \qquad (\operatorname{mod} I)$$

where $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X, Y]$. Indeed, by the expression

$$\left(\sum_i w_i g_i^2\right) f \equiv u + \sum_j w'_j g'^2_j \qquad (\operatorname{mod} I),$$

we have

$$\left(\sum_i (u_2 w_i) g_i^2\right) f \equiv uu_2 + \sum (u_2 w'_j) g'^2_j \qquad (\operatorname{mod} I) \quad \text{and}$$

$$\left(uu_1 + \sum_j (u_1 w'_j) g'^2_j\right) f \equiv \sum_i (u_1 w_i)(g_i f)^2 \qquad (\operatorname{mod} I).$$

Notice that all the summands in the expressions above have the same X-degree. Then the sum of the two expressions is required.

4. The homogeneous semialgebraic Nichtnegativstellensatz. In this section, we shall adopt the same notations as in §3 to investigate the representation of nonnegative forms.

First, we have

THEOREM 4.1. *With $F[X, Y]$, I, U, W and f as in Theorem 3.1, the following are equivalent:*

(1) *f is nonnegative in every ordered extension of F with respect to $\{U > 0; W \geq 0; I = 0\}$.*

(2) *There is an X-homogeneous inclusion*

$$\left(uf^{2e} + \sum_i w_i g_i^2\right) f \equiv \sum_j w'_j g'^2_j \qquad (\operatorname{mod} I)$$

where $e \in \mathbf{N}$, $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X, Y]$.

Proof. (2) $\Rightarrow$ (1): Obvious.

(1) $\Rightarrow$ (2): Let U^* be the multiplicative semigroup generated by U and $-f$, and W^* the one generated by W and $-f$. Then both U^* and W^* are multiplicative semigroups of X-homogeneous forms

in $F[X, Y]$. Here, we can assert that $1 \in {}^{(U^*, W^*)}\sqrt{I}$. Indeed, if $1 \notin {}^{(U^*, W^*)}\sqrt{I}$, then the set $\Omega := \{J | J \supseteq {}^{(U^*, W^*)}\sqrt{I}$ is an X-homogeneous (U^*, W^*)-radical ideal of $F[X, Y]$, and $J \cap \{1\} = \varnothing\}$ contains a prime ideal Q.

As the proof of Theorem 3.1, the field F^* of fractions of $F[X, Y]/Q$ possesses an ordering P^* such that $u^*(\overline{X}, \overline{Y}) >_{P^*} 0, \forall u^* \in U^*$; $w^*(\overline{X}, \overline{Y}) \geq_{P^*} 0, \forall w^* \in W^*$; and $h(\overline{X}, \overline{Y}) = 0, \forall h \in I$. From this, we have $u(\overline{X}, \overline{Y}) >_{P^*} 0, \forall u \in U$; $w(\overline{X}, \overline{Y}) \geq_{P^*} 0, \forall w \in W$; and $-f(\overline{X}, \overline{Y}) >_{P^*} 0$. Thus f is not nonnegative in (F^*, P^*) with respect to $\{U > 0; W \geq 0; I = 0\}$. This contradicts (1).

By $1 \in (U^*, W^*)/\sqrt{I}$, $1 \in H_{(U^*, W^*)}(I)$, and we have an X-homogeneous inclusion $u^* + \sum_k w_k^* h_k^2 \in I$, where $u^* \in U^*$, $w_k^* \in W^*$, and $h_k \in F[X, Y]$. Now, u^* can be written in the form $u(-f)^s$, where $u \in U$, and $s \in \mathbf{N}$. Then, by the preceding inclusion, for every—in particular, the least—$e \in \mathbf{N}$ such that $2e + 1 \geq s$, we have

$$u(-f)^{2e+1} + \sum_k w_k^*(-f)^{2e-s+1} h_k^2 = (-f)^{2e-s+1} \left(u^* + \sum_k w_k^* h_k^2 \right) \in I.$$

Since the $w_k^*(-f)^{2e-s+1}$ can be written in the form $w_k(-f)^{l_k}$, where $l_k \in \mathbf{N}$, and $w_k \in W$, and the even powers of $-f$ can be included in h_k^2, we have the X-homogeneous inclusion

$$u(-f)^{2e+1} + \sum_i w_i(-f) g_i^2 + \sum_j w'_j g_j'^2 \in I,$$

where $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X, Y]$. Therefore

$$\left(u f^{2e} + \sum_i w_i g_i^2 \right) f \equiv \sum_j w'_j g_j'^2 \pmod{I}. \qquad \square$$

Likewise, we have

THEOREM 4.2. *Let the notations be as in Theorem 4.1, and let W be finitely expressed. Then the following are equivalent:*

(1) *f is nonnegative in every real closure of F with respect to $\{U > 0; W \geq 0; I = 0\}$.*

(3) *There is an X-homogeneous inclusion*

$$\left(u f^{2e} + \sum_i w_i g_i^2 \right) f \equiv \sum_j w'_j g_j'^2 \pmod{I},$$

where $u \in U$, $w_i, w'_j \in W$, and $g_i, g'_j \in F[X, Y]$.

The proof is similar to that of Theorem 3.2, and the reader can give its procedure.

By Theorem 4.2, it is easy to prove Theorem 4.3 in the introduction. The proof of Theorem 4.3 is similar to that of Theorem 3.3, and we leave it to the reader as an exercise.

REMARK. In the inhomogeneous semialgebraic Nichtnegativstellensatz (cf. Theorem 8.6(2) in [5]), the required congruence is written in the form

$$\left(uf^{2e}+\sum_i w_i g_i^2\right)f \equiv uf^{2e}+\sum_j w'_j g_j'^2 \qquad (\operatorname{mod} I)$$

where the appearing symbols are as in Theorem 4.1.

Evidently, it is impossible that such a congruence is X-homogeneous, if the X-degree of f is positive. However, provided that there exist some $u_1, u_2 \in U$ such that $u_1 f$ and u_2 have the same X-degree, then the expression in Theorem 4.1 may be improved as follows:

$$\left(uu_1f^{2e}+\sum_i w_i g_i^2\right)f \equiv uu_2f^{2e}+\sum_j w'_j g_j'^2 \qquad (\operatorname{mod} I).$$

Here, the argument is similar to the remark in §3.

5. Related quantitative aspects. The purpose of this section will be to prove Theorem 5 in the introduction. In this section, we shall adopt the same notations as in Theorems 2.3, 3.3 and 4.3. For convenience, we give a name "general X-homogeneous form". For d_1, $d \in \mathbf{N}$ with $d_1 \le d$, the general X-homogeneous form g of type (d_1, d) is an X-homogeneous form in $Z[X, Y, T]$, which has X-degree d_1 and (total) degree d, with parameter coefficients $T = (T_k)$, $1 \le k \le \binom{n+d_1}{n}\binom{m+d-d_1}{m}$; explicitly $g = \sum_{|\lambda|=d_1, |\sigma|\le d-d_1} T_{(\lambda,\sigma)} Y^\sigma X^\lambda$, where $(\lambda, \sigma) = (\lambda_0, \dots, \lambda_n, \sigma_1, \dots, \sigma_m) \in \mathbf{N}^{n+1} \times \mathbf{N}^m$ is a multi-index, $|\lambda| = \sum \lambda_i$, $|\sigma| = \sum \sigma_j$, $X^\lambda = X_0^{\lambda_0} \cdots X_n^{\lambda_n}$, $Y^\sigma = Y_1^{\sigma_1} \cdots Y_m^{\sigma_m}$, and $T_{(\lambda,\sigma)}$ is a reindexing of T_k. Evidently, every X-homogeneous form in $K[X, Y]$ of (total) degree $\le d$ can be obtained by substituting its coefficients for parameters T in a general X-homogeneous form of type (d_1, d) for some $d_1 \in \mathbf{N}$.

Before proving Theorem 5, we give the following

LEMMA. *Given n, m and $d \in \mathbf{N}$, there exists $r \in \mathbf{N}$ depending only on (n, m, d) such that every X-homogeneous ideal of degree $\le d$ may be generated by r X-homogeneous forms of degree $\le d$.*

Proof. Let I be an X-homogeneous ideal of degree $\leq d$. Then $I = (h_1, \ldots, h_s)$, where every h_k is of degree $\leq d$. By the X-homogeneity of I, we may assume all the h_k are X-homogeneous. Furthermore, since $K[X, Y]$ can be considered as a vector space over K, we may assume that $\{h_k\}$ is linearly independent.

Denote the number of all monic monomials of degree $\leq d$ in $K[X, Y]$ by r; in fact, $r = \binom{m+n+d}{d}$. Since every h_k is a linear combination of the monic monomials, we have $s \leq r$. In case $s < r$, we may put $h_{s+1} = \cdots = h_r = 0$. This completes the proof. □

Proof of Theorem 5. We shall prove the result only for Theorem 2.3. Another two cases may similarly be proved.

Fix n, m, s, t and d. Let r be the number depending on (n, m, d) as in the lemma above. Obviously, the number of all $r + s + t + 1$-tuples $(d_1, \ldots, d_{r+s+t+1})$ with $d_p \leq d$ is finite and depends only on (d, n, m, s, t).

For a given tuple $(d_1, \ldots, d_{r+s+t+1})$, we denote the general X-homogeneous forms of type $(d_1, d), \ldots, (d_{r+s+t+1}, d)$ with parameter coefficients $T_1, \ldots, T_{r+s+t+1}$ by $\hat{h}_1, \ldots, \hat{h}_r$, $\hat{u}_1, \ldots, \hat{u}_s$, $\hat{w}_1, \ldots, \hat{w}_t, \hat{f}$, respectively. Here, when $i \neq j$, T_i and T_j have no common parameter. Put $T = (T_1, \ldots, T_{r+s+1+1})$ and denote the number of all parameters in T by $|T|$ (evidently, $|T| = |T_1| + \cdots + |T_{r+s+t+1}|$). Then these general forms are all in $\mathbf{Z}[X, Y, T]$.

Now consider the following (elementary) statement with (parameter) constants T:

$$\psi\colon \forall(X, Y) \left(\left(\bigwedge_{i=1}^{s} \hat{u}_i(X, Y, T) > 0 \right) \wedge \left(\bigwedge_{j=1}^{t} \hat{w}_j(X, Y, T) \geq 0 \right) \right.$$
$$\left. \wedge \left(\bigwedge_{k=1}^{r} \hat{h}_k(X, Y, T) = 0 \right) \rightarrow \hat{f}(X, Y, T) = 0 \right).$$

By Elimination of Quantifiers for real closed fields (see Theorem 5.1 in [8]), there is a quantifier free sentence ϕ such that, for every real closed field $\hat{R}$ and any $t_0 \in \hat{R}^{|T|}$,

$$(\hat{R}, t_0) \models (\psi \leftrightarrow \phi).$$

If we take ϕ in disjunctive norm form, then ϕ may be written in the form

$$\phi_1 \vee \phi_2 \vee \cdots \vee \phi_q$$

where ϕ_l is a conjunction of prime or negated prime formulas, $l = 1, \ldots, q$.

For the elementary language of ordered fields enlarged by the constants T, a prime formula is logically equivalent to a formula of the form $E(T) = 0$ or $E(T) > 0$, where $E(T) \in Z[T]$. Then, a negated prime formula is logically equivalent to $E(T) \neq 0$ or $E(T) \not> 0$, and it is thereby logically equivalent to $E^2(T) > 0$ or $-E(T) \geq 0$. So, for every l, ϕ_l may be written in the form

$$\left(\bigwedge_{i'=1}^{s'} B_{i'}(T) > 0\right) \wedge \left(\bigwedge_{j'=1}^{t'} G_{j'}(T) \geq 0\right) \wedge \left(\bigwedge_{k'=1}^{r'} E_{k'}(T) = 0\right)$$

where s', t', $r' \in \mathbf{N}$, $B_{i'}(T)$, $G_{j'}(T)$, $E_{k'}(T) \in \mathbf{Z}[T]$.

Let U^* be the multiplicative semigroup generated by the $\hat{u}_i$ and $B_{i'}(T)$, let W^* be the multiplicative semigroup generated by the $\hat{w}_j$, $G_{j'}(T)$ and U^*, and let I^* be the ideal of $\mathbf{Q}[X, Y, T]$ generated by the $\hat{h}_k$ and $E_{k'}$. Then I^* is X-homogeneous. Indeed, if $h \in I^*$, then $h = \sum_k a_k \hat{h}_k + \sum_{k'} b_{k'} E_{k'}(T)$. Denote the X-degree of $\hat{h}_k$ by d_k for $k = 1, \dots, r$, we have $(h)_d = \sum_k (a_k)_{d-d_k} \hat{h}_k + \sum_{k'} (b_{k'})_d E_{k'}(T) \in I^*$.

Now, we may assert that $\hat{f}(X, Y, T)$ is vanishing in $\mathbf{R}$ with respect to $\{U^* > 0; W^* \geq 0; I^* = 0\}$. Indeed, if false, then there is some $(x_0, y_0, t_0) \in \mathbf{R}^{n+1} \times \mathbf{R}^m \times \mathbf{R}^{|T|}$ such that $u^*(x_0, y_0, t_0) > 0$, $\forall u^* \in U^*$; $w^*(x_0, y_0, t_0) \geq 0$, $\forall w^* \in W^*$; $h^*(x_0, y_0, t_0) = 0$, $\forall h^* \in I^*$; but $\hat{f}(x_0, y_0, t_0) \neq 0$. From this, $(\mathbf{R}, t_0) \vDash \phi_l$, and $(\mathbf{R}, t_0) \vDash \phi$. Since $(\mathbf{R}, t_0) \vDash (\psi \leftrightarrow \phi)$, we have $(\mathbf{R}, t_0) \vDash \psi$. Now $\hat{u}_i(x_0, y_0, t_0) > 0$ for $i = 1, \dots, s$; $\hat{w}_j(x_0, y_0, t_0) \geq 0$ for $j = 1, \dots, t$; and $\hat{h}_k(x_0, y_0, t_0) = 0$ for $k = 1, \dots, r$, we have $\hat{f}(x_0, y_0, t_0) = 0$, a contradiction.

Observe that every element in $\mathbf{Q}^+$ is a sum of squares in $\mathbf{Q}$. Then, by Theorem 2.3, we have an X-homogeneous inclusion $(*)$

$$u^* \hat{f}^{2e} + \sum_v w_v^* g_v^2 \equiv 0 \qquad (\operatorname{mod} I^*)$$

where $e \in \mathbf{N}$, $u^* \in U^*$, $w_v^* \in W^*$, and $g_v \in \mathbf{Q}[X, Y, T]$.

Along the way, we can obtain finitely many such inclusions $(*)$ as above. Moreover, we may point out that the X-homogeneous inclusion in Theorem 2.3(2) can be obtained by substituting suitable coefficients for T in one of the obtained inclusions $(*)$, if all the w_i, w_j, I and f satisfying Theorem 2.3(1) are of degree $\leq d$.

Let $u_1, \dots, u_s$, $w_1, \dots, w_t$, f and I satisfy Theorem 2.3(1) and be all of degree $\leq d$. By the lemma above, $I = (h_1, \dots, h_r)$, where h_k is an X-homogeneous form of degree $\leq d$, $k = 1, \dots, r$. Then, there are the general X-homogeneous forms $\hat{u}_i(X, Y, T)$, $\hat{w}_j(X, Y, T)$, $\hat{h}_k(X, Y, T)$

and $\hat{f}(X, Y, T)$ of (total) degree d with parameter coefficients T such that, for some $c \in K^{|T|}$, $u_i = \hat{u}_i(X, Y, c)$, $w_j = \hat{w}_j(X, Y, c)$, $h_k = \hat{h}_k(X, Y, c)$, and $f = \hat{f}(X, Y, c)$, where $i = 1, \ldots, s$; $j = 1, \ldots, t$; $k = 1, \ldots, r$, and the X-degrees of the $\hat{u}_i$, $\hat{w}_j$, $\hat{h}_k$ and $\hat{f}$ constitute a $r+s+t+1$-tuple $(d_1, \ldots, d_{r+s+t+1})$ with $d_p \leq d$.

As above, let ψ, ϕ be two sentences corresponding to the tuple $(d_1, \ldots, d_{r+s+t+1})$. Then Theorem 2.3(1) implies that $(R, c) \models \psi$. Since $(R, c) \models (\psi \leftrightarrow \phi)$, $(R, c) \models \phi$, and $(R, c) \models \phi_l$ for some l.

Substituting c for T in the inclusion $(*)$ corresponding to the ϕ_l, we have

$$u^*(X, Y, c) f^{2e} + \sum_v w_v^*(X, Y, c) g_v^2(X, Y, c) \equiv 0 \qquad (\operatorname{mod} I).$$

Here, $u^* = \hat{u}(X, Y, T)B(T)$, where $\hat{u}$ is (not necessarily distinct) a product of the $\hat{u}_i$, and $B(T)$ is (not necessarily distinct) a product of the $B_{i'}(T)$. Since $(R, c) \models \phi_l$, $B_{i'}(c) > 0$ for $i' = 1, \ldots, s'$. Thus $b := B(c) \in K^+$, and $b \neq 0$. Hence $u^*(X, Y, c) = bu$, where $u := \hat{u}(X, Y, c)$ is a product of the u_i. Similarly, $w_v^*(X, Y, c) = b_v w_v$, where $b_v \in K^+$, and w_v is (not necessarily distinct) a product of the u_i and w_j. Therefore, we have

$$u f^{2e} + \sum_v a_v w_v g_v^2(X, Y, c) \equiv 0 \qquad (\operatorname{mod} I),$$

where $a_v = b^{-1} \cdot b_v \in K^+$. This completes the proof for the Nullstellensatz. □

REMARK. In reference [10], Stengle established the following result: Let $f \in \mathbf{R}[X_0, X_1, \ldots, X_n]$ be a homogeneous form. Then f is positive semidefinite iff there exists a homogeneous polynomial relation $\varphi(-f) = 0$, where $\varphi(Y)$ is a monic polynomial of odd degree with coefficients which are sums of squares of forms.

Furthermore, by $v(f)$, he denotes the lowest degree in Y of any polynomial $\varphi(Y)$ appearing in the preceding result. Then he posed the following

Problem 2. If f is a positive semidefinite form of degree $2d$ in $X_0, X_1, \ldots, X_n$, can $v(f)$ be bounded (or effectively bounded) from above in terms of d and n?

If we specialize Theorem 5 about the Nichtnegativstellensatz to the case in which $K = R = \mathbf{R}$, $s = t = 1$, $u_1 = w_1 = 1$, $I = 0$ and $m = 0$, then we give an affirmative answer to the problem above.

Acknowledgment. The author is very grateful to the referee for his extraordinarily detailed report on this paper.

REFERENCES

[1] J. Bochnak, M. Coste and M.-F. Roy, *Géométrie Algébrique Réelle*, Springer-Verlag, 1987.

[2] J.-L. Colliot-Théléne, *Variantes du Nullstellensatz réel et anneaux formellement réels, Géometrie algébrique réelle et formes quadratiques*, Proc. Rennes Conference, 1981. Eds.: J.-L. Colliot-Théléne, M. Coste, L. Mahé and M.-F. Roy, LNM 959, Springer, 1982, 98–108.

[3] C. N. Delzell, *A continuous, constructive solution to Hilbert's 17th problem*, Invent. Math., **76** (1984), 365–384.

[4] D. W. Dubois, *A Nullstellensatz for ordered fields*, Ark. für Math., **8** (1969), 111–114.

[5] T. Y. Lam, *An introduction to real algebra*, Rocky Mountain J. Math., **14**, No. 4, Fall (1984), 767–814.

[6] ———, *The theory of ordered fields*, Lecture Notes in Pure and Appl. Math. 55, New York, Dekker, 1980, 1–152.

[7] S. Lang, *The theory of real places*, Ann. of Math., **57** (1953), 378–391.

[8] A. Prestel, *Lectures on formally real fields*, IMPA. Lecture Notes 22, Rio de Janeiro, 1975.

[9] G. Stengle, *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry*, Math. Ann., **207** (1974), 87–97.

[10] ———, *Integral solution of Hilbert's 17th problem*, Math. Ann., **246** (1979), 33–39.

[11] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 2, Van Nostrand, New York, 1960.

Received July 20, 1987 and in revised form April 8, 1988.

FUZHOU TEACHERS COLLEGE
JIANGXI, PEOPLE'S REPUBLIC OF CHINA