A CONSTRUCTIVE, CONTINUOUS SOLUTION TO HILBERT'S 17th PROBLEM, AND OTHER RESULTS IN SEMI-ALGEBRAIC GEOMETRY

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

By

Charles Neal Delzell

June 1980

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

(Principal Adviser)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and quality, as a dissertation for the degree of Doctor of Philosophy.

(Mathematics/Philosophy)

Approved for the University Committee of Graduate Studies:

Dean on Graduate Studies

ACKNOWLEDGEMENTS

I would like to express my sincere thanks to Professor Gregory Brumfiel, my thesis advisor, for guiding and encouraging me in my research. He has been very generous with his time and has given me much helpful advice.

The same must be said for Professor Georg Kreisel, who raised the main question which this dissertation answers.

I thank Dr. Jussi Ketonen for many helpful conversations, and Professors Tsit-Yuen Lam and Solomon Feferman for their interest in this research. The Department of Mathematics of Stanford University has supported me financially with a Teaching Assistantship throughout my graduate work.

While "typesetting" this draft with TEX (Tau Epsilon Chi, Donald Knuth's system for technical text), I received expert answers to many questions from Brent Hailpern and Arthur Keller of the Department of Computer Science at Stanford.

I am grateful to Maharishi Mahesh Yogi for making available to the world the Transcendental Meditation and TM-Sidhi programs, which, I feel, have improved my mathematical intuition, and thereby contributed to this research.

Finally, I am indebted to my parents for their constant support on all levels.

ABSTRACT

The main result (3.1) is a proof of the affirmative answer to a question raised in the early sixties by G. Kreisel: "Is there a continuous solution to Hilbert's 17^{th} Problem?"

More precisely, suppose R is a real closed field, $X = (X_0, \ldots, X_n)$ are indeterminates, $x = (x_0, \ldots, x_n) \in R^{n+1}$, $f \in \mathbb{Z}[C; X]$ is the general form in X of degree d with $\binom{n+d}{n}$ coefficients C, and

$$P_{nd} = \{\, c \in R^{\binom{n+d}{d}} \mid f(c; X) \text{ is positive semidefinite (psd) over } R \text{ in } X \,\}.$$

Then we construct $s \in \mathbb{N}$ and functions $a_{ij}\colon P_{nd} \to R^{m_i}$ which are semi-algebraic over $\mathbb{Q}$ (for short, $\mathbb{Q}$-s.a, or, roughly equivalently, real algebraic over $\mathbb{Q}$), and continuous with respect to the usual interval topology such that, for all $c \in P_{nd}$,

$$f(c; X) = \frac{\sum_j f_1\big(a_{1j}(c); X\big)^2}{f(c; X)^{2s} + \sum_j f_2\big(a_{2j}(c); X\big)^2}. \tag{3.1.1}$$

Here $m_i = \binom{n+e_i}{n}$ (where $i = 1, 2$, $e_1 = ds + \frac{d}{2}$, and $e_2 = ds$) and f_i is the general form of degree e_i in X; the coefficients of the polynomials giving the $\mathbb{Q}$-s.a. description of the graphs of the a_{ij} are in $\mathbb{Z}$ and are computable from n and d.

(3.1.1) leads immediately to a representation of $f(c; X)$ as a sum of squares (SOS) of functions which are homogeneous and rational in X, and continuous simultaneously in c and x, for $(c, x) \in P_{nd} \times R^{n+1}$, for the usual topology on $\mathbb{R}$; this continuity automatically implies continuity for the "computational" topology on "enrichments" of $\mathbb{R}$ by certain kinds of representations. (Whenever

we say that a function, defined on a subset of a set, is continuous, we mean that it can be extended to a continuous function on the set.) Thus we obtain, for the first time, a procedure to solve Hilbert's 17^{th} Problem constructively over $\mathbb{R}$ (or over any real closed field with a dense computable subfield): we can compute the $a_{ij}(c)$ to any accuracy by computing $a_{ij}(c')$, for $c' \in \mathbb{Q}^{\binom{n+d}{n}}$ close enough to c, by continuity for the usual topology.

We also construct a representation of psd quadratic forms in $X = (X_1, \ldots, X_n)$ as sums of (slightly fewer than $n!\,e$) positively weighted squares of linear forms which are continuous rational functions of the variables and the data (the usual diagonalization of symmetric matrices gives a weighted SOS-representation with only n summands, but their coefficients are discontinuous and *piecewise*-rational). We also give discontinuity results for quartic forms (3.4 and 4.2).

Also, we prove a foundational result (2.1) in s.a. geometry, a "Finiteness Theorem for Open S.A. Sets," conjectured by G. Brumfiel ("Unproved Proposition" 8.1.2 of [1979]): An open s.a. set may be written as a finite union of finite intersections of sets of the form $f^{-1}((0,\infty))$ ($f \in K[X]$, K an ordered field). (2.1) is used in the proof of (3.1); it also can be viewed as an improvement of the Tarski-Seidenberg algorithm for quantifier-elimination: if an open s.a. set F is defined by an elementary formula, the Tarski-Seidenberg algorithm eliminates its quantifiers, showing that F is s.a, but leaves both relations, $<$ and $=$, *obscuring* the fact that F is open; the Finiteness Theorem eliminates the quantifiers but leaves only the $<$ relation (and no negations), *revealing* the fact that F is open.

Finally, among the other results is the fact that the "bad set" of a psd polynomial f (i.e. the set in R^n where, no matter how f is written as a SOS of rational functions, the denominators must vanish) has codimension $\geq$ 3. Another result is that if f is a SOS of formal power series, over *any* field, then it is already a SOS of algebraic power series.

CONTENTS

I. History of the 17th Problem, and Statement of Results 1

II. A Finiteness Theorem for Open Semi-Algebraic Sets 29

III. The Continuous, Constructive Solution 39

IV. Continuous Sums of Squares of Forms 51

A. Quadratic Forms 51

B. Quaternary Quartic Forms 54

C. Binary Forms 55

V. Bad Points, and Other Results 57

A. Bad Sets 57

B. Formal Power Series 62

C. Symmetric Psd Polynomials 63

D. Filters and Partial Orders 64

Bibliography 69

CHAPTER I:

HISTORY OF THE 17th PROBLEM, AND STATEMENT OF RESULTS

The study of the connection between sums of squares (SOS) and positivity goes back at least to Lagrange [1770][1] who proved that every positive integer is a sum of 4 squares of integers (this may have been known to Diophantus). Hilbert's 17th Problem stems from a different investigation of this connection which began with the theorem, for which "M. Cauchy has somewhere given a proof,"[2] that a symmetric bilinear form on a finite dimensional vector space over a field can be diagonalized, for from this it is obvious that a positive semidefinite (psd) quadratic form $f(X) = f(X_1, \ldots, X_n) = \sum a_{ij}X_iX_j \quad (a_{ij} = a_{ji})$ over an ordered field K is a SOS of linear forms:

$$f(X) = \sum_{i=1}^{n} c_i\left(\sum_{j=1}^{n} b_{ij}X_j\right)^2, \tag{1.1.1}$$

some c_i, $b_{ij} \in K$, with $c_i \geq 0$.[3]

1 Brackets refer to entries in the bibliography, e.g. "[Landau 1903]"; if the author is clear from the context, we bracket only the year, e.g. "[1903]." A year in brackets is the year of publication, not the year of discovery.

2 According to Sylvester [1852].

3 A field K is called *ordered* once we have specified an *ordering*, i.e. a set $P \subseteq K$ (the "positive" elements), such that $P+P \subseteq P$, $P \cdot P \subseteq P$, $P \cup (-P) = K$, and $P \cap -P = \{0\}$ (consequences: $-1 \notin P \supseteq \{\text{SOS in } K\}$, char $K = 0$, and K has a topology generated by the open intervals (a, b); examples: C has no ordering, Q, R, and the real algebraic numbers (herein denoted by $\overline{\mathbb{Q}}$) have unique orderings, $\mathbb{Q}(\sqrt{2})$ has 2 orderings, $\mathbb{Q}(t)$ has uncountably many orderings, one for each Dedekind cut of Q). From now on, K will denote an ordered field. $f \in K(X)$ is called *psd* (*over K*) if $\forall x = (x_1, \ldots, x_n) \in K^n$ for which $f(x)$ is defined, $f(x) \geq 0$. We write K^+ for P.

Also, psd binary forms (i.e. homogeneous polynomials in two variables) over **R** are SOS of (2) forms. This follows from the 2-square identity and the factorization of binary forms over **R**. Although Hilbert described this as "well-known" in [1888], I do not know of a *published* proof before [Landau 1903]. Here, **R** can be replaced by any *real closed field* R, i.e. a field which is *formally real* (i.e. -1 is not a sum of squares in R; equivalently, R can be ordered) but which has no proper algebraic formally real extension. In [Artin and Schreier 1927a, 1927b] and [Artin 1927], real closed fields were introduced and characterized among all fields by any of the following properties:

(1) $\sqrt{-1} \notin R$ and $R(\sqrt{-1})$ is algebraically closed;

(2) R is formally real, $|R^*/R^{*2}| = 2$, and any odd degree polynomial in $R[X]$ has a root in R;

(3) R has finite codimension in its algebraic closure.

Examples of real closed fields include $\overline{\mathbf{Q}}$ (the smallest example), **R**, the algebraic closure, in a given real closed field, of any subfield, and any *real closure*, which we shall denote by $\overline{K}$, of any ordered field K (i.e. any real closed algebraic extension whose (unique) ordering induces the ordering of K; real closures always exist and are unique up to unique isomorphism). Treatments of the Artin-Schreier theory of real closed fields are available in Chapter 6 of [Bourbaki 1959], [Brumfiel 1979], Chapter 6 of [Jacobson 1964], Chapter 5 of [Jacobson 1974], [Lam 1973, 1980], [Lang 1965], [Prestel 1975], and Chapter 9 of [van der Waerden 1953].

The reason that **R** can be replaced in the above result by any real closed field is that this result, for each fixed degree, is an *elementary statement* in the first order language of ordered fields; that is, it is expressible using the usual symbols $0, 1, +, \cdot, =, <$, logical connectives $\wedge, \vee, \neg, \rightarrow, \exists, \forall$, and variables $x_1, x_2, \ldots$, where quantification is over R (as opposed to allowing quantification, say, over the power set of R, or over certain subsets such as $\mathbf{N}$). The Theorem of Tarski [1948, 1951][4] and Seidenberg [1954] (stated on p. 8) may then be applied to an elementary formula to construct a logically equivalent quantifier-free formula, thereby showing that the choice of the real closed field R is irrelevant to the truth or falsity of elementary statements. This remark applies to this entire dissertation, where almost all the results are elementary. For a discussion of the distinction between "elementary" and "transcendental" applications of the Tarski-Seidenberg Theorem, see the Introduction and §8.1 of [Brumfiel 1979].

Hilbert [1888] determined those n and d such that all real psd forms f in n variables of degree d are SOS (of necessarily homogeneous elements) in $\mathbf{R}[X]$, or equivalently, upon dehomogenization, those n and d such that all polynomials in $n-1$ variables are SOS. His answer was $\{ (n, 2), (2, d), (3, 4) \mid n, d \in \mathbf{N} \}$ (we shall never consider odd d). Improvements on his methods, but not his results, are as follows: Choi and Lam [1977b] gave a more elementary proof that psd ternary quartics are SOS. Ellison (1968, unpublished) actually carried out the lengthy construction indicated by Hilbert of the main coun-

4 This Theorem was discovered independently by Gödel, Herbrand, and Tarski around 1930. Gödel never published it, the others mentioned it in print a year later, and the full proof was not published until 1948, by Tarski.

terexamples needed for the rest of his answer, namely, psd ternary sextics and quaternary quartics which are not SOS. Motzkin ([1967], p. 217), pursuing a different investigation, published the first explicit such counterexample, $Z^6+X^4Y^2+X^2Y^4-3X^2Y^2Z^2$. In 1969, R. M. Robinson [1973] drastically simplified Hilbert's ideas to produce independently the counterexamples

$$X^2(X^2-Z^2)^2+Y^2(Y^2-Z^2)^2-(X^2-Z^2)(Y^2-Z^2)(X^2+Y^2-Z^2)$$

and

$$X^2(X-W)^2+Y^2(Y-W)^2+Z^2(Z-W)^2+2XYZ(X+Y+Z-2W).$$

Choi and Lam [1977a,b] constructed the counterexamples

$$X^4Y^2+Y^4Z^2+Z^4X^2-3X^2Y^2Z^2$$

and

$$W^4+X^2Y^2+Y^2Z^2+Z^2X^2-4XYZW,$$

which have the most symmetry. Reznick [1978] showed the Motzkin and Choi-Lam forms to be the simplest possible, and proceeded to classify similar counterexamples. All of the above psd forms become *strictly* definite (i.e. having no non-trivial zero) without becoming SOS as soon as we add $\epsilon(X^6+Y^6+Z^6)$ (or $\epsilon(X^4+Y^4+Z^4+W^4)$) for small $\epsilon>0$; indeed, Hilbert [1888] showed that (the convex cone of) SOS of n-ary forms of degree $d/2$ must form a *closed* set of the ($\binom{n-1+d}{n-1}$-dimensional) vector space of all n-ary forms of degree d.[5]

After showing that a psd form need not be a sum of squares of real forms, Hilbert [1900] raised his 17th Problem (cf. [1976]), "whether every definite form may not be expressed as a quotient of SOS of forms. At the same time it is desirable, for certain questions as to the possibility of certain geometrical constructions, to know whether the coefficients of the forms to be used in the expression may always be taken from the realm of rationality given by the form represented." There is an equivalent formulation of the question in terms of psd homogeneous rational functions, or quotients of psd forms; also, we can convert back and forth between a quotient of SOS and a sum of squares of quotients. See [Prestel 1979] for a discussion of the origins of the 17th Problem in §§36–8 of Hilbert's *Grundlagen der Geometrie* [1899]. For ternary forms, Hilbert [1893] had answered the question affirmatively, except for the rationality of the coefficients. His argument was essentially constructive, but it had the disadvantage of being long and difficult (relying on the theory of Abelian functions) and of not being extendible to more variables. In a different direction, Hilbert had also proved (Theorem 43 of [1899]) the affirmative answer for binary forms; here what was needed was the rationality of the coefficients

5 For an English version of Hilbert's argument, see [Robinson 1973]. Here the reader will also find a theorem which is in striking contrast to this result: *If $f(X_1,\ldots,X_n)$ is any real form (not necessarily psd) of degree d, then $f(X_1,\ldots,X_n)+b(X_1^d+\cdots+X_n^d)$ is a SOS of forms (of degree $\frac{d}{2}$) when b is sufficiently large. Furthermore, these forms of degree $\frac{d}{2}$ may be chosed to be monomials or binomials.* From this he deduces the non-trivial fact that the cone of SOS of forms, and even the smaller cone of SOS of binomial forms, of degree $\frac{d}{2}$ has interior (hence dense interior, by translation of neighborhoods); in fact, $X_1^d+\cdots+X_n^d$ is an inner point.

to be used. By a subsequent algorithm of Landau [1906], the rational functions in Hilbert's result could have been transformed into polynomials (still with rational coefficients); however by then, Landau had already [1903] obtained directly this improvement of the classical result on binary forms. In passing from $\mathbf{R}$ to $\mathbf{Q}$, the number of required squares in Landau's representation of [1903] increased from 2 to $2d+2$, where d is the degree of the form. In [1904], he lowered this number of squares to 5 for quadratics (smallest possible) and ≤ 6 for quartics; Fleck [1906] reduced the 6 to 5. Using the 8-square identity, Landau [1906] finally proved that, regardless of the degree, 8 squares are enough. Pourchet [1971] extended Landau's result by replacing $\mathbf{Q}$ with any algebraic number field, and simultaneously reduced the number of required squares to 5, the smallest possible.

The main step in the history of the 17th Problem was Artin's [1927] nonconstructive proof of the affirmative answer, and not only for the ground fields $\mathbf{Q}$ and $\mathbf{R}$, but simultaneously for any uniquely orderable subfield K of $\mathbf{R}$; dropping the unique orderability hypothesis, Artin represented psd (rational) functions f as $f(X) = \sum p_i r_i(X)^2$, where $p_i \in K^+$ and $r_i \in K(X)$. Artin proved this using his result that in any field F of characteristic $\neq 2$, an element is "totally positive with respect to the ordered subfield k"[6] if and only if $f = \sum p_i r_i^2$, for some $p_i \in k^+$, $r_i \in F$. Thus it remained to show that a psd function $f \in K(X_1, \ldots, X_n)$ is totally positive in $K(X_1, \ldots, X_n)$ with

[6] I.e., nonnegative in every ordering of F extending k; of course, F need not have any ordering.

respect to K. For this he used a series of "specialization lemmas" using Sturm's Theorem.

In solving the problem, Artin had recognized that it had more to do with the algebraic than the arithmetic properties of **Q** and **R**. By introducing his axioms (for real closed fields), he not only achieved greater generality, but he actually made the problem easier; thus, his solution was perhaps the first spectacular use of the axiomatic method for mathematical as opposed to metamathematical purposes, such as independence results.

At this point we review additional terminology which we shall need more and more. R will always denote (any of) the real closure(s) of the ordered field K. Let $X = (X_1, \ldots, X_n)$ be indeterminates, and $x = (x_1, \ldots, x_n) \in R^n$ (if $n = 1$ we shall say so explicitly). Throughout, all indices range over finite sets whose sizes are rarely specified, but which will be computable if K is computable.[7] For $\{f_i\} \subseteq K[X]$ let[8]

$$U\{f_i\} = \{\, x \in R^n \mid \bigwedge_i f_i(X) > 0 \,\},$$
$$W\{f_i\} = \{\, x \in R^n \mid \bigwedge_i f_i(x) \geq 0 \,\}, \text{and}$$
$$Z\{f_i\} = \{\, x \in R^n \mid \bigwedge_i f_i(x) = 0 \,\}.$$

A set is called a *basic open semialgebraic (s.a.) set* (more precisely, a *basic open K-s.a. set*), or simply a U, if it is of the form $U\{f_i\}$; and similarly with U

---

[7] A *computable* field is one whose field operations are computable, and whose order relation is decidable. Examples of computable fields include **Q**, $\overline{\mathbf{Q}}$, but not **R**.

[8] $\bigwedge_i$ [resp. $\bigvee_i$] means iterated conjuntion [resp. disjunction], indexed by i.

and "open" replaced by W and "closed." A set $S \subseteq R^n$ is called (K-)s.a. if it is a finite union of finite intersections of basic open and closed (K-)s.a. sets. A function from one (K-)s.a. set to another is called (K-)s.a. if its graph is a (K-) s.a. set (in the product space). All our sets and functions will be understood to be s.a. and, if K is computable, defined as certain real roots of polynomials with computable coefficients; this will always follow from (if nothing else) the Tarski-Seidenberg Theorem, whose most succinct formulation is now that the projection to R^{n-1} of a s.a. set in R^n is s.a. Thus, the Tarski-Seidenberg Theorem consists of a procedure to eliminate one (hence any number of) existential (hence also universal) quantifiers from a first order formula.

Artin wondered if a constructive version of his solution could be given, and he considered this question in a seminar which he led between the wars. In particular, he wished to eliminate his appeal to an infinite tower of field extensions, and he desired a bound on the number and degree of the summands in the representation.

Habicht [1940] gave an elementary, explicit construction of a SOS-representation of forms f *strictly* definite over R. In fact, the denominator he gives is $(X_1^2 + \cdots + X_n^2)^N$, some $N \in$ N, and the numerator contains only rational coefficients if the given form does. If we try to extend his method to psd forms by approximating by strictly definite forms, we find that N may grow without bound; this is inevitable if the form has any "bad points," i.e. non-trivial points in R^n where, in any SOS-representation, the common denominator must vanish; on the other hand, since his denominator has no non-trivial zero, we conclude that strictly definite forms have empty bad sets (we return to bad sets in Chapter V). He derived his representation by combining the "Rabinowitch trick" (i.e. adding a new indeterminate X_{n+1}) with a theorem of Pólya on the representation of forms which are positive when all $X_i \geq 0$, i.e. on $W\{X_i\}$ (except the origin).[9] Habicht's algorithm is fully constructive: it can easily be made to produce a representation correct to any desired accuracy in an estimable amount of time.

A. Robinson used lower predicate calculus and the model completeness of **R** to prove a number of overlapping results. First, in [1955] he showed that if K is either real closed, or Archimedean,[10] then if $f(x) \geq 0 \quad \forall x \in K^n \cap U\{g_i\}$ (where $\{f, g_i\} \subseteq K[X]$), then $f = \sum c_I g_I r_I^2$, for some $c_I \in K^+$, where the g_I are (not necessarily distinct) products of the g_i, and $\{r_I\} \subseteq K(X)$; further, if the ordering on K is unique, then the c_I are totally positive, hence SOS in K, so that the c_I may be dropped; better still, for K real closed, he proved the existence of a bound on the number and degrees of the summands which depends on $\{g_i\}$ and deg f but not on the coefficients of f (or, of course, on R). In [1956] Robinson extended the real closed case as follows: if $V \neq \phi$ is an irreducible algebraic variety in R^n with prime ideal P, $\{f, g_i\} \subseteq R[X]$, and $f(x) \geq 0 \quad \forall x \in V \cap U\{g_i\}$, then $h^2 f \equiv \sum g_I h_I^2 \pmod{P}$, for some $\{h, h_I\} \subseteq$

9 See the *second* edition [1952] of [Hardy, Littlewood, and Pólya 1939] for an enjoyable English version of both results.

10 An ordered field K is *Archimedean* over the subfield k if $\forall c \in K \quad \exists d \in k$ such that $c < d$; if k is Q, we omit "over k." We shall have more to say on the rôle of the Archimedean condition on p. 16.

$R[X]$, where the g_I are products of the g_i; we still have a bound on the number and degrees of the $\{h, h_I\}$, which depends only on the $\{g_i\}$ and deg f, not on the coefficients of f.

In October 1955 Artin asked Kreisel if explicit bounds could be found. In Nov. 1955, somewhat before the appearance of Robinson's result, Kreisel succeeded in obtaining, by two proof theoretic methods, a *primitive* recursive bound (Robinson's was only general recursive). The first method ([1957a,b]; pp. 165–6 of [1958], and [1960]) used proof theoretical results: Hilbert's first and second ϵ-Theorems (or Herbrand's Theorem). The second method [1960] consisted of extracting the constructive content of Artin's original argument, by replacing Artin's use of a real closed extension of an ordered field with a specific finite extension sufficient for the result; in this replacement some elegance and clarity is lost, but some explicitness is gained; here the ideas but no theorem of proof theory for first order logic are used. In [1957b] Kreisel gave a rough estimate (for $n = 2$) of this primitive recursive bound. A sharper estimate is

$$2^{2^{\cdot^{\cdot^{\cdot^{2^{cd}}}}}},$$

where there are n 2's, where $d =$deg f, and where c is a positive constant.

Stimulated by these results, Henkin [1960] used model theoretic methods similar to Robinson's to prove what is now accepted as the most natural formulation of the answer to Hilbert's question: if $f \in K[X]$ is psd (over R) and if deg $f \leq d$, then $f = \sum c_i r_i^2$, where $r_i \in K(X)$ and $c_i \in K^+$ (Artin had obtained this representation under the hypotheses that $K \subseteq \mathbf{R}$ and that f be psd over K; for $K \subseteq \mathbf{R}$, psd over K is equivalent to psd over R and to psd over $\mathbf{R}$, since K is then dense in $\mathbf{R}$). Henkin also showed that the (bounded number of) c_i and the (bounded number of) coefficients of the r_i can be taken to be functions of the coefficients of f which are "piecewise-rational" over $\mathbf{Z}$ (abbreviated "Z-p.r.," or simply "p.r."), where the finitely many "pieces" are s.a. subsets of $R^{\binom{n+d}{n}}$, the space of coefficients of f; the coefficients of these rational functions and the polynomials defining these domains are recursive but not necessarily primitive recursive functions of n and d.

Robinson gave a correspondingly improved formulation of his results. In §5 of [1957] he proved for $f,g \in K[X]$, that if $f(x) \geq 0 \quad \forall x \in Z\{g\}$, then $h^2 f = \sum_i c_i h_i^2 + kg$ for some $\{h, h_i, k\} \subseteq K[X]$, where $c_i \in K^+$; this time the bound is on the number and degrees of h, k and the h_i, and it depends on deg f, deg g, but not on K or the coefficients of f and g. In §8.5 of [1963] he replaced $Z\{g\}$ above with $Z\{g\} \cap U\{g_i\}$ (any $\{g_i\} \subseteq K[X]$) provided that g generates the ideal of $Z\{g\}$ and that $g \not| g_i$; the conclusion then is

$$h^2 f = \sum_I c_I g_I h_I^2 + kg, \tag{1.2.1}$$

where the g_I are products of the g_i. The bound no longer applies to deg k, and now the bound depends also on the degree of the g_i.

Robinson further proved [1957] that if p is totally positive in a finite, formally real (order-)extension F of K, then $p = \sum_{i=1}^r c_i r_i^2$, where $c_i \in K^+$, $r_i \in F$; what was new was that r depends only on $[F{:}K]$, not on F, K, or p. Thus if all the positive elements of K are SOS, and if the number of required squares is bounded, then we may drop the c_i in the above representation, but make r dependent also on this bound; this overlaps an important theorem stated by Hilbert (first proved by Siegel [1921]) that if $K = \mathbf{Q}$, then $r = 4$, independent even of $[F{:}K]$.

Daykin [1960] constructed a primitive recursive, piecewise-rational solution which was superior to the Henkin-Robinson solutions, by working out Kreisel's [1960] sketch of the "constructivization" of Artin's original proof. A little more notation at this point will help us describe Daykin's representation (and eventually many others as well). Let $X = (X_0, \ldots, X_n)$ be indeterminates, let $x = (x_0, \ldots, x_n) \in R^{n+1}$, let $a = (a_0, \ldots, a_n) \in \mathbf{N}^{n+1}$ be a multi-index, let $|a| = \sum a_i$, fix $d \in \mathbf{N}$, let $C = \langle C_a \rangle_{|a|=d}$ be $\binom{n+d}{n}$ indeterminates (in some fixed order), let $c = \langle c_a \rangle_{|a|=d}$ be an element of $R^{\binom{n+d}{n}}$, let $f \in \mathbf{Z}[C; X]$ be the general form of degree d in X with coefficients C (i.e. $f(C; X) = \sum_{|a|=d} C_a X^a$, where $X^a = X_0^{a_0} \cdots X_n^{a_n}$), and let

$$P_{nd} = \{\, c \in R^{\binom{n+d}{n}} \mid f(c; X) \text{ is psd (over } R) \text{ in } X \,\}.$$

Daykin showed how to compute effectively, from n and d alone, $p_{ij} \in \mathbf{Z}[C]$ and $r_{ij} \in \mathbf{Q}(C; X)$ (homogeneous in X) such that

$$\begin{aligned} &(1) \quad \bigwedge_i \quad f(C;X) = \sum_j p_{ij}(C) r_{ij}(C;X)^2 \text{ and} \\ &(2) \quad \forall c \in P_{nd} \quad \bigvee_i \bigwedge_j \left[\begin{array}{c} p_{ij}(c) \geq 0, \text{ and the denominator of} \\ r_{ij}(c;X) \text{ does not vanish identically in } X \end{array} \right]. \end{aligned} \qquad (1.3.1)$$

The superiority of this representation consists not only in the explicitness of the bound, but also in the choice of pieces on which the rational functions are defined: the earlier pieces were s.a., but Daykin's are basic closed s.a., namely, $W_i = W\{g_{ij}\}$. In Chapter II we give a quick proof and refinement of his representation, using powerful results in s.a. geometry.

The improvements found in the fifties to Artin's solution brought only temporary satisfaction, and by the early sixties Kreisel wondered if one could not do better. In particular, the piecewise character of the representations meant that when computing a representation from given coefficients of f, one first had to determine in which piece of the domain the coefficients lay. This amounts to testing various polynomial inequalities in the coefficients. While this presents no difficulty in computable fields, it is precisely what we cannot do in, say, **R**, an element of which must be presented as, say, a decimal, or an oscillating decimal used in computer science, or a pair $(\langle r_n \rangle, \mu)$ of some kind of Cauchy sequence of rationals and a "modulus of convergence" function μ satisfying $\forall k > 0 \, \forall n, m \geq \mu(k) \, [|r_n - r_m| < \frac{1}{k}]$. While this "fine point" is not considered by classical algebraists, it is enough of a problem to leave Hilbert's 17th Problem still unsolved from a constructivist point of view.

Thus, in the early sixties, the question was open whether the piecewise character could be dispensed with, or at least whether a topological version of Artin's Theorem could be given (the question appeared in print, e.g., on pp. 115–6 of [Kreisel 1977a] and in footnote 1 of [1977b]). Precisely, (1) can we choose representing rational functions which are continuous in R^{n+1} (where by a "continuous rational function" we shall always mean a continuously-extendible rational function) (example: the representation

$$1 = \frac{X^2}{X^2+Y^2} + \frac{Y^2}{X^2+Y^2}$$

is discontinuous at the origin in R^2), and (2) can the coefficients of the numerators and denominators in each rational function be chosen to be continuous functions of the given coefficients? In the case of an ordered ground field, we should allow positive constant weights on the squares, as in Henkin's formulation, and arrange for *their* continuous variation as well, or at least for the continuity of the coefficients of the resulting *product* of the weight and the squared rational function. In the above, the ordered (and possibly real closed) ground field has been given the usual order topology. Kreisel also posed the question for the finer "computational topology" on "enrichments" of **R** by specific representations, say oscillating binary expansions with the corresponding Baire space or "weak" topology on 3^ω, or Cauchy sequences of rationals with the topology inherited from the product topology on $\mathbf{Q}^\omega$. While any $f: \mathbf{R} \to \mathbf{R}$ continuous with respect to the usual topology is obviously continuous with respect to the computational topology on Cauchy sequences, the following example of Kreisel[11] disproves the converse: consider the construction of a zero for a cubic equation from its coefficients, say $f(c) = x$, for $x^3 - 3x = c$. There is clearly no such mapping f which is continuous for the usual topology, but continuity can be arranged for the computational topology.

The reason for considering computational topologies goes back to Brouwer's intuitionism, in which he observed that every constructively defined function from **R** to **R** (whose elements he described by "free choice sequences"

---

11 §2 of [Kreisel 1974], footnote 10 of [1976], [1977b], and elsewhere.

$\langle r_n \rangle \in \mathbf{Q}^\omega$) is continuous relative to the product topology on $\mathbf{Q}^\omega$; for if $f(\langle r_n \rangle) = \langle s_n \rangle$, and a value s_n has been established, then f can only have used a finite amount of information about $\langle r_n \rangle$. Thus, if Hilbert's 17th Problem cannot be solved continuously with respect to this computational topology, then it cannot be solved constructively. From now on all topological terms such as "continuous" refer to the usual topology.[12]

In view of the geometric origin of Hilbert's 17th Problem, stressed in his own presentation, it seems natural enough to impose topological conditions. Kreisel's interest is logical: To determine the extent to which current mathematical notions express adequately or better the aims usually stated in terms of so-called constructive, in particular, of intuitionistic foundations.

In a parallel development, Heilbronn [1964] gave a surprising answer to another question originating from Kreisel, by giving an *analytic* version of Lagrange's Theorem: he constructed functions f_1, f_2, f_3, f_4, which are analytic on the complex plane minus the negative real axis, which take rational values for positive rational arguments, and which satisfy $z = \sum f_i(z)^2$.

[12] Simultaneously, Kreisel posed the same continuity question for the classical "weak" Hilbert Nullstellensatz. Here the answer turned out to be easy for the usual topology: if we let X be a single indeterminate, and $a, b \in \mathbf{C}$, then the two polynomials $f(X) = a$ and $g(X) = bX + 1$ in $\mathbf{C}[X]$ have no common zero in $\mathbf{C}^1$ for $(a, b) \in S = \{(a, b) \in \mathbf{C}^2 \mid a \neq 0 \vee b = 0\}$. But if we write $1 \equiv p(X)f(X) + q(X)g(X)$ (with $p(X), q(X) \in \mathbf{C}[X]$), then the coefficients of p and q, as functions on S, must vary discontinuously near $a = b = 0$. Again we could consider various enrichments of the data, in particular, enrichments of the real and imaginary parts, say, by Cauchy sequences of rationals with moduli of convergence, by binary or oscillating binary expansions, by Dedekind cuts, etc., and for each kind of enrichment there is a corresponding topology.

However, before any progress was made on Kreisel's question, other aspects of the problem were considered. It was well-known that the Archimedean property played a rôle in Artin's original formulation of his theorem. For example,[13] over the non-Archimedean ordered field $\mathbf{Q}(X)$ (where $X^{-1} > \mathbf{Q}$, i.e. the indeterminate X is infinitesimally small compared to $\mathbf{Q}$, and positive), $f(Y) = (Y^2 - X)^2 - X^3 \in \mathbf{Q}(X)[Y]$ (Y an indeterminate) is psd over $\mathbf{Q}(X)$ but not a (positively weighted) SOS even in $\overline{\mathbf{Q}(X)}(Y)$. Indeed, upon factoring over $\overline{\mathbf{Q}(X)}$, we see that $f < 0$ precisely on the two intervals I and $-I$, where $I = \left(\sqrt{X(1-\sqrt{X})}, \sqrt{X(1+\sqrt{X})}\right)$, which contain no point of $\mathbf{Q}(X)$.[14]

It is no accident that in the logical treatments of the 17$^{\text{th}}$ Problem, the Archimedean property was replaced by the condition that the given polynomial be psd over the *real closure* of the ordered field of coefficients, because the Archimedean property cannot be expressed by an elementary statement. Since Archimedean ordered fields are isomorphic to subfields of $\mathbf{R}$, and are therefore dense in their real closures, "psd" over an Archimedean field already implies "psd" over its real closure.

However, it was not known whether the Archimedean hypothesis could be dropped from Artin's theorem provided the unique orderability was retained. An incorrect proof by Lang [1965] of the affirmative answer was followed by a counterexample from Dubois [1967]: Let F be the "Euclidean closure" of $\mathbf{Q}(t)$ (t an indeterminate, $t^{-1} > \mathbf{Q}$), i.e. the smallest extension closed under

13 P. 99 of [Artin and Schreier 1927a].

14 Robinson [1955] gave a similar example.

extraction of square roots of positive elements. Then F, being Euclidean, has a unique order, relative to which Dubois showed $f(X) = (X^3 - t)^2 - t^3 \in F[X]$ to be (strictly) definite; on the other hand, $f(1)$ and $f(t^{1/3})$ have opposite signs, so f cannot be a SOS in $\overline{F}(X)$.

The main result in the sixties was Pfister's elegant "2^n bound" [1967] on the number of square summands required to represent a psd $f \in R(X_1, \ldots, X_n)$, independent of deg f (Hilbert had proved this for $n = 2$ in his [1893] result). More precisely, Pfister has shown [1974]: if

$$f = \sum_{i=1}^{2^n+M} f_i^2$$

with $f_i \in R(X_1, \ldots, X_n)$ and $\deg f_i \leq d$, then there is a representation

$$f = \sum_{i=1}^{2^n} g_i^2$$

with $g_i \in R(X_1, \ldots, X_n)$ and

$$\deg g_i \leq C(n)^{\frac{n^M - 1}{n-1}} d^{n^M};$$

the constant $C(n)$ depends only on n, and could be determined explicitly; it probably grows quickly with n.

His proof uses (1) a special case of the Tsen-Lang Theorem: if C is an algebraically closed field and F is a field of transcendence degree n over C, then every quadratic form with coefficients in F, of dimension $> 2^n$, has a non-trivial zero in F; and (2) his theorem that the non-zero elements of a field F of characteristic $\neq 2$ represented by (what is now called) a "Pfister form," form a subgroup of F^*. (An independent, unpublished study by Ax in 1966, showed that 8 squares suffice when $n = 3$.) It is not known whether Pfister's bound applies in the case of ordered coefficient fields K, in particular $\mathbf{Q}$; again, we should allow positive constant weights on the squares ~~et alte~~ in the ordered field case, since positive elements in K need not be sums of (even an unbounded number of) squares.

For real closed fields it is not known whether 2^n is best possible, except for $n \leq 2$: Cassels, Ellison, and Pfister [1971] showed that the (psd) Motzkin polynomial $1 + X^2Y^4 + X^4Y^2 - 3X^2Y^2$ is not a sum of three squares in $R(X,Y)$; but their method uses the theory of elliptic curves, and does not extend to $n \geq 2$. Christie [1976] used this method to show that

$$(1 + 250XY^2)^2 + X(X+3)^3Y^2$$

is *strictly* definite but not a sum of three squares in $R(X,Y)$. The only known lower bound is $n+1$: Cassels [1964] showed that $1 + X_1^2 + \cdots + X_n^2$ is not a sum of n squares in $R(X_1, \ldots, X_n)$, by sharpening a result of Landau [1906] that a SOS of rational functions can be reduced to a SOS of rational functions in which any one variable, say X_1, does not occur in the (common) denominator; Cassels did this without increasing the number of summands. Hsia and Johnson [1974] have conjectured that a psd $f \in \mathbf{Q}(X_1, \ldots, X_n)$ must be a sum of $2^n + 3$ squares in $\mathbf{Q}(X_1, \ldots, X_n)$ (this is Lagrange's Theorem for $n = 0$ and Pourchet's [1971] result for $n = 1$, but it is not known whether *any* bound, independent of degree, exists for $n > 1$). All these results have nothing to do with Kreisel's question, since Pfister's techniques add to whatever discontinuities may have been present in the original representation.

We now return to Kreisel's question, and again write $X = (X_0, \ldots, X_n)$. The first part of the question, continuity in the *variables* of the rational functions, was answered by Stengle's [1974] "Positivstellensatz:" for $\{f, g_i\} \subseteq K[X]$, if $\forall x \in W\{g_i\}$, $f(x) \geq 0$, then

$$f = \frac{\sum_I c_{1I} g_I h_{1I}^2}{f^{2s} + \sum_I c_{2I} g_I h_{2I}^2}, \tag{1.4.1}$$

some $s \in \mathrm{N}$, $c_{jI} \in K^+$, and $h_{jI} \in K[X]$ $(j = 1, 2)$, where the g_I are products of the g_i. If we want to transform this into a (positively weighted) SOS of rational functions, we just multiply the numerator and denominator of (1.4.1) by the denominator. However, the numerator and denominator of (1.4.1) are not homogeneous in X if f is, nor can they instantly be made so, as in the earlier representations. On the other hand if the representation were homogeneous for homogeneous f, then we instantly get an inhomogeneous representation for inhomogeneous f. In [1979] Stengle retraced his proof (which used, by the way, the Rabinowitch trick again) back to his use of the real Nullstellensatz and from there carried out the delicate homogenization process; however he did this under the assumption $\{g_i\} = \{0\}$. Although Hilbert's 17[th] Problem does not require the extra generality of the $\{g_i\}$, the proof of our main Theorem (3.1) does.

Anyway, since $W\{g_i\} \cap Z\{\text{denominator}\} \subseteq Z\{f\} \subseteq R^{n+1}$, the Squeeze theorem easily implies that the rational functions extend (namely, by 0) to functions of X which are continuous throughout $W\{g_i\}$. It therefore remained (for Kreisel's question) to arrange in addition for the *coefficients* of each rational function to vary continuously in the coefficients of f.

Stengle's theorem includes a number of results which have appeared independently in the more recent literature. For example, Prestel [1975] used model theory to show (Theorem 5.10) that for f strictly definite,

$$f = \frac{1 + \sum g_i^2}{\sum h_i^2},$$

$\{g_i, h_i\} \subseteq K[X]$. Also, Swan [1977] asked whether the denominator in Artin's representation could be chosen strictly definite (i.e. whether the "bad set" of f is always empty, where the bad set of f consists of those points in R^{n+1} at which the common denominator of any SOS-representation of f must vanish). Choi and Lam [1977a] gave the answer "Yes" for binary psd polynomials but in general "No" for psd polynomials of more variables. Then Prestel and Knebusch improved the denominators so as to show that the bad set of any psd polynomial f is contained in $Z\{f\}$. (E. G. Straus was the first to verify the existence of bad points:[15] the psd quaternary quartic form described by Hilbert [1888] must have a non-trivial bad point.)

Another important virtue (this one for s.a. geometry) of the relation $W\{g_i\} \cap Z\{\text{denominator}\} \subseteq Z\{f\}$ is that it guarantees the nonnegativity of f on $W\{g_i\}$ (the earlier representations of Robinson (e.g. (1.2.1)), et. al., guaranteed nonnegativity of f only on the closure of $U\{g_i\}$; the rational func-

[15] In a reply to Kreisel, 1956.

tions could degenerate to 0/0 over the "degenerate" (or thin) parts of $W\{g_i\}$).

Brumfiel suggested that I try to characterize the bad set in some way. Towards this end, we give a few new examples of bad sets, and prove our main partial result in this direction:

Proposition 5.1: *For psd $f \in K[X]$, cod(bad set of f) ≥ 3.*[16]

Back to Kreisel's continuity requirement, we now state our main result:

Theorem 3.1: *There are $s \in \mathbb{N}$ and continuous* $\mathbb{Q}$-s.a. *functions $a_{ij}: P_{nd} \to R^{m_i}$ such that $\forall c \in P_{nd}$,*

$$f(c;X) = \frac{\sum_j f_1\big(a_{1j}(c);X\big)^2}{f(c;X)^{2s} + \sum_j f_2\big(a_{2j}(c);X\big)^2}. \tag{3.1.1}$$

Here $m_i = \binom{n+e_i}{n}$ (where $i = 1, 2$, $e_1 = ds + \frac{d}{2}$, and $e_2 = ds$) and f_i is the general form of degree e_i in X; the (integral) coefficients of the polynomials giving the $\mathbb{Q}$-s.a. *description of the graphs of the a_{ij} are computable from n and d.*

For the case of real closed fields, this answers affirmatively both parts of Kreisel's question, and, when $R = \mathbb{R}$, for both topologies;[17] hence we shall ignore the computational topology in the sequel; in fact, (3.1.1) leads to a SOS of functions which are clearly continuous *simultaneously* in c and x for $(c, x) \in P_{nd} \times R^{n+1}$.

Furthermore, viewing these functions as rational functions in X, their coefficients are given explicitly by $\mathbb{Q}$-s.a. functions, so that both (1) the

[16] Cod $= (n+1) -$ dim, and dim $=$ maximal dimension of a cell which can be embedded in the set.

[17] Most people expected continuity only for the computational topology on $\mathbb{R}$.

coefficients, and (2) the values of the functions at any point in R^{n+1}, can be computed in a finite number of steps, if R is computable (e.g. if $R = \overline{\mathbb{Q}}$). And even if R is not computable but at least contains a dense computable subfield K, so that we may approximate elements of R by elements of K, then we can still carry out the computations to any desired accuracy: for (1), simply calculate $a_{ij}(c')$ for $c' \in K^{\binom{n+d}{n}}$ close enough to c, since the a_{ij} are continuous (with respect to the usual topology); for (2), compute the values of the functions at a nearby point in K^{n+1}, since the functions are continuous simultaneously in c and x. Taking $R = \mathbb{R}$ and $K = \mathbb{Q}$ in the above sentence, we therefore have, for the first time, a constructive, in particular, intuitionistic,[18] solution to Hilbert's 17th Problem over R. Although Kreisel did not ask for semi-algebraicity of the coefficients, this comes along naturally in the proof, and is to be expected: s.a. functions are precisely those natural functions which map any real closed field to itself. Unfortunately, Kreisel's question for ordered fields has not been answered, although we suspect the answer is "Yes:"

Conjecture 1.5: *There exist $s \in \mathbb{N}$ and continuous $\mathbb{Q}$-piecewise-polynomial functions $a_{ij}: P_{nd} \to R^{m_i}$ and $p_{ij}: P_{nd} \to R^+$, with m_i and f_i as in 3.1, such that $\forall c \in P_{nd}$,*

$$f(c;X) = \frac{\sum_j p_{1j}(c) f_1\big(a_{1j}(c);X\big)^2}{f(c;X)^{2s} + \sum_j p_{2j}(c) f_2\big(a_{2j}(c);X\big)^2}. \tag{1.5.1}$$

By "$\mathbb{Q}$-piecewise-polynomial" we mean that P_{nd} has been written as a finite union of $\mathbb{Q}$-W's upon each of which a_{ij} and p_{ij} are described by polynomials $\in \mathbb{Q}[C]$; as in (3.1), the $\mathbb{Q}$-s.a. descriptions of the a_{ij} and the p_{ij} are computable

---

[18] Here we mean intuitionistic in the traditional sense, *viz.* as described above. Our solution is probably not intuitionistic in the sense of sheaf models, where the axioms are weaker.

from n and d.

Note: it may be necesary to replace "piecewise-polynomial" with "piecewise-rational" (p.r.) to get the special denominator in (1.5.1). Also, we do not necessarily insist on continuity of the a_{ij} and p_{ij} separately; we would settle for continuity either of the *products* $p_{ij}f_i(a_{ij};x)^2$ (as functions of (c,x)), or, equivalently, of the X-coefficients of the $p_{ij}f_i(a_{ij};X)^2$ (after expanding out), though this weakening is probably not necessary. Just as semi-algebraicity was expected of functions mapping any real closed field to itself, we see here that functions mapping any ordered field to itself are expected to be Q-p.r.

The primary interest of the conjecture is not as an aid to the "constructivization" of Artin's theorem over various ordered fields, partly because this has already been accomplished for the fields of original interest: (1) for computable ordered fields (mainly, real number fields such as Q), first by Robinson and Henkin, giving general recursive bounds, and second by Kreisel, giving primitive recursive bounds; and (2) for R, and in fact for any real closed field containing a dense computable subfield, by Theorem 3.1. The only new fields that the conjecture could add to this list are ordered fields with dense computable subfields, such as R(T), where R has the usual ordering, and where the indeterminate T defines a Dedekind cut in R with the property that Q(T) inherits from R(T) a decidable order relation. Rather, 1.5 is primarily of independent interest, since we interpret 3.1 as showing that *constructivity* is not the right thing to be seeking anyway, and that instead *continuity*, and Q-s.a.'ity or even Q-p.r.'ity, is the more natural goal.

In Chapter III we give a necessary and sufficient condition (Corollary 3.4) for the truth of the conjecture when the word "piecewise" is deleted: namely, $d \leq 2$ and n arbitrary. In fact, in 4.1 we prove much more than the conjecture for $d = 2$: Let $\sum C_{ij}X_iX_j$ be the general quadratic form in $X_0, \ldots, X_n$ and write $C = (C_{ij})_{0 \leq i \leq j \leq n}$. Set

$$N(n) = (n+1)! \sum_{k=0}^{n} \frac{1}{k!}.$$

Theorem 4.1: *For fixed n and for $0 \leq l \leq n$, $1 \leq k \leq N(n)$, we can construct p_k, $a_{kl} \in \mathbf{Q}(C)$ such that*

$$\sum C_{ij}X_iX_j = \sum_{k=1}^{N(n)} p_k(c)\Big(\sum_{l=0}^{n} a_{kl}(c)X_l\Big)^2 \text{ and,} \tag{4.1.1}$$

throughout $P_{n2} \times R^{n+1}$,

$$\bigwedge_{k=1}^{N(n)} \left[p_k(c) \geq 0, \text{ and } p_k(c)\Big(\sum_l a_{kl}(c)x_l\Big)^2 \text{ is continuous in } (c,x)\right]. \tag{4.1.2}$$

Note that

$$\sum_{l=0}^{n} a_{kl}(c)x_l$$

alone is not continuous in $P_{n2} \times R^{n+1}$. Here we must use slightly fewer than $(n+1)!\,e$ summands; the classical SOS-representation (1.1.1) requires only $n+1$ summands, but their coefficients are discontinuous and *piecewise*-rational.

Theorem 4.1 suggests the problem of parametrizing the representations of psd forms as SOS of forms in the remaining cases where this is possible (recall

p. 3): binary forms, and ternary quartic forms. We show (Theorem 4.2) that ternary quartics cannot be continuously represented, even as SOS of formal power series whose coefficients are allowed to take irrational values; in fact, a low order coefficient must jump at $(X^2 + Y^2)^2$. Finally, we indicate why we suspect that psd binary forms *can* be continuously represented as SOS of forms (but with irrational coefficients).

Chapter II contains a proof of a "Finiteness Theorem for Open S.a. Sets," conjectured by Brumfiel ("Unproved Proposition" 8.1.2 of [1979]): An open s.a. set F is a finite union of U's (see p. 5). In other words, we can define F entirely by *strict* inequalities (using finite unions and intersections but no complements). Taking complements and distributing, we get equivalently, that a closed s.a. set is a finite union of W's. The Theorem would be trivially true if the word "finite" were omitted; hence the name "Finiteness Theorem." An extensive theory of s.a. sets is developed in Chapter 8 of [Brumfiel 1979] without this theorem. "It would be nice to have a simple proof of 8.1.2 right at the beginning. On the other hand, all the results we will prove in order to circumvent 8.1.2 are results we would want anyway."

The statement of the theorem is deceptively simple for s.a. sets in R^1, and deceptively difficult for sets in $R^n, n \geq 2$. Our proof proceeds by (1) giving a more delicate analysis of the case $n = 1$ (with paramaters), and (2) using the "Good Direction Lemma," for a straightforward (and occasionally a "straightbackward" (cf. proof of 2.7)) algebraic proof by induction.

We later learned that this theorem had recently been proved in two other papers: first, M. and M. F. Coste [1979] derived it as a consequence of Efroymson's Separation Lemma [1976]. Bochnak and Efroymson [to appear] adapted to the polynomial case Lojasiewicz's [1965][19] proof without induction, using the Hörmander-Lojasiewicz inequality.

We apply the Finiteness Theorem to the (closed, s.a.) cone P_{nd} during the proof of the continuous solution to the 17th Problem. Later (Theorem 3.3) we make a finer analysis of P_{nd} by showing that it is a *single* W precisely when $d = 2$; this has consequences for certain types of SOS-representations (Corollary 3.4).

The Finiteness Theorem is also an improvement of the Tarski-Seidenberg Theorem: if a closed s.a. set F is defined by an elementary formula, the Tarski-Seidenberg algorithm eliminates its quantifiers (showing that F is s.a) but leaves a mixture of both relations, $<$ and $\leq$, *obscuring* the fact that F is closed; the Finiteness Theorem eliminates the quantifiers but leaves only the $\leq$ relation (and no negations), *revealing* the fact that F is closed. This qualitative improvement of the Tarski-Seidenberg Theorem is more satisfying than the (basically unsuccessful attempts at) quantitative improvements given in recent years (e.g. by Collins [1974] and Monk [1975]) expressed in terms of the (still large) amount of time and space needed to carry out the elimination. Indeed, Fischer and Rabin [1974] have shown that every decision method, deterministic or non-deterministic, for the elementary theory of real closed fields has a

[19] On p. 68 of [1965]; for a translation from the French into English, see [Hironaka 1975b].

maximum computing time which dominates 2^{cN}, where N = length of the input formula and c is some positive constant, and is therefore unfeasible given the current speed of computers. On the other hand, an efficient *description* of the elimination procedure is possible, and has been given by Cohen [1969].[20]

Our history has focused on the bounds and constructivity results that have been obtained for Hilbert's original problem. However, a large literature on other aspects of the problem has developed, and we now mention enough references to guide the interested reader into these areas. Bochnak and Efroymson [to appear] cover the current knowledge of SOS of C^∞ functions, Nash functions (real analytic algebraic functions), and real analytic functions. They generalize both Stengle's and Pfister's Theorems to certain subrings of the ring of Nash functions on open s.a. subsets of irreducible nonsingular algebraic sets in $\mathbf{R}^n$. They consider both global functions and germs of functions. They similarly generalize Procesi's [1978] representation of symmetric psd functions to Nash functions invariant under a Lie group action on $\mathbf{R}^n$. One of the problems they suggest (p. 23) is to find a psd C^∞ function of one variable which is not a SOS in $C^\infty(\mathbf{R})$; this had been solved by P. Cohen (see p. 25 of [Brumfiel 1979]). (The study of SOS of real algebraic functions was initiated by Artin [1927].)

Lam [1980] gives a bibliography on the 17$^{\text{th}}$ Problem, including references to a non-commutative generalization of the problem, a p-adic analog, and a generalization to psd symmetric matrices over polynomial rings. Pfister [1976]

---

20 This has been reproduced in Efroymson [1974] and the appendix of [Brumfiel 1979].

also gives historical references. We shall not try to duplicate here these three main bibliographies, but instead conclude with some references not included in these bibliographies.

Berg, Christenson, and Ressel [1976] studied positive definite functions on Abelian semigroups, and approximated definite polynomials by SOS of polynomials, of not necessarily (and usually necessarily not) bounded degrees. Bose [1976] gave algorithms to test polynomials for psd-ness. Ellison [1969] considered a "Waring's problem" for forms. Gorin [1961] showed that

$$(XY-1)^2+Y^2$$

is strictly definite on R^2 but has infimum $=0$ on R^2 (of course, it *does* have a zero on the line at infinity). Dickmann [1980] characterized definite polynomials over "real closed rings."

CHAPTER II:

A FINITENESS THEOREM FOR OPEN S.A. SETS

Throughout this chapter, $X = (X_1, \ldots, X_n)$, and $x = (x_1, \ldots, x_n) \in R^n$.

Theorem 2.1 (the Finiteness theorem): *If $S \subseteq R^n$ is s.a., then*

(a) S is open if and only if $S = \bigcup_i U\{g_{ij}\}$, some $\{g_{ij}\} \subseteq K[X]$; equivalently,

(b) S is closed if and only if $S = \bigcup_i W\{g_{ij}\}$, some $\{g_{ij}\} \subseteq K[X]$.

If K is computable, the g_{ij} are computable from the presentation of S as a s.a. set.

There is a trade-off in complexity between polynomials and s.a. functions: s.a. functions are complicated while polynomials are simple. But while representing S as a union of U's of polynomials as in the Theorem is complicated, representing S as a "union" of U's of s.a. functions is simple: $S = U\{\text{dist}(X, R^n - S)\}$, where $U\{f\}$, for f s.a., has the obvious definition.

Corollary 2.2: *A s.a. set S is relatively open in a s.a. set $T \subseteq R^n$ if and only if $S = T \cap \bigcup_i U\{g_{ij}\}$, and similarly with "closed" and "W" in place of "open" and "U."*

Proof of 2.2 from 2.1: $S = T \cap U\{\text{dist}(X, T - S)\}$, and $U\{\text{dist}\ (X, T - S)\}$ is open (and s.a.; see also 8.13.12 of [Brumfiel 1979]) in R^n,[1] hence it is a union

[1] Proof: for *any* non-empty set S (s.a. or not), $\text{dist}(X, S)$ is a (uniformly) continuous function of X, since it is the infimum of the equicontinuous family of functions $\{\text{dist}(X, y) \mid y \in S\}$.

of U's by 2.1. Q. E. D.

The projective analogue of the Theorem may be formulated in terms of cones, i.e. sets S in R^n such that $x \in S \rightarrow cx \in S, \forall c > 0$.

Corollary 2.3: *If the S in the Theorem is also a cone, then we may take the $\{g_{ij}\}$ to be homogeneous.*

Proof of 2.3 from 2.1: We may assume that S does not contain the origin, for otherwise by openness, $S = R^n = U\{1\}$. Thus

$$S = R^+ \cdot \bigcup_{\substack{1 \leq k \leq n \\ l=0,1}} [S \cap Z\{X_k - (-1)^l\}].$$

Identifying $Z\{X_k - (-1)^l\}$ with $Z\{X_k\}$, apply 2.1 to each $S \cap Z\{X_k - (-1)^l\}$ to write it as $\bigcup_i U\{g_{klij}\}$, with $\{g_{klij}\} \subseteq K[X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n]$. Homogenize the g_{klij} by multiplying their monomial terms by suitable powers of X_k. Then $R^+ \cdot [S \cap Z\{X_k - (-1)^l\}] = U\{(-1)^l X_k\} \cap \bigcup_i U\{g_{klij}\}$, so that S is the union over k and l of such unions of U's of homogeneous polynomials. Q. E. D.

Proof of 2.1: For $R^n \supseteq S$ s.a., define dim $S = \max\{m \in \mathbb{N} \mid S$ contains a (s.a.) homeomorphic image of a non-empty open s.a. subset of $R^m\}$ if $S \neq \emptyset$; define dim $\emptyset = -1$. (Cf. §§8.9–10 of [Brumfiel 1979] for invariant definitions of dimension.) Let $X' = (X_1, \ldots, X_{n-1})$ and $x' = (x_1, \ldots, x_{n-1}) \in R^{n-1}$. We shall prove 2.1 with the help of a stratification lemma (2.7) whose proof requires

Lemma 2.4 (The Good Direction Lemma): *If T is s.a. and nowhere dense in*

R^n (equivalently, dim $T < n$), then there exists $v \in S^{n-1}$ (the unit sphere in R^n) such that, writing $\Pi_v: T \to R^{n-1}$ for projection in the v direction into any subspace complementary to $R \cdot v$, we have $\forall x' \in R^{n-1}$, $\Pi_v^{-1}(x')$ is a discrete set. In fact, the other v (the "bad" v) form a set of dim $< n-1$ in S^{n-1}.

Remark: It makes no difference which complementary subspace we use.

Corollary 2.5: *dim $\Pi_v T$ =dim T for good v.* (Q. E. D.)

Proof of 2.4: For a "transcendental" proof, we could observe that the Lemma is an elementary statement which is true for the case $R = \mathbf{R}$,[2] and thus is true for all real closed R, by Tarski-Seidenberg.

For an elementary algebraic proof, let $v_n = (0, \ldots, 0, 1) \in S^{n-1}$, and suppose the set of bad directions contains a non-empty (relatively) open set $U \subseteq S^{n-1}$. We shall show that T must then contain a non-empty open set, contrary to hypothesis. We may assume $U \cap U\{X_n\} \neq \emptyset$. If we replace U by $U \cap U\{X_n\}$, then (1) we may identify U with $\Pi_{v_n} U$ (used at the end of the proof), and (2) simultaneously $\forall v \in U$, set $S_v = \{\, x' \in R^{n-1} \mid \Pi_v^{-1}(x')$ is not discrete$\}$. Then the hypothesis of the following Lemma is satisfied:

Lemma 2.6 ("s.a. choice function"): *Let $U \subseteq R^n$ be s.a. and $\forall v \in U$ let $\emptyset \neq S_v \subseteq R^m$ (some m) be s.a., described by a bounded number of polynomials of bounded degrees, in some fixed sequence. Furthermore, assume that the coefficients (in some order) of these polynomials are s.a. functions of v.*

[2] (see, e.g. [Hironaka 1975a] for a proof; in fact, when $R = \mathbf{R}$, the Lemma is true even for T semi-analytic)

Then we may construct a s.a. "choice function" $c: U \to R^m$ such that $\forall v \in U$, $c(v) \in S_v$.

Proof of 2.6: Induction on m. For $m = 1$, write $S_v = \bigcup_i I_i$ where $\{I_i\}$ = the connected components (which depend on v) of S_v, i.e. disjoint intervals in R^1, possibly infinite, open, or closed, some just points. Let I be the left-most interval. Then we may define c by

$$c(v) = \left\{ \begin{array}{c} 0 \text{ if } I = R^1 \\ a - 1 \text{ if } \bar{I} = (-\infty, a] \\ a + 1 \text{ if } \bar{I} = [a, \infty) \\ \text{midpoint of } I \text{ if } I \text{ bounded or a point} \end{array} \right\}$$

(c is s.a. by Tarski-Seidenberg).

For $m > 1$, let $\Pi'_v: S_v \to R^1$ be projection onto the first coordinate. By the inductive hypothesis, we define $c_1: U \to R^1$ such that $c_1(v) \in \text{im } \Pi'_v$, and $c_2: U \to R^{m-1}$ such that the map $c: U \to R^m$ given by $c(v) = (c_1(v), c_2(v))$ has the required properties. This proves 2.6. Q. E. D.

Returning to the proof of 2.4, apply 2.6. For all $v \in U$ write $\Pi_v^{-1}(c(v)) = \{ c(v) + tv \mid t \in I(v) \}$, thereby defining $I(v) \subseteq R$. Let $\{I_i(v)\}$ be the connected components of $I(v)$, i.e. points or intervals. Let $I_1(v)$ be the left-most of those intervals which are not points ($I_1(v)$ exists by hypothesis). Let $e_1(v) < e_2(v)$ be the endpoints (possibly $\pm\infty$) of $I_1(v)$.

Shrinking U if necessary, we may assume, since c is s.a., that c is a certain real root of a fixed Y-irreducible polynomial $f \in K[X'][Y]$, i.e. $f(x', c(x')) = 0 \quad \forall x' \in U$ (identifying U with $\Pi_{v_n} U$). Shrinking U again, e_1 and e_2 are either constantly $\pm\infty$, or are also roots of such polynomials. By the implicit function theorem (proved algebraically in 8.7.2 of [Brumfiel 1979]), c is C^1 off the discriminant locus $\Pi_{v_n} Z\{f, \partial f/\partial Y\} = Z\{\text{resultant of } f, \partial f/\partial Y\} \subseteq R^{n-1}$ of f. Similarly e_1 and e_2 are C^1 on a dense open subset. Therefore shrinking U one more time, we construct an open interval $I \neq \emptyset$ such that $\forall v \in U$, $I \subseteq I_1(v)$. We therefore have a C^1 map $p: U \times I \to T$ defined by $p(x', t) = c(x') + t \cdot (x', 1) = \big(c_1(x') + tx_1, \ldots, c_{n-1}(x') + tx_{n-1}, t\big)$. The derivative of p is

$$dp = \begin{bmatrix} \frac{\partial c_1}{\partial x_1} + t & \frac{\partial c_1}{\partial x_2} & \cdots & \frac{\partial c_1}{\partial x_{n-1}} & x_1 \\ \frac{\partial c_2}{\partial x_1} & \frac{\partial c_2}{\partial x_2} + t & \cdots & \frac{\partial c_2}{\partial x_{n-1}} & x_2 \\ \vdots & \vdots & & \vdots & \vdots \\ \frac{\partial c_{n-1}}{\partial x_1} & \frac{\partial c_{n-1}}{\partial x_2} & \cdots & \frac{\partial c_{n-1}}{\partial x_{n-1}} + t & x_{n-1} \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

For any fixed $x' \in U$, $|dp_{(x',t)}| = |dc_{x'} + tI_{n-1}|$ (here $I_{n-1} =$ the $(n-1) \times (n-1)$ identity matix), and for all but a discrete set of t, this determinant is $\neq 0$. Therefore, except at those t, p is locally onto (i.e. im p, hence T, contains a non-empty open set), by the inverse function theorem (proved algebraically in §8.13 III of [Brumfiel 1979]). This completes the algebraic proof of 2.4. Q. E. D.

We now continue the proof of 2.1 by introducing a "topographic stratification" (2.7) of s.a. sets; to state it, we need the following notation. For $0 \leq m \leq n$, write $X' = (X_1, \ldots, X_m)$, $x' = (x_1, \ldots, x_m) \in R^m$, and let $\Pi_m: T \to R^m$ be projection onto the first m coordinates, i.e. $x \mapsto x'$. $U = \sqcup_i T_i$ will mean that $U = \bigcup_i T_i$ and that the T_i are disjoint s.a. sets.

Lemma 2.7 (Topographic Stratification): *Let $0 \leq \dim T \leq m \leq n$ and let $\Pi_m: T \to R^m$ be projection onto the first m coordinates. Then we may choose the last $n-m$ coordinates so that*

(a) $\dim \Pi_m T = \dim T$,

(b) $\Pi_m T = \sqcup_i T_i$, *some* T_i *such that*

(c) $$\left[\begin{array}{l} \bigwedge_i \text{ there exists } J_i \subseteq \mathrm{N}^{n-m} \text{ such that for } j \in J_i \text{ and } m < k \leq n, \\ \text{there is a s.a. function } c_{ijk}: T_i \to R \text{ with, } \forall x' = (x_1, \ldots, x_m) \in T_i, \\ \qquad \Pi_m^{-1}(x') = \{ (x', c_{i,j,m+1}(x'), \ldots, c_{ijn}(x')) \mid j \in J_i \}. \end{array}\right].$$

Remark: It will be evident from the proof of 2.7 that we may further arrange that if $j = (j_{m+1}, \ldots, j_n)$ and $j' = (j_{m+1}, \ldots, j_l, j'_{l+1}, \ldots, j'_n) \in J_i$, and $j_{l+1} < j'_{l+1}$, then throughout T_i, $c_{i,j,l+1} < c_{i,j',l+1}$ and for $k \leq l$, $c_{ijk} = c_{ij'k}$. Thus the graphs of the s.a. functions $(c_{i,j,m+1}, \ldots, c_{ijn})$: $T_i \to R^{n-m}$ (for all i, and $\forall j \in J_i$) form a partition of T. Since all s.a. functions are piecewise real algebraic analytic, we could therefore also arrange for each stratum to be a real algebraic analytic manifold of some dimension $\leq \dim T$. The term "topographic" was proposed by Andreotti (*cf.* [Lojasiewicz 1964], footnote 11) to describe a similar situation. Henkin [1960] stated a slightly weaker form of this result; he gave no proof, but indicated how a model theoretic proof could be given. This stratification is also similar to Collin's [1974] cylindrical algebraic decomposition.

Proof of 2.7: We use "reverse induction" on m. The statement is vacuous for $m = n$, so assume it has been established for some $m > \dim T$; we establish it for $m-1$. Using 2.4 with m in place of n, pick a good direction $v \in R^m$ (with non-zero m^{th} coordinate) for $\Pi_m T$ (possible, since $m >\dim T = \dim$

$\Pi_m T$), and adjust the X_m-axis so as to be parallel to v. Let $\Pi'_i\colon T_i \to R^{m-1}$ be projection onto the first $m-1$ coordinates (where the T_i are given by the inductive hypothesis). Using Tarski-Seidenberg, write $\Pi'_i T_i = \sqcup_l T_{il}$ such that there exist $p_{il} \in \mathrm{N}$ and s.a. functions $c'_{ilk}\colon T_{il} \to R$ $(1 \le k \le p_{il})$ such that $\forall x'' = (x_1, \ldots, x_{m-1}) \in T_{il}$, $c'_{il1}(x'') < \cdots < c'_{ilp_{il}}(x'')$, and $\Pi'^{-1}_i(x'') = \{(x'', c'_{ilk}(x'')) \mid 1 \le k \le p_{il}\}$. Write $\Pi_{m-1}T = \sqcup_a T'_a$ in such a way that each T_{il} is a union of some of the T'_a; set $I_a = \{(i,l) \in \mathrm{N}^2 \mid T'_a \subseteq T_{il}\}$. By the inductive hypothesis, $\forall x'' \in T'_a$,

$$\Pi^{-1}_{m-1}(x'') = \{(x'', c'_{ilk}(x''), c_{i,j,m+1}(x'', c'_{ilk}(x'')), \ldots, c_{ijn}(x'', c'_{ilk}(x''))) \mid (i,l) \in I_a, 1 \le k \le p_{il}, j \in J_i\}.$$

But this is just the statement of 2.7 for $m-1$, after a change of notation. Q.E.D.

With this stratification procedure we can now prove the main inductive step (2.8) in the proof of 2.1; in fact, taking $T = S$ in 2.8, 2.1(a) follows immediately.

Lemma 2.8: *If $T \subseteq S \subseteq R^n$ are s.a. and S is open, then $T \subseteq \bigcup_i U\{g_{ij}\} \subseteq S$, for some $\{g_{ij}\} \subseteq K[X]$, computable from the presentations of T and S (if K is computable).*

Proof of 2.8: Induction on $m = \dim T$. For $m = -1$, just take $\{g_{ij}\} = \{0\}$. For $m \ge 0$, assume 2.8 has been proved for subsets of S of dim $< m$; we prove it for T. Apply 2.7 to this T and m. Set $\delta(x) = \max\{\delta \mid \bigwedge_{i=1}^n |y_i - x_i| < \delta \to y \in S\}$ ($\delta(x) < \infty$ unless $S = R^n$). We have $T \subseteq \bigcup_i V_i \subseteq S$, where V_i

is

$$\{\, x \mid x' \in T_i \wedge \bigvee_{j \in J_i} \bigwedge_{m<k\leq n} |x_k - c_{ijk}(x')| < \delta\big(x', c_{i,j,m+1}(x'), \ldots, c_{ijn}(x')\big)\,\}.$$

(This uses the fact that $\delta > 0$ throughout S, which is the only consequence of the openness of S that we use.) It would suffice to enclose each V_i in a union of U's contained in S. However, we do not quite achieve this; instead, we shall enclose in a union of U's in S, all but a subset of dim $< m$ of $\Pi_m^{-1}(T_i)$; by the inductive hypothesis, this will prove 2.8.

We need a definition and one more lemma, in which we analyze a parametrized version of 2.1, for the case $n = 1$. The formulation is simplified if we agree that $1 \cdot \infty = \infty$, $(-1) \cdot \infty = -\infty$, $a + \infty = \infty$, and $a - \infty = -\infty$.

Definition: For $A \subseteq R^n$ s.a., we shall call a function $c\colon A \to R \cup \{\pm\infty\}$ *s.a. of degree* $\leq d$ if $A = \sqcup_i A_i$, for some A_i such that $\bigwedge_i$ either

(1) $\forall x \in A_i, c(x) = \infty$, or $\forall x \in A_i, c(x) = -\infty$, or

(2) $\left[\begin{array}{c} \exists k \in \mathrm{N} \text{ and } \exists P_i \in K[X,Y] \text{ of } Y\text{-degree } \leq d, \text{ such that } \forall x \in A_i, \\ P_i(x,Y) = 0 \text{ has a finite and constant number } j_i \\ \text{of real roots } c_{i1}(x) < \cdots < c_{ij_i}(x), \text{ and } c(x) = c_{ik}(x). \end{array}\right]$

Lemma 2.9: *If $c\colon A \to R \cup \{\pm\infty\}$ is s.a. of degree $\leq d$, and $C = \{\,(x,y) \mid x \in A \wedge y > c(x)\,\}$, then we may construct $\{g_{ijk}\} \subseteq K[X,Y]$ and A_i such that $A = \sqcup_i A_i$ and $C = \bigcup_i [(A_i \times R) \cap \bigcup_j U\{g_{ijk}\}]$.*

Proof of 2.9: Induction on d. For $d = 0$, take, for $i = 0, 1$, $A_i = c^{-1}((-1)^i \cdot \infty)$ and $g_{i11}(X,Y) = (-1)^{i+1}$. For $d > 0$, assume that 2.9 has been proved for s.a. functions of deg $\leq d - 1$, and that c is s.a. of deg $\leq d$, presented as in the Definition. We shall prove it for $c. \bigwedge_i$, for $0 \leq e \leq d$, and for $j = 0, 1$, set

$$A_{iej} = \left\{ x \in A_i \;\middle|\; \begin{array}{l} \text{either } e = 0 \wedge c(x) = (-1)^j \cdot \infty, \\ \text{or } e = \text{ smallest integer s.t. } \dfrac{\partial^{e+1} P_i}{\partial Y^{e+1}}(x, c(x)) \neq 0, \\ \qquad \text{and } (-1)^j \cdot \dfrac{\partial^{e+1} P_i}{\partial Y^{e+1}}(x, c(x)) > 0 \end{array} \right\}.$$

Define $b: A \to R \cup \{\pm\infty\}$ by cases: for i such that $c(A_i) = \pm\infty$, let $b(x) = c(x) \quad \forall x \in A_i$; for the other i, define $b(x)$ throughout each A_{iej} to be the largest root $< c(x)$ of $\partial^{e+1}P_i/\partial Y^{e+1}(x, Y)$ if this exists, and $-\infty$ otherwise. Set

$$B = \left(\bigcup_{\substack{c(A_i)= \\ -\infty}} A_{i01} \times R \right)$$

$$\bigcup \left[\bigcup_{\substack{c(A_i) \subseteq R, \\ \text{all } e,j}} \left[(A_{iej} \times R) \cap U\left\{ (-1)^j \frac{\partial^e P_i}{\partial Y^e} \right\} \right] \bigcap \{ (x, y) \mid x \in A \wedge y > b(x) \} \right].$$

Define $a: A \to R \cup \{\pm\infty\}$ by cases: for i such that $c(A_i) = \pm\infty$, let $a(x) = c(x) \quad \forall x \in A_i$; for the other i, define $a(x)$ throughout each A_{iej} to be the smallest root $> c(x)$ of $\partial^{e+1}P_i/\partial Y^{e+1}(x, Y)$ if this exists, and ∞ otherwise. By calculus, we have $C = B \cup \{ (x, y) \mid x \in A \wedge y > a(x) \}$. By the inductive hypothesis, C can be written in the required form. This proves 2.9. Q. E. D.

Returning to the proof of 2.8, write V_i as a finite union of finite intersections of sets of the form

$$\{ x \mid x' \in T_i \wedge (-1)^l x_k > (-1)^l c_{ijk}(x') - \delta(x', c_{i,j,m+1}(x'), \ldots, c_{ijn}(x')) \}$$

(for $m < k \leq n$, $j \in J_i$, and $l = 0,1$). 2.9 applies to each of these sets (taking $A = T_i$, etc.) to give $\{g_{iruv}\} \subseteq K[X]$ and $T_i = \sqcup_r T_{ir}$ such that $V_i = \bigcup_r [(T_{ir} \times R^{n-m}) \cap \bigcup_u U\{g_{iruv}\}]$ (in fact, $\bigwedge_i$ no more than one of the variables $X_{m+1}, \ldots, X_n$ will occur in any of the g_{iruv}). Each T_{ir}, being s.a., can be written as $\bigcup_s (Z\{f_{irst}\} \cap U\{f'_{irst}\})$, some $\{f_{irst}, f'_{irst}\} \subseteq K[X']$. Therefore $V_i = \bigcup_{r,s} V_{irs}$, where $V_{irs} = [(Z\{f_{irst}\} \cap U\{f'_{irst}\}) \times R^{n-m}] \cap \bigcup_j U\{g_{iruv}\}$. For those r, s such that $\wedge_t f_{irst} = 0$, V_{irs} is evidently a union of U's. For the other r, s, dim $\Pi_m^{-1}(Z\{f_{irst}\} \cap U\{f'_{irst}\}) =$ dim $(Z\{f_{irst}\} \cap U\{f'_{irst}\}) < m$. This, as remarked before the Definition, completes the proof of 2.8 and hence, as remarked before 2.8, completes the proof of 2.1. Q. E. D.

We now can give a quick proof and refinement of Daykin's result (1.3.1), as promised in Chapter I (we use the notation established there, e.g. $X = (X_0, \ldots, X_n)$).

Proposition 2.10: *There exist* $\{g_{iJ}\} \subseteq \mathbb{Q}[C]$, *and* $\{h_{kiJ}\} \subseteq \mathbb{Q}[C;X]$, *and* $s_i \in \mathbb{N}$ $(k = 1,2)$ *such that*

(1) $$\bigwedge_i f(C;X) = \frac{\sum_J g_{iJ}(C) h_{1iJ}(C;X)^2}{f(C;X)^{2s_i} + \sum_J g_{iJ}(C) h_{2iJ}(C;X)^2} \quad \text{and}$$

(2) $$\forall c \in P_{nd} \qquad \bigvee_i \bigwedge_J g_{iJ}(c) \geq 0.$$

Proof: By the Finiteness Theorem, we can write $P_{nd} = \bigcup_i W_i$, where $W_i = W\{g_{ij}\} \subseteq R^{\binom{n+d}{n}}$, for some $\{g_{ij}\} \subseteq \mathbb{Q}[C]$. For each i we apply the Positivstellensatz (1.4.1) to f, which is nonnegative on $W_i \subseteq R^{\binom{n+d}{n}+n+1}$ (we now are viewing $\{g_{ij}\}$ as being in the larger ring $\mathbb{Q}[C;X]$). 2.10 follows immediately, taking the g_{iJ} to be products of the g_{ij}, as usual. Q. E. D.

CHAPTER III:

THE CONTINUOUS, CONSTRUCTIVE SOLUTION

In this chapter we prove our main theorem (3.1). In this chapter and the next, $X = (X_0, \ldots, X_n)$ and $x = (x_0, \ldots, x_n)$.

Theorem 3.1: *There are $s \in \mathbb{N}$ and continuous $\mathbb{Q}$-s.a. functions $a_{ij}: P_{nd} \to R^{m_i}$ such that $\forall c \in P_{nd}$,*

$$f(c;X) = \frac{\sum_j f_1(a_{1j}(c);X)^2}{f(c;X)^{2s} + \sum_j f_2(a_{2j}(c);X)^2}. \tag{3.1.1}$$

Here $m_i = \binom{n+e_i}{n}$ (where $i = 1, 2$, $e_1 = ds + \frac{d}{2}$, and $e_2 = ds$) and f_i is the general form of degree e_i in X; the (integral) coefficients of the polynomials giving the $\mathbb{Q}$-s.a. description of the graphs of the a_{ij} are computable from n and d.

As explained in Chapter I, (3.1.1) easily leads to a representation of $f(c;X)$ as a (SOS) of functions which are continuous simultaneously in c and x, and homogeneous and rational in X, with coefficients which are continuous in c. Therefore this solution is constructive over $\mathbb{R}$, as explained before.

Before proving 3.1, we must first prove the following theorem, which is inspired by two results of Stengle, namely, his s.a. Nullstellensatz [1974] and his proof of his integral homogeneous representation [1979]. Let $Y = (Y_1, \ldots, Y_m)$ be indeterminates, let I be an ideal in $K[X,Y]$, homogeneous in X,[1] and call a relation of the form $f + g + \cdots \in I$, in which all summands are X-homogeneous of the same X-degree, an *X-homogeneous inclusion*.

[1] Here we mean that for all $f \in I$, all X-homogeneous components of f are in I.

Theorem 3.2 (A Homogeneous S.A. Nullstellensatz): *Let $\{g_j\} \subseteq K[Y]$, and let g_J be products of the g_j. For $f \in K[X,Y]$ of X-degree d, if $f(x,y) = 0 \quad \forall (x,y) \in Z\{I\} \cap W\{g_j\}$, then f satisfies an X-homogeneous inclusion*

$$f(X,Y)^{2s} + \sum_J a_J(X,Y)^2 g_J(Y) \in I, \tag{3.2.1}$$

for some $s \in \mathbf{N}$ and $a_J \in K[X,Y]$.

Remark: There are surely stronger homogeneous versions of the s.a. Nullstellensatz.

Proof: Let H be the set of elements f of $K[X,Y]$ satisfying an X-homogeneous inclusion (3.2.1). First we show

(1) If $f \in H$, and $h \in K[X,Y]$ is X-homogeneous, then $fh \in H$;

(2) If $f, h \in H$ have the same X-degree, then $f + h \in H$; and

(3) If $h^{2s} + f + \sum a_J^2 g_J \in I$ is an X-homogeneous inclusion, and if $f \in H$, then $h \in H$.

To verify (1), note that its hypotheses imply that $(fh)^{2s} + \sum (a_J h^s)^2 g_J \in I$ is a homogeneous inclusion, so that the conclusion of (1) holds. To verify (2), write the two given X-homogeneous inclusions as $f^{2s} + \sum a_J^2 g_J \in I$ and $h^{2t} + \sum b_J^2 g_J \in I$. Since for $r = \max(s,t)$,

$$[(f+h)^2 + (f-h)^2]^{2r} = [2f^2 + 2h^2]^{2r} = f^{2s} \sum \alpha_J^2 + h^{2t} \sum \beta_J^2, ~~\in I~~$$

~~is an X-homogeneous inclusion,~~ we have an X-homogeneous inclusion

$$\begin{aligned}[(f+h)^2 + (f-h)^2]^{2r} &+ \sum \alpha_J^2 \sum a_J^2 g_J + \sum \beta_J^2 \sum b_J^2 g_J \\ &= \left(f^{2s} + \sum a_J^2 g_J\right) \sum \alpha_J^2 + \left(h^{2t} + \sum b_J^2 g_J\right) \sum \beta_J^2 \in I;\end{aligned}$$

upon expanding out the binomial on the left, we see that $f+h \in H$.[2] To verify (3), first observe (by factoring) that $(h^{2s}+\sum a_J^2 g_J)^{2q} - f^{2q} \in I$. By hypothesis we have an X-homogeneous inclusion $f^{2q}+\sum b_J^2 g_J \in I$, which now yields the X-homogeneous inclusion $(h^{2s}+\sum a_J^2 g_J)^{2q} - f^{2q} + (f^{2q}+\sum b_J^2 g_J) \in I$, which shows $h \in H$.

We now assume the hypotheses of 3.2 and use our three properties of H to derive from the (possibly inhomogeneous) inclusion $f^{2s}+\sum a_J^2 g_J \in I$ given by Stengle's s.a. Nullstellensatz [1974] the existence of a similar X-homogeneous inclusion. If the lowest degree terms in this inclusion are of X-degree $2sd$ then the necessary inclusion of all X-homogeneous terms of this X-degree in the X-homogeneous ideal I gives the desired relation (here we use $g_J \in K[Y]$). If lower X-degree terms are present, then the X-homogeneous part of each a_J of lowest X-degree p, call it $(a_J)_p$, must satisfy the inclusion $\sum (a_J)_p^2 g_J \in I$. By definition of H, for each J we conclude $(a_J)_p g_J \in H$ by multiplying this inclusion by g_J (using (1)). For $p < k < sd$ suppose, as induction hypothesis, that the homogeneous parts $(a_J)_p g_J, \ldots, (a_J)_{k-1} g_J$ belong to H.[3] Then extraction of terms of X-degree $2k$ gives the X-homogeneous inclusion:

$$\sum_J (a_J)_k^2 g_J + \sum_J g_J \sum_{l>0} (a_J)_{k+l}(a_J)_{k-l} \in I.$$

By the hypotheses and (1) and (2), this has the form $\sum (a_J)_k^2 g_J + h \in I \quad (h \in$

[2] Stengle raised this binomial to the power $2r+1$ on p. 34 of [1979]; it appears that this is unnecessarily high, and that $2r$ will do.

[3] It is from this point on that our proof of 3.2, in multiplying by g_J, is a little subtler than Stengle's.

H). Hence, multiplying by g_J and using (3), we see that each $(a_J)_k g_J \in H$. Also the same argument applied to the terms of X-degree $2sd$ shows that first the $(a_J)_{sd} g_J$ (all J) and then f belong to H. This is 3.2. Q. E. D.

Proof of 3.1: The proof is a kind of partition of unity argument to glue together (by averaging) locally smooth representations given by the Positivstellensatz (1.4.1). Use Corollary 2.3 of the Finiteness Theorem to write $P_{nd} = \bigcup_{i \in I} W_i$, where $W_i = W\{G_i\}$, with each G_i a set of homogeneous polynomials in $\mathbf{Z}[C]$.[4] Construct s.a. retractions $r_i: U_i \to W_i$, where U_i is a s.a. (regular) relatively open neighborhood of W_i in P_{nd}; this is done by (1) applying to W_i Hironaka's [1975a] Triangulation Theorem: given a bounded s.a. set $S \subseteq R^n$, there exists a simplicial decomposition $R^n = \bigcup_a \Delta_a$ and a s.a. homeomorphism h of R^n with itself such that S is a finite union of some of the $h(\Delta_a)$;[5] (2) using the fact that any subcomplex is a s.a. (in fact, piecewise-linear) neighborhood retract, and (3) transporting via h this piecewise-linear retraction to the desired retraction onto W_i. These retractions, with the help of the following "cut-off" functions, will help us cross smoothly (in the non-technical sense) over the junction points between different W_i.

---

4 As noted in Chapter I, Daykin's [1960] representation (1.3.1) also leads to this W-representation.

5 Hironaka states his theorem for bounded S, while our W_i are unbounded. There are several ways to overcome this. Hironaka remarks (1.10 in [1975a]) that we have a real algebraic embedding of $\mathbf{R}^n$ into some $\mathbf{R}^N$ (*via* $\mathbf{R}P^N \subseteq R^N$) which maps every s.a. set in $\mathbf{R}^n$ to a bounded s.a. set in $\mathbf{R}^N$. Alternatively, one could triangulate the intersection of the cones W_i with the unit sphere in $R^{\binom{n+d}{n}}$ and proceed in a natural way, choosing G_i to be homogeneous as in (2.3).

For all non-empty subsets I' of the index set I of i, define a cut-off function $d_{I'}: P_{nd} \to R^+$ by $d_{I'}(c) = \mathrm{dist}(c, P_{nd} - V_{I'})$, where $V_{I'} = \left(\bigcup_{i \in I'} W_i\right) \cap \bigcap_{i \in I'} U_i$; note that this is well-defined, i.e. we do not have $\mathrm{dist}(c, \emptyset)$, except in the trivial case where $\bigcap_{i \in I'} U_i = P_{nd}$.[6] Clearly, $d_{I'}^{-1}((0,\infty)) = \text{rel int } V_{I'}$. While rel int $V_{I'}$ may be empty for some I', nevertheless $D(c) = \sum_{I' \subseteq I} d_{I'}(c)^2 > 0 \quad \forall c \in P_{nd}$, since $\forall c\, \exists I'$ such that $c \in \text{rel int } V_{I'}$ (namely, set $I' = \{\, i \in I \mid c \in W_i \,\}$). As mentioned in the proof of 2.2, distance is s.a. and continuous in c.

Assign degree $\frac{d}{2}$ to a new indeterminate T and regard $T^2 + f(C;X)$ and G_i as being in (the graded ring) $\mathbf{Z}[C;X,T]$. By the definition of W_i,

$$\bigwedge_i \quad Z\{T\} \supseteq Z\{T^2 + f(C;X)\} \cap W_i \subseteq R^{\binom{n+d}{n}+n+2}. \tag{3.1.2}$$

Apply the homogeneous s.a. Nullstellensatz (3.2) to (3.1.2), with Y of 3.2 replaced by C of (3.1.2), with X of 3.2 replaced by (X,T) of (3.1.2), and with $\{g_j\}$ of 3.2 replaced by G_i of (3.1.2). Then $\bigwedge_i T$ satisfies an (X,T)-homogeneous inclusion

$$T^{2s_i} + \sum_J A_{iJ}(C;X,T)^2 g_{iJ}(C) = B_i(C;X,T)\big(T^2 + f(C;X)\big), \tag{3.1.3}$$

for some $s_i \in \mathbf{N}$, and $A_{iJ}, B_i \in \mathbf{Q}[C;X,T]$. In other words, there are continuous functions $b_{iJ}: W_i \to R^{m_{1i}}$ and $b_i: W_i \to R^{m_{2i}}$ such that

$$T^{2s_i} + \sum_J F_{1i}\big(b_{iJ}(c);X,T\big)^2 = F_{2i}\big(b_i(c)X,T\big)\big(T^2 + f(C;X)\big); \tag{3.1.4}$$

---

[6] This pathology can easily be avoided by choosing any U_i a little smaller, unless $\bigcap_{i \in I'} W_i = P_{nd}$, which is then the easiest possible case: then each piece $W_i = P_{nd}$, so that we shall have, by 2.10 without the index i (i.e. with $|I| = 1$), a continuous, *polynomially* varying representation. Alternatively, we shall see in Theorem 3.3 that $P_{nd} = W_i$ implies $d \leq 2$, in which case we can get an even better representation (Theorem 4.1) as a continuous SOS of *linear forms*.

here $m_{li} = \binom{n+1+e_{li}}{n+1}$ (where $l = 1, 2$, $e_{1i} = ds_i/2$, and $e_{2i} = ds_i - d$), and $F_{li} \in \mathbf{Z}[C_{li}; X, T]$ is the general form of degree e_{li} in (X, T) with coefficients C_{li}; i.e. $F_{li}(C_{li}; X, T) = \sum_{|(a, a_{n+1})| = e_{li}} C_{li;(a,a_{n+1})} X^a T^{a_{n+1}}$.

So far we have for each i an identity valid only for c in W_i. Replacing each occurrence of c with $r_i(c)$, the identity is now defined throughout U_i. For fixed non-empty $I' \subseteq I$, take the product over $i \in I'$ of each side:

$$\prod_{i \in I'} \left[T^{2s_i} + \sum_J F_{1i}\big(b_{iJ}(r_i(c)); X, T\big)^2 \right] = \prod_{i \in I'} \left[F_{2i}\big(b_i(r_i(c)); X, T\big)\big(T^2 + f(r_i(c); X)\big) \right].$$

This identity is valid for $c \in \bigcap_{i \in I'} U_i$; it becomes valid throughout P_{nd} after we multiply each side (i.e. the coefficients of each monomial in (X, T) of the expansion of each side) by $d_{I'}(c)^2$, since $d_{I'}$ vanishes outside $\bigcap_{i \in I'} U_i$. We shall make a convex combination of these identities, but for this they must all have the same degree (in (X, T)); in fact, we can make them all homogeneous of (X, T)-degree $ds = d \sum_{i \in I} s_i$ by multiplying each identity by an even power of T, say $T^{2s_{I'}}$. Now sum over I' and divide by $D(c) > 0$:

$$\frac{1}{D(c)} \sum_{\emptyset \neq I' \subseteq I} T^{2s_{I'}} d_{I'}(c)^2 \prod_{i \in I'} \left[T^{2s_i} + \sum_J F_{1i}\big(b_{iJ}(r_i(c)); X, T\big)^2 \right]$$
$$= \frac{1}{D(c)} \sum_{\emptyset \neq I' \subseteq I} T^{2s_{I'}} d_{I'}(c)^2 \prod_{i \in I'} \left[F_{2i}\big(b_i(r_i(c)); X, T\big)\big(T^2 + f(r_i(c); X)\big) \right].$$

This simplifies to

$$T^{2s} + \sum_k F'_1\big(b'_{1k}(c); X, T\big)^2 = \frac{1}{D(c)} \sum_{\emptyset \neq I' \subseteq I} d_{I'}(c)^2 F'_{2,|I'|}\big(b'_{2I'}(c); X, T\big) \prod_{i \in I'} \big(T^2 + f(r_i(c); X)\big),$$

for some new continuous, s.a. functions $b'_{1k}: P_{nd} \to R^{m'_1}$ and $b'_{2I'}: P_{nd} \to R^{m'_{2,|I'|}}$, where $m'_1 = \binom{n+1+e'_1}{n+1}$ and $m'_{2,|I'|} = \binom{n+1+e'_{2,|I'|}}{n+1}$ (here $e'_1 = ds/2$, and $e'_{2,|I'|} = ds - d|I'|$) and F'_1 [resp. $F'_{2,|I'|}$] is the general form of degree e'_1 [resp. $e'_{2,|I'|}$] in (X,T).

We now carry out step by step Stengle's proof of his Positivstellensatz. Separate the even from the odd powers of T as follows:

$$T^{2s} + \sum_k \left[F'_1(b^e_{1k}(c); X, T^2) + TF'_1(b^o_{1k}(c); X, T^2)\right]^2$$

$$= \frac{1}{D(c)} \sum_{I'} d_{I'}(c)^2 \left[F'_{2,|I'|}(b^e_{2I'}(c); X, T^2) + TF'_{2,|I'|}(b^o_{2I'}(c); X, T^2)\right] \prod_{i \in I'} \left[T^2 + f(r_i(c); X)\right],$$

some new continuous b^e_{ik}, b^o_{ik}, $b^e_{2I'}$, $b^o_{2I'}$. Expand, extract the even part of T, and replace T^2 by a new indeterminate U (assigned degree d):

$$U^s + \sum_k \left[F'_1(b^e_{1k}(c); X, U)^2 + UF'_1(b^o_{1k}(c); X, U)^2\right]$$

$$= \frac{1}{D(c)} \sum_{I'} d_{I'}(c)^2 F'_{2,|I'|}(b^e_{2I'}(c); X, U) \prod_{i \in I'} \left[U + f(r_i(c); X)\right].$$

We may assume s is odd, since multiplying both sides by U, if necessary, gives us an equation of the same form. Let us accordingly replace s by $2s+1$. Replacing U by $-f(c;X)$ causes each summand of the right hand side to vanish identically in (c, X, U); indeed, given c, for each I' with $d_{I'}(c) > 0$, there exists $i \in I'$ with $c \in W_i$ (by definition of $d_{I'}$), so that $r_i(c) = c$ (since r_i is a retraction onto W_i) and hence the factor corresponding to i vanishes. So we have

$$-f(c;X)^{2s+1} - f(c;X) \sum_k F'_1(b^o_{1k}(c); X, -f(c;X))^2 + \sum_k F'_1(b^e_{1k}(c); X, -f(c;X))^2 = 0,$$

which is easily converted into (3.1.1). Q.E.D.

We now review the above proof to see how it might be strengthened to prove Conjecture 1.4, that the coefficients of the representation (including the weights) can in addition be chosen as Q-p.r. functions of the given coefficients.

First, the statement of Theorem 3.2 needs no change, and neither does the finiteness theorem. The first (and we shall see, the only) problematic step is the construction of the Q-s.a. retraction $r_i: U_i \cap \mathbb{Q}^{\binom{n+d}{n}} \to W_i \cap \mathbb{Q}^{\binom{n+d}{n}}$. Can a Q-p.r. retraction be found? Or at least can W_i be covered with finitely many closed neighborhoods V_j for which Q-p.r. retractions can be constructed? (for in the latter case we could average as we have already done, and still succeed.) This question is tricky: While any closed s.a. set is a s.a. neighborhood retract (*via* the triangulation homeomorphism h, which surely cannot be made p.r.), it need not be a Q-*p.r.* retract if it has "degenerate" or "thin" points with irrational coordinates. One possibility is that the set could be *empty* over Q; then we do not need to construct a retraction anyway. If the set is not empty over Q, we should make the retraction p.r., or at least be careful to make it take rational points to rational points. There is hope here in the case that the set has dense interior: for example, for $W\{2-X^2\} \cap \mathbb{Q}^1 = [-\sqrt{2}, \sqrt{2}] \cap \mathbb{Q}^1 \subseteq \mathbb{Q}^1$, we have the Q-p.r. (in fact, piecewise-polynomial) retraction $r: (-\sqrt{2} - \epsilon, \sqrt{2} + \epsilon) \cap \mathbb{Q}^1 \to [-\sqrt{2}, \sqrt{2}] \cap \mathbb{Q}^1$, some $\epsilon > 0$, given by

$$r(x) = \begin{cases} x - (2 - x^2) & \text{for } x \in (-\sqrt{2} - \epsilon, -\sqrt{2}) \cap \mathbb{Q}^1, \\ x & \text{for } x \in (-\sqrt{2}, \sqrt{2}) \cap \mathbb{Q}^1, \text{ and} \\ x + (2 - x^2) & \text{for } x \in (\sqrt{2}, \sqrt{2} + \epsilon) \cap \mathbb{Q}^1. \end{cases}$$

(This is the first retraction we have seen which had to "push in" to the interior of the retract and not simply stop at its boundary.) Of course, this method easily extends to cover all closed sets in $\mathbf{Q}^1$, but higher dimensions seem difficult. In our case we *may* restrict our attention to closed s.a. sets with dense interior, since P_{nd} has dense interior (footnote 5 of Chapter I).

Continuing our review of the proof of 3.1, we come next to the (continuous) cut-off functions $d_{I'}: P_{nd} \to R^+$, which had to be positive on the relative interior of $V_{I'}$ and zero elsewhere. The distance function is not p.r., but there is a more complicated way to define a suitable $d_{I'}$ which is p.r.: first use Corollary 2.2 to construct $\{f_{ij}\} \subseteq \mathbf{Z}[C]$ such that rel. int. $V_{I'} = P_{nd} \cap \bigcup_i U_i$, where $U_i = U\{f_{ij}\}$; then let

$$d_{I'}(c) = \sum_{c \in U_i} \prod_j f_{ij}(c),$$

where the summation is over those $i \in I'$ such that $c \in U_i$. $d_{I'}$ *is* continuous, since even when c passes through ∂U_i, the summand corresponding to i is zero. The other properties are likewise obvious. By the way, the Finiteness Theorem plays a more or less indispensible rôle here, in contrast to its usual rôle.

The only remaining source of irrationality in the proof is the transition from (3.1.3) to (3.1.4); but this was a non-essential simplification in the situation where we were allowed to take square roots of nonnegative constants. So in the ordered field version we would keep the weights visible. The rest of the proof is just formal algebraic manipulation, and hence no problem.

We conclude this chapter by proving (3.4) that Conjecture 1.4 becomes false if the word "piecewise" is dropped (except when $d \leq 2$). We do this by first giving a finer analysis of P_{nd} than that given by the Finiteness Theorem:

Theorem 3.3: *P_{nd} is a single W if and only if $d \leq 2$.*

Proof: For the "if" direction, we assume $d = 2$ and use induction on n. For $n = 2$, $P_{22} = W\{A,\ C,\ 4AC - B^2\}$ (writing $f(A, B, C; X, Y) = AX^2 + BXY + CY^2$). To prove P_{n2} is a single W for $n > 2$, we may suppose, inductively, that the condition for a quadratic form in $X_0, \ldots, X_{n-1}$ to be psd is a conjuction of non-strict inequalities in C. Write

$$f(X_0, \ldots, X_n) = f_2(X_0, \ldots, X_{n-1}) + f_1(X_0, \ldots, X_{n-1})X_n + f_0 X_n^2,$$

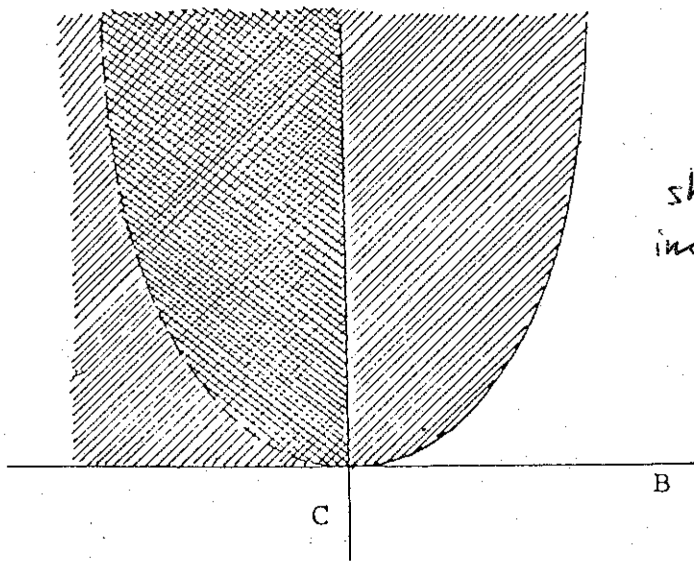
where $\deg f_i = i$ $(i = 0, 1, 2)$. Then f is psd if and only if f_2, f_0, and $4f_0f_2 - f_1^2$ are all psd in $X_0, \ldots, X_{n-1}$; this is just a conjunction of three conjuctions, since these three forms are quadratic (except the constant form f_0, for which the psd property is an "improper" conjunction, namely, with only one conjunct).

For the "only if" part we use *reductio ad absurdum*: If $P_{nd} = W\{g_i(C)\}$, then $P_{24} = W\{g_i(C', 0)\}$ (i.e., we set some of the C equal 0), which gives $W\{g_i(B, C, 0)\} = \{(B, C) \in R^2 \mid X^4 + BX^2Y^2 + CY^4 \text{ is psd}\} =$

$$\{(B, C) \mid \forall x \geq 0, \forall y \geq 0,\ x^2 + Bxy + Cy^2 \geq 0\}$$

$$= \{(B, C) \mid B^2 - 4C \leq 0 \vee -B + \sqrt{B^2 - 4C} \leq 0\}$$

$= W\{4C - B^2\} \cup W\{-B, C\}$. But now we see that this set (striped in the figure below) cannot be written as a single $W\{g_i\}$, since one of the g_i would have to be divisible by (precisely) an odd power of $B^2 - 4C$, which would make it change sign across even the dotted part of the parabola. Q. E. D.



shaded incorrectly

Corollary 3.4: *For $d \leq 2$, Conjecture 1.4 is true even if we drop the word "piecewise." For $d > 2$, not only must we keep the word "piecewise," but also there do not exist $e \in \mathbb{N}, p_j \in K[C]$, and functions (even discontinuous and non-s.a.) a_{ij}: $P_{nd} \to \mathbb{R}^{m_i}$ such that $\forall c \in P_{nd}$*

(1) $$f(c;X) = \sum_j p_j(c) \left[\frac{f_1(a_{1j}(c);X)}{f_2(a_{2j}(c);X)} \right]^2, \text{ and}$$

(2) $$\bigwedge_j [p_j(c) \geq 0 \text{ and, (if } c \neq 0) \; a_{2j}(c) \neq 0 \in K^{m_2}],$$

even if we also allow the rational functions to be discontinuous in X. Here, $m_i = \binom{n+e_i}{n}$ (where $i = 1, 2$ and $e_1 = \frac{d}{2} + e_2$) and f_i is the general form of degree e_i in X.

Proof: For $d = 2$ we just combine 3.3 and the proof of 2.10, with a single W_i, so that we may drop the i.

For $d > 2$, we note that if 3.4 were false, then we could conclude that $P_{nd} = W\{p_j\}$ ($\subseteq$ by (2) and $\supseteq$ by (1)), contradicting 3.3. Q. E. D.

CHAPTER IV:
CONTINUOUS SUMS OF SQUARES OF FORMS

Having analyzed continuity properties of SOS of rational functions, it is natural to focus next on those psd forms which are even SOS of *forms*, namely, (A) the quadratic, (B) the ternary quartic, and (C) the binary psd forms (cf. p. 3), and see whether we can arrange for the continuous variation of their simpler representations. Before giving details, we state the answers, roughly: (A) Yes, (B) No (even for real closed fields), and (C) Probably, at least for real closed fields.

A. Quadratic Forms

Let $\sum C_{ij}X_iX_j$ be the general quadratic form in $X_0,\ldots,X_n$ and write $C = \langle C_{ij}\rangle_{0\le i\le j\le n}$. Set

$$N(n) = (n+1)!\sum_{k=0}^{n}\frac{1}{k!}.$$

Theorem 4.1: *For fixed n and for $0\le l\le n$, $1\le k\le N(n)$, we can construct $p_k,\ a_{kl}\in \mathbb{Q}(C)$ such that*

$$\sum C_{ij}X_iX_j = \sum_{k=1}^{N(n)} p_k(C)\Big(\sum_{l=0}^{n} a_{kl}(C)X_l\Big)^2 \ \textit{and,} \tag{4.1.1}$$

throughout $P_{n2}\times R^{n+1}$,

$$\bigwedge_{k=1}^{N(n)}\left[p_k(c)\ge 0,\ \text{and } p_k(c)\Big(\sum_l a_{kl}(c)x_l\Big)^2 \text{ is continuous in } (c,x)\right]. \tag{4.1.2}$$

Before going through the proof, it is instructive to consider the simplest case, $n = 1$. The usual representation of $aX^2 + bXY + cY^2$, for $a \geq 0$, $c \geq 0$, and $4ac - b^2 \geq 0$, obtained by "completing the square,"

$$a\left(X + \frac{b}{2a}Y\right)^2 + \left(c - \frac{b^2}{4a}\right)Y^2, \text{ or } \left(a - \frac{b^2}{4c}\right)X^2 + c\left(Y + \frac{bX}{2c}\right)^2,$$

is *not* continuous near $(0,0,c)$ $(c > 0)$ [resp., $(a,0,0)a > 0$], since the coefficient $b^2/(4a)$ [resp $b^2/(4c)$] can vary between 0 and c [resp., a]. But suitable convex combinations (by $a/(a+c)$ and $c/(a+c)$) ensure continuity (and the argument extends to any number of variables (see below)):

$$aX^2 + bXY + cY^2 = (a+c)\left[\frac{2aX + bY}{2(a+c)}\right]^2 + \frac{4ac - b^2}{4(a+c)}X^2 + \frac{4ac - b^2}{4(a+c)}Y^2 + (a+c)\left[\frac{bX + 2cY}{2(a+c)}\right]^2.$$

For continuity $(a \geq 0, c \geq 0, 4ac \geq b^2)$ at $(0,0,0)$, note, for example, that $4ac - b^2 \leq 4ac$ and $a \leq a + c$, hence $\frac{(4ac - b^2)}{4(a+c)} \leq c$. On the other hand, $(2aX + bY)/(a+c)$ alone is not continuous there.

Proof of 4.1: Induction on n. For $n = 0$, take $p_1 = C_{00}$ and $a_{10} = 1$.

For $n > 0$ we make use of the representation constructed for $P_{n-1,2}$ to construct the representation for P_{n2}, as follows. We have, for each $c \in R^{\binom{n+2}{2}}$,

$$\bigwedge_{l=0}^{n} \quad \sum c_{ij}X_iX_j = c_{ll}X_l^2 + 2X_l\sum_{i \neq l} c_{il}X_i + q_l(X_l'),$$

where $X_l' = (X_0, \ldots, \hat{X_l}, \ldots, X_n)$, and where $q_l(X_l') = \sum_{i \neq l \neq j, i \leq j} c_{ij}X_iX_j$. We also have $(c_{ij}) \in P_{n2}$ iff, for $0 \leq l \leq n$,

$$c_{ll} \geq 0 \text{ and both } q_l(X_l') \text{ and } d_l(X_l') = c_{ll}q_l(X_l') - \left(\sum_{i \neq l} c_{il}X_i\right)^2 \text{ are psd in } X_l'. \tag{4.1.3}$$

Writing tr $c = \sum c_{ii}$, (4.1.3) implies that if c varies within P_{n2}, then tr $c \to 0$ forces $c \to 0$. For those l such that $c_{ll} \neq 0$, we may complete the square with respect to X_l:

$$\sum c_{ij}X_iX_j = c_{ll}\left(X_l + \frac{\sum_{i \neq l} c_{il}X_i}{c_{ll}}\right)^2 + \frac{d_l(X_l')}{c_{ll}}.$$

We now form the convex combination

$$\sum c_{ij}X_iX_j = \frac{1}{\text{tr } c}\sum_{l=0}^{n}\left[\left(\sum_{i=0}^{n} c_{il}X_i\right)^2 + d_l(X_l')\right]. \tag{4.1.4}$$

Since in P_{n2},

$$\frac{|c_{ij}c_{lm}|}{\text{tr } c} \leq \frac{c_{ij}^2}{\text{tr } c} \leq \frac{c_{ii}c_{jj}}{c_{ii} + c_{jj}} \leq c_{ii} \to 0$$ [1]

as tr $c \to 0$, we conclude that $d_l(X_l')/\text{tr } c$ varies continuously within $P_{n-1,2}$ as c varies in P_{n2}. By the construction for $P_{n-1,2}$, we have d_l represented as a continuous sum of

$$n!\sum_{k=0}^{n-1}\frac{1}{k!}$$

squares of linear forms in X_l' multiplied by positive constants. Therefore (4.1.4) becomes (4.1.1), and $N(n) = (n+1)[1 + N(n)]$, as required. Q. E. D.

[1] Use (4.1.3) to see $c_{ij}^2 \leq c_{ii}c_{jj}$.

As noted in Chapter I, the classical SOS representation (1.1.1) given by the usual diagonalization has discontinuous and only *piecewise*-rational coefficients; however, in 4.1 we were forced to increase the number of summands from n to slightly less than $(n+1)!\,e$.

B. ternary Quartic Forms

We dehomogenize, and prove a "strongest possible" negative answer to the continuity question for the case of ternary quartics.

Proposition 4.2: *Let* $f(C;X,Y) = \sum_{i+j\leq 4} C_{ij}X^iY^j \in \mathbb{Z}[C;X,Y]$ *be the general quartic polynomial in 2 variables,* X *and* Y*, with coefficients* C*; let* $f'(C';X,Y) = \sum_{i,j\geq 0} C'_{ij}X^iY^j \in \mathbb{Z}[[C';X,Y]]$ *be the general formal power series in* X *and* Y*, with coefficients* C'*. Then there do not exist functions* $a_k\colon P_{24} \to R^\omega$ *such that for all* $c \in P_{24}$

(1) $f(c;X,Y) = \sum_k f'(a_k(c);X,Y)^2$ and

(2) for each $(i,j) \in \{(1,0),(2,0),(0,2)\}$*, the* ij*-component*

$(a_k)_{ij}\colon P_{24} \to R$ *of* a_k *is continuous.*

Proof: We show that one of the $(a_k)_{ij}$'s ($(i,j) \in \{(1,0),(2,0),(0,2)\}$) must have a jump discontinuity at $f(\bar{c};X,Y) = (X^2+Y^2)^2$. We shall approach $\bar{c}$ along two paths α and β in P_{24}. Define $\alpha\colon R \to P_{24}$ by $f\big(\alpha(t);X,Y\big) = (X^2 + Y^2 + tX)^2$, and β by $f\big(\beta(t);X,Y\big) = X^2(X+t)^2 + 2X^2Y^2 + Y^4$. Equating coefficients in (1), we see immediately (even without a continuity hypothesis) that $(a_k)_{00}\big(\gamma(t)\big) \equiv 0$, hence $(a_k)_{01}\big(\gamma(t)\big) \equiv 0$ and $\sum_k (a_k)_{10}\big(\gamma(t)\big)^2 = t$ (where we have let γ stand for either α or β). Therefore, first, $\sum_k (a_k)_{10}(\alpha(t))(a_k)_{20}(\alpha(t)) = t$, whence the CBS-inequality implies $\exists\lambda \in R$ s.t.

$$\forall k\ (a_k)_{20}(\alpha(t)) = \lambda \cdot (a_k)_{10}(\alpha(t)). \tag{4.2.1}$$

Second, $\sum_k (a_k)_{10}(\alpha(t))(a_k)_{02}(\alpha(t)) = t$, whence by the CBS-inequality again,

$$\forall k\ (a_k)_{02}(\alpha(t)) = \mu \cdot (a_k)_{10}(\alpha(t)), \tag{4.2.2}$$

some $\mu \in R$. (4.2.1) and (4.2.2) together say that the vector $(a)_{20}(\alpha(0))$ is a constant multiple of $(a)_{02}(\alpha(0))$ (here we need continuity of the $(a)_{ij}$, since $(a)_{10}(\gamma t) \to 0$); but $\sum_k (a_k)_{10}(\beta(t))(a_k)_{20}(\beta(t)) = t$ implies (by CBS) that $(a)_{10}(\beta(t))$ is a multiple of $(a)_{20}(\beta(t))$, and $\sum_k (a_k)_{10}(\beta(t))(a_k)_{02}(\beta(t)) \equiv 0$ implies that $(a)_{10}(\beta(t))$ is not a multiple of $(a)_{02}(\beta(t))$ $(t \neq 0)$, so that $(a)_{20}(\beta(0))$ is not a multiple of $(a)_{02}(\beta(0))$; thus a jump discontinuity has occurred. Q. E. D.

C. Binary Forms

Conjecture 4.3: *Let $f(C;X,Y) = \sum_{i=0}^{d} C_i X^i Y^{d-i}$ be the general binary form of degree d, and similarly let f' be the general binary form of degree $e = d/2$. Then there exist continuous Q-s.a. functions $a_i\colon P_{2d} \to R^{1+d/2}$ $(i = 1, 2)$ such that $\forall c \in P_{2d}$,*

$$f(c;X,Y) = f'(a_1(c);X,Y)^2 + f'(a_2(c);X,Y)^2.$$

4.3 would be obvious if the d roots of $f(c;X,Y)$ in the "complex" projective line $R[i]P$ were not merely locally but also globally continuous functions of

c, for then, factorization over R would yield in the usual way a representation of f as a product of squares and sums of two squares, which can be reduced to a single sum of 2 squares by the 2-square identity. However, the roots of the form $X^2 - cY^2$, for example, cannot be continuously be defined as c wraps around the origin of the complex plane; moreover, it is not much harder to find paths of forms with *real* coefficients whose roots are not definable by globally continuous functions. We could still prove 4.3 if for every c we could define, in a neighborhood of c, d continuous functions giving the roots of $f(c; X, Y)$, for then (ostensibly by a compactness argument, but also on purely algebraic grounds) one could select a finite subcover of the unit sphere in the coefficient-space, and then average the SOS-representations by a partition of unity method as in 3.1.

CHAPTER V:
BAD POINTS AND OTHER RESULTS

A. Bad Sets

1. *Theory*.

Let $X = (X_1, \ldots, X_n)$, let $f \in K[X]$ (K an ordered field), let $\mathfrak{P}_w = \{\,\text{SOS in } K[X]\,\}$ (= "the weak order" in [Brumfiel 1979]), and define $(\mathfrak{P}_w{:}f) = \{\,h^2 \in K[X] \mid h^2 f \in \mathfrak{P}_w\}$. The *set of bad points of* f is defined to be $Z(\mathfrak{P}_w{:}f) \subseteq R^n$, i.e. the set of common zeros of all possible denominators. For indefinite f, $(\mathfrak{P}_w{:}f) = \{0\}$, so the bad set of f is R^n. For any f, there exists $h^2 \in (\mathfrak{P}_w{:}f)$ such that $Z(\mathfrak{P}_w{:}f) = Z\{h^2\}$, for since the ideal $\big((\mathfrak{P}_w{:}f)\big)$ is generated by a finite set of elements of $(\mathfrak{P}_w{:}f)$ (Hilbert Basis Theorem), we may take h to be their sum.

Part of the significance of the bad set of f is that if $f = \sum r_i^2 \quad (r_i \in K(X))$, then all the r_i fail to be regular or smooth (C^∞) throughout the bad set, while r_i's can be chosen which are smooth off the bad set. This is because if $g, h \in K[X]$ and $(g, h) = 1$, then g/h is smooth at the origin iff $h(0) \neq 0$. To see this, suppose $h(0) = 0$ and g/h is smooth at 0. Then over the algebraic closure $R(i)$ of R, g and h have a common factor p which vanishes at 0. Since g (and h) are real, they also have the common factor $\overline{p}$. But now $p\overline{p}$ is a non-constant common factor over R of g and h, implying that g and h have a non-constant common factor over K also, contradiction. The converse is obvious, that is, $h(0) \neq 0$ implies g/h is smooth at 0.

As noted on p. 19, Stengle's Theorem gives $Z(\mathfrak{P}_w{:}f) \subseteq Z\{f\}$. The following Proposition gives another constraint on the size of the bad set:

Proposition 5.1: *If f is psd, then cod $Z(\mathfrak{P}_w{:}f) \geq 3$.*[1]

Proof: We rule out cod $= 0$ by Artin's Theorem. We rule out cod $= 1$ by factoring out all hypersurfaces from the relation $h^2 f = \sum g_i^2$ (hypersurfaces are real varieties of cod 1; they correspond to *principal* ideals, thereby making the factorization possible). Finally, we shall rule out cod $= 2$ with the help of the following

Lemma 5.2 [Cassels 1964]: *For $f \in F[Y]$ (Y an indeterminate, and F any field), if $f = \sum_{i=1}^{m} g_i^2 \quad (g_i \in F(Y))$, then there are $h_i \in F[Y]$ such that $f = \sum_{i=1}^{m} h_i^2$.*

The lemma has been generalized by Pfister [1965] and Gerstein [1973]. We shall use the special case $F = K(X_1, \ldots, X_{n-1})$, which was proved (except for control over the number of summands) by Artin [1927]. The main idea of the proof (an application of the division algorithm) goes back to Landau [1906], who proved it for the slightly more special case $K = \mathbf{R}$ and $n = 2$ (in 1906 there was little motivation to generalize it).

Now suppose cod $Z(\mathfrak{P}_w{:}f) = 2$. Use the Good Direction Lemma (2.4) to adjust the X_n-axis so that dim $\Pi_{X_n}(Z(\mathfrak{P}_w{:}f)) = n - 2$ (where Π_{X_i} is

---

1 Cod $= (n)$ — dim, and dim = maximal dimension of a cell which can be embedded in the set.

projection along the X_i-axis onto a complementary subspace). Use 5.2 to construct from the relation $h^2 f = \sum_i g_i^2$ a new relation $h'^2 f = \sum g_i'^2$ (with $h' \in K[X_i, \ldots, X_{n-1}]$), from which, we may assume, all hypersurfaces have been factored out. Since $Z\{h'\} \supseteq Z(\mathfrak{P}_w{:}f)$, since h' does not involve X_n, and since $\dim \Pi_{X_n}(Z(\mathfrak{P}_w{:}f)) = n-2$, $\dim Z(h') = n-1$, contradiction. This rules out cod $= 2$ and completes the proof of 5.1. Q. E. D.

After proving this, I learned that the special case of $n = 2$ had already been discovered by Choi and Lam [1977a]. In other words, psd polynomials in two variables never have bad points (by convention, only the empty set has $\dim = -1$).

2. *Examples.*

Example 1 (p. 196 of [Brumfiel 1979][2]): For any $n \geq 2$, bad sets of all codimensions ≥ 3 occur. *Proof:* For $n = 2$ there is nothing to show. For $n \geq 3$ construct a psd but inhomogeneous $f \in \mathbb{Z}[X_1, X_2, X_3]$ with lowest degree homogeneous component $\notin \mathfrak{P}_w$ (the last requirement uses $n \geq 3$). $Z(\mathfrak{P}_w{:}f)$ includes any zero x of f such that the homogeneous component of lowest degree in the Taylor expansion of f about x is $\notin \mathfrak{P}_w$, since if $h^2 f = (1 + h_1 + \cdots + h_r)^2 (f_{2s} + f_{2s+1} + \cdots + f_{2t}) = f_{2s} + ((\text{higher degree comp.s})) = \sum g_i^2 = \sum (g_{i,s} + g_{i,s+1} + \cdots + g_{i,s+t})^2$, then $f_{2s} = \sum g_{i,s}^2$. Thus 0 is a bad point of our f. Therefore, since f does not involve $X_4, \ldots, X_n$, the cod 3 subspace

[2] A special case of this example has also appeared in [Choi, Lam, Reznick, and Rosenberg (to appear)] (Proposition 3.5) and [Bochnak and Efroymson (to appear)] (Counterexample 9.1).

spanned by the $X_4, \ldots, X_n$-axes is also included in the bad set.

Example 2 (Brumfiel): Even if the lowest degree component is $\in \mathfrak{P}_w$, 0 can still be bad when $n \geq 4$: construct psd forms $f_{2s} \in \mathbb{Z}[X_1, \ldots, X_m]$ and $f_{2t} \in \mathbb{Z}[X_{m+1}, \ldots, X_n]$ of degrees $2s$ and $2t$, respectively $(1 \leq s < t, 1 \leq m \leq n-3)$ with $f_{2s} \in \mathfrak{P}_w$ and $f_{2t} \notin \mathfrak{P}_w$ (this last uses $m \leq n-3$). Then $s < t$ implies the lower order component of $f_{2s}+f_{2t} \in \mathbb{Z}[X_1, \ldots, X_m, X_{m+1}, \ldots, X_n]$ is in $\mathfrak{P}_w$ but the origin is still a bad point: $(1+h_1+\cdots)^2(f_{2s}+f_{2t}) = \sum g_i^2$ implies (setting $X_1 = \cdots = X_m = 0$ and using $s \geq 1$ and $m \geq 1$) $f_{2s} \in \mathfrak{P}_w$, contradiction.

Example 2 leads to the study of how bad points behave under various maps from R^n to R^m: e.g., the above polynomial $f_{2s} + f_{2t}$ becomes f_{2t} under the projection map from R^n to R^{n-m}; thus here badness of the origin is preserved. All this led to a conjecture that for $n = 3$, if the lowest degree component is a SOS, then 0 is "good." However, we discovered the following counter-

Example 3: $f(X,Y,Z) = Z^6 + X^6Y^2 - 3X^2Y^4Z^2 + Y^{10}$ is psd by the arithmetic-geometric $\leq$: the arithmetic mean of Z^6, X^6Y^2, and Y^{10}, is $\frac{1}{3}(Z^6+X^6Y^2+Y^{10})$; the geometric mean of Z^6, X^6Y^2, and Z^{10} is $X^2Y^4Z^2$. Although the lowest degree component is a SOS (it is a perfect square), the origin is still bad:

$$h^2 f = (1+h_1+h_2+\cdots)^2(Z^6+X^6Y^2-3X^2Y^4Z^2+Y^{10})$$

$$= Z^6 + 2h_1 Z^6 + \left[(h_1^2 + 2h_2)Z^6 + X^6Y^2 - 3X^2Y^4Z^2\right] + ((\text{higher degree comp.s}))$$

$$= \sum_i g_i^2 = \sum_i \left[g_{i3}^2 + 2g_{i3}g_{i4} + (g_{i4}^2 + g_{i3}g_{i5}) + \cdots\right]$$

$$= \sum_i \left[a_i^2 Z^6 + 2a_i Z^3 g_{i4} + (g_{i4}^2 + 2a_i Z^3 g_{i5}) + \cdots\right]$$

(since g_{i3} must be a_iZ^3, some $a_i \in R$) implies (equating eighth degree components)

$$\sum_i g_{i4}^2 = X^6Y^2 - 3X^2Y^4Z^2 + Z^3k_5(X,Y,Z)$$

$[k_5(X,Y,Z) = Z^3(h_1^2+2h_2) - 2\sum a_i g_{i5}]$, which implies (eliminating terms one by one—see the figure below) that no g_{i4} has a Y^4-term, which implies that none has a Y^3Z-term or Y^3X-term, implying that none has X^2Y^2, which implies that $-3 = \sum (a_k)_{121}^2$, an impossibility. Here we wrote

$$g_{i4} = \sum_{\substack{\alpha+\beta+\gamma=4 \\ \alpha,\beta,\gamma\geq 0}} a_{i\alpha\beta\gamma} X^\alpha Y^\beta Z^\gamma.$$

$$\begin{array}{c} 004 \quad 013 \quad 022 \quad \boxed{031}\ \boxed{040} \\ 103 \quad 112 \quad \boxed{121}\ \boxed{130} \\ 202 \quad 211 \quad \boxed{220} \\ 301 \quad 310 \\ 400 \end{array}$$

Figure

This kind of application of the arithmetic-geometric inequality and the method of eliminating terms from a ternary form from the outside of its triangle of coefficients, inward, is due to Choi and Lam [1977a].

The problem of characterizing the bad set is still unsolved.

B. Formal Power Series

We make a simple application of a theorem of M. Artin [1968]:

Theorem 5.3: *Suppose that* $\overline{y}(X) = (\overline{y}_1(X), \ldots, \overline{y}_N(X))$ $(\overline{y}_i(X) \in F[[X]])$ *are formal power series such that* $p(X, \overline{y}(X)) = 0$, *where* $p = (p_1, \ldots, p_m)$ *and* $p_i \in F[X]$ *(F any field). Let* $c \in \mathrm{N}$. *Then there exists an algebraic power series solution* $y(X) = ((y_1(X), \ldots, y_N(X))$ *of the system p such that* $y(X) \equiv \overline{y}(X)$ $(\mathrm{mod}\ \mathfrak{m}^c)$.

Here $\mathfrak{m}$ denotes the maximal ideal of the ring $F[[X]]$.

Corollary 5.4: *If* $f \in F[X]$ *is a SOS of formal power series in* $F[[X]]$ *(F any field), then it is also a SOS of algebraic power series in* $F[[X]]$.

Proof: Take the system $p = (p_1)$ in 5.3 to be

$$p_1(X, y_1, \ldots, y_N) = f(X) - y_1^2 - \cdots - y_N^2.$$

Q. E. D.

While we are on the subject of power series, we mention a question of Brumfiel: If $f \in K[X]$ is psd and a SOS of formal power series, is the origin a good point of f? The converse is obvious.

This Theorem does not lead to an improvement of Heilbronn's Theorem (p. 15), for if we replace his four analytic power series with power series which are algebraic over $\mathbf{Q}$, they will necessarily take irrational values at most positive rational arguments.

C. Symmetric Psd Polynomials

We combine the Positivstellensatz (1.4.1) with the following methods of Procesi [1978]. Let $\psi_i = \sum_{j=1}^{n} X_j^i$ denote the ith Newton function and

$$A = \begin{bmatrix} \psi_0 & \psi_1 \cdots & \psi_{n-1} \\ \psi_1 & \psi_2 \cdots & \psi_n \\ \vdots & \vdots & \vdots \\ \psi_{n-1} & \psi_n \cdots & \psi_{2n-2} \end{bmatrix},$$

the (so-called) Bézoutiant matrix. Let g_j be the determinant of the minor formed by the first j rows and columns of A. Procesi revived Sylvester's version of Sturm's Theorem and showed that im S, where $S: R^n \to R^n$ is $(x_1, \ldots, x_n) \mapsto (\sigma_1(x), \ldots, \sigma_n(x))$ (where $\sigma_1, \ldots, \sigma_n$ are the elementary symmetric functions in $X_1, \ldots, X_n$), equals $W\{g_i\}$. Now if $f \in K[X]$ is symmetric, then we may construct $f' \in K[X]$ such that $f = f' \circ S$. And if f is also psd, then f' is ≥ 0 on im $S = W\{g_i\}$. Then Procesi applied Robinson's [1955] representation (1.2.1) to f' and $\{g_i\}$ to obtain immediately a symmetric (positively weighted) SOS-representation; we only add the observation that Stengle's Positivstellensatz (1.4.1) may be applied instead to obtain just as easily the following improvement of Procesi's representation:

Theorem 5.5: *If $f, f' \in K[X]$ with f symmetric and $f = f' \circ S$, and if f is psd, then*

$$f' = \frac{\sum_J c_{1J} g_J h_{1J}^2}{f'^{2s} + \sum_J c_{2J} g_J h_{2J}^2}, \tag{5.5.1}$$

for some $c_{iJ} \in K$ and $h_{iJ} \in K[X]$, where the g_J are, as usual, products of the (above) g_j. To get a (symmetric) representation of f, compose both sides of (5.5.1) with S. By construction, the $g_J \circ S$ are psd (and symmetric), though they are not here expressed as SOS themselves.

In the statement (but not the proof) of his Theorem, Procesi did not mention the need to compose his representation with S.

D. Filters and Partial Orders

In this section we use Stengle's Positivstellensatz (one more time) to clarify and generalize Brumfiel's Proposition 8.11.1 [1979]. We first review some of Brumfiel's notation. By a *partial ordering* (or, from now on, simply, an *ordering*) on the ring A (commutative, with unit), we mean a subset $\mathfrak{P} \subseteq A$ satisfying

(1) $\mathfrak{P} \cap (-\mathfrak{P}) = \{0\}$,

(2) $\mathfrak{P} + \mathfrak{P} \subseteq \mathfrak{P}$ and $\mathfrak{P} \cdot \mathfrak{P} \subseteq \mathfrak{P}$, and

(3) $A^2 \subseteq \mathfrak{P}$.

$\mathfrak{P}_w$, the "weak" order (introduced in 5A), is the smallest order on A, namely, the set of SOS. $\mathfrak{P}_w[g_i]$ is the smallest order on A containing $\{g_i\} \subseteq A$. For an order $\mathfrak{P}$, we write $\mathfrak{P}_d = \{ f \in A \mid h^2 f \in \mathfrak{P},\ h$ not a zero divisor $\}$ and $\mathfrak{P}_p = \{ f \in A \mid f = g/(f^{2s} + h)$, some $g, h \in \mathfrak{P}, s \in \mathbb{N} \}$. One verifies purely formally that $\mathfrak{P}_d$ is an order; but as for $\mathfrak{P}_p$, Brumfiel stated, "It is not clear under what conditions this set will be closed under sums."[3] He did observe that when A is a reduced R-algebra of finite type and $\mathfrak{P} = \mathfrak{P}_w[g_i]$ for some finite set $\{g_i\} \subseteq A$, then Stengle's Theorem implies $\mathfrak{P}_p$ is closed under sums.[4] Actually, for *any* order $\mathfrak{P} \subseteq A =$ a reduced R-algebra of finite type, $\mathfrak{P}_p$ will be closed under sums: let $f_i \in \mathfrak{P}_p\ (i = 1, 2)$, so that

$$f_i = \frac{g_i}{f^{2s_i} + h_i},$$

some $g_i,\ h_i \in \mathfrak{P},\ s_i \in \mathbb{N}$; then $f_1 + f_2 \geq 0$ on $W\{g_i, h_i\}$,[5] so by Stengle's Theorem,

$$f_1 + f_2 = \frac{g}{(f_1 + f_2)^{2s} + h},$$

some $g,\ h \in \mathfrak{P}_w[g_i, h_i] \subseteq \mathfrak{P},\ s \in \mathbb{N}$; i.e. $f_1 + f_2 \in \mathfrak{P}_p$, i.e. $\mathfrak{P}_p$ is an order.

From now on, $A = K[X]$. Define a new, larger kind of basic open s.a. set $V\{g_i\} = W\{g_i\}^\circ\ (= \overline{U\{g_i\}}^\circ)$.

Let $\mathcal{V}$ (resp. $\mathcal{W}$) be the collection of sets of the form $V\{g_i\}$ (resp. $W\{g_i\}$) with non-empty interior. We shall review Brumfiel's analysis of $\mathcal{V}$ in such a

---

3 P. 98 of [Brumfiel 1979].

4 P. 173, *Ibid.*

5 We have defined $W\{g_i\}$ and stated Stengle's Theorem only when the ring A is $K[X]$; however, with a little more work, Brumfiel develops this theory when A is any reduced R-algebra of finite type. To keep this section short, we shall stick to the case $A = K[X]$; our statements can be readily generalized.

way that we can replace each occurrence of $\mathcal{V}$ and of the subscript d with $\mathcal{W}$ and the subscript p; this will clarify, as well as generalize, parts of his §8.11.

$V\{g_i\} \in \mathcal{V}$ (i.e., $U\{g_i\} \neq \emptyset$) if and only if $\mathfrak{P}_w[g_i]$ is an order on A (cf. Corollary 8.4.6(a) of [Brumfiel]; this is essentially a result of Artin). By a *prefilter* $\mathfrak{F} \subseteq \mathcal{V}$ (precisely, a *$\mathcal{V}$-prefilter*) ~~$\mathfrak{F} \subseteq \mathcal{V}$~~ we mean a non-empty subset of $\mathcal{V}$, closed under finite intersections. A ($\mathcal{V}$-)prefilter is a ($\mathcal{V}$-)*filter* if $V \in \mathfrak{F}$, and $V \subseteq V' \in \mathcal{V}$ imply $V' \in \mathfrak{F}$. A ($\mathcal{V}$-)filter is a(n) ($\mathcal{V}$-)*ultrafilter* if it is not properly contained in any other ($\mathcal{V}$-)filter in $\mathcal{V}$. Note that $V\{g_i\} \subseteq V\{h\}$ if and only if $h(V\{g_i\}) \geq 0$. This is the property of the $V\{g_i\}$[6] which makes them more convenient than the $U\{g_i\}$ for the purposes of this section.

The set of filters in $\mathcal{V}$ is partially ordered by inclusion, an arbitrary intersection of filters is a filter (every filter contains $R^n = V\{1\}$), and unions of chains of filters are filters. Thus every filter is contained in an ultrafilter. Each prefilter $\mathfrak{F} \subseteq \mathcal{V}$ is contained in a smallest filter $\mathfrak{F}_d \subseteq \mathcal{V}$.

Let $\mathfrak{P} \subseteq A$ be any partial order. Define $\mathfrak{F}_{\mathcal{V}}(\mathfrak{P}) \subseteq \mathcal{V}$ by $V\{g_i\} \in \mathfrak{F}_{\mathcal{V}}(\mathfrak{P})$ if $g_i \in \mathfrak{P}$. $\mathfrak{F}_{\mathcal{V}}(\mathfrak{P})$ is a prefilter since $\mathfrak{P}_w[g_i]$ is an order on A if and only if $V\{g_i\} \in \mathcal{V}$, which implies the desired finite intersection property for $\mathfrak{F}_{\mathcal{V}}(\mathfrak{P})$. If $\mathfrak{P}_1 \subseteq \mathfrak{P}_2$, then $\mathfrak{F}_{\mathcal{V}}(\mathfrak{P}_1) \subseteq \mathfrak{F}_{\mathcal{V}}(\mathfrak{P}_2)$.

Let $\mathfrak{F} \subseteq \mathcal{V}$ be an arbitrary prefilter in $\mathcal{V}$. Define $\mathfrak{P}(\mathfrak{F}) \subseteq A$ by $g \in \mathfrak{P}(\mathfrak{F})$ if there is $V \in \mathfrak{F}$ with $g(V) \geq 0$. Equivalently, this says $V \subseteq V\{g\}$. Since the sets V are Zariski dense, it is clear that $\mathfrak{P}(\mathfrak{F})$ is an order on A. In fact,

6 We do not need to read this sentence after changing the V's to W's, etc.

$\mathfrak{P}(\mathfrak{F}) = \mathfrak{P}(\mathfrak{F})_d$, since if $h^2 f = g \in \mathfrak{P}(\mathfrak{F})$, $h \neq 0$, and $g(V) \geq 0$, then f must be nonnegative on V. [When replacing the V's by W's and d's by p's, etc., this last equation should be changed to $(f^{2s} + h)f = g$, g and h nonnegative on W. For the $\mathcal{V}$ but not the $\mathcal{W}$ reading, we need the following statement: Otherwise, f would vanish on the Zariski dense set $U\{g_i\} \cap U\{-g\}$, where $V = V\{g_i\}$.] If $\mathfrak{F}_1 \subseteq \mathfrak{F}_2$, then $\mathfrak{P}(\mathfrak{F}_1) \subseteq \mathfrak{P}(\mathfrak{F}_2)$. Also $\mathfrak{P}(\mathfrak{F}) = \mathfrak{P}(\mathfrak{F}_d)$, where $\mathfrak{F}_d$ is the filter generated by $\mathfrak{F}$.

We now study the compositions $\mathfrak{P}\big(\mathfrak{F}_{\mathcal{V}}(\mathfrak{P})\big)$ and $\mathfrak{F}_{\mathcal{V}}\big(\mathfrak{P}(\mathfrak{F})\big)$. First, $\mathfrak{P} \subseteq \mathfrak{P}\big(\mathfrak{F}_{\mathcal{V}}(\mathfrak{P})\big)$ and $\mathfrak{F} \subseteq \mathfrak{F}_{\mathcal{V}}\big(\mathfrak{P}(\mathfrak{F})\big)$ are obvious from the definitions.

Proposition (8.11.1 in [Brumfiel]):

(a) If $\mathfrak{F} \subseteq \mathcal{V}$ is any prefilter, then $\mathfrak{F}_{\mathcal{V}}\big(\mathfrak{P}(\mathfrak{F})\big) = \mathfrak{F}_d \subseteq \mathcal{V}$.

(b) If $\mathfrak{F}$ is an ultrafilter, then $\mathfrak{P}(\mathfrak{F}) \subseteq A$ is a total order (i.e., $\mathfrak{P}(\mathfrak{F}) \cup \big(-\mathfrak{P}(\mathfrak{F})\big) = A$).

Also, if $\mathfrak{P} \subseteq A$ is a total order, then $\mathfrak{F}(\mathfrak{P}) \subseteq \mathcal{V}$ is an ultrafilter.

(c) If $\mathfrak{P} \subseteq A$ is any order, then $\mathfrak{P}\big(\mathfrak{F}_{\mathcal{V}}(\mathfrak{P})\big) = \mathfrak{P}_d$.

Furthermore, this Proposition (as well as the rest of this section, except where noted) remains true if $\mathcal{V}$ is replaced by $\mathcal{W}$ and d by p (and V by W).

Proof: (a) Since $\mathfrak{P}(\mathfrak{F}) = \mathfrak{P}(\mathfrak{F}_d)$, we may as well assume $\mathfrak{F}$ is a filter. We know $\mathfrak{F} \subseteq \mathfrak{F}_{\mathcal{V}}\big(\mathfrak{P}(\mathfrak{F})\big)$. Conversely, if $g_i \in \mathfrak{P}(\mathfrak{F})$, so that $V\{g_i\} \in \mathfrak{F}_{\mathcal{V}}\big(\mathfrak{P}(\mathfrak{F})\big)$, let $g_j(V_j) \geq 0$, $V_j \in \mathfrak{F}$. Then $V_j \subseteq V\{g_i\}$ and since $\mathfrak{F}$ is a filter, $V\{g_j\} \in \mathfrak{F}$. Thus $V\{g_i\} \in \mathfrak{F}$ and $\mathfrak{F}_{\mathcal{V}}\big(\mathfrak{P}(\mathfrak{F})\big) \subseteq \mathfrak{F}$.

(b) Suppose $\mathfrak{P} = \mathfrak{P}(\mathfrak{F})$ admits a proper refinement, $\mathfrak{P} \subseteq \mathfrak{P}[g]$. Then $\mathfrak{F}\gamma(\mathfrak{P}) = \mathfrak{F} \subseteq \mathfrak{F}\gamma(\mathfrak{P}[g])$ and since $\mathfrak{F}$ is an ultrafilter, $\mathfrak{F} = \mathfrak{F}\gamma(\mathfrak{P}[g])$. But now $g \in \mathfrak{P}(\mathfrak{F}\gamma(\mathfrak{P}[g])) = \mathfrak{P}(\mathfrak{F})$, contradiction.

Secondly, assume $\mathfrak{P} \subseteq A$ is a total order and suppose $\mathfrak{F} = \mathfrak{F}\gamma(\mathfrak{P})$ is properly contained in a filter $\mathcal{G}$. Let $V = V\{g_i\} \in \mathcal{G} - \mathfrak{F}$. Since $\mathfrak{P} \subseteq \mathfrak{P}(\mathfrak{F}\gamma(\mathfrak{P})) \subseteq \mathfrak{P}(\mathcal{G})$, we have $\mathfrak{P} = \mathfrak{P}(\mathcal{G})$. But $g_i \in \mathfrak{P}(\mathcal{G})$, hence $V\{g_i\} \in \mathfrak{F}\gamma(\mathfrak{P})$, contradiction.

(c) Finally, $\mathfrak{P} \subseteq \mathfrak{P}(\mathfrak{F}\gamma(\mathfrak{P}))$ and $\mathfrak{P}(\mathfrak{F}\gamma(\mathfrak{P})) = \mathfrak{P}(\mathfrak{F}\gamma(\mathfrak{P}))_d$, so $\mathfrak{P}_d \subseteq \mathfrak{P}(\mathfrak{F}\gamma(\mathfrak{P}))$. Conversely, if $f \geq 0$ on $W\{g_i\}$, $\{g_i \in \mathfrak{P}\}$, then Robinson's theorem gives $f = p/q$, $p, q \in \mathfrak{P}_w[g_i] \subseteq \mathfrak{P}$; i.e., $f \in \mathfrak{P}_d$. [In the W-reading, replace the last equation by $f = p/(f^{2s} + q)$.] (This proof of the second inclusion in (c) is simpler than Brumfiel's: e.g., it does not use (b).) Q. E. D.

BIBLIOGRAPHY

Artin, E., Über die Zerlegung definiter Funktionen in Quadrate, *Abhandl. Math. Sem. Hamburg* **5** (1927), 100–15. (An English version of the main proof here is on p. 289ff of [Jacobson 1964].)

Artin, E. and Schreier, O., Algebraische Konstruktionen reeller Körper, *Abhandl. Math. Sem. Hamburg* **5** (1927), 85–99.

Eine Kennzeichnung der reell abgeschlossenen Körper, *Abhandl. Math. Sem. Hamburg* **5** (1927), 225–31.

Artin, M., On the Solutions of Analytic Equations, *Inventiones Math.* **5**, (1968), 277–91.

Berg, C., Christenson, J. P. R., and Ressel, P., Positive Definite Functions on Abelian Semigroups, *Math. Ann.* **223**(3), (1976), 253–74.

Bochnak, J. and Efroymson, G., Real Algebraic Geometry and the 17th Hilbert Problem, to appear.

Bose, N. K., New Techniques and Results in Multi-dimensional Problems, *Journal of the Franklin Institute* **301**(1–2), (1976), 83–101.

Bourbaki, N., *Algèbra* (Hermann, Paris, 1959).

Brumfiel, G., *Partially Ordered Rings and Semi-Algebraic Geometry*. Lecture note Series of the London Math. Soc. (Cambridge Univ. Press, Cambridge, 1979).

Cassels, J. W. S., On the Representation of Rational Functions as Sums of Squares, *Acta Arith.* **9**, (1964), 79–82.

Cassels, J. W. S., Ellison, W. J., and Pfister, A., On Sums of Squares and on Elliptic Curves over Function Fields, *J. Number Theory* **3**(2), (1971), 125–49.

Choi, M. D., and Lam, T. Y., An Old Question of Hilbert, *Proceedings of Conference on Quadratic Forms—1976*, (Queen's Papers on Pure and Applied Math., No. 46 (G. Orzech, ed.), Queen's Univ., Kingston, Ontario, 1977), 385–405.

Extremal Positive Semidefinite Forms, *Math. Ann.* **231**, (1977), 1–18.

Choi, M. D., Lam, T. Y., and Reznick, B., Real Zeros of Positive Semidefinite Forms, I, *Math. Z.* **171**, 1980, 1–26.

Choi, M. D., Lam, T. Y., Reznick, B. and Rosenberg, A., Sums of Squares in Some Integral Domains, to appear.

Christenson, J. P. R., with Berg, C., and Ressel, P.: see Berg, C., Christenson, J. P. R., and Ressel, P.

Christie, M. R., Positive-Definite Rational Functions of Two Variables which are not Sums of Three Squares, *J. Number Th.* 8(2), (1976), 224–32.

Cohen, P. J., Decision Procedures for Real and P-adic Fields, *Commun. Pure & Applied Math.* **22**, (1969),131–51.

Collins, G. E., Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition—Preliminary Report, *SIGSAM Bull.* 8(3), issue #31, (1974), 80–90.

Coste, M. and M. F., Topologies for Real Algebraic Geometry, *Topos theoretic Methods in Geometry*, in *Various Publications Series* **30**, A. Kock, ed. (Matematisk Institut, Aarhus Univ., 1979).

Daykin, Thesis, Univ. of Reading, 1960 (unpublished).

Dickmann, M. A., Sur Les Anneaux de Polynôme à Coefficients dans un Anneaux réel Clos, *Comptes rendus (Paris)*, Serie A **290**, (1980), 57.

Dubois, D. W., Note on Artin's Solution of Hilbert's 17th Problem, *Bull. Amer. Math. Soc.* **73**, (1967), 540–1.

Efroymson, G., A Nullstellensatz for Nash Rings, *Pacific J. Math.* **54**, (1974), 101–12.

Efroymson, G., Substitution in Nash Functions, *Pacific J. Math.* **63**, (1976), 137–45.

Efroymson, G., with Bochnak, J.: see Bochnak, J. and Efroymson, G.

Ellison, W. J., A "Waring's Problem" for Homogeneous Forms, *Proc. Cambridge Philos. Soc.* 65, (1969), 663–72.

Ellison, W. J., with Cassels, J. W. S. and Pfister, A.: See Cassels, J. W.

S., Ellison, W. J., and Pfister, A.

Fischer, M. J. and Rabin, M. O., Super-Exponential Complexity of Presburger Arithmetic, *M.I.T., MAC Tech. Memo.* **43**, (Feb. 1974).

Fleck, A., Zur Darstellung Definiter binäre Formen als Summen von Quadraten Ganzer Rationalzahligen Formen, *Arkiv der M. & Physik* 3d Ser. **10**, (1906), 23–38, and 3d Ser. **16**, (1910), 275–6.

Gerstein, L. J. New Proof of a Theorem of Cassels-Pfister, *Proc. Amer. Math. Soc.* 41(1), (1973), 327–8.

Gorin, E. A., Asymptotic Properties of Polynomials and Algebraic Functions of Several Variables, *Russian Math. Surveys* **16**, (1961), 93–119.

Habicht, W., Über die Losbarkeit gewissen algebraischer Gleichungssysteme, *Comm. M. Helv.* **12**, (1940), 317–22. (An English version is in the second [1952] edition of [Hardy, Littlewood, and Pólya, 1934] (below).)

Hardy, G. H., Littlewood, J. E., and Pólya, G., *Inequalities* (Cambridge Univ. Press, Cambridge, 1934); second edition, (1952).

Heilbronn, H., On the Representation of a Rational as a Sum of Four Squares by means of Regular Functions, *J. London Math. Soc.* **39**, (1964),72–6.

Henkin, L., Sums of Squares, *Summaries of Talks Presented at the Summer Institute of Symbolic Logic in 1957 at Cornell University*, (Institute Defense Analyses, Princeton, 1960), 284–91.

Hilbert, D., Über die Darstellung definiter Formen als Summe von Formenquadraten, *Math. Ann.* **32**, (1888), 342-50; see also *Ges. Abh.* **2**, (Springer, Berlin, 1933), 154–61.

Über Ternäre definite Formen, *Acta Math.* **17**, (1893), 169–97; see also *Ges. Abh.* **2**, (Springer, Berlin, 1933), 345–66.

Grundlagen der Geometrie (Teubner,1899); transl. by E. J. Townsend (Open Court Publishing Co., La Salle, IL, 1962).

Mathematische Probleme, *Göttinger Nachrichten* (1900), 253–97, and *Archiv der Mathematik und Physik* 3d ser. **1**, (1901), 44–63, 213–37. Transl. by M. W. Newson, *Bull. Amer. Math. Soc.* 8, (1902), 437–79; reprinted in *Mathematical Developments Arising from Hilbert Problems* (F. Browder, ed.), *Proc. Symp. in Pure Math.* **28**, (Amer. Math. Soc., Providence, 1976), 1–34.

HIRONAKA, H., Triangulations of Semi-Algebraic Sets, *Proc. Symp. in Pure Math.* **29**, (Amer. Math. Soc., Providence, 1975), 165–85.

Subanalytic Sets, *Number Theory, Algebraic Geometry, and Commutative Algebra—in Honor of Yasuo Akizuki*, (Kusunoki, Y., *et al*, eds.) (Kinokuniya Book-Store Co., Ltd., Tokyo, 1975) 453–93.

HSIA, J. S., and JOHNSON, R. P., On the Representation in sums of Squares for Definite Functions in one Variable over an Algebraic Number Field, *Amer. J. Math.* 96(3), (1974), 448–53.

JACOBSON, N., *Lectures in Abstract Algebra* 3 (D. van Nostrand Co., Inc., Princeton, 1964) (reissued by Springer Verlag).

Basic Algebra 1 (Freeman, San Francisco,1974).

JOHNSON, R. P., with HSIA, J. S.: see HSIA, J. S. and JOHNSON, R. P.

KREISEL, G., Hilbert's 17th Problem, I and II, *Bull. Amer. Math. Soc.* **63**, (1957), 99 and 100.

Mathematical Significance of Consistency Proofs, *J. Symb. Logic* **23**, (1958), 155-82 (reviewed by A. Robinson, *J. Symb. Logic* **31**, 128).

Sums of Squares, *Summaries of Talks Presented at the Summer Institute for Symbolic Logic in 1957 at Cornell University*, (Institute for Defense Analyses, Princeton, 1960), 313–20 (discussed in [Kreisel 73], below).

A Survey of Proof Theory, *J. Symb. Logic* **33**, (1968), 321–88.

The Need for Abstract Methods in Mathematics: A Topic for Proof Theory (talk delivered at the U. S.-Japanese Conference of Proof Theory, Sept. 1973, Harvard Univ.); to appear in *Proofs and Provability*.

A Notion of Mechanistic Theory, *Synthese* **29** (1974), 11–26.

What Have We Learnt from Hilbert's Second Problem?, *Mathematical Developments Arising from Hilbert Problems* (F. Browder, ed.), *Proc. Symp. in Pure Math.* **28**, (Amer. Math. Soc., Providence, 1976), 93–130.

On the Kind of Data Needed for a Theory of Proofs, *Logic Colloquium 1976* (Gandy, R. O. and Hyland, J. M. E., eds.), (North-Holland Publishing Co., Amsterdam, 1977), 111–28. MR58#21397.

Review of *L. E. J. Brouwer, Collected Works, Vol. I, Philosophy and Foundations of Mathematics* (A. Heyting, ed.), *Bull. Amer. Math. Soc.* **83** (1977), 86–93.

Lagrange, J. L., Démonstration d'un Théorème d'Arithmétique, *Nouveaux Mémoires de l'Açadémie Royale des Sciences et Belle-Lettres de Berlin* (1770); *Œuvres* 3, 187–201.

Lam, T. Y., *The Algebraic Theory of Quadratic Forms* (W. A. Benjamin, Reading, MA, 1973).

The Theory of Ordered Fields, *Proceedings of the Algebra and Ring Theory Conference* (B. McDonald, ed.), Univ. of Oklahoma, March 1979; to be published by Marcel Bekker, 1980.

Lam, T. Y., with Choi, M. D.: see Choi, M. D. and Lam, T. Y.

Lam, T. Y., with Choi, M. D. and Reznick, B.: see Choi, M. D., Lam, T. Y., and Reznick, B.

Lam, T. Y., with Choi, M. D., Reznick, B., and Rosenberg, A.: see Choi, M. D., Lam, T. Y., Reznick, B., and Rosenberg, A.

Landau, E., Über die Darstellung definiter binärer Formen durch Quadrate, *Math. Ann.* 57 (1903), 53–64.

Über die Zerlegung definiter Funktionen durch Quadraten, *Ark. für Math. und Physik*, 3d Ser.7 (1904), 271–7.

Über die Darstellung definiter Funktionen in Quadraten, *Math. Ann.* 62, (1906), 272–85.

Lang. S., *Algebra* (Addison-Wesley, Reading, MA, first edition, 1965).

Littlewood, J. E., with Hardy, G. H. and Pólya, G.: see Hardy, G. H., Littlewood, J. E., and Pólya, G.

Lojasiewicz, S., Triangulations of Semi-Analytic Sets, *Ann. Scuola Norm. Sup. Pisa* 18, (1964), 449–74.

Emsembles Semi-analytiques, Lecture Note (1965) at I. H. E. S., Bures-sur-Yvettes, Reproduit N° A66.765, École Polytechnique, Paris. (An English version of p. 65ff. appears in [Hironaka 1975b].)

Monk, L. G., Elementary-Recursive Decision Procedures, Ph.D. Thesis (U. C. Berkeley, 1975).

Motzkin, T. S., Algebraic Inequalities, *Inequalities* 1, Shisa, O., ed., (Academic

Press, New York, 1967), 204–24.

PFISTER, A., Multiplikative Quadratic Formen, *Arch. Math.* **16**, (1965), 363–70.

Zur Darstellung definiter Funktionen als Summe von Quadraten, *Invent. Math.* 4, (1967), 229–37. (An English version is in [1976] below.)

Letter to Kreisel, *The Kreisel Papers* (Stanford Univ. Archives, 1974).

Hilbert's 17th Problem and Related Problems on Definite Forms, *Mathematical Developments Arising from Hilbert Problems* (F. Browder, ed.), *Proc. Symp. in Pure Math.* 28, (Amer. Math. Soc., 1976), 483–9.

PFISTER, A., with CASSELS, J. W. S. and ELLISON, W. J.: see CASSELS, J. W. S., ELLISON, W. J., and PFISTER, A.

PÓLYA, G., with HARDY, G. H. and LITTLEWOOD,, J. E.: see HARDY, G. H., LITTLEWOOD, J. E. and PÓLYA, G.

POURCHET, Y., Sur la Représentation en Somme de Carrés des Polynômes à Une Indeterminée sur un Corps de Nombres Algébriques, *Acta Arith.* **19**, (1971), 89–104.

PRESTEL, A., *Lectures on Formally Real Fields* (IMPA Lecture Notes, No. 22, Rio de Janeiro, 1975).

Sums of Squares over Fields, *Atas da 5ª Escola de Algebra* (Soc. Brasileira de Matemática, Rio de Janeiro, 1978).

PROCESI, C., Positive Symmetric Functions, *Advances in Math.* **29**, (1978), 219–25.

RABIN, M. O., with FISCHER, M. J.: see FISCHER, M. J. and RABIN, M. O.

RESSEL, P., with BERG, C. and CHRISTENSON, J. P. R.: see BERG, C., CHRISTENSON, J. P. R., and RESSEL, P.

REZNICK, B., Extremal Psd Forms with Few Terms, *Duke Math. J.* **45**(2) (1978), 363–74.

REZNICK, B., with CHOI, M. D. and LAM, T. Y.: see CHOI, M. D., LAM. T. Y., and REZNICK, B.

REZNICK, B.. with CHOI, M. D., LAM, T. Y., and ROSENBERG, A.: see CHOI, M. D., LAM, T. Y., REZNICK, B., and ROSENBERG, A.

ROBINSON, A., On Ordered Fields and Definite Forms, *Math. Ann.* **130**, (1955), 257–71.

Further Remarks on Ordered Fields and Definite Forms, *Math. Ann.* **130**, (1956), 405–9.

Some Problems of Definability in the Lower Predicate Calculus, *Funda. Math.* **44**, (1957), 309–29.

Introduction to Model Theory and the Metamathematics of Algebra (North-Holland Publishing Co., Amsterdam, 1963).

ROBINSON, R. M., Some Definite Polynomials which are not Sums of Squares of Real Polynomials, *Notices Amer. Math. Soc.* **16**, (1969), 554; *Selected Questions in Algebra and Logic* (Vol. dedicated to the memory of A. I. Mal'cev), *Izdat. "Nauka." Sibirsk Otdel Novosibirsk,* (1973), 264–82; or Acad. Sci. USSR. (MR49#2647).

ROSENBERG, A., with CHOI, M. D., LAM, T. Y., AND REZNICK, B.: see CHOI, M. D., LAM, T. Y., REZNICK, B., and ROSENBERG, A.

SCHREIER, O., with ARTIN, E.: see ARTIN, E. and SCHREIER, O.

SEIDENBERG, A., A New Method for Elementary Algebra and Geometry, *Ann. Math.* **60**, (1954), 365–74.

SEIGEL, C. L., Darstellung total positiver Zahlen durch Quadrate, *Math. Zeit.* **11**, (1921), 246–75; *Ges. Abh.* **1**, (1966), 47–76.

STENGLE, G., A Nullstellensatz and a Positivstellensatz for Semi-Algebraic Geometry, *Math. Ann.* **207**, (1974), 87–97.

Integral Solution of Hilbert's 17^{th} Problem, *Math. Ann.* **246**, (1979), 33–39.

SWAN, R. G., Topological Extensions of Projective Modules, *Transa. Amer. Math. Soc.* **230**, (1977), 201.

SYLVESTER, J. J., A Demonstration of the Theorem that Every Quadratic Polynomial is Reducible by Real Orthogonal Substitutions to the Form of a Sum of Positive and Negative Squares, *Philosophical Magazine*, 4th Ser. 4(23), (1852), 138–42; *Collected Mathematical Papers* 1, 378–81.

TARSKI, A., *A Decision Method for Elementary Algebra and Geometry*, First Edition, 1948; Second Edition, revised (UC Press, Berkeley and Los Angeles (1951).

WAERDEN, R. L., VAN DER, *Modern Algebra* 1, (Fred Blum, tr.) (Frederick Ungar Pub. Co., New York, 1953).