Progress in Mathematics Volume 109

Series Editors
J. Oesterlé
A. Weinstein

Computational Algebraic Geometry

Frédéric Eyssette André Galligo Editors

Birkhäuser Boston · Basel · Berlin

06108 Nice Cedex 2 Mathématiques U.F.R. Faculté des Sciences Université de Nice-Sophia Antipolis Frédéric Eyssette 06108 Nice Cedex 2 Mathématiques André Galligo

U.F.R. Faculté des Sciences Université de Nice-Sophia Antipolis

Library of Congress Cataloging-in-Publication Data

Computational algebraic geometry / edited by F. Eyssette, A. Galligo 516.3'5'0285--dc20 QA564.C6564 1993 Progress in mathematics (Boston, Mass); vol. 109. Geometry, Algebraic--Data processing--Congresses.
 Eyssette, F. (Frédéric), 1952- II. Galligo, A. III. Papers from a symposium held in Nice, France, Apr. 21-25, 1992. Includes bibliographical references. ISBN 0-8176-3678-1 (alk. paper). -- ISBN 3-7643-3678-1 (alk. cm. - (Progress in mathematics; v. 109) 92-44350

Printed on acid-free paper.

© Birkhäuser Boston 1993.

copying, recording, or otherwise, without prior permission of the copyright owner. system, or transmitted, in any form or by any means, electronic, mechanical, photo-All rights reserved. No part of this publication may be reproduced, stored in a retrieval Copyright is not claimed for works of U.S. Government employees.

02139, U.S.A. directly to CCC, 21 Congress Street, Salem, MA 01970, U.S.A. Special requests should Center (CCC), provided that the base fee of \$6.00 per copy, plus \$0.20 per page is paid Birkhäuser Boston for libraries and other users registered with the Copyright Clearance be addressed directly to Birkhäuser Boston, 675 Massachusetts Avenue, Cambridge, MA Permission to photocopy for internal or personal use of specific clients is granted by

ISBN 3-7643-3678-1 ISBN 0-8176-3678-1

Printed in the U.S.A. Camera-ready copy prepared by the Editors. Printed and bound by Quinn-Woodbine, Woodbine, NJ.

87654321

111

Table of Contents

s of Eisenbud-Levine's theorem to real reometry nd Z. Szafraniec	Computing subfields: Reverse of the primitive element problem D. Lazard and A. Valibouze	. Ħ	Arrangements of singularities and proper partitions of Dynkin diagrams P. Jaworski	Shade, Shadow and Shape JP. Henry and M. Merle	Computational Complexity of Sparse Real Algebraic Function Interpolation D. Grigoriev, M. Karpinski, and M. F. Singer	The analytic spread of the ideal of a monomial curve in projective 3-space P. Gimenez, M. Morales, and A. Simis	A Continuous and rational splution to Hilbert's 17th problem and several cases of the Positivstellensatz C. N. Delzell, L. González-Vega, and H. Lombardi	Gröbner Bases and Standard Monomial Theory A. M. Cohen and R. H. Cushman	The Resultant via a Koszul Complex M. Chardin	Semialgebraic geometry of polynomial control problems M. Briskin and Y. Yomdin	Computation of Real Radicals of Polynomial Ideals E. Becker and R. Neuhaus	Preface
•	•	•	•	•	•	•	•	•	•	•	•	•
177	163	143	129	105	91	77	61	41	29	21	•	∑ :

≤

Applications of Algebraic Geometry to Computer Vision S. J. Maybank
Disproving Hibi's Conjecture with CoCoA or Projective Curves with bad Hilbert Functions G. Niesi and L. Robbiano
Counting real zeros in the multivariate case P. Pedersen, MF. Roy, and A. Szpirglas 203
Finding the number of distinct real roots of sparse polynomials of the form $p(x, x^n)$ D. Richardson
Locally effective objects and algebraic topology J. Rubio and F. Sergeraert
Decision of Algebra Isomorphisms using Gröbner Bases K. Shirayanagi
Complexity of Bezout's Theorem II: Volumes and Probabilities M. Shub and S. Smale
A Parametrized Nullstellensatz F. Smietanski
ation Method Based on Seidenberg's Theory pplications
D. Wang

Preface

The theory and practice of computation in algebraic geometry and related domains, from a mathematical point of view, has generated an increasing interest both for its rich theoretical possibilities and its usefulness in applications in science and engineering. In fact, it is one of the master keys for future significant improvement of the computer algebra systems (e.g., Reduce, Macsyma, Maple, Mathematica, Axiom, Macaulay, etc.) that have become such useful tools for many scientists in a variety of disciplines.

The major themes covered in this volume, arising from papers presented at the conference MEGA-92 were:

- Effective methods and complexity issues in commutative algebra projective geometry, real geometry, and algebraic number theory
- Algebro-geometric methods in algebraic computing and applicaions.

MEGA-92 was the second of a new series of European conferences on the general theme of Effective Methods in Algebraic Geometry. It was held in Nice, France, on April 21–25, 1992 and built on the themes presented at MEGA-90 (Livorno, Italy, April 17–21, 1990). The next conference — MEGA-94 — will be held in Santander, Spain in the spring of 1994. The Organizing committee that initiatiod and supervises this bienniel conference consists of A. Conte (Torino), J. H. Davenport (Bath), A. Galligo (Nice), D. Yu. Grigoriev (Petersburg), J. Heintz (Buenos Aires), W. Lassner (Leipzig), D. Lazard (Paris), H. M. Möller (Hagen), T. Mora (Genova), M. Pohst (Düsseldorf), T. Recio (Santander), J. J. Risler (Paris), M. F. Roy (Rennes), R. Schoof (Utrecht), and C. Traverso (Pisa).

During the conference, an informal session was organized, in which some participants were given the opportunity to give short talks on current research, of too informal a nature for inclusion in the volume. In addition, the decision since was made to publish only in English, some excellent papers do not appear here. The following papers given at the conference were omitted from the volume:

Assi (Grenoble): Homogenization and standard bases with minimal ecart

Bjorck (Stockholm): There are $\infty + 1152$ cyclic 8-roots

A.M. COHEN, R.H. CUSHMAN

- [Deo] V.V. Deodhar, "Some characterizations of Bruhat ordering on a Coxeter group and determination of the relative Möbius Function", Inventiones Math. 39, (1977), 187-198.
- [Hill] H. Hiller, Geometry of Coxeter Groups, Research Notes in Math., Pitman, Boston, 1982.
- [Hum] J.E. Humphreys, Reflection groups and Coxeter groups, Cambridge University Press, 1990.
- [LaSh] V. Lakshmibai and C.S. Seshadri, "Geometry of G/P V", J. Algebra 100, (1986), 462-557.
- [Lich] W. Lichtenstein, "A system of quadrics describing the orbit of the highest weight vector", Proc. Amer. Math, Soc. 84, (1982), 605-608.
- [LiE] M.A.A. van Leeuwen, A.M. Cohen, B. Lisser, LiE manual, describing version 2.0, CAN, Amsterdam, 1992.
- [Proc] R.A. Proctor, "Bruhat lattices, plane partition generating functions, and minuscule representations", European J. Combinatorics 5, (1984), 331-350.
- [Sesh] C.S. Seshadri, Geometry of G/P I, Theory of standard monomials for minuscule representations, pp. 207-239 in "C.P. Ramanujam A tribute", (for Tata Institute) Springer-Verlag, Berlin, 1978.
- [StWh1] B. Sturmfels and N. White, "Gröbner bases and invariant theory" Adv. in Math. 76, (1989), 245-259.
- [StWh2] B. Sturmfels and N. White, "Stanley decompositions of the bracket ring", Math. Scandinavia 87, (1990), 183-189.

Arjeh M. Cohen & Richard H. Cushman Mathematics Institute Rijksuniversiteit Utrecht, 3508 TA Utrecht, The Netherlands

A continuous and rational solution to Hilbert's 17th problem

and several cases of the Positivstellensatz

C.N. Delzell¹ L. González-Vega² H. Lombardi

Abstract: From the Positivstellensatz we construct a continuous and rational solution for Hilbert's 17th problem and for several cases of the Positivstellensatz. The solutions are obtained using an especially simple method.

I. Introduction.

Let K be an ordered field, and R its real closure. Hilbert's 17^{th} problem asks if an everywhere nonnegative polynomial $f \in K[X] := K[X_1, ..., X_n]$ can be expressed as a sum of squares of rational functions in K(X) with positive weights in K. Since the answer is well known to be 'Yes,' we now seek more information, in particular, on the way the coefficients of the solution can vary in terms of the coefficients of f. The main tools we shall use to obtain this extra information are the notion of semipolynomial function and the Positivstellensatz for K[X].

A semipolynomial function with coefficients in K (a K-semipolynomial) from \mathbb{R}^n to \mathbb{R} is a function obtained by a finite iteration of composition of polynomials in K[X] and the function absolute value. A well-known proposition, not used here, assures that the set of K-semipolynomials agrees with the minimal max-min stable set of functions containing polynomials in K[X] (see, for example, [Del4]).

By the name Positivstellensatz we shall refer to the more general version of this theorem, i.e., the one assuring that it is possible to associate to every incompatible finite conjunction of generalized sign conditions on a list of polynomials in K[X] an algebraic identity in K[X] making this incompatibility evident (see the beginning of §II).

. O

i Supported by NSF, the Louisiana Board of Regents Research and Development Program (Education Quality Support Fund), and the Alexander von Humboldt Foundation.

² Partially supported by CICyT PB 89/0379/C02/01 and Esprit/Bra 6846 (Pos-

Using this Positivstellensatz we shall provide, in a constructive way, a continuous and rational solution for Hilbert's 17^{th} problem. More precisely, let $f_{n,d}(c, \mathbf{X})$ be the general polynomial of degree d in the n variables $\mathbf{X} := (X_1, \ldots, X_n)$ with coefficients $\mathbf{c} := (c_1, \ldots, c_m)$, and consider the semialgebraic set

$$\mathbb{F}_{n,d} = \{ \mathbf{c} \in \mathbb{R}^m : \forall \mathbf{x} \in \mathbb{R}^n \mid f_{n,d}(\mathbf{c},\mathbf{x}) \ge 0 \}.$$

Theorem II.5. (Main Theorem) The general polynomial $f_{n,d}$ of degree d in n variables can be written as a weighted sum of squares of rational functions

$$f_{n,d}(\mathbf{c}, \mathbf{X}) = \sum_{j} p_{j}(\mathbf{c}) \left(\frac{q_{j}(\mathbf{c}, \mathbf{X})}{k(\mathbf{c}, \mathbf{X})} \right)^{2}$$

(for all $c \in \mathbb{R}^m$), where

- k(c, X) and the $q_j(c, X)$ are polynomials in the variables X whose coefficients are Q-semipolynomials in the coefficients c. Moreover, if $c \in \mathbb{F}_{n,d}$, then k(c, X) vanishes only on the zeros of $f_{n,d}(c, X)$, and
- each p_j(c) is a Q-semipolynomial which is nonnegative on F_{n,d}. Moreover, under the hypothesis c ∈ F_{n,d}, the nonnegativity of p_j(c) is 'clearly' evident.

A. Prehistory of Theorem II.5

Hilbert posed his 17^{th} problem in 1900 [Hil]; E. Artin solved it in 1927 [Art] by a non-constructive method. In 1955 Artin asked Kreisel whether, from Artin's own proof, one could extract bounds on the number and degrees of the rational functions, in terms of suitable elements of the data (n, d, and possibly c); Kreisel gave a sketch of such an 'unwinding' in [Kre2]; the bounds so constructed were in terms of n and d (not c), and primitive recursive; in 1961 Daykin [Day] worked out Kreisel's sketch, showing that, roughly, the bounds were obtained by applying primitive recursion at least twice to exponential functions of n and d. Independently, A. Robinson (see [Rob1] and [Rob2]) got (by definition total) general recursive bounds. These authors also expressed the weights and coefficients of the rational functions as \mathbb{Z} -piecewise-polynomial functions g of g. All this handles the case in which g is given with computable arithmetic operations and sign test (e.g., when g is given with computable arithmetic and sign that g is given with computable arithmetic operations and sign test (e.g., when g is given with computable arithmetic operations and sign test (e.g., when g is g in g is g in g is g in g in

But the fact that those g were, a priori, discontinuous in c for the usual, order topology on R, meant that they were computationally inadequate for the case where K = R, since if we want to have computable arithmetic operations, elements of R must be given by, say, rational approximations; this makes equality and, a fortiori, the order relation, undecidable. Intuitionistic logic gives small changes in the logical laws which do ensure

continuity of functions constructed (and for a wide range of topologies). So after the above contributions by classical logic, Kreisel asked in 1962 [Kre3] whether intuitionistic logic could also contribute, by determining whether the g could be chosen to be continuous, or the rational functions $\in K(X)$ could be chosen to be continuously extendible to \mathbb{R}^n . So far, intuitionistic logic has contributed little, and real algebraic geometry much:

- (a) In 1978 Kreisel noticed [Kre4] that Stengle's 1974 "Positivstellensatz" [Ste] (which others have called a "Nichtnegativstellensatz") easily represents a positive semidefinite ('psd') $f \in K[X]$ in the form $f = \sum_j p_j (q_j/k)^2$ with $0 \le p_j \in K$ and $k, q_j \in K[X]$ and, most importantly here, such that the functions q_j/k extend continuously to \mathbb{R}^n (see the end of §II below for details).
- (b) In 1980 the first author showed [Del₂] that for even $d \ge 4$, the weights $p_i(c)$ in (II.5)(*) cannot be chosen to be rational functions ($\in R(c)$); and in 1990 ([Del₆] and [Del₇]) he excluded even (germs of) real analytic functions when R = R.
- (c) Also in 1980 he found his first positive result on this ([Del3]): for all $d \ge 0$ the p_j and the coefficients of k and the q_j can be chosen to be (locally uniformly) continuous Q-semialgebraic functions of c; functions with these properties can be effectively evaluated even over R, in the—only reasonable—sense that they are computable on, say, the rationals, and they take approximations to approximations. And from the mere existence of this representation of f (and the completeness of the theory of real closed fields), the semialgebraic descriptions of these functions are given by general recursive functions of n and d.

functions). The third author gave a direct, constructive proof of the Pos (intuitionistic or classical, both having the same provably total recursive the proper subset of those which are provably total in formal arithmetic which belong not only to the set of general recursive functions, but to other constructively dubious principle; if successful it would yield bounds [Sco1] offered a sketch of a proof of Stengle's theorem without AC or any ZF with intuitionistic logic seems not constructively meaningful. Scowcroft choice, namely purging the principle of the excluded middle. Note also that however: often there is more to constructivity than purging the axiom of further ado. It is clear that this 'trick' would not satisfy constructivists, Ax and Kochen). Thus, being arithmetic (at least if, say, $K = \mathbb{Q}$, which was the only case used in (c)), Stengle's theorem follows from ZF without sults on the order of homotopy groups (by Serre) and on p-adic fields (by arithmetical theorem, a fact which has been used to sanitize proofs of regeneralized continuum hypothesis) can be eliminated from any proof of an a proof to the constructible universe, the axiom of choice (and even the namely, the use of Stengle's theorem, proved up until then by means of Zorn's lemma. In 1956 Kreisel had observed [Kre1] that by relativising third author [Lom₂] remarked, it contained (only) one nonconstructive step, There were two shortcomings in (c): (1) As Scowcroft [Sco1] and the

³ The statement of Daykin's bounds was oversimplified in [Del1] and [Del2].

itivstellensatz [Lom₁], with explicit (primitive recursive) bounds [Lom₃]. Thus, by changing only one entry in the bibliography of [Del₃] (namely, from [Ste] to [Lom₁] and [Lom₃]), the proof in [Del₃] becomes constructive, and the semialgebraic descriptions of those functions also become primitive recursive. Thus, if all that we had wanted in a solution to Hilbert's 17th problem over IR were brutal constructivity, then we could have stopped here; in particular, there would have been no need for (II.5) (though the luxury of a simpler proof is welcome).

(2) The other shortcoming of (c), which was not to be overcome by the above kind of tinkering with the proof in [Del3], was that the functions which it produced are 'only' semislgebraic, and therefore do not necessarily take K-rational values at K-rational arguments c, as Hilbert asked for (unless K is real-closed). So in the first author's thesis, and in [Del1], [Del3], and elsewhere, he proposed to construct continuous, Z-piecewise-polynomial weights and coefficients; such functions obviously do take values in K at K-rational arguments c, uniformly for all K. And in [Del4] he conjectured the full statement of Theorem II.5, that the functions could even be chosen to be Z-semipolynomials, which would make their continuity 'evident'. This last conjecture/theorem appears to be 'strongest possible' by (b), and it contains the results in (a) and (c) above, as explained in more detail at the end of §II below.

B. History of Theorem II.5

Theorem II.5 is a special case of the Positivstellensatz for semipolynomials ('Pfs'). The first author proved II.5 and the Pfs in 1988 (see the abstracts [Dels] and [Del7]). The second and third authors, jointly, rediscovered these results in 1991, independently of the first author, and by a different method. This paper presents their proof of (II.5), along with their view (\$IV) of it as being primarily a contribution to constructive mathematics (à la Bishop). Their proof of the Pfs will appear in [GV-L]. The first author's proof of both results will appear in [Dels], along with his view of them as being primarily a contribution to (classical) topological algebra and to the examination of assumptions of the logical tradition, specifically, the assumption that logic contributes to this part of mathematics.

Perhaps the main difference between the two proofs of the Pfs is that the first author reduces it to the abstract Stellensätze for the real spectrum of an arbitrary commutative ring, while the second and third authors reduce it to the Positivstellensatz for polynomials. An advantage of the former proof is that it has some surprising facts about abstract semialgebraic (in particular, abstract 'semipolynomial') functions in f-rings as by-products. For example, while the absolute value function $c_1 \mapsto |c_1|$ is obviously positive semidefinite on R, it is not psd on the real spectrum of the ring of semipolynomials. This example motivated a large part of N. Schwartz's recent investigation [Sch] into abstract piecewise-polynomial functions. An advantage of the latter proof of (II.5) is that it avoids even

the appearance of reliance on Zorn's lemma, simply by avoiding the abstract Stellensätze. This relies, instead, on—the third author's direct, constructive proof of—the Positivstellensatz for polynomials $[Lom_1]$; as a result, the functions produced by this proof are primitive recursive in n and d; as in (A.c.1) and in Kreisel's and Daykin's results at the beginning of subsection A, these primitive recursive functions are of iterated exponential complexity in n and d, while those of [Delg] are only general recursive. Thus the latter proof provides another constructive solution to Hilbert's 17th problem over \mathbb{R} , simpler and more informative than that described in (A.c.1) above (see §IV for details).

The first author's proof of (II.5) was, at first, more complicated than necessary; A. Prestel simplified the proof, and incidentally rearranged it along the lines of the method below by the second and third authors. He also asked in [BP] whether the result extended to higher even powers; cf. the abstract in [Pre₂] when n = 1.

The underlying ideas used to prove (II.5) and the Pfs led all of us (again independently) to improve the continuous and semialgebraic variation in Scowcroft's Positivstellensatz [Sco₂] to semipolynomial variation.

Finally, unlike the proofs of (II.5) presented in this paper and in [Del₈] the proof presented in [GV-L] reduces the result to the Pfs.

II. A rational and continuous solution to Hilbert's 17 $^{ m th}$ problem.

First we recall the definitions of strong incompatibility and the general form for the Real Nullstellensatz in the polynomial case (see [Lom₁] and [Lom₃]). We consider an ordered field K, and K denotes a list of variables X_1, X_2, \ldots, X_n . We then denote by K[X] the ring $K[X_1, X_2, \ldots, X_n]$. If F is a finite subset of K[X], we let F^{*2} be the set of squares of elements in F, and $\mathcal{M}(F)$ be the multiplicative monoid generated by $F \cup \{1\}$. Cp(F) will be the positive cone generated by F (= the additive monoid generated by elements of type pPQ^2 , where $0 \le p \in K$, $P \in \mathcal{M}(F)$, and $Q \in K[X]$). Finally, let I(F) be the ideal generated by F.

Definition II.1. Consider 4 finite subsets of $K[X]: F_>, F_>, F_=, F_\neq$, containing polynomials for which we want respectively the sign conditions > 0, ≥ 0 , = 0, and $\neq 0$: we say that $F := [F_>, F_>, F_=, F_\neq]$ is strongly incompatible in K if we have in K[X] an equality of the following type:

$$S + P + Z = 0$$
 with $S \in \mathcal{M}(F_{>} \cup F_{\neq}^{*2})$, $P \in Cp(F_{\geq} \cup F_{>})$, $Z \in I(F_{=})$.

It is clear that a strong incompatibility is a very strong form of incompatibility. In particular, it implies that it is impossible to give the indicated signs to the polynomials considered, in any ordered extension of K. If one

⁴ However, they involve fewer iterations of the exponential function than Daykin's unds.

POSITIVSTELLENSATZ

considers the real closure R of K, the previous impossibility is testable by Hörmander's algorithm, for example (see [BCR], chapter 1).

The different variants of the Nullstellensatz in the real case are a consequence of the following general theorem:

Theorem II.2. Let K be an ordered field and R a real closed extension of K. The three following conditions, concerning a generalized system of sign conditions on polynomials of K[X], are equivalent:

- strong incompatibility in K;
- impossibility in R; and
- impossibility in all the ordered extensions of K.

This Nullstellensatz was first proved in 1974 [Ste]. Less general variants were given by Krivine [Kri], Dubois [Du], Prestel [Pre₁], Risler [Ris] and Efroymson [Efr]. All the proofs until [Lom₁] and the sketch in [Sco₁] 'used' the axiom of choice (recall (I.A.c.1)).

II.3 Parameterizing Hilbert's 17th problem.

Let $f_{n,d}(c, \mathbf{X})$ be the general polynomial of degree d in n variables (c denotes the list of coefficients c_1, \ldots, c_m and \mathbf{X} the list of variables X_1, \ldots, X_n). It is a standard fact in real algebraic geometry that the set

$$\mathbb{F}_{n,d} = \{ \mathbf{c} \in \mathbb{R}^m : \forall \mathbf{x} \in \mathbb{R}^n \mid f_{n,d}(\mathbf{c}, \mathbf{x}) \ge 0 \}$$

is a closed Q-semialgebraic set. So, applying the Finiteness Theorem, we have that $\mathbb{F}_{n,d}$ is a finite union of 'basic' closed Q-semialgebraic sets:

$$\mathbb{F}_{n,d} = \bigcup_{i=1}^k \bigcap_{j=1}^{n_i} \{ \mathbf{c} : R_{n,d,i,j}(\mathbf{c}) \ge 0 \}$$

Here the $R_{n,d,i,j}$ are polynomials in $\mathbb{Z}[c]$.⁵ The last equation allows us to describe the set $\mathbb{F}_{n,d}$ in the following way:

$$\mathbb{F}_{n,d} = \left\{ c : \max_{i=1,\ldots,k} \left\{ \min \{ R_{n,d,i,j}(c) : j = 1,\ldots,n_i \} \right\} \ge 0 \right\}.$$

So, if for every i in $\{1, ..., k\}$ we define

$$H_{n,d,i}(\mathbf{c}) = \min_{j=1,\dots,n_i} \{R_{n,d,i,j}(\mathbf{c})\}$$

and

$$H_{n,d}(\mathbf{c}) = \max_{i=1,...,k} \{H_{n,d,i}(\mathbf{c})\},$$

we have obtained the following description for the set $\mathbf{F}_{n,d}$:

$$\mathbb{F}_{n,d} = \{ \mathbf{c} : H_{n,d}(\mathbf{c}) \ge 0 \},$$

where $H_{n,d}(\mathbf{c})$ is a Q-semipolynomial. Therefore we have shown the equivalence

$$c \in \mathbb{F}_{n,d} \iff H_{n,d}(c) \ge 0 \iff \forall \mathbf{x} \in \mathbb{R}^n \ f_{n,d}(c,\mathbf{x}) \ge 0.$$

II.4 The proof of the parameterized theorem

The last equivalence allows us to conclude

$$\forall \mathbf{c} \in \mathbf{R}^m \ \forall \mathbf{x} \in \mathbf{R}^n \ \left\{ H_{n,d}(\mathbf{c}) \ge 0 \implies f_{n,d}(\mathbf{c},\mathbf{x}) \ge 0 \right\},$$

or, what is the same, the incompatibility of the system of generalized sign conditions

$$H_{n,d}(\mathbf{c}) \ge 0, \quad f_{n,d}(\mathbf{c}, \mathbf{X}) < 0.$$
 (1)

If $H_{n,d}(c)$ were a polynomial and not a semipolynomial, then, applying the classical Positivstellensatz (theorem II.2) to the incompatibility (1), we would get an algebraic identity in c and X making this incompatibility evident. This would give, for the polynomial $f_{n,d}(c, X)$, a solution to Hilbert's 17^{th} problem parameterized by polynomials in c and so, a rational and continuous solution.

As this way of attacking the problem is not feasible, we shall try to translate our incompatible system to another one using only polynomials in order to be able to apply the Positivstellensatz (Theorem II.2). To achieve this goal we introduce new variables z_1, \ldots, z_k , and for every $i \in \{1, \ldots, k\}$ we consider the following polynomial system of generalized sign conditions:

$$\mathbf{H}_{i} = \begin{cases} (z_{i} - R_{n,d,i,1}(\mathbf{c}))(z_{i} - R_{n,d,i,2}(\mathbf{c})) \cdots (z_{i} - R_{n,d,i,n_{i}}(\mathbf{c})) = 0, \\ z_{i} - R_{n,d,i,1}(\mathbf{c}) \leq 0, \\ z_{i} - R_{n,d,i,2}(\mathbf{c}) \leq 0, \\ \vdots \\ \vdots \\ z_{i} - R_{n,d,i,n_{i}}(\mathbf{c}) \leq 0. \end{cases}$$

It is clear from the definitions of $H_{n,d,i}$ and H_i that, for fixed $c \in \mathbb{R}^m$, if the system H_i is verified then $z_i = H_{n,d,i}(c)$.

Next we consider a new variable z and the following polynomial systems of generalized sign conditions:

$$\mathbf{H} = \begin{cases} (z - z_1)(z - z_2) \cdots (z - z_k) = 0, \\ z - z_1 \ge 0, \\ z - z_2 \ge 0, \end{cases} \quad \mathbf{K} = \{\mathbf{H}_1, \dots, \mathbf{H}_k, \mathbf{H}\}.$$

$$z - z_k \ge 0.$$

mention the fact that the coefficients of the $F_{n,d,i,j}$ may be chosen to be rational numbers (even integers, after clearing denominators), while others (e.g., [BCR]) assert only that they can be chosen in R_i but even these other proofs actually do yield the integrality of the coefficients, if one merely pays attention to it. Likewise, in most of the proofs, the authors do not pay attention to the constructive character of their proofs; if one does, one sees that in fact most of the proofs are constructive; [Del₁] does pay attention, and [Sol] goes even further, by giving a careful complexity analysis.

POSITIVSTELLENSATZ

Clearly we have that, for fixed $c \in \mathbb{R}^m$, if the system K is verified, then $z = H_{n,d}(c)$.

After introducing in this way the variables z, z_1, \ldots, z_k , what we have obtained is the following incompatible system of generalized sign conditions on polynomials in $\mathbb{K}[X, z, z_1, \ldots, z_k]$:

$$\mathbb{K}, z \ge 0, f_{n,d}(\mathbf{c}, \mathbf{X}) < 0.$$

Applying to this system the Positivstellensatz (theorem II.2) and replacing in the equality obtained every z_i by $H_{n,d,i}(c)$ and z by $H_{n,d}(c)$, we obtain an algebraic identity concerning polynomials in X whose coefficients are \mathbb{Q} -semipolynomials in \mathbf{c} .

Next we study the different parts appearing in this algebraic identity

- The strictly positive part in the initial identity (before the z_i 's replacement) was $f_{n,d}(c, \mathbf{X})^{2r}$ and remains unchanged.
- The null part in the initial identity was a polynomial in the ideal of $\mathbb{K}[X, z, z_1, \dots, z_k]$ generated by the polynomials with '= 0' in \mathbb{K} , i.e.,

$$(z_i - R_{n,d,i,1}(\mathbf{c}))(z_i - R_{n,d,i,2}(\mathbf{c})) \cdots (z_i - R_{n,d,i,n,i}(\mathbf{c})) \quad 1 \leq i \leq k$$

$$(z-z_1)(z-z_2)\cdots(z-z_k).$$

After replacing z by $H_{n,d}(c)$ and every z_i by $H_{n,d,i}(c)$, this part becomes a function of c identically 0 (zero for all $c \in \mathbb{R}$), and this is the reason why it will not appear in the final identity which concerns polynomials in X with coefficients \mathbb{Q} -semipolynomials in c.

• The nonnegative part in the initial identity was a polynomial in the positive cone generated by the polynomials:

$$-f_{n,d}(\mathbf{c},\mathbf{X}),z,z-z_1,\ldots,z-z_k,$$

$$R_{n,d,i,1}(c) - z_i, \ldots, R_{n,d,i,n,i}(c) - z_i \qquad i \in \{1,\ldots,k\}.$$

After the replacement only $-f_{n,d}(c, \mathbf{X})$ remains unchanged, and the other generators of the cone become Q-semipolynomials in c which are clearly nonnegative for every c (by the definition of the functions $H_{n,d,i}(c)$ and $H_{n,d}(c)$ in terms of max and min) or the Q-semipolynomial $H_{n,d}(c)$ that is nonnegative if $f_{n,d}(c, \mathbf{x})$ is nonnegative for all $\mathbf{x} \in \mathbb{R}^n$.

Summarizing, we have found an algebraic identity with the following structure:

$$f_{\mathbf{n},d}(\mathbf{c}, \mathbf{X})g(\mathbf{c}, \mathbf{X}) = f_{\mathbf{n},d}(\mathbf{c}, \mathbf{X})^{2r} + h(\mathbf{c}, \mathbf{X}), \tag{2}$$

where $g(\mathbf{c}, \mathbf{X})$ and $h(\mathbf{c}, \mathbf{X})$ are polynomials in \mathbf{X} whose coefficients are Q-semipolynomials in \mathbf{c} . More precisely, $g(\mathbf{c}, \mathbf{X})$ and $h(\mathbf{c}, \mathbf{X})$ are sum of terms

where the $q_j(\mathbf{c}, \mathbf{X})$ are polynomials in \mathbf{X} with coefficients Q-semipolynomials in \mathbf{c} and the $p_j(\mathbf{c})$ are Q-semipolynomials nonnegative under the hypothesis $H_{n,d}(\mathbf{c}) \geq 0$. More precisely we have that every $p_j(\mathbf{c})$ is a product whose factors have one of the following type:

- the Q-semipolynomial $H_{n,d}(\mathbf{c})$,
- a Q-semipolynomial $H_{n,d}(c) H_{n,d,i}(c)$,
- a Q-semipolynomial $R_{n,d,i,j}(\mathbf{c}) H_{n,d,i}(\mathbf{c})$, and
- a positive rational or the square of a Q-semipolynomial in c

If we multiply by $f_{n,d}(c, X)$ every member of equation (2), we get

$$f_{n,d}(\mathbf{c}, \mathbf{X}) = \frac{f_{n,d}(\mathbf{c}, \mathbf{X})^2 g(\mathbf{c}, \mathbf{X})}{f_{n,d}(\mathbf{c}, \mathbf{X})^{2r} + h(\mathbf{c}, \mathbf{X})}$$

and denoting by k(c, X) the denominator of this fraction, we obtain finally

$$f_{n,d}(\mathbf{c}, \mathbf{X}) = \frac{f_{n,d}(\mathbf{c}, \mathbf{X})^2 g(\mathbf{c}, \mathbf{X}) k(\mathbf{c}, \mathbf{X})}{k(\mathbf{c}, \mathbf{X})^2} = \frac{g_1(\mathbf{c}, \mathbf{X})}{k(\mathbf{c}, \mathbf{X})^2},$$

where $g_1(\mathbf{c}, \mathbf{X})$ is of the same type as $g(\mathbf{c}, \mathbf{X})$ and $h(\mathbf{c}, \mathbf{X})$. Moreover, $k(\mathbf{c}, \mathbf{X})$ vanishes only at the zeros of $f_{n,d}(\mathbf{c}, \mathbf{X})$ if $H_{n,d}(\mathbf{c}) \geq 0$, because then $h(\mathbf{c}, \mathbf{x})$ is positive for all $\mathbf{x} \in \mathbf{R}^n$.

Most of the following theorem has now been proved

Theorem II.5. The general polynomial $f_{n,d}$ of degree d in n variables can be written as a weighted sum of squares of rational functions

$$f_{n,d}(\mathbf{c}, \mathbf{X}) = \sum_{j} p_{j}(\mathbf{c}) \left(\frac{q_{j}(\mathbf{c}, \mathbf{X})}{k(\mathbf{c}, \mathbf{X})} \right)^{2},$$
 (*)

where

- the $q_j(c, \mathbf{X})$ and $k(c, \mathbf{X})$ are polynomials in the variables \mathbf{X} whose coefficients are \mathbb{Q} -semipolynomials in the coefficients \mathbf{c} . Moreover, if $\mathbf{c} \in \mathbb{F}_{n,d}$, then $k(\mathbf{c}, \mathbf{X})$ vanishes only on the zeros of $f_{n,d}(\mathbf{c}, \mathbf{X})$;
- each $p_j(c)$ is a product whose factors are $H_{n,d}(c)$, or one of the Q-semipolynomials $H_{n,d}(c) H_{n,d,i}(c)$, or one of the Q-semipolynomials $R_{n,d,i,j}(c) H_{n,d,i}(c)$, or a positive rational, or the square of a Q-semipolynomial in c. So, under the hypothesis $H_{n,d}(c) \geq 0$, the nonnegativity of $p_j(c)$ is 'clearly' evident; and
- the equation

$$f_{n,d}(\mathbf{c}, \mathbf{X})k(\mathbf{c}, \mathbf{X})^2 - \sum_j p_j(\mathbf{c})q_j(\mathbf{c}, \mathbf{X})^2 = 0$$

POSITIVSTELLENSATZ

c which are identically 0 (without assuming $c \in \mathbb{F}_{n,d}$). equality, as polynomial in X, has as coefficients Q-semipolynomials in is especially evident in the following sense: the first member of the

17th problem, because Equation (*) provides a continuous, rational-valued solution to Hilbert's

- all the coefficients (the p_j(c) and the X-coefficients of the q_j(c, X) and k(c, X)) appearing in equation (*) are continuous, rational-valued functions of c; more precisely, they are Q-semipolynomials in c; and
- every summand in (*)

$$p_j(\mathbf{c}) igg(rac{q_j(\mathbf{c},\mathbf{X})}{k(\mathbf{c},\mathbf{X})}igg)^2$$

semialgebraically extended to the closed semialgebraic set $\mathbb{F}_{n,d} \times \mathbb{R}^n$ is a function which is rational in X, and which can be continuously and

δ's to the reader (see [GV-L] for details). uniform follows from the corresponding property of f; we leave the ϵ 's and nonnegative over $\mathbb{F}_{n,d} \times \mathbb{R}^n$), which can vanish at some point $(c; \mathbf{x}) \in$ of Kreisel [Kre3] (with parameters c): note that $k = f^{2r} + h$ (with h (c; x), by (*). The fact that this pointwise continuity is actually locally $\mathbb{F}_{n,d} \times \mathbb{R}^n$ only if f vanishes there, forcing each $p_j(q_j/k)^2$ to tend to 0 near extension of $p_j(q_j/k)^2$ is obvious. To see its continuity, we use an argument The only statement not yet proved is the last: the semialgebraicity of the

Real Positivstellensatz. III. Rational and continuous solution to other cases of the classical

is to generalize this result to other cases. previous section, the existence of a solution depending on the parameters of the problem in a semipolynomial way. So what we shall do in this section the Real Positivstellensatz, and for this case we have just proved, in the The solution for Hilbert's 17th problem can be seen as a particular case of

als in K[c, X] where the X_i 's are considered as variables and the c_j 's as parameters. We denote by SH the semialgebraic set defined by Let $\mathbb{H}(\mathbf{c}, \mathbf{X})$ be a system of generalized sign conditions on polynomi-

$$S_H = \{c : \forall x \in \mathbb{R}^n \mid H(c, x) \text{ is incompatible}\}.$$

is possible to construct two K-semipolynomials $H_1(c)$ and $H_2(c)$ satisfying where) and the strategy followed in \$II when dealing with the set IF n,d, it algebraic set), then, applying the Finiteness Theorem (see [BCR] or else-If SH is locally closed (i.e., intersection of a closed and an open semi-

$$c \in S_{H} \iff \left[H_{1}(c) \geq 0, H_{2}(c) > 0 \right] \iff$$

 $\iff \forall x \in \mathbb{R}^n \quad \mathbb{H}(c,x) \text{ is incompatible}$

We have obtained the incompatible system of sign conditions

$$H_1(\mathbf{c}) \ge 0, \ H_2(\mathbf{c}) > 0, \ \mathbf{H}(\mathbf{c}, \mathbf{X})$$

 z_2 and $z_{2,i}$ $(i \in \{1, ..., k_2\})$, which are used to construct a system of same way as in §II: we consider new variables $z_1, z_{1,i}$ ($i \in \{1, ..., k_1\}$), $H_2(c)$ as semipolynomials. polynomial sign conditions $\mathbb{K}(\mathbf{c})$ translating the definition of $H_1(\mathbf{c})$ and but with $H_1(c)$ and $H_2(c)$ K-semipolynomials. Now we proceed in the

As the incompatible system of generalized sign conditions

$$\{\mathbb{K}(\mathbf{c}), z_1 \geq 0, z_2 > 0, \, \mathbb{H}(\mathbf{c}, \mathbf{X})\}$$

cerning polynomials in the variables X with coefficients K-semipolynomials als they are representing. So we have obtained an algebraic identity con $z_{1,i}$ $(i \in \{1,...,k_1\}), z_2$ and $z_{2,i}$ $(i \in \{1,...,k_2\})$ by the K-semipolynomi-Finally, we replace in the algebraic identity obtained the variables z₁, II.2), obtaining an algebraic identity making this incompatibility evident. involves only polynomials, we can apply the Positivstellensatz (theorem

provides a rational and continuous solution for some cases of the Real Pos-The next theorem summarizes the results obtained in this section and

on polynomials in K(c, X), where the X_i 's are considered as variables and the c; 's as parameters. If SH is the semialgebraic set defined by Theorem III.1. Let H(c, X) be a system of generalized sign conditions

$$c \in S_H \iff \forall x \in \mathbb{R}^n \ \mathbb{H}(c,x)$$
 is incompatible,

semipolynomials $H_1(c)$ and $H_2(c)$ such that and if SH is locally closed, then (Finiteness Theorem) there exist K.

$$c \in S_H \iff [H_1(c) \ge 0, H_2(c) > 0].$$

obvious by a strong incompatibility of fixed type (independent of c) and with coefficients given by K-semipolynomials in c. Moreover, If $c \in S_H$, then the incompatibility of H(X) := H(c, X) inside R^n is made

- the algebraic identity obtained, seen as a polynomial in X, has an especially simple structure. More precisely, every X-coefficient of this $H_1(c) \ge 0$ and $H_2(c) > 0$), and identity is a K-semipolynomial in c identically 0 (without assuming
- every coefficient p(c) in the algebraic identity which must be nonnegative (resp. positive) is given by a K-semipolynomial showing such

ī

દ

POSITIVSTELLENSATZ

and $H_2(c) > 0$. character in an especially clear way under the hypothesis $H_1(c) \geq 0$

Scowcroft's results [Sco₂] in four respects: 17th problem (§II) improves the first author's result [Del3], (III.1) improves In the same way that our rational and continuous solution for Hilbert's

- a-. for us, the semialgebraic set SH need not be closed (Scowcroft knew this, but chose to use hypotheses involving the logical form of the implications implicit in H, rather than topological hypotheses on S_H);
- the coefficients of our solution are continuous, rational-valued functions continuous semialgebraic as in [Sco₂]; (more precisely, K-semipolynomials) in the parameters c and not only
- ? the algebraic identity obtained, seen as a polynomial in X, has an identically 0 (without assuming $H_1(c) \ge 0$ and $H_2(c) > 0$); and especially simple structure: its coefficents are K-semipolynomials in c
- d-. the nonnegativity or positivity of those coefficients in the solution pothesis $H_1(\mathbf{c}) \geq 0$ and $H_2(\mathbf{c}) > 0$. which must satisfy such conditions, is clearly evident under the hy-

(or even continuously) varying Positivstellensatz; the proof is in [Dela]. be locally closed is also necessary, for the existence of a semipolynomially Finally, we note a strong converse of (III.1): the hypothesis that $\mathbf{S}_{\mathbf{H}}$

IV. Conclusion: the constructive content of the results.

the Positivstellensatz ([Lom₁]). discrete field [LR], because in this setting we have a constructive proof of in §§II and III are valid when the parameters c take values in an ordered In constructive mathematics (see [BB] and [MRR]), the theorems presented

the problem. rithms if the structure of the field of parameters is given by an oracle giving of choice and, more precisely, providing uniformly primitive recursive algothe sign of every polynomial with integer coefficients on the parameters of ing one: all our proofs are effective, in particular without using the axiom An interpretation of the results admissible for everybody is the follow-

recursive algorithm. More details on this question can be found in [GV-L] the real numbers involved, and that we are looking for a uniformly primitive rational approximations (depending on the request made to the oracle) of this means that the real parameters c are given by oracles providing suitable analysis [BB], i.e., the real numbers defined as-equivalence classes of-Cauchy sequences of rational numbers. From an algorithmic point of view the results when dealing with the field IR of the real numbers in constructive The only thing remaining to be mentioned is the constructive content of

tive point of view when dealing with real numbers "à la Cauchy" under puted explicitly. The nonnegativity of the weights is clear from a construcpolynomials and semipolynomials with coefficients in Q that can be com-The answer to Hilbert's 17th problem provided by theorem II.5 uses

> solved in a continuous, rational-valued way with respect to its coefficients nonnegative. So, for the polynomial $f_{n,d}(c, X)$, Hilbert's 17th problem is the hypothesis $H_{n,d}(c) \ge 0$. This implies that, if the parameters c satisfy the condition $H_{n,d}(c) \ge 0$, then the polynomial $f_{n,d}(c,\mathbf{X})$ is everywhere Moreover, since we can constructively prove (see [Lom₂] or [GV-L]) the

$$\forall \mathbf{x} \in \mathbb{R}^n$$
 $f_{n,d}(\mathbf{c}, \mathbf{x}) \geq 0 \implies H_{n,d}(\mathbf{c}) \geq 0$,

Hilbert's 17th problem is complete and constructive for the field R. we can conclude that also this continuous, rational-valued solution for

- [Art] Artin E.: Uber die Zerlegung definiter Funktionen in Quadrate. Abh. Math. Sem. Hamburg, 5 (1927), 100-115.
- Bishop E., Bridges D.: Constructive Analysis. Springer-Verlag (1985).
- [BCR] Bochnak J., Coste M. and Roy M.-F.: Géométrie Algébrique Réelle. Ergebnisse vol. 12, Springer-Verlag (1987).
- Bradley M., Prestel A.: Representation of a real polynomial f(X) as a tures, J. Martinez, ed., Kluwer (1989), 197-207. sum of 2m-th powers of rational functions. Ordered Algebraic Struc-
- Daykin D.: Hilbert's 17th problem. Ph.D. Thesis, unpublished (1961).
- Delzell C.N.: A finiteness theorem for open semialgebraic sets, with braic Geometry, Contemp. Math. 8, AMS, D. Dubois and T. Recio applications to Hilbert's 17th problem. Ordered Fields and Real Alge-(eds.), Providence 1982, 79-97.
- Delzell C.N.: Case distinctions are necessary for representing polyno-J. Stern (ed.), Amsterdam-Oxford-New York 1982, 87-103. mials as sums of squares. Proc. Herbrand Symp., Logic Coll. 1981,
- Delzell C.N.: A continuous, constructive solution to Hilbert's 17th problem. Inventiones Mathematicae 76 (1984), 365-384
- [Del4] Delzell C.N.: On the Pierce-Birkhoff conjecture over ordered fields. Rocky Mountain Journal of Mathematics 19(3) (Summer 1989), 651-
- [Dels] Delzell C.N.: A sup-inf-polynomially varying solution to Hilbert's 17th problem. AMS Abstracts 10(3), (Issue 63, April 1989), 208-209, #849-
- Delzell C.N.: On analytically varying solutions to Hilbert's 17th problem. Submitted to Proc. Special Year in Real Algebraic Geometry and R. Robson, eds.), Contemporary Mathematics. Quadratic Forms at UC Berkeley, 1990-1991, (W. Jacob, T.-Y. Lam.
- [Del7] Delzell C.N.: On analytically varying solutions to Hilbert's 17th problem. AMS Abstracts 12(1), (Issue 73, January 1991), page 47, #863.

[Du] Dubois D.W.: A nullstellensatz for ordered fields. Arkiv for Mat. 8 (1969), 111-114.

[Efr] Efroymson G.: Local reality on algebraic varieties. Journal of Algebra 29 (1974), 113-142.

[GV-L] González-Vega L., Lombardi H.: A Real Nullstellensatz and Positivstellensatz for the Semipolynomials over an Ordered Field. Submitted to the Journal of Pure and Applied Algebra (1992).

[Hil] Hilbert D.: Mathematische Probleme. Göttinger Nachrichten (1900), 253-297, and Archiv der Math. u. Physik (3rd ser.) 1 (1901), 44-53, 213-237.

[Kre₁] Kreisel G.: Some uses of metamathematics. British J. Phil. Sci. 7(26) (August 1956), 161-173.

[Kre2] Kreisel G.: Sums of squares. Summaries of Talks Presented at the Summer Institute in Symbolic Logic in 1957 at Cornell Univ., Institute Defense Analyses, Princeton (1960), 313-320.

[Kre3] Kreisel G.: Review of Goodstein, MR 24A, 336-7, #A1821 (1962).

[Kre4] Kreisel G.: Review of Ershov, Zbl. 374, 02027 (1978).

[Kri] Krivine J.L.: Anneaux préordonnés. Journal d'Analyse Mathématique 12 (1964), 307-326.

[Lom₁] Lombardi H.: Effective real Nullstellensatz and variants. Effective Methods in Algebraic Geometry. Editors T. Mora and C. Traverso. Progress in Mathematics 94 (1991), 263-288, Birkhauser. Detailed French version in Théorème effectif des zéros réel et variantes (avec une majoration explicite des degrés), Memoire d'habilitation (1990).

[Lom₂] Lombardi H.: Une étude historique sur les problèmes d'effectivité en algèbre réelle. Memoire d'habilitation (1990).

[Lom3] Lombardi H.: Une borne sur les degrés pour le théorème des zéros réel effectif. Proceedings of the conference on Real Algebraic Geometry held in La Turballe (1991). To appear as Lecture Notes in Mathematics.

[LR] Lombardi H., Roy M.-F.: Théorie constructive élémentaire des corps ordonnés. Publications Mathematiques de Besançon, Théorie de Nombres, 1990-1991. English version in: Constructive elementary theory of ordered fields, Effective Methods in Algebraic Geometry. Editors T. Mora and C. Traverso. Progress in Mathematics 94 (1991), 249-262, Birkhauser.

[MRR] Mines R., Richman F., Ruitenburg W.: A Course in Constructive Algebra. Universitext, Springer-Verlag (1988).

[Pre₁] Prestel A.: Lectures on Formally Real Fields. IMPA Lecture Notes 22, R10 de Janeiro 1975; reprinted in Lecture Notes in Mathematics 1093

ĉ

(1983), Springer-Verlag.

[Pre2] Prestel A.: Continuous representations of real polynomials as sums of 2^m-th powers. Math. Forschungsinst. Oberwolfach Tagungsbericht (Reelle algebraische Geometrie, June 10-16, 1990) 25 (1990), 18.

[Ris] Risler J.-J.: Une caractérisation des idéaux des variétés algébriques réelles. C.R.A.S. Paris, Série A, 271 (1970), 1171-1173.

[Rob₁] Robinson A.: On ordered fields and definite forms. Math. Ann. 130 (1955), 257-271.

[Rob₂] Robinson A.: Further remarks on ordered fields and definite forms Math. Ann. 130 (1956), 405-409.

[Sch] Schwartz N.: Piecewise-polynomial functions. Submitted

[Sco1] Scowcroft P.: A transfer theorem in constructive real algebra. Ann. Pure and Appl. Logic 40(1), 29-87 (1988).

[Sco₂] Scowcroft P.: Some continuous Positivstellensatze. Journal of Algebra 124 (1989), 521-532.

[Sol] Solernó P.: Effective Lojasiewicz inequalities in semialgebraic geometry. Applicable Algebra in Engineering, Communication and Computing 2(1) (1991), 1-14.

[Ste] Stengle G.: A Nullstellensatz and a Positivstellensatz in semialgebraic geometry. Math. Ann. 207 (1974), 87-97.

Dept. Mathematics
Louisiana State University
Baton Rouge, LA 70803, U.S.A.
(delzell@lsuvax.sncc.lsu.edu)

Charles N. Delzel

Laureano González-Vega Dept. Matemáticas Universidad de Cantabria Santander 39071, Spain (g_vega@ccucvx.unican.es)

Henri Lombardi Lab. de Mathématiques Université de Franche-Comté Besançon 25030, France (tdnbesac@frgren81.bitnet)